2024 TRAINING CATALOG

Courses, Labs, Bundles, Micro Degrees, Readiness Range, IT PRO Library

IMTS TRAINING INSTITUTE (ITI)

IMTS
INNOVATIVE MANAGEMENT & TECHNOLOGY
SERVICES

Table of Contents

Welcome to the IMTS Training Institute 2024 Catalog

At the Innovative Management and Technology Services, LLC (IMTS) Training Institute (ITI), we are dedicated to providing cutting-edge training solutions that equip professionals with the skills they need to excel in today's dynamic IT landscape. As a direct partner with industry leaders like CompTIA and EC-Council, we offer authorized training that meets the highest standards of quality and effectiveness. Our partnership with Cyber Defense Solutions further enhances our catalog, allowing us to offer specialized training in cyber security and defense.

We understand that learning preferences vary, which is why we offer a flexible training model that includes both online self-paced instructor-led training (ILT) and live sessions. This approach ensures that every learner finds a training method that suits their style and schedule.

Beyond our direct partnerships, we have also formed alliances with other renowned training providers, creating a robust network that supports a wide range of professional development needs. Through these partnerships, the IMTS Training Institute is proud to offer an expansive selection of courses—ranging from technical certifications to micro-degrees in specialized fields. Our comprehensive course offerings are designed to provide learners with the skills they need to succeed in their careers and stay ahead of industry trends.

Whether you are starting your IT career or looking to advance further, our catalog provides all the resources you need for success. From detailed course descriptions to structured learning paths, each program is tailored to ensure comprehensive understanding and practical application of skills.

Join us at ITI to advance your career with training that sets the standard for excellence in IT education.

Terms of Use, Policy and Intellectual Property

1. Introduction

Welcome to the Innovative Management and Technology Services, LLC (IMTS) Training Catalog and E-Commerce platform. By accessing or using any of our services, you agree to comply with the following terms and conditions ("Terms of Use") and acknowledge our practices regarding the collection, use, and sharing of your information, as described in our Privacy Policy.

These Terms apply to all users of the catalog and visitors to **IMTS.US** and **Training.IMTS.Store**.

2. Terms of Use

2.1. Service Availability

- Course offerings, schedules, and prices are subject to change without prior notice.
- IMTS reserves the right to modify, suspend, or discontinue any service at any time.

2.2. Registration and Enrollment

- Users must provide accurate and complete information during registration.
- IMTS reserves the right to deny or revoke access if false or incomplete information is provided.
- By enrolling in a course, users agree to follow any specific policies related to attendance, conduct, and assessment.

2.3. Intellectual Property

- All materials provided in this catalog and associated courses, including course content, logos, and trademarks, are the intellectual property of IMTS (and the ITI) and/or our partners.
- Unauthorized reproduction, distribution, or use of course materials is prohibited.

2.4. Liability and Disclaimer

- IMTS makes every effort to ensure the accuracy of the information in this catalog, but does not guarantee it to be error-free or comprehensive.
- IMTS is not responsible for any technical issues, course cancellations, or disruptions in service that may affect your learning experience.

3. Privacy Policy

3.1. Information We Collect

- **Personal Information**: Name, email address, phone number, and other contact details during registration or enrollment.

- **Payment Information**: When purchasing a course through our e-commerce platform, we may collect billing information, including credit card details, which will be processed securely by our payment partners.
- **Technical Information**: IP address, browser type, and cookies used to enhance your browsing experience on our website.

3.2. How We Use Your Information

- To process course registrations and payments.
- To communicate with users regarding course updates, announcements, or cancellations.
- To improve our website and catalog offerings.

3.3. Information Sharing

- We do not sell your information to third parties. However, we may share your information:
  - With trusted partners to facilitate course delivery (e.g., Cyber Defense Solutions, CompTIA, EC-Council).
  - With payment processors to complete transactions securely.
  - If required by law or to protect the legal rights of IMTS.

3.4. Cookies and Tracking

- Our website may use cookies to enhance the user experience. Users can adjust their browser settings to limit cookie tracking, though this may affect site functionality.

3.5. Your Rights and Choices

- You have the right to access, correct, or delete your personal information.
- To make such requests, contact us at **[insert contact email/phone number]**.

4. Changes to Terms and Privacy Policy

IMTS may update these Terms of Use and Privacy Policy from time to time. Changes will be posted on our website and will take effect immediately. Continued use of our services indicates acceptance of the updated policies.

5. Contact Information

For any questions regarding these Terms or our Privacy Policy, please contact:

- **IMTS**
- Email: [Insert email]
- Phone: [Insert phone number]

6. Copyright Notice

7. Use of IMTS Trademarks (TM) and Intellectual Property

Permitted Uses

IMTS Training Institute trademarks, including logos and certification titles, may only be used:

1. By candidates who have successfully completed and earned IMTS certifications, to accurately represent their credentials.
    - Certification logos may be displayed on resumes, LinkedIn profiles, business cards, and other professional materials to indicate certification achievement.
    - Trademarked certification titles (e.g., Certified Cybersecurity Expert™) may be used in written communications and professional profiles to describe the credential earned.
2. By authorized licensees, partners, or affiliates, in accordance with specific terms outlined in their agreements with IMTS.
3. To accurately refer to or describe the certifications or programs offered by IMTS, without misrepresentation.

Prohibited Uses

IMTS Training Institute trademarks, including logos and certification titles, may not be used:

1. Without express written permission from IMTS for purposes other than representing earned certifications.
2. In any way that could mislead, confuse, or imply endorsement or affiliation with any non-IMTS entity, product, or service.
3. To claim certifications not earned or to misrepresent one's qualifications.
4. In a derogatory, defamatory, or otherwise harmful manner that could damage the reputation of IMTS or its offerings.
5. As part of any unauthorized certification title, program, or course name.

Intellectual Property Rights

All IMTS trademarks, logos, course titles, and associated intellectual property remain the exclusive property of IMTS. Unauthorized use, reproduction, or distribution of these assets is strictly prohibited and subject to legal enforcement.

Revocation of Use

IMTS reserves the right to revoke the use of its trademarks, logos, or certification titles if:

1. A candidate or organization is found to misuse these assets.
2. The certification associated with the trademark is revoked due to non-compliance with IMTS certification requirements or policies.

Current Trademarks

The current trademarks of IMTS and the ITI include, but are not limited to:

1. Certified COMSEC Manager™ (CCM™)
2. Certified Cyber Policy and Strategy Planner™ (CCPSP™)
3. Certified Cyber Workforce Developer™ (CCWD™)
4. Certified Cyber Curriculum Developer™ (CCCD™)
5. Certified Cyber Instructor™ (CCI™)
6. Certified Cyber Legal Advisor™ (CCLA™)
7. Certified Executive Cyber Leader™ (CECL™)
8. Certified Privacy Compliance Manager™ (CPCM™)
9. Certified Product Support Manager™ (CPSM™)
10. Certified Program Manager™ (CPM™)
11. Certified IT Project Manager™ (CITPM™)
12. Certified Security Control Assessor™ (CSCA™)
13. Certified Cyber Authorizing Official™ (CCAO™)
14. Systems Certified Security Manager™ (SCSM™)
15. Certified IT Portfolio Manager™ (CITPM™)
16. Certified IT Program Auditor™ (CITPA™)
17. Certified Security Architect™ (CSA™)
18. Certified Enterprise Security Architect™ (CESA™)
19. Certified Secure Development Professional™ (CSSDP™)
20. Certified Systems Security Developer™ (CSSD™)
21. Certified Secure Software Assessor™ (CSSA™)
22. Certified Systems Requirements Planner™ (CSRP™)
23. Certified System Testing and Evaluation Specialist™ (CSTES™)
24. Certified Research & Development Specialist™ (CRDS™)
25. Certified Data Analyst Professional™ (CDAP™)
26. Certified Database Admin Professional™ (CDAP™)
27. Certified Secure Knowledge Manager™ (CSKM™)
28. Certified Network Operations Specialist™ (CNOS™)
29. Certified Secure System Administrator™ (CSSA™)
30. Certified Systems Security Analyst™ (CSSA™)
31. Certified Technical Support Technician™ (CTST™)
32. Certified Cyber Defense Analyst™ (CCDA™)
33. Certified Cyber Forensics Analyst™ (CCFA™)
34. Certified Cyber Incident Responder™ (CCIR™)
35. Certified Infrastructure Support Specialist™ (CISS™)
36. Certified Threat Warning Analyst™ (CTWA™)
37. Certified Insider Threat Program™ – Insider Threat Core
38. Certified Insider Threat Professional - Investigative Analyst™ (CITP-IGA™)

39. Certified Insider Threat Professional - Cyber Analytics™ (CITP-CA™)
40. Certified Insider Threat Professional - Infrastructure Engineer™ (CITP-IE™)
41. Certified Insider Threat Professional - Data Analytics™ (CITP-DA™)
42. Certified Insider Threat Professional – Infrastructure Operator™ (CITP-IO™)
43. Certified Insider Threat Professional - Program Manager™ (CCITP-PM™)
44. Certified Insider Threat Professional - Hub Chief™ (CITP-HC™)
45. Certified Insider Threat Professional - Senior Official™ (CITP-SO™)
46. Certified Insider Threat Professional - Incident Responder™ (CITP-IR™)
47. Certified Insider Threat Professional - Cyber Leader (CITP-CL™)
48. Certified Insider Threat Professional - ICS-SCADA Analyst™ (CITP-ICS™)
49. Certified Insider Threat Professional - Data Scientist™ (CITP-DS™)
50. Certified Insider Threat Professional – User Activity Monitoring™ (CITP-UAM™)
51. Vulnerability Assessor Certified™ (VAC™)
52. Certified Intrusion Forensics Analyst™ (CIFA™)
53. Certified Cyber Crime Forensic Investigator™ (CCCFI™)
54. Certified All-Source Analyst™ (CASA™)
55. Certified All-Source Collection Manager™ (CASCM™)
56. Certified All-Source Requirements Manager™ (CASRM™)
57. Certified Cyber Intel Planner Professional™ (CCIPP™)
58. Certified Cyberspace Operator™ (CCO™)
59. Certified Cyber Operations Planner™ (CCOP™)
60. Certified Exploitation and Penetration Analyst™ (CEPA™)
61. Certified Mission Assurance Specialist™ (CMAS™)
62. Certified Joint Targeting Analyst™ (CJTA™)
63. Certified Target Developer™ (CTD™)
64. Certified Target Digital Network Analyst™ (CTDNA™)
65. Certified AI Adoption Specialist™ (CAIAS™)
66. Certified AI Innovation Leader™ (CAIL™)
67. Certified AI Risk & Ethics Specialist™ (CARES™)
68. Certified AI Test & Evaluation Specialist™ (CATES™)
69. Certified AI/ML Specialist™ (CAIMLS™)
70. Certified Control Systems Security Specialist™ (CCSSS™)
71. Certified Digital Network Exploitation Analyst™ (CDNEA™)
72. Certified Data Architect™ (CDA™)
73. Certified Data Officer™ (CDO™)
74. Certified Data Operations Specialist™ (CDOS™)
75. Applied Data Scientist Certified Professional (ADSCP)
76. Certified Data Steward Analyst™ (CDSA™)
77. DevSecOps Specialist Certified™ (DevSC™)
78. Certified Secure Host Configuration Analyst™ (CSHCA™)
79. Certified Network Monitoring Analyst™ (CNMA™)
80. Certified Network Technician™ (CNT™)
81. Certified User Interface Designer™ (CUID™)
82. Certified Product Manager Professional™ (CPMP™)
83. Certified User Experience Service Designer™ (CUXSD™)
84. Certified Software Test & Evaluation Specialist™ (CSTES™)
85. Certified Software & Cloud Architect™ (CSCA™)
86. Certified Information Systems Developer™ (CISD™)
87. Certified Target Analyst Reporter™ (CTAR™)

88. Certified Site Reliability Engineer™ (CSRE™)
89. Certified Malware Reverse Engineer™ (CMRE™)
90. Chief Information Officer Certified™ (CIOC™)
91. Defensive Cyber Operations Expert – Cyber (Defense)™ (DCOE-CD™)
92. Defensive Cyber Operations Expert – Cyber (Infrastructure) ™ (DCOE-CI™)
93. Defensive Cyber Operations Expert – Cyber (Management)™ (DCOE-CM™)
94. Defensive Cyber Operations Expert – Cyber (Assessments)™ (DCOE-CA™)
95. Defensive Cyber Operations Expert – Cyber (Red Team)™ (DCOE-CR™)
96. Defensive Cyber Operations Expert – Investigations (Analytics)™ (DCOE-IA™)
97. Defensive Cyber Operations Expert – Intelligence (Cyberspace)™ (DCOE-IC™)
98. Defensive Cyber Operations Expert – Cyber Enabler (Leaders)™ (DCOE-CL™)
99. Defensive Cyber Operations Expert – Cyber Enabler (Legal/LE)™ (DCOE-CLE™)
100. Defensive Cyber Operations Expert – Cyber Enabler (Training)™ (DCOE-TR™)
101. Defensive Cyber Operations Expert – Cyber Enabler (Programs)™ (DCOE-PM)
102. Offensive Cyber Operations Expert (OCOE) - Cyber Effects (CE)™ (OCOE-CE™)
103. Technical Support Operations Expert – IT (Cyberspace)™ (TSOE-IT™)
104. Technical Support Operations Expert – Software Engineering™ (TSOE-SE™)
105. Technical Support Operations Expert – Data/AI™ (TSOE-DA™)
106. Critical Infrastructure Certified Expert™ (CICE™)
107. Certified Insider Threat Expert – Cyber™ (CITE-C™)
108. Certified Insider Threat Expert – Infrastructure™ (CITE-I™)
109. Certified Insider Threat Expert – Data™ (CITE-D™)
110. Certified Insider Threat Expert – Operations™ (CITE-O™)

8. Policy for Candidates with Existing Certifications and ITI Certifications

Replacement Certification Policy:
If a candidate already holds one or more certifications included in an IMTS Training Institute certification course bundle or micro degree, they are required to complete alternative IMTS Training Institute certifications to fulfill the program requirements.

- **Certification Validation**
  - Candidates must provide proof of their existing certifications during the enrollment process.
  - Accepted forms of proof include certification ID numbers, digital badges, or official certificates.
- **Replacement Certifications**
  - IMTS Training Institute will recommend alternative certifications of equal or higher value from its catalog of certifications that align with the program's objectives and the candidate's professional development.
  - Replacement certifications will only be selected from IMTS Training Institute offerings.
- **Program Fee**
  - The total program fee remains unchanged, regardless of certification replacements.

- **Customized Learning Path**
    - Replacement certifications are selected to ensure that candidates gain equivalent value and expertise within the IMTS Training Institute framework, maintaining the program's rigor and comprehensiveness.
- **Program Completion**
    - Candidates must complete all required certifications, including any replacements, to earn the designation associated with the program.

Government Training Center of Excellence

Introduction: Welcome to the Government Training Center of Excellence, a pivotal component of the IMTS Training Institute (ITI). We specialize in offering Applied Micro Degrees and targeted certification training programs designed to meet the needs of government employees, focusing on critical product, project, program, agile, technical and cybersecurity knowledge, skills, and abilities to accomplish tasks, based on established frameworks and standards.

Mission: Empower government employees through applied training solutions designed to develop the knowledge and skills necessary to develop abilities and accomplish tasks (KSATs) and ensure mission readiness.

Expertise: Through the collective efforts of ITI and its strategic partners, we have trained over 1 million individuals and certified more than 500,000 professionals. This collaboration enriches our government training programs with extensive expertise and a deep understanding of the specific needs and standards required by government roles.

Framework and Certification Alignment:

- **DCWF and DoD 8140:** Our courses are meticulously aligned with the Defense Cyber Workforce Framework (DCWF) and DoD Directive 8140, catering specifically to the needs of the defense sector's cybersecurity workforce.
- **NICE Framework and C3 Mappings:** Utilizing the Cybersecurity Credentials Collaborative (C3) mappings, we connect the NICE Framework's roles to relevant certifications, providing clear competency development paths for our participants.
- **Comprehensive Integration:** By aligning these certifications further with NICE C3, the DCWF and 8140 standards, we ensure our training is both comprehensive and applicable to the broad needs of both civilian and defense roles within the government.

Key Features:

- **Applied Learning with Labs:** Each course incorporates practical labs that allow participants to demonstrate the skills acquired from their training, improving their abilities to perform essential tasks effectively.
- **Optional Capstone Integration/Master Designation: Mission Readiness Range:** Each Applied Micro Degree may conclude with this suite, serving as a capstone project where

participants apply their learned KSATs in realistic scenarios, further cementing their skills.

Primary Goals:

1. **Professional Competence:** Enhance the competencies of government employees to exceed the demands of modern public sector roles.
2. **Certification Achievement:** Prepare employees for certification exams that validate their skills in alignment with government-recognized standards.
3. **Workforce Development:** Address skill gaps and prepare a workforce capable of tackling contemporary and future challenges.
4. **Continuous Learning and Adaptation:** Promote a culture of continuous learning to navigate the evolving technological and policy landscape effectively.

From DoD DCWF and NIST/NICE:

- **DoD DCWF:** Each work role is defined with a list of core and additional tasks along with the required knowledge, skills, and abilities (KSAs).
- **NIST and NICE:** The NICE Framework components—Task, Knowledge, and Skill (TKS) statements; Work Roles and Work Role Categories; and Competency Areas—are regularly reviewed and adjusted to ensure they remain effective and responsive to the changing needs of the cybersecurity workforce.

Begin Your Journey to Success: Embark on your path to professional excellence with the Government Training Center of Excellence. For more details on our courses and to enroll, visit IMTS Training E-commerce Site.

Need Guidance? Contact our expert advisors for personalized assistance in selecting the right training pathway to meet your career objectives and fulfill government training standards.

Mission Readiness Range and KSA Assessment

Overview: Enhance your team's cybersecurity, technical and insider threat training with our exclusive Mission Readiness Range. This premier solution offers a comprehensive SaaS product (hardware products available) that elevates theoretical learning with immersive, real-world application in a controlled, gamified environment. Designed for accessibility from anywhere with an internet connection, this suite is perfect for individuals or teams seeking to deepen their practical skills collaboratively.

Applicability: This suite can be added to any cybersecurity or insider threat course offered on our platform, enhancing its practical application.

Target Audience: Specifically designed for both individuals or teams of 5 or more, ideal for organizational training sessions and enhancing organizational skill sets. Contact us on a case-by-case basis for individual licensing.

Access Duration: Provides three months of extensive access to interactive simulations and assessments.

Cost: Priced at $2,000 for individuals and $9,500 for a team of five for three months, delivering significant value through intensive, hands-on training and skill enhancement. Contact us for potential individual pricing.

Accessibility: Participants can log in and engage from any location, ensuring flexible learning schedules and adaptable environments.

Key Benefits

Real-World Application: Seamlessly transition from theoretical concepts to practical application with scenarios that mirror actual cybersecurity and insider threat challenges. Participants apply their learned KSATs in realistic scenarios through labs and simulations.

Standards-Aligned Skill Development: Fully integrated with NICE and DCWF/8140 standards, ensuring that training is relevant and applicable.

Team Building and Skill Validation: Foster team collaboration and evaluate individual and group skills through engaging and comprehensive activities.

Enrollment Process

Contact Us to Enroll: Due to the tailored nature of the training and the need to capture specific details for each participant, enrollment in the "Mission Readiness Range" requires direct contact with our sales or training team.

Personalized Setup: Our team will assist you in selecting the appropriate courses, capturing all participant details, and ensuring that the suite meets your specific training needs.

Start Training: Once setup is complete, your team can begin their comprehensive training journey, with our support throughout the process to maximize learning outcomes.

Certified Insider Threat Program

In the evolving landscape of insider threat mitigation, integrating cybersecurity data with User Activity Monitoring (UAM) and other insider threat data is essential for a successful program. The Committee on National Security Systems Directive (CNSSD) 504, Executive Order (EO) 13587, and the National Insider Threat Task Force (NITTF) emphasize the critical need for this integration. Despite the importance of combining cybersecurity with insider threat core knowledge, skills, and abilities (KSAs), there are no existing training programs that adequately cover both areas. Our CITP™ bundles fill this gap by providing comprehensive training that encompasses both the insider threat core KSAs and the essential cybersecurity aspects. ITI offers a comprehensive Certified Insider Threat Program tailored to meet the ever-evolving needs of insider threat professionals. Our program culminates in the awarding of a Certified Insider Threat Professional™ Certification (with option of apply for the Master Certification), valid for three years with an evergreen option, alongside a perpetual micro degree, designed to provide lifelong credentials to our graduates.

Our unique training bundles are meticulously crafted to align with the NICE Insider Threat Analysis Work role, as well as additional NICE and DCWF work roles. This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans). By integrating certifications from the NICE Framework Work Role Mapping to Cybersecurity Credentials Collaborative (C3), found at Cybersecuritycc.org/role-mapping, and qualifications matrices of 8140 DCWF, our program ensures that participants receive training that is both comprehensive and compliant with current industry standards.

Each bundle within the program is enhanced by strategic partnerships with renowned certification bodies, including CompTIA, EC-Council, ISACA, ISC^2, PECB, Microsoft, and AWS. These partnerships allow us to incorporate commercial certifications that are highly valued in the industry, providing our students with a competitive edge in the job market.

A distinctive feature of our program is the integration of applied labs, which occur both throughout the individual

stackable certifications and culminate in an optional capstone KSAT assessment through our Mission Readiness Range. This hands-on component ensures that participants not only understand theoretical concepts but are also proficient in practical, real-world applications to further the mission. Individuals that choose this add one, or pursue and pass this after earning CITP, will be provided the Master designation—Certified Insider Threat Professional - Master™. Not all Certified Insider Threat Professional certifications are eligible.

IMTS stands out as the only insider threat training provider that includes such a diverse range of commercial certifications, coupled with rigorous practical labs and assessments, setting our graduates apart in the field of Insider Threat and Cybersecurity.

Tech Pro Annual Library

The **Tech Pro Library** is a comprehensive resource designed to provide continuous learning and professional development for IT and cybersecurity professionals. By subscribing to the Tech Pro Library, users gain access to an extensive range of training materials and resources, ensuring they stay current with the latest industry standards and practices.

Subscription Information:

- **Annual Subscription Fee:** $749 per year with course purchase or $999 without (but $749 annually thereafter)
- **Access Period:** 12 months from the date of purchase

Features of the Tech Pro Library:

1. **Custom Instructor-Led Training (ILT) and Labs (add on):** Access to a wide array of courses (including popular certifications) and hands-on labs (available as a paid add on) provided by our partner CTI (CDS). These courses are tailored to enhance skills and knowledge across various IT and cybersecurity domains, from foundational to advanced levels.
2. **EC-Council Annual Pro Subscription:**
    - Includes over 600 premium online IT and cybersecurity courses, ensuring comprehensive coverage of key topics and emerging threats.
    - More than 15,000 labs or lab demos to provide practical, hands-on experience in a controlled environment.

- Over 15,500 questions to test your newly gained skills and knowledge.
- A shareable certificate of achievement after completing each course.
- 50+ learning paths for structured learning, helping you navigate your professional development journey efficiently.

3. **Continuous Learning and Professional Development:**
   - Regularly updated content to reflect the latest trends, technologies, and best practices in IT and cybersecurity.
   - Access to webinars, thought-leadership materials, and supplemental resources to support ongoing education and professional growth.
4. **ITI Certification Renewal and Maintenance:**
   - By maintaining an active subscription to the Tech Pro Library, ITI certification holders can ensure their credentials remain current.
   - The library supports the renewal of the ITI's evergreen certifications, such as the Certified Cyber Policy and Strategy Planner™ (CCPSP™), which renews every three years with an active subscription.
5. **Courses for Leading Certifications:**
   - The library includes training for many leading certifications from renowned organizations such as AWS, EC-Council, ISC2, ISACA, Microsoft, Oracle, and others, providing a wide array of professional development opportunities.
6. **Course Discounts:** With an active Tech Pro subscription, you can get an additional 5% off from the sales price of all ITI courses and course bundles.
7. **CTI Labs**
   - 12-month access to all CTI course labs included in the annual subscription fee.

Additional Optional Elements:

1. **12-Month Access to Any CompTIA Course:**
   - For an additional $999 per year, subscribers can gain 12 months of access to any CompTIA course, including one exam voucher.
2. **Discounted CompTIA Vouchers:**
   - Access CompTIA vouchers at 20% off the MSRP, providing significant savings for certification exams.
3. **EC-Council Certification Club Upgrade (Add on):**

- The option to upgrade to 12 months of access to EC-Council's entire OnDemand catalog with an MSRP of $2,999, including exams, at a discounted rate and only $999 to renew it after the first year. Contact us for more information on this exclusive offer.

4. **Mission Readiness Range and KSAT Assessment:**
    - Add on 3 months of access to Mission Readiness Range for an additional $2,000. This suite provides a hands-on, experiential training environment designed to prepare technical personnel and teams with practical skills for advanced applications.

By subscribing to the Tech Pro Library, IT, threat analysts and cybersecurity professionals can ensure they have the resources and support needed to stay at the forefront of their field, maintain their certifications, and continuously enhance their skills and knowledge.

Exam Prerequisites, and Certification Validity and other Policies

Because each vendors requirements can change, we have provided basic information below and links to their websites to ensure you have the most up to date and accurate information.

IMTS Training Institute (ITI)

ITI Applied Micro Degrees do not expire. See each individual course regarding the requirements for award of each individual Applied Micro Degree. ITI certifications are good for 3 years. To renew your certification, you have to retake the courses and associated exams, or sign up for (and stay enrolled in) our evergreen option, the Tech Pro Library, within 12 months of completing your program.

CompTIA

There aren't any age requirements or educational prerequisites to take a CompTIA exam, but CompTIA does outline recommended experience for each exam. You can find this information on their website in the exam details chart for any CompTIA certification. Certifications are valid for three years but can be renewed. Their websites: (IT) Information Technology Certifications | CompTIA IT Certifications and How To Renew Your Certification | CompTIA IT Certifications

EC-Council

There are varying exam prerequisites for EC-Council exams. Information can be located on their website. Certifications are valid for 3 years and can be renewed. Their websites: Application Process Eligibility - CERT (eccouncil.org) and ECE Policy - CERT (eccouncil.org)

PECB

Each PECB certification has specific education and a set of experience requirements. PECB certifications are valid for three years and to maintain a certification, candidates must submit continuing professional development hours and meet other requirements. Their websites : Certification Maintenance Policy | PECB and Certification Process | PECB

Microsoft

Currently, all Microsoft certifications (credentials), except fundamentals, are valid for one year and must be renewed annually by passing an online assessment: Credential expiration policies | Microsoft Learn

AWS

All AWS Certifications may be earned without completing specific prerequisites. However, AWS provides recommendations for knowledge and experience that are aligned to the content and level of proficiency for each certification. AWS Certifications are valid for three years. To maintain your AWS Certified status, they require you to periodically demonstrate your continued expertise through a process called recertification. Their websites: Before Testing | AWS Certification Information and Policies | AWS (amazon.com) and AWS Recertification | AWS Certification Renewal | AWS (amazon.com).

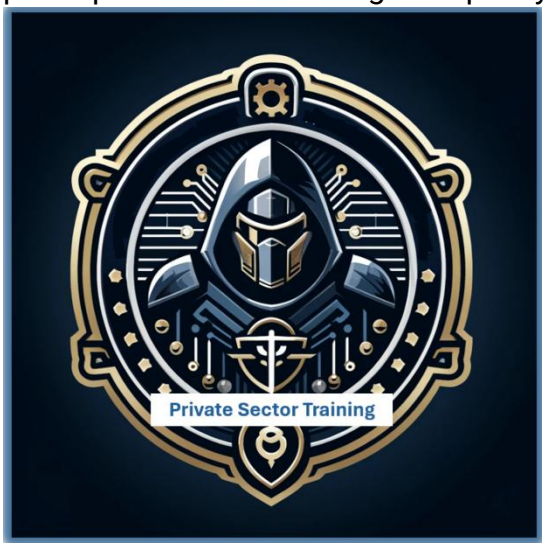
Other Vendors

Please visit their websites for more information.

Current Catalog

Private Sector Training

With our Private Sector Training at the IMTS Training Institute, we provide a comprehensive range of training solutions designed to meet the diverse needs of professionals and organizations. Our bundles include official training courses from renowned providers such as CompTIA, EC-Council, and PECB, ensuring that our participants receive the highest quality education and credentials. Additionally, we offer custom training solutions tailored to the specific requirements of our clients, featuring courses from ISACA, ISC2, and specialized training in areas like Malware Analysis and Reverse Engineering, Data Analytics, and more.



In line with our commitment to delivering cutting-edge training, we also provide vendor-authorized programs from industry leaders such as RedHat, Microsoft, and AWS. These courses are designed to equip participants with the skills and knowledge necessary to excel in today's rapidly evolving technological landscape.

With over three thousand courses available, our catalog is extensive, but not exhaustive. If you do not see a specific course listed, we encourage you to reach out to us. Our team is dedicated to working with you to identify and develop the training solutions that best meet your needs, ensuring that you and your organization remain at the forefront of your industry.

Network Engineer Bundle

ITI SKU: Cisco-1

MSRP: $2,499

Sales Price: $1,999

Bundle Access Period: 12 months from purchase.

Course in bundle: Cisco CCNA 200-301, Network+ N10-008 and CCNP Enterprise Bundle

High-level description: The Cisco CCNA 200-301 certification is a globally recognized credential that validates the fundamental skills necessary to perform essential networking functions. Our Cisco CCNA 200-301 Bundle combines custom self-paced

online instructor-led training (ILT) courses with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. This approach ensures a thorough understanding by offering theoretical knowledge and practical skills, leading to better retention and mastery of networking concepts.

This CompTIA Network+ course provides students with the fundamental skills, practical experience, and in-depth knowledge necessary to design, construct, and manage robust networks. It encompasses a wide range of essential activities, from maintenance to troubleshooting, across diverse components of contemporary digital infrastructure. Upon completing the course, students will possess a thorough grasp of the N10-008 exam objectives and be well-prepared to succeed in the certification process.

Enhance your networking skills with our CCNP Enterprise Core Online Self-Paced ILT Course. This course covers advanced enterprise networking concepts, preparing you for the core exam necessary for CCNP Enterprise certification.

Dive deeper into enterprise networking with our CCNP ENARSI Online Self-Paced ILT Course. This course covers advanced routing and services necessary for the CCNP Enterprise concentration exam.

The bundle also includes an exam pass guarantee for the Network+ exam.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT followed by the CertMaster Network+ with integrated labs and then the TestOut CCNA integrated training and hands-on labs, then the CCNP courses.

CTI Custom Online Self-Paced Network+ ILT with Labs Description: Our training includes a detailed certification program designed to equip individuals with fundamental to advanced networking skills. Covering topics from basic network concepts to modern technologies such as virtualization and cloud services, the course prepares students for the globally recognized CompTIA N10-008 exam. This exam assesses one's proficiency in designing, managing, and troubleshooting both wired and wireless networks. The course includes 45+ training hours, 185+ on-demand videos, 16 topics, and 175+ prep questions. Upon completion, students receive a certificate of completion and are expected to have a deep understanding of all the objectives required to pass the CompTIA Network+ N10-008 exam.

CompTIA Network+ N10-008 Course Content

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)

- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

CompTIA Network+ N10-008 Lab (33+ hours) Modules

1. Introduction to the
2. OSI Model
3. Networking Topologies and Characteristics
4. Internet Protocol Addressing Solutions
5. Cable and Connector Types
6. Cable Management Solutions
7. Virtual Network Concepts
8. Network Security Concept Fundamentals
9. General Network Attacks
10. Network Services and Protocols
11. Network Command Line Tools
12. Network Analysis Software
13. Configuring and Maintaining DNS Servers
14. DHCP Server Installation and Configuration
15. Remote Access and Management
16. Load Balancing and NIC Teaming
17. NTP Server Management
18. High Availability and Disaster Recovery Concepts

19. Configuring Switching Features
20. Routing Concepts and Protocols
21. Troubleshooting Common Networking Issues
22. Cloud Concepts
23. Network Architecture
24. Networking Device Monitoring
25. Network Troubleshooting Techniques
26. Networking Hardening Techniques and Best Practices
27. Physical Networking Tools
28. Defining Networking Devices
29. Troubleshooting Cable Connectivity
30. Wireless Configuration Techniques and Standards
31. Troubleshooting and Securing Wireless Networks
32. Physical Network Security Concepts
33. Organizational Documentation and Procedures
34. Organizational Networking Diagrams and Agreements

CTI Custom Online Self-Paced CCNA ILT with Labs Description: Master networking with our Cisco CCNA 200-301 Online Self-Paced ILT Course, designed for aspiring network specialists, administrators, and IT professionals. This course offers 45+ hours of content delivered over 150 short, easily digestible videos, covering 28 topics and providing more than 295 prep practice questions. Once purchased, you have 12 months' access to the course.

Topics Areas Included:

- Network Fundamentals
- Network Access
- IP Connectivity
- IP Services
- Security Fundamentals

Modules Included:

Module 1: Exploring the Functions of Networking

Module 2: Introducing the Host-To-Host Communications Model

Module 3: Introducing LANs

Module 4: Exploring the TCP/IP Link Layer
Module 5: Subnetting
Module 6: Explaining the TCP/IP Transport Layer and Application Layer
Module 7: Exploring the Functions of Routing
Module 8: Exploring the Packet Delivery Process
Module 9: Troubleshooting a Simple Network
Module 10: Introducing Basic IPv6
Module 11: Configuring Static Routing
Module 12: Implementing VLANs and Trunks
Module 13: Routing Between VLANs
Module 14: Introducing OSPF
Module 15: Building Redundant Switched Topologies
Module 16: Improving Redundant Switched Topologies with EtherChannel
Module 17: Exploring Layer 3 Redundancy
Module 18: Introducing WAN Technologies
Module 19: Explaining Basics of ACL
Module 20: Enabling Internet Connectivity
Module 21: Introducing QoS
Module 22: Introducing Architectures and Virtualization
Module 23: Introducing System Monitoring
Module 24: Managing Cisco Devices
Module 25: Examining the Security Threat Landscape
Module 26: Implementing Threat Defense Technologies
Module 27: Exam Preparation
Module 28: Practice Demos

Labs included:

1. Networking Concepts - Part One
2. Networking Concepts - Part Two
3. IP Addressing and Virtualization Concepts
4. Switching Fundamentals - Part One
5. Switching Fundamentals - Part Two

6. Configuring VLANs - Part One
7. Configuring VLANs - Part Two
8. Static and Dynamic Routing Principles
9. Configure OSPFv2
10. FHRP Configuration and Verification
11. Static NAT Configuration
12. NTP Configuration
13. DHCP Concepts, Configuration and Verification
14. Network Traffic Management using SNMP
15. Configuring Syslog for Switching and Routing
16. Remote Management Techniques
17. Using File Transfer Protocols on Routers
18. Network Management Tools
19. Applying Security Protocols
20. QoS for Routing Configuration using PHB
21. Security Mitigation Techniques
22. Wireless Architecture and Application

Network+ CertMaster Learn with integrated CertMaster Labs Description: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow. Easy-to-use course management tools provide a comprehensive suite of instructor resources alongside a reporting dashboard, making course preparation and progress tracking simple and efficient.

Topics Covered

Lesson 1: Comparing OSI Model Network Functions

Lesson 2: Deploying Ethernet Cabling

Lesson 3: Deploying Ethernet Switching

Lesson 4: Troubleshooting Ethernet Networks

Lesson 5: Explaining IPv4 Addressing

Lesson 6: Supporting IPv4 and IPv6 Networks

Lesson 7: Configuring and Troubleshooting Routers

Lesson 8: Explaining Network Topologies and Types

Lesson 9: Explaining Transport Layer Protocols

Lesson 10: Explaining Network Services

Lesson 11: Explaining Network Applications

Lesson 12: Ensuring Network Availability

Lesson 13: Explaining Common Security Concepts

Lesson 14: Supporting and Troubleshooting Secure Networks

Lesson 15: Deploying and Troubleshooting Wireless Networks

Lesson 16: Comparing WAN Links and Remote Access Methods

Lesson 17: Explaining Organizational and Physical Security Concepts

Lesson 18: Explaining Disaster Recovery and High Availability Concepts

Lesson 19: Applying Network Hardening Techniques

Lesson 20: Summarizing Cloud and Datacenter Architecture

Integrated Labs:

Assisted Lab: Exploring the Lab Environment

Assisted Lab: Configure a SOHO Router

Assisted Lab: Capture Network Traffic

Assisted Lab: Configure Interface Settings

Assisted Lab: Configure IPv4 Static Addressing

Assisted Lab: Analyze ARP Traffic

Assisted Lab: Use Tools to Test IP Configuration

Assisted Lab: Configure IPv6 Static Addressing

Assisted Lab: Configure Static Routing

Assisted Lab: Configure Dynamic Routing

APPLIED Lab: Troubleshoot IP Networks

Assisted Lab: Use Network Scanners

Assisted Lab: Analyze a DHCP Server Configuration

Assisted Lab: Analyze a DNS Server Configuration

Assisted Lab: Analyze Application Security Configurations

Assisted Lab: Configure Secure Access Channels

Assisted Lab: Configure SNMP and Syslog Collection

Assisted Lab: Analyze Network Performance

APPLIED Lab: Verify Service and Application Configuration

Assisted Lab: Configure a NAT Firewall

Assisted Lab: Configure Remote Access

APPLIED Lab: Troubleshoot Service and Security Issues

Assisted Lab: Develop Network Documentation

Assisted Lab: Backup and Restore Network Device Configurations

Assisted Lab: Analyze an On-Path Attack

Assisted Lab: Configure Port Security

License Information

- One license provides access to CertMaster Learn for Network+ (N10-008) with CertMaster Labs integrated throughout the course
- Once activated, the license is valid for 12 months

How to Access CertMaster Learn integrated with CertMaster Labs

An access key and instructions will be sent via email after your purchase is complete.

TestOut CCNA Routing and Switching Pro Description: Unlock your potential with our comprehensive Routing and Switching Pro course. Designed for junior network administrators and seasoned professionals, this course includes:

- Self-paced instructor-led and demonstration video lessons
- Visual text lessons
- Quizzes
- Lab simulations
- Certification practice exams It prepares you for the modern demands in networking, IP services, security, automation, and programmability, and prepares you for the Cisco CCNA 200-301 certification exam.

Topics Covered (Integrated lessons and labs):

- Introduction to Routing and Switching Pro
- Networking Concepts
- Cisco Devices
- IP Addressing
- Switching
- IPv4 Routing
- IPv4 Routing Protocols
- IPv6 Routing
- Wireless Networks
- WAN Implementation
- Advanced Switching
- Access Control Lists
- Network Management
- Network Security
- Cryptography

CCNP Enterprise Core (ENCOR 350-401): Enhance your networking skills with our CCNP Enterprise Core Online Self-Paced ILT Course. This course covers advanced enterprise networking concepts, preparing you for the core exam necessary for CCNP Enterprise certification. The course includes 47 hours of in-depth content across multiple topics, with numerous practice questions to test your knowledge.

Topics Areas Included:

- Dual Stack Architecture
- Virtualization
- Infrastructure
- Network Assurance
- Security
- Automation

CCNP ENARSI (300-410): Dive deeper into enterprise networking with our CCNP ENARSI Online Self-Paced ILT Course. This course covers advanced routing and services necessary for the CCNP Enterprise concentration exam. It includes 32 hours of

comprehensive training across multiple topics, featuring hands-on labs and practice exams.

Topics Areas Included:

- Layer 3 Technologies
- VPN Technologies
- Infrastructure Security
- Infrastructure Services

License Information:

- One TestOut Routing & Switching Pro license valid for 12 months once activated. 12 months access to CompTIA CertMaster Learn and Integrated Labs and ITI courses.
- Access keys must be redeemed within 12 months of purchase.
- Instructions for accessing the course will be emailed after purchase.

Exam Pass Guarantee: This bundle includes an exam pass guarantee for Network+: if you don't pass the exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Security+ Blended Bundle

ITI SKU: CompTIA-3

MSRP: $1,999

Sales Price: $1,499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career. Our blended learning bundles combine custom self-paced online instructor lead training (ILT) courses with CompTIA's official CertMaster Learn training and Integrated CertMaster Labs, over a 12-month period. This approach ensures a comprehensive understanding by offering theoretical knowledge, practical skills, and hands-on experience, leading to better retention and mastery of cybersecurity concepts. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exam on the first try, we will provide a second voucher and another 12 months of access to our custom online self-paced ILT.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT, followed by the integrated CompTIA Learn and Labs.

Recommended prerequisites: While there are no prerequisites for CompTIA Security+, it is recommended that students have at least two years of IT administration experience with a security focus and hold the CompTIA Network+ or similar certification.

CTI Custom Online Self-Paced ILT with Labs Description

Master cybersecurity with our Security+ 701 Online, Self-Paced ILT Course, designed for aspiring security specialists, network administrators, and IT auditors. This course covers essential cybersecurity principles and practices, aligning with the latest trends and techniques. Gain the core skills necessary to protect against digital threats and excel in today's dynamic IT security landscape. Included in this course is 30 hours of content, delivered over 100+ short easily digestible videos, covering 5 topic areas, and providing more than 250 prep practice questions. Once purchased, you have 12 months' access to the course.

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules include:

- Module 1 - SY0-701 General Security Concepts
- Module 2 - SY0-701 Threats, Vulnerabilities, and Mitigations
- Module 3 - SY0-701 Security Architecture
- Module 4 - SY0-701 Security Operations
- Module 5 - SY0-701 Security Program Management and Oversight

Labs Included (17 hours):

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Mitigation Techniques
7. Security Architecture Models
8. Securing Enterprise Infrastructures
9. Data Protection Strategies
10. Resilience in Security Architecture
11. Securing Computing Resources
12. Asset Management Techniques
13. Vulnerability Management
14. Monitoring Computing Resources
15. Enhancing Enterprise Security
16. Implement Identity & Access Management
17. Implementation of Automation & Orchestration for Security Operations
18. Investigative Data Sources

Official CompTIA CertMaster Learn with Integrated CertMaster Labs Description

CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification

exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered

- Lesson 1: Summarize Fundamental Security Concepts
- Lesson 2: Compare Threat Types
- Lesson 3: Explain Cryptographic Solutions
- Lesson 4: Implement Identity and Access Management
- Lesson 5: Secure Enterprise Network Architecture
- Lesson 6: Secure Cloud Network Architecture
- Lesson 7: Explain Resiliency and Site Security Concepts
- Lesson 8: Explain Vulnerability Management
- Lesson 9: Evaluate Network Security Capabilities
- Lesson 10: Assess Endpoint Security Capabilities
- Lesson 11: Enhance Application Security Capabilities
- Lesson 12: Explain Incident Response and Monitoring Concepts
- Lesson 13: Analyze Indicators of Malicious Activity
- Lesson 14: Summarize Security Governance Concepts
- Lesson 15: Explain Risk Management Processes

- Lesson 16: Summarize Data Protection and Compliance Concepts

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Perform System Configuration Gap Analysis
- Assisted Lab: Configuring Examples of Security Control Types
- Assisted Lab: Finding Open Service Ports
- Assisted Lab: Using SET to Perform Social Engineering
- Applied Lab: Using Storage Encryption
- Assisted Lab: Using Hashing and Salting
- Assisted Lab: Managing Password Security
- Assisted Lab: Managing Permissions
- Assisted Lab: Setting up Remote Access
- Assisted Lab: Using TLS Tunneling
- Assisted Lab: Using Containers
- Assisted Lab: Using Virtualization
- Assisted Lab: Implement Backups
- Assisted Lab: Performing Drive Sanitization
- Assisted Lab: Exploiting and Detecting SQLi
- Assisted Lab: Working with Threat Feeds
- Assisted Lab: Performing Vulnerability Scans
- Assisted Lab: Understanding Security Baselines
- Applied Lab: Implementing a Firewall
- Assisted Lab: Using Group Policy
- Applied Lab: Hardening
- Assisted Lab: Performing DNS Filtering
- Assisted Lab: Configuring System Monitoring
- Applied Lab: Incident Response: Detection
- Applied Lab: Performing Digital Forensics
- Assisted Lab: Performing Root Cause Analysis
- Assisted Lab: Detecting and Responding to Malware
- Assisted Lab: Understanding On-Path Attacks
- Adaptive Lab: Using a Playbook
- Assisted Lab: Implementing Allow Lists and Deny Lists
- Assisted Lab: Performing Reconnaissance
- Assisted Lab: Performing Penetration Testing
- Assisted Lab: Training and Awareness through Simulation
- Capstone Lab: Discovering Anomalous Behavior
- Assisted Lab: Use Cases of Automation and Scripting
- Applied Lab: Using Network Sniffers

License Information

One license provides access to CertMaster Learn for Security+ (SY0-701) with CertMaster Labs integrated throughout the course and ITU custom Security+ training and labs.

Once activated, the license is valid for 12 months

How to Access the training and labs

An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee

This bundle includes an exam voucher and an exam pass guarantee: if you don't pass the exam on the first try, we will provide a second voucher and another 12 months of access to our custom online self-paced ILT. In order to qualify for the exam pass guarantee, you have to show proof that you completed all training materials, to include course content, labs and practice prep questions prior to taking your exam.

CompTIA PenTest+ Bundle

ITI SKU: CompTIA-4

MSRP: $1,999

Sales Price: $1,499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA PenTest+ certification is an industry-recognized credential that validates the skills necessary to perform penetration testing and vulnerability management. Our blended learning bundles combine custom self-paced online instructor lead training (ILT) courses with CompTIA's official CertMaster Learn training and Integrated CertMaster Labs, over a 12-month period. This approach ensures a thorough understanding by offering theoretical knowledge and practical skills, leading to better retention and mastery of penetration testing concepts. The bundle also includes an exam voucher and an exam pass guarantee.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT with Labs Description: Master penetration testing with our CompTIA PenTest+ Online Self-Paced ILT Course, designed for aspiring penetration testers, security consultants, and IT professionals. This course offers comprehensive content delivered through engaging video lessons, quizzes, and hands-on labs. Once purchased, you have 12 months' access to the course.

Course Highlights:

- Duration: 34+ hours
- Content: 200+ On-demand Videos
- Exam Prep: 240+ Prep Questions
- Certificate of Completion for CompTIA PenTest+

Topics Areas Included:

- Penetration Test Engagement
- Passive Reconnaissance:
- Active Reconnaissance
- Physical Security
- Social Engineering
- Vulnerability Scan Analysis
- Password Cracking
- Network Penetration Testing
- Exploitation of Windows and Linux Systems
- Web Application Testing

Modules:

- Module 1 - The Pen Test Engagement
- Module 2 - Passive Reconnaissance
- Module 3 - Active Reconnaissance
- Module 4 - Physical Security
- Module 5 - Social Engineering
- Module 6 - Vulnerability Scan Analysis
- Module 7 - Password Cracking
- Module 8 - Penetrating Wired Networks
- Module 9 - Penetrating Wireless Networks
- Module 10 - Windows Exploits
- Module 11 - Linux Exploits
- Module 12 - Mobile Devices
- Module 13 - Specialized Systems

- Module 14 - Scripts
- Module 15 - Application Testing
- Module 16 - Web App Exploits
- Module 17 - Lateral Movement
- Module 18 - Persistence
- Module 19 - Cover Your Tracks
- Module 20 - The Report
- Module 21 - Post Engagement Cleanup

Labs included (15 hours):

- Planning and Preparing for a Penetration Test Engagement
- Using the Metasploit Framework
- Performing Social Engineering
- Conducting Passive Reconnaissance for Vulnerabilities in a Network
- Conducting Active Reconnaissance for Vulnerabilities in a Network
- Perform Vulnerability Scan and Analyze Vulnerability Scan Results
- Exploiting the Network Vulnerabilities
- Exploiting Desktop Systems Vulnerabilities
- Exploit Web Application Vulnerabilities
- Performing Password Attacks
- Exploiting Discovered Vulnerabilities
- Work with Various Tools
- Performing Physical Security
- Working with Scripts
- Complete Post Exploit Tasks
- Analyzing and Reporting the Pen Test Results

CompTIA CertMaster Learn and Labs Description: CertMaster Learn and Labs for CompTIA PenTest+ (PT0-002) provides a comprehensive eLearning experience, helping learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career. The learning plan includes:

- Scoping Organization/Customer Requirements
- Defining the Rules of Engagement

- Footprinting and Gathering Intelligence
- Evaluating Human and Physical Vulnerabilities
- Preparing the Vulnerability Scan
- Scanning Logical Vulnerabilities
- Analyzing Scanning Results
- Avoiding Detection and Covering Tracks
- Exploiting the LAN and Cloud
- Testing Wireless Networks
- Targeting Mobile Devices
- Attacking Specialized Systems
- Web Application-Based Attacks
- Performing System Hacking
- Scripting and Software Development
- Leveraging the Attack: Pivot and Penetrate
- Communicating During the PenTesting Process
- Summarizing Report Components
- Recommending Remediation
- Performing Post-Report Delivery Activities

Integrated Labs:

- Exploring the Lab Environment
- Gathering Intelligence
- Performing Social Engineering using SET
- Discovering Information using Nmap
- Performing Vulnerability Scans and Analysis
- Penetrating an Internal Network
- Exploiting Web Authentication
- Exploiting Weaknesses in a Website
- Exploiting Weaknesses in a Database
- Using SQL Injection
- Performing an AitM Attack

- Performing Password Attacks
- Using Reverse and Bind Shells
- Performing Post-Exploitation Activities
- Establishing Persistence
- Performing Lateral Movement

License Information:

- One license provides access to CertMaster Learn for PenTest+ (PT0-002) with CertMaster Labs integrated throughout the course and ITI Custom course and labs.
- Once activated, the license is valid for 12 months.
- Access keys must be redeemed within 12 months of purchase.

How to Access CertMaster Learn integrated with CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee: This bundle includes an exam voucher and an exam pass guarantee: if you don't pass the exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Server+ and Microsoft Server Bundle

ITI SKU: CompTIA-5

MSRP: $1999

Sales Price: $1899

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Server+ and Microsoft Bundle are designed to provide comprehensive training for individuals looking to gain expertise in server management and hybrid cloud environments. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Server+ and Microsoft technologies, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. Although the Microsoft MTA 98-365 is no longer offered, the training, in addition to the AZ-104 Azure Administrator training, prepares you for both the Server+ and Microsoft Hybrid Core exams. The bundle also includes an exam voucher and an exam pass guarantee for Server+.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT, followed by the integrated CompTIA Server+ CertMaster Learn and Labs and TestOut training for Microsoft Hybrid Core.

CTI Custom Online Self-Paced ILT Descriptions:

Microsoft MTA 98-365 course and labs: This training provides valuable knowledge and skills necessary for server management, which is useful for preparing for the Server+ certification. This course offers comprehensive content delivered through engaging video lessons, quizzes, and hands-on labs. Once purchased, you have 12 months' access to the course.

Course Highlights:

- Duration: 5+ Training Hours
- Content: 35+ On-demand Videos, covering essential server management topics
- Preparation Questions: 74

Modules:

- Module 1 Introducing Windows Server 2016
- Module 2 Managing Windows Server 2016
- Module 3 Managing Storage
- Module 4 Monitoring and Troubleshooting Servers
- Module 5 Essential Services
- Module 6 Understanding File and Print Services
- Module 7 Windows Network Services and Applications
- Mod 8 Key Takeaways
- Mod 9 Terms to Know
- Mod 10 Hands on Labs

Labs included (30 hours)

- Install and Configure Nano Server
- Install and Configure Server Core
- Configure Network Installation of Windows
- Manage Windows Services
- Working with Mail Servers
- Configure Remote Assistance and Remote Server Admin Tools

- Manage Remote Access with VPN
- Configure Application Virtualization
- Manage Active Directory Infrastructure - Part 1
- Manage Active Directory Infrastructure - Part 2
- Manage Active Directory Infrastructure - Part 3
- Manage Virtual Hard Disks with Hyper-V
- Enable Nested Virtualization
- Manage Shared Storage using iSCSI
- Manage Updates with Windows Server Update Services
- Configure Group Policy Settings
- Configure Disk Types
- Configure Distributed File System
- Manage Disk Redundancy
- Manage File System Security
- Manage Windows Event Logs
- Configure Audit Policies
- Administer OUs and Containers
- Administer User and Group Accounts
- Implement Group Nesting
- Backup and Restore Active Directory
- Install and Configure a Database Server
- Install and Configure a Failover Cluster
- Configure User Profiles
- Implement Folder Redirection
- Implement Performance Monitor
- Install and Configure Web Services
- Working with Collaboration Software
- Install and Configure Threat Management Software
- Manage Remote Desktop Services

CompTIA Server+ labs: The Server+ Practice Lab's primary focus is the practical application of the CompTIA exam objectives, providing a 19-hour hands-on practical lab experience. Once purchased, you have 12 months' access to the labs.

Labs included (19 hours):

- Server Operating Systems Installation Methods
- Server Network Infrastructure Configuration
- Installing and Configuring Server Roles and Features
- Server Identity and Access Management
- Deploying and Managing Server Storage
- Implementing a Backup and Restore Solution
- Automation of Server Administration using Scripts
- Server Virtualization Concepts
- Configuring Server High Availability
- Server and Application Hardening Techniques
- Server Hardware Components
- Securing a Physical Server Infrastructure
- Server Hardware Maintenance
- Server Licensing Concepts
- Data Security Concepts
- Troubleshooting Server Storage Related Issues
- Server Operating Systems Troubleshooting Techniques
- Troubleshooting Network Connectivity Issues

AZ-104 Microsoft Azure Administrator Certification: Prepare for the Microsoft AZ-104 Azure Administrator certification with this comprehensive course. This course covers advanced Azure administration, including managing Azure identities and governance, implementing and managing storage, and configuring and managing virtual networks.

Course Highlights:

- Duration: 35+ Training Hours
- Content: 85+ On-demand Videos, covering Azure administration topics
- Preparation Questions: 200

Modules:

- Module 1 – Overview: Azure Essentials for Success
- Module 2 – Tools: Navigating the Azure Ecosystem
- Module 3 – Identities and Governance: Secure and Efficient Identity Management
- Module 4 – Master Data Storage and Security
- Module 5 – Compute Resources: Unlock the Power of Azure Compute
- Module 6 – Virtual Networks: Connect and Secure Your Resources
- Module 7 – Monitoring and Backup: Ensure Stability and Recovery

Labs included (8 hours):

- Azure Management Concepts Lab (3 Hours):
  - Azure Service Level Agreements (SLAs)
  - Management Tools
  - Monitoring Tools
  - The Azure Marketplace
- Azure Storage Management Lab (2 Hours):
  - Azure Storage Services
  - Working with Blobs
  - Azure SQL Databases
  - Azure Cosmos Databases
- Azure Security Concepts Lab (3 Hours):
  - Using Azure Key Vault
  - Security Tools
  - Network Security

Sever+ CertMaster Learn with Labs:

Server+ CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow. Easy-to-use course management tools provide a comprehensive suite of instructor resources alongside a reporting dashboard, making course preparation and progress tracking simple and efficient.

Topics Covered:

- Lesson 1: Understanding Server Administration Concepts
- Lesson 2: Understanding Virtualization and Cloud Computing
- Lesson 3: Understanding Physical and Network Security Concepts
- Lesson 4: Managing Physical Assets
- Lesson 5: Managing Server Hardware
- Lesson 6: Configuring Storage Management
- Lesson 7: Installing and Configuring an Operating System
- Lesson 8: Troubleshooting OS, Application, and Network Configurations
- Lesson 9: Managing Post-Installation Administrative Tasks
- Lesson 10: Managing Data Security
- Lesson 11: Managing Service and Data Availability
- Lesson 12: Decommissioning Servers

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Reporting Windows Server Specifications
- Assisted Lab: Reporting Linux Server Specifications
- Assisted Lab: Deploying a Hyper-V VM
- Assisted Lab: Deploying a Docker Container
- Assisted Lab: Auditing Network Services
- Assisted Lab: Securing Network Traffic with IPSec
- Assisted Lab: Managing System Inventories
- Assisted Lab: Monitoring Performance in Windows
- Assisted Lab: Monitoring Performance in Linux
- APPLIED LAB: Deploying and Monitoring Servers
- Assisted Lab: Managing Event Logs in Windows
- Assisted Lab: Managing Event Logs in Linux
- Assisted Lab: Configuring RAID Storage in Windows
- Assisted Lab: Provisioning iSCSI Storage
- Assisted Lab: Deploying a Linux Application Server
- Assisted Lab: Configuring Volumes in Linux
- Assisted Lab: Managing Network Configurations
- Assisted Lab: Developing Network Documentation

- Assisted Lab: Developing Administrative Bash Scripts
- Assisted Lab: Developing Administrative PowerShell Scripts
- APPLIED LAB: Managing Storage and Networks
- Assisted Lab: Troubleshooting a Network Issue
- Assisted Lab: Auditing Accounts and Permissions in Windows
- Assisted Lab: Configuring Server Roles
- Assisted Lab: Configuring Administrative Interfaces
- Assisted Lab: Managing Virtual Memory
- Assisted Lab: Configuring Group Policy Objects
- Assisted Lab: Analyzing Configuration Baselines
- APPLIED LAB A: Troubleshooting Servers Scenario #1
- APPLIED LAB B: Troubleshooting Servers Scenario #2
- APPLIED LAB C: Troubleshooting Servers Scenario #3
- Assisted Lab: Configuring EFS and BitLocker
- Assisted Lab: Troubleshooting a Security Issue
- Assisted Lab: Configuring Backup Solutions on Windows Server
- Assisted Lab: Configuring Backup Solutions on Linux
- Assisted Lab: Configuring a File Server Cluster
- Assisted Lab: Decommissioning a Domain Controller
- APPLIED LAB A: Troubleshooting Server Security Scenario #1
- APPLIED LAB B: Troubleshooting Server Security Scenario #2

TestOut Hybrid Server Pro: Core

Hybrid Server Pro: Core is a high-quality, easy-to-use curriculum where you will gain the knowledge and skills you need to configure and manage both on-premise and cloud based servers. Hosted on the online TestOut learning platform, LabSim, it provides a comprehensive experience for gaining knowledge and practical skills through interactive learning modules like video lessons and lab simulations.

LabSim is ideal for learning server technology in a self-paced engaging way. Instructional lessons are combined with instructor-led videos, demonstrations, quizzes, practice exams, and performance-based lab simulations to provide hours of content to prepare you for the ***Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure*** certification exam.

- Engaging video lessons and text lessons teach you key on-premise and cloud concepts and skills
- Section quizzes help you gauge how well you're retaining what you've learned
- Performance-based labs simulations let you apply what you've learned in real-world scenarios and provide detailed feedback reports and scores

- Exam practice for Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure certification exam includes Readiness Reports, Domain Exams, and full-length exams that emulate the real certification exam

Topics and Integrated Labs Covered

- Chapter 1: Course Introduction
- Chapter 2: On-Premises Windows Server
- Chapter 3: Cloud and Azure
- Chapter 4: Manage IP Addressing
- Chapter 5: Implement DNS
- Chapter 6: Active Directory
- Chapter 7: Active Directory Objects
- Chapter 8: Group Policy
- Chapter 9: Manage Servers and Workloads in a Hybrid Environment
- Chapter 10: Manage Storage Devices
- Chapter 11: Manage File Services
- Chapter 12: Virtualization and Containers
- Chapter 13: On-Premises and Hybrid Network Connectivity
- Appendix A: TestOut Hybrid Server Pro: Core - Practice Exams
- Appendix B: Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure - Practice Exams

License Information

- One license provides access to CertMaster Learn for Server+ (SK0-005) with CertMaster Labs integrated throughout the course, TestOut, as well as ITI custom courses and labs.
- Once activated, the license is valid for 12 months

How to Access Courses and Labs

An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Server+ only): This bundle includes an exam voucher and an exam pass guarantee for Server+: if you don't pass the Server+ exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Project+ and PMP Bundle

ITI SKU: CompTIA-6

MSRP: $1,999

Sales Price: $1,499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Project+ and PMP Bundle is designed to provide comprehensive training for individuals aiming to excel in project management. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Project+ and PMP certifications, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for Project+ only: if you don't pass the Project+ exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for PMP, followed by the integrated CompTIA CertMaster Learn and Labs for Project+.

CTI Custom Online Self-Paced ILT Description: Master project management with our PMP Exam Prep Online Self-Paced ILT Course, designed for aspiring project managers. This course offers comprehensive content delivered through engaging video lessons, quizzes, and hands-on labs. Once purchased, you have 12 months' access to the course.

Course Highlights:

- Duration: 19+ hours
- Content: 55+ On-demand Videos
- Exam Prep: 250+ Prep Questions
- Certification: Certificate of Completion for Project Management Professional – PMP Exam Prep

Topics Areas Included:

- Project Initiation
- Project Planning
- Project Execution
- Project Monitoring and Controlling
- Project Closing

Modules:

- Module 1 : Getting Certified to take the Examination
- Module 2 : Project Management Framework
- Module 3 : Project Integration Management
- Module 4 : Project Scope Management
- Module 5 : Project Schedule Management
- Module 6 : Project Cost Management
- Module 7 : Project Quality Management
- Module 8 : Project Resource Management
- Module 9 : Project Communications Management
- Module 10 : Project Risk Management
- Module 11 : Project Procurement Management
- Module 12 : Project Stakeholder Management
- Module 13 : Review

CompTIA Project+ CertMaster Learn and Labs Description: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

Lessons cover all exam objectives with integrated videos:

- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis

- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Preparing for the Project
- Lesson 2: Selecting the Project Framework
- Lesson 3: Initiating the Project
- Lesson 4: Facilitating Effective Meetings
- Lesson 5: Implementing Solution Design
- Lesson 6: Managing Resources
- Lesson 7: Managing Risk
- Lesson 8: Creating a Project Schedule
- Lesson 9: Creating a Project Plan
- Lesson 10: Procuring Solutions
- Lesson 11: Managing Project Execution
- Lesson 12: Managing Issues and Changes
- Lesson 13: Managing Performance
- Lesson 14: Wrapping Up the Project

Labs Available:

- Assisted Lab: Identify Project Roles and Responsibilities
- Assisted Lab: Select a Project Methodology
- APPLIED LAB: Prepare a Project Charter
- Assisted Lab: Create a Communication Plan
- APPLIED LAB: Interpret Solution Requirements
- Assisted Lab: Assign Project Resources
- Assisted Lab: Analyze Risk
- APPLIED LAB: Build a Project Schedule
- Assisted Lab: Identify the Critical Path
- Assisted Lab: Compare Resource Procurement Methods
- APPLIED LAB: Build a Sprint Plan

- Assisted Lab: Identify Issues
- Assisted Lab: Measure Project Performance
- APPLIED LAB: Reconcile the Project Budget

Product Information:

- One license provides access to CertMaster Learn for Project+ (PK0-005) with CertMaster Labs integrated throughout the course plus ITI courses.
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Project+ only): This bundle includes an exam voucher and an exam pass guarantee for Project+: if you don't pass the Project+ exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Data+ and Data Analyst Bundle

ITI SKU: CompTIA-7

MSRP: $1999

Sales Price: $1,499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Data+ and Data Analyst Bundle is designed to provide comprehensive training for individuals aiming to excel in data analytics. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Data+ and Data Analyst certifications, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for Data+: if you don't pass the Data+ exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Data Analyst, followed by the integrated CompTIA CertMaster Learn and Labs for Data+.

CTI Custom Data Analyst Online Self-Paced ILT Description: Embark on the Data Analyst Career Path with our comprehensive Online Self-Paced ILT bundle of mini-courses, designed for aspiring data analysts. This course covers a wide range of topics, including data collection, analysis, visualization, and advanced techniques using tools like Microsoft Power BI, Excel, and SQL Server. This course offers 42 hours of content delivered through 278 on-demand videos and includes 100 prep questions. Once purchased, you have 12 months' access to the course.

Topics Areas Included:

- Data Collection and Management
- Data Analysis and Interpretation
- Database Management and Querying
- Data Visualization and Reporting
- Excel Proficiency
- Big Data Technologies
- Advanced Analysis Techniques

Once purchased, you have 12 months' access to the course.

Course Highlights:

- Duration: 56+ hours
- Content: 350+ On-demand Videos
- Exam Prep: 400+ Prep Questions
- Certification: Certificate of Completion for Data Analyst

Topics Areas Included:

- Data Visualization
- Data Cleaning
- Data Analysis Techniques
- Data Interpretation

Courses Included:

- Course 1 Microsoft SQL Server – Introduction to Data Analysis
- Course 2 Microsoft SQL Server – Querying SQL Server

- Course 3 Introduction to Microsoft Power BI
- Course 4 Microsoft Excel for Data Analysis
- Course 5 Microsoft SQL Server – Big Data
- Course 6 Microsoft SQL Service Analysis Services (SSAS)

CTI Custom Data+ Online Self-Paced ILT Description: This course prepares participants to manage and analyze data effectively, covering topics like data mining, visualization, statistical analysis, and governance. Learners gain practical experience using tools such as AWS Redshift and Google Cloud SQL, with a focus on creating dashboards and ensuring data quality. The course is ideal for aspiring data analysts, business intelligence professionals, and database managers, providing both theoretical knowledge and hands-on labs to prepare for the CompTIA Data+ certification exam. This course offers 5 hours of content delivered through 70+ on-demand videos and includes 90+ prep questions. Once purchased, you have 12 months' access to the course.

Topics Areas Included:

Introduction to CompTIA Data+

- Course Welcome
- Module Overview
- Instructor Introduction
- What is the CompTIA Data+ Exam
- Roles that Should Consider the Exam
- Exam Objectives
- Discussion – The Importance of Data
- US DOD Member Data Directives and 8570

Module 1 – Data Concepts and Environments

- Understanding Data Schemes
- Databases
- Demonstration – Google Cloud SQL
- Data Warehouses and Data Lakes
- Comparing OLTP and OLAP Processing

- Demonstration – AWS Redshift
- Demonstration – Deploy SQL DemoBench
- What is Column Database
- Data Structures, Files, and Types
- Module Summary Review
- Module Review Questions

Module 2 – Data Mining

- Data Acquisition and Integration
- Demonstration – Data Integration Techniques
- API Fundamentals
- Demonstration – Google Vision API
- Data Profiling and Cleansing
- Data Collection Method Options
- Data Outliers
- Understanding ETL and ELT
- Query Optimization
- Understanding Data Manipulation Techniques
- Module Summary Review
- Module Review Questions

Module 3 – Data Analysis

- Descriptive Statistical Methods
- Measures of Tendency and Dispersion
- Understanding Percentages
- Inferential Statistical Methods
- Hypothesis Testing with Excel
- Whiteboard – Linear Regression and Correlation
- Whiteboard – Analysis Testing

- Module Summary Review
- Module Review Questions

Module 4 – Data Visualization

- Translate Business Requirements to Reports
- Whiteboard – Translate Business Requirements
- Dashboard Fundamentals
- Demonstration – Dashboard Components
- Data Sources and Attributes
- Understanding Charts and Graphs
- Report Types and Elements
- Module Summary Review
- Module Review Questions

Module 5 – Data Governance, Quality, and Controls

- Introduction to Data Governance
- The Data Lifecycle
- Determining Data Classification
- Data Ownership
- Data Storage Access
- Data Privacy and Frameworks
- Information Rights Management (IRM) and Data Loss Prevention (DLP)
- Setting Data Quality Control
- Methods to Validate Quality
- Data Transformation Tools
- Data Security Fundamentals
- Master Data Management (MDM)
- Module Summary Review
- Module Review Questions

Module 6 – Exam Preparation and Practice Exams

- Course Summary Review
- Data Plus Exam Experience
- Certification CEU Requirements
- Practice Exams – Additional Resources
- Course Closeout

CompTIA Data+ CertMaster Learn and Labs Description: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

Lessons cover all exam objectives with integrated videos:

- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Identifying Basic Concepts of Data Schemas
- Understanding Different Data Systems
- Understanding Types and Characteristics of Data

- Comparing and Contrasting Different Data Structures, Formats, and Markup Languages
- Explaining Data Integration and Collection Methods
- Identifying Common Reasons for Cleansing and Profiling Data
- Executing Different Data Manipulation Techniques
- Explaining Common Techniques for Data Manipulation and Optimization
- Applying Descriptive Statistical Methods
- Describing Key Analysis Techniques
- Understanding the Use of Different Statistical Methods
- Using the Appropriate Type of Visualization
- Expressing Business Requirements in a Report Format
- Designing Components for Reports and Dashboards
- Distinguishing Different Report Types
- Summarizing the Importance of Data Governance
- Applying Quality Control to Data
- Explaining Master Data Management Concepts

Labs Available:

- Assisted Lab: Navigating and Understanding Database Design
- Assisted Lab: Understanding Data Types and Conversion
- Assisted Lab: Working with Different File Formats
- APPLIED LAB: Understanding Data Structure and Types and Using Basic Statements
- Assisted Lab: Using Public Data
- Assisted Lab: Profiling Data Sets
- Assisted Lab: Addressing Redundant and Duplicated Data
- Assisted Lab: Addressing Missing Values
- APPLIED LAB: Preparing Data for Use
- Assisted Lab: Recoding Data
- Assisted Lab: Working with Queries and Join Types
- APPLIED LAB: Building Queries and Transforming Data
- Assisted Lab: Using the Measures of Central Tendency

- Assisted Lab: Using the Measures of Variability
- APPLIED LAB: Analyzing Data
- Assisted Lab: Building Basic Visuals to Make Visual Impact
- Assisted Lab: Building Maps with Geographical Data
- Assisted Lab: Using Visuals to Tell a Story
- Assisted Lab: Filtering Data
- Assisted Lab: Designing Elements for Dashboards
- Assisted Lab: Building an Ad Hoc Report
- APPLIED LAB: Visualizing Data
- Assisted Lab: De-Identifying Records

Product and License Information:

- One license provides access to CertMaster Learn for Data+ (DA0-001) with CertMaster Labs integrated throughout the course
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, Learn for Data+ (DA0-001) with CertMaster Labs integrated will be valid for 12 months

How to Access CertMaster Learn integrated with CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Data+ only): This bundle includes an exam voucher and an exam pass guarantee for Data+: if you don't pass the Data+ exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA DataSys+ and MSSQL and Oracle Database Bundle

ITI SKU: CompTIA-8

MSRP: $1999

Sales Price: $1499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA DataSys+ and MSSQL and Oracle Database Bundle provides comprehensive training for individuals seeking to excel in database management and systems administration. This blended bundle includes custom self-

paced online instructor-led training (ILT) courses for Microsoft SQL Server 2019 Administration and Oracle 12c OCP, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for DataSys+: if you don't pass the DataSys+ exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with an additional exam voucher.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for MSSQL and Oracle Database, followed by the integrated CompTIA CertMaster Learn and Labs for DataSys+.

CTI Custom Online Self-Paced ILT Descriptions:

Microsoft SQL Server 2019 Administration: Master SQL Server administration with our comprehensive course designed to provide the skills needed to manage MS SQL databases effectively.

Course Highlights:

- Duration: 6+ hours
- Content: 40+ On-demand Videos
- Exam Prep: 70+ Prep Questions
- Certificate of Completion for Microsoft SQL Server 2019 Administration

Topics Areas Included:

- SQL Server Installation
- Data Storage Management
- Data Recovery Planning
- Monitoring and Performance Tuning
- Security Management
- Maintenance Tasks

Modules:

- Module 1: Installation
- Module 2: Data Storage
- Module 3: Data Recovery
- Module 4: Monitoring
- Module 5: Security

- Module 6: Maintenance

Oracle 12c OCP: Gain expertise in Oracle database administration with our Oracle 12c OCP course (covers exam objectives for 1Z0-061 & 1Z0-062), focusing on installation, administration, and optimization.

Oracle 12c OCP 1Z0-061- SQL Fundamentals Course Highlights:

- Duration: 16+ hours
- Content: 44+ On-demand Videos
- Exam Prep: 240+ Prep Questions
- Certificate of Completion for Oracle 12c OCP 1Z0-061: Installation and Administration

Topics Areas Included:

- Introduction to Oracle 12c SQL Fundamentals
- Structure of SQL and basic SELECT statements
- Retrieving data with WHERE and ORDER BY clauses
- SQL functions, including single row and aggregate functions
- Subqueries and their types
- Data Manipulation Language (DML) operations: adding, changing, and deleting data
- Data Control Language (DCL): security and object privileges
- Data Definition Language (DDL): creating objects, sequences, indexes, and views
- Combining queries
- Comprehensive review of Oracle 12c SQL Fundamentals

Modules

- Module 1: Introduction To Oracle 12c SQL Fundamentals
- Module 2: Retrieving Data
- Module 3: SQL Functions
- Module 4: Subqueries
- Module 5: Data Manipulation Language

- Module 6: Data Control Language
- Module 7: Data Definition Language
- Module 8: Combining Queries
- Module 9: Oracle 12C SQL Fundamentals Review

Labs Included (10 hours):

- Features of Oracle Database 12c
- Retrieving Data Using SQL Statements
- Restricting and Sorting Data
- Using Single Row Functions to Customize Output
- Conversion Functions and Conditional Expressions
- Reporting Aggregated Data Using Group Function
- Displaying Data from Multiple Tables using JOIN
- Using Subqueries
- Managing Tables using DML Statements
- Introduction to DDL Language

1Z0-062 Oracle Database 12c - Installation and Administration Course Highlights:

- Duration: 19+ hours
- Content: 50+ On-demand Videos
- Exam Prep: 55+ Prep Questions
- Certificate of Completion for Oracle 12c OCP 1Z0-062: Installation and Administration

Topics Areas Included:

- Oracle Database Installation
- Database Architecture
- Managing Database Instances
- Performance Monitoring and Tuning
- Backup and Recovery Techniques
- Security Implementation

Modules:

- Module 1: Database Concepts And Tools
- Module 2: Memory Structure
- Module 3: Tables
- Module 4: Indexes
- Module 5: Constraints And Triggers
- Module 6: Users
- Module 7: Internal Structures
- Module 8: Starting Up and Shutting Down Database
- Module 9: Critical Storage Files
- Module 10: Data Manipulation Language
- Module 11: Data Concurrency
- Module 12: BackUp And Recovery
- Module 13: Installation
- Module 14: Course Review

1Z0-062 Labs (18 hours):

- Oracle Database Instances
- Configuring an Oracle Network Environment
- Managing Database Storage Structures
- Administering User Security
- Managing Space
- Managing Data Concurrency and Undo
- Implementing Oracle Database Auditing
- Using Backup and Recovery Concepts
- Performing Database Recovery
- Moving Data
- Managing Database Performance
- Managing Resource Using Database Resource Manager
- Automating Tasks Using Oracle Scheduler
- Installing Oracle Grid Infrastructure and Using Oracle Restart

- Installing Oracle 12c
- Creating an Oracle Database Using DBCA
- Upgrading to Oracle 12c
- Migrating Data Using Oracle Data Pump

CompTIA DataSys+ CertMaster Learn and Labs Description: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

Lessons cover all exam objectives with integrated videos:

- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Understanding Database Types and Structures
- Lesson 2: Recognizing Standards and Commands
- Lesson 3: Running Scripts for Data and Data Systems
- Lesson 4: Explaining the Impact of Programming on Database Operations
- Lesson 5: Understanding Database Planning and Design

- Lesson 6: Implementing, Testing, and Deploying Databases
- Lesson 7: Monitoring and Reporting on Database Performance
- Lesson 8: Understanding Common Data Maintenance Processes
- Lesson 9: Understanding Governance and Regulatory Compliance
- Lesson 10: Securing Data
- Lesson 11: Securing Data Access
- Lesson 12: Securing the Database and Server
- Lesson 13: Classifying Types of Attacks
- Lesson 14: Planning for Disaster Recovery
- Lesson 15: Implementing Backup and Restore Best Practices

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Exploring a Database Environment
- Assisted Lab: Using Command Prompt and PowerShell
- Assisted Lab: Using Data Definition Language (DDL)
- Assisted Lab: Using Data Manipulation Language (DML)
- Assisted Lab: Using Transaction Control Language (TCL)
- Applied Lab: Creating and Manipulating Databases and Data
- Assisted Lab: Using Stored Procedures and Triggers
- Assisted Lab: Using GROUP BY to Group and Aggregate Data
- Assisted Lab: Creating Views with Functions
- Applied Lab: Creating Views and Building Functions
- Assisted Lab: Diagramming Databases
- Assisted Lab: Installing and Configuring Database Connectivity
- Assisted Lab: Validating Data
- Assisted Lab: Monitoring Databases
- Applied Lab: Configuring and Monitoring Databases
- Assisted Lab: Optimizing Queries
- Assisted Lab: Ensuring Data Integrity with Constraints
- Assisted Lab: Masking Data Using Pseudonymization and Anonymization

- Assisted Lab: Using Queries to Conduct Security Audits
- Assisted Lab: Using Queries for Code Review and Code Auditing
- Assisted Lab: Implementing Role-Based Access
- Assisted Lab: Reducing Privileges for Users
- Assisted Lab: Rewriting Queries to Prevent SQL Injection
- Assisted Lab: Backing Up and Restoring Databases with Backup Validation
- Applied Lab: Creating Roles and Establishing a Backup Plan

Product and License Information:

- One license provides access to CertMaster Learn for DataSys+ (DS0-001) with CertMaster Labs integrated throughout the course and ITU courses/labs.
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (DataSys+ only): This bundle includes an exam voucher and an exam pass guarantee for DataSys+: if you don't pass the DataSys+ exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with an additional exam voucher. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA IT Operations Specialist (A+ / Network+) Bundle

ITI SKU: CompTIA-10

MSRP: $2,499

Sales Price: $2,299

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA IT Operations Specialist (A+ / Network+) Bundle provides comprehensive training for individuals seeking to excel in IT operations. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA A+ and Network+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for A+ and Network+.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for A+ and Network+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA IT Operations Specialist (A+ / Network+) Course and Labs: Master IT operations with our comprehensive CompTIA IT Operations Specialist Stackable course and labs, designed to provide the skills needed to manage and troubleshoot various IT systems effectively.

Course Highlights:

- Duration: 85+ hours
- Content: 450+ On-demand Videos
- Exam Prep: 675+ Prep Questions
- Certificate of Completion for CompTIA IT Operations Specialist

Topics Areas Included:

CompTIA A+ 220-1101 (Core 1) Course Content

- Module 1 - Devices, Setups, and Installs
- Module 2 - Displays and Multimedia Devices
- Module 3 - Supporting Multiple Drive Types
- Module 4 - Accounting for CPUs and Internal Components
- Module 5 - All About Network Theories
- Module 6 - Network Operations and Diagnostics
- Module 7 - Cloud and Virtualization Computing
- Module 8 - Laptop Features and Troubleshooting
- Module 9 - Syncing and Setup of Mobile Devices
- Module 10 - All Things Printing
- Module 11 - Resources and Testing

CompTIA A+ 220-1102 (Core 2) Course Content

- Module 1 - Operating System Management
- Module 2 - Configuring and installing the OS

- Module 3 - Tools to Troubleshoot and Maintain the OS
- Module 4 - Network Management Tools
- Module 5 - Sharing Resources and Wrights Management
- Module 6 - Threats and Security Measures
- Module 7 - Policies to Protect Data
- Module 8 - Prevent Malware and Security Threats
- Module 9 - Supporting and Troubleshooting Mobile Devices
- Module 10 - Implementing Operational Procedures
- Module 11 - Resources and Testing

CompTIA Network+ N10-008 Course Content

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

Labs included:

CompTIA A+ (56 hours)

1. Operating System Types and Features
2. Implementing Different Boot Methods and Types of Operating System Installation
3. Disk Partitioning Methods and File Systems
4. Installing System Configuration Settings
5. Using Microsoft Command Line Tools
6. Using Microsoft Operating System Tools and Features
7. Microsoft Windows System Utilities
8. Using Microsoft Windows Control Panel Utilities
9. Using Microsoft Windows Control Panel's User Related Utilities
10. Application Software Installation and Configuration Methods
11. Features and Tools of Mac OS and Linux Desktop Operating System
12. Logical Security Concepts
13. Wi-fi Security Protocols and Authentication Methods
14. Working with Tools and Methods of Malware Prevention, Detection and Removal
15. Microsoft Windows OS Security Settings
16. Implementing Security Best Practices to Secure a Workstation
17. Using Data Destruction and Disposal Methods
18. Troubleshooting Microsoft Windows Issues
19. Troubleshooting PC Security Issues
20. Malware Removal Best Practices
21. Implementing Basic Change Management Best Practices
22. Implement Basic Disaster Prevention and Recovery Methods
23. Basics of Scripting
24. Working with Remote Access Technologies
25. Documentation and Licenses Best Practices
26. Using Proper Communication Techniques and Professionalism

27. Using System Restore
28. Working with BitLocker
29. Identifying different Windows Operating System Editions
30. Managing a Windows device using the Command Line Interface
31. Managing a Windows device using the Graphical User Interface (GUI)
32. Configuring a Windows Device using the Control Panel
33. Configuring and Managing a Windows Device using Settings
34. Configuring Networking Settings on a Windows Device
35. Install and Configure Applications on a Windows Device
36. Identify different Operating Systems and functionality
37. Different Operating System Installation methods
38. Tools for Managing and Maintaining MAC Operating Systems
39. Tools for Managing and Maintaining Linux Operating Systems
40. Implementing Physical Security Measures
41. Implementing Network Security Measures
42. Authentication and Authorization Methods
43. Wireless Security Implementation
44. Malware and Social Engineering Prevention Methods
45. Security Implementation on a Windows Device
46. Password and Account Management on a Windows Device
47. Mobile Security Solutions
48. Secure Data Disposal Methods
49. Securing a SOHO Network
50. Securing Web Browsers on a Windows Device
51. Troubleshooting Windows Operating Systems
52. Troubleshooting Personal Computer Security Settings
53. Malware Removal and Remediating Best Practices

54. Troubleshooting Mobile Device Security Settings
55. Documentation Best Practices
56. Implementing Basic Change Management Best Practices
57. Backup and Recovery Implementation
58. Safety and Environmental Procedures
59. Privacy, Licensing & Policy Concepts
60. Using Proper Communication Techniques and Professionalism
61. Basic Scripting Techniques
62. Remote Access Methods

CompTIA Network+ (33 hours)

1. Introduction to the OSI Model
2. Networking Topologies and Characteristics
3. Internet Protocol Addressing Solutions
4. Cable and Connector Types
5. Cable Management Solutions
6. Virtual Network Concepts
7. Network Security Concept Fundamentals
8. General Network Attacks
9. Network Services and Protocols
10. Network Command Line Tools
11. Network Analysis Software
12. Configuring and Maintaining DNS Servers
13. DHCP Server Installation and Configuration
14. Remote Access and Management
15. Load Balancing and NIC Teaming
16. NTP Server Management
17. High Availability and Disaster Recovery Concepts

18. Configuring Switching Features
19. Routing Concepts and Protocols
20. Troubleshooting Common Networking Issues
21. Cloud Concepts
22. Network Architecture
23. Networking Device Monitoring
24. Network Troubleshooting Techniques
25. Networking Hardening Techniques and Best Practices
26. Physical Networking Tools
27. Defining Networking Devices
28. Troubleshooting Cable Connectivity
29. Wireless Configuration Techniques and Standards
30. Troubleshooting and Securing Wireless Networks
31. Physical Network Security Concepts
32. Organizational Documentation and Procedures
33. Organizational Networking Diagrams and Agreements

CompTIA CertMaster Learn and Labs for A+ and Network+ Descriptions:

CompTIA A+ (220-1101 and 220-1102) CertMaster Learn and Labs: CertMaster Learn for CompTIA A+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career. There is 40+ hours of training and the A+ Core 1 and Core 2 have 190 (100 practice questions/90 final assessment questions) each.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis

- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Installing Motherboards and Connectors
- Lesson 2: Installing System Devices
- Lesson 3: Troubleshooting PC Hardware
- Lesson 4: Comparing Local Networking Hardware
- Lesson 5: Configuring Network Addressing and Internet Connections
- Lesson 6: Supporting Network Services
- Lesson 7: Summarizing Virtualization and Cloud Concepts
- Lesson 8: Supporting Mobile Devices
- Lesson 9: Supporting Print Devices
- Lesson 10: Configuring Windows
- Lesson 11: Managing Windows
- Lesson 12: Identifying OS Types and Features
- Lesson 13: Supporting Windows
- Lesson 14: Managing Windows Networking
- Lesson 15: Managing Linux and macOS
- Lesson 16: Configuring SOHO Network Security
- Lesson 17: Managing Security Settings
- Lesson 18: Supporting Mobile Software
- Lesson 19: Using Support and Scripting Tools
- Lesson 20: Implementing Operational Procedures

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Installing a Motherboard
- Assisted Lab: Installing Power Supplies

- Assisted Lab: Installing and Configuring System Memory
- Assisted Lab: Installing RAM
- Assisted Lab: Installing CPU and Cooler
- Assisted Lab: Upgrading and Installing GPU and Daisy-Chain Monitors
- Assisted Lab: Exploring the Virtual Machine Lab Environment
- Assisted Lab: Compare Networking Hardware
- Assisted Lab: Compare Wireless Network Technologies
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Compare Protocols and Ports
- Assisted Lab: Troubleshoot a Network #1
- Assisted Lab: Troubleshoot a Network #2
- APPLIED Lab: Troubleshoot a Network #1
- APPLIED Lab: Troubleshoot a Network #2
- Assisted Lab: Adding Expansion SSD in a Laptop
- Assisted Lab: Upgrading Laptop RAM
- Assisted Lab: Replacing Laptop Non-User Removable Battery
- Assisted Lab: Configuring Laptop Dock and External Peripherals
- Assisted Lab: Deploy a Printer
- Assisted Lab: Manage User Settings in Windows
- Assisted Lab: Support Windows 11
- Assisted Lab: Configure Windows System Settings
- Assisted Lab: Use Management Consoles
- Assisted Lab: Use Task Manager
- Assisted Lab: Monitor Performance and Event Logs
- Assisted Lab: Use Command-line Tools
- APPLIED Lab: Support Windows 10
- Assisted Lab: Perform Windows 10 OS Installation

- Assisted Lab: Perform Ubuntu Linux OS Installation
- Assisted Lab: Install and Configure an Application
- Assisted Lab: Troubleshoot a Windows OS Issue
- Assisted Lab: Configure Windows Networking
- Assisted Lab: Configure Folder Sharing in a Workgroup
- Assisted Lab: Manage Linux using Command-line Tools
- Assisted Lab: Manage Files using Linux Command-line Tools
- APPLIED Lab: Support and Troubleshoot Network Hosts
- Assisted Lab: Configure SOHO Router Security
- Assisted Lab: Configure Workstation Security
- Assisted Lab: Configure Browser Security
- Assisted Lab: Troubleshoot Security Issues Scenario #1
- APPLIED Lab: Troubleshoot Security Issues Scenario #2
- Assisted Lab: Use Remote Access Technologies
- Assisted Lab: Implement Backup and Recovery
- Assisted Lab: Implement a PowerShell Script
- Assisted Lab: Implement Bash Script
- Assisted Lab: Manage a Support Ticket
- Assisted Lab: Support Active Directory Domain Networking

Product and License Information:

- One license provides access to CertMaster Learn for A+ Core 1 & Core 2 (220-1101 & 220-1102) with CertMaster Labs integrated throughout the course
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, Learn for A+ Core 1 & Core 2 (220-1101 & 220-1102) with CertMaster Labs integrated will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

CompTIA Network+ (N10-008) CertMaster Learn and Labs: CertMaster Learn for CompTIA Network+ provides a comprehensive eLearning experience that helps learners

gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career. There is 40+ hours of training, and 20 lessons with interactive Performance-Based Questions, 263 practice questions with immediate feedback and a 90-question final assessment simulates the test experience.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Comparing OSI Model Network Functions
- Lesson 2: Deploying Ethernet Cabling
- Lesson 3: Deploying Ethernet Switching
- Lesson 4: Troubleshooting Ethernet Networks
- Lesson 5: Explaining IPv4 Addressing
- Lesson 6: Supporting IPv4 and IPv6 Networks
- Lesson 7: Configuring and Troubleshooting Routers
- Lesson 8: Explaining Network Topologies and Types
- Lesson 9: Explaining Transport Layer Protocols
- Lesson 10: Explaining Network Services
- Lesson 11: Explaining Network Applications
- Lesson 12: Ensuring Network Availability
- Lesson 13: Explaining Common Security Concepts
- Lesson 14: Supporting and Troubleshooting Secure Networks

- Lesson 15: Deploying and Troubleshooting Wireless Networks
- Lesson 16: Comparing WAN Links and Remote Access Methods
- Lesson 17: Explaining Organizational and Physical Security Concepts
- Lesson 18: Explaining Disaster Recovery and High Availability Concepts
- Lesson 19: Applying Network Hardening Techniques
- Lesson 20: Summarizing Cloud and Datacenter Architecture

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Capture Network Traffic
- Assisted Lab: Configure Interface Settings
- Assisted Lab: Configure IPv4 Static Addressing
- Assisted Lab: Analyze ARP Traffic
- Assisted Lab: Use Tools to Test IP Configuration
- Assisted Lab: Configure IPv6 Static Addressing
- Assisted Lab: Configure Static Routing
- Assisted Lab: Configure Dynamic Routing
- APPLIED Lab: Troubleshoot IP Networks
- Assisted Lab: Use Network Scanners
- Assisted Lab: Analyze a DHCP Server Configuration
- Assisted Lab: Analyze a DNS Server Configuration
- Assisted Lab: Analyze Application Security Configurations
- Assisted Lab: Configure Secure Access Channels
- Assisted Lab: Configure SNMP and Syslog Collection
- Assisted Lab: Analyze Network Performance
- APPLIED Lab: Verify Service and Application Configuration
- Assisted Lab: Configure a NAT Firewall

- Assisted Lab: Configure Remote Access
- APPLIED Lab: Troubleshoot Service and Security Issues
- Assisted Lab: Develop Network Documentation
- Assisted Lab: Backup and Restore Network Device Configurations
- Assisted Lab: Analyze an On-Path Attack
- Assisted Lab: Configure Port Security

Product Information:

- One license provides access to CertMaster learn and labs and ITI courses and/or labs
- Once activated, the license is valid for 12 months

How to: Instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee: This bundle includes an exam voucher and an exam pass guarantee for A+ and Net+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with an additional exam voucher. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Systems Support Specialist (A+ / Linux+) Bundle

ITI SKU: CompTIA-11

MSRP: $2799

Sales Price: $2,299

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Systems Support Specialist (A+ / Linux+) Bundle provides comprehensive training for individuals seeking to excel in IT operations and Linux administration. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA A+ and Linux+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for A+ and Linux+.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for A+ and Linux+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Systems Support Specialist (A+ / Linux+): Master IT operations and Linux administration with our comprehensive CompTIA Systems Support Specialist course, designed to provide the skills needed to manage and troubleshoot various IT systems effectively.

Course Highlights:

- Duration: 65+ hours
- Content: 340+ On-demand Videos
- Exam Prep: 600+ Prep Questions
- Certificate of Completion for CompTIA Systems Support Specialist

Topics Areas Included:

CompTIA A+ 220-1101 (Core 1) Course Content

- Module 1: Devices, Setups, and Installs
- Module 2: Displays and Multimedia Devices
- Module 3: Supporting Multiple Drive Types
- Module 4: Accounting for CPUs and Internal Components
- Module 5: All About Network Theories
- Module 6: Network Operations and Diagnostics
- Module 7: Cloud and Virtualization Computing
- Module 8: Laptop Features and Troubleshooting
- Module 9: Syncing and Setup of Mobile Devices
- Module 10: All Things Printing
- Module 11: Resources and Testing

CompTIA A+ 220-1102 (Core 2) Course Content

- Module 1: Operating System Management
- Module 2: Configuring and installing the OS
- Module 3: Tools to Troubleshoot and Maintain the OS
- Module 4: Network Management Tools

- Module 5: Sharing Resources and Wrights Management
- Module 6: Threats and Security Measures
- Module 7: Policies to Protect Data
- Module 8: Prevent Malware and Security Threats
- Module 9: Supporting and Troubleshooting Mobile Devices
- Module 10: Implementing Operational Procedures
- Module 11: Resources and Testing

CompTIA Linux+ Course Content

- Lesson 1: Introducing Linux
- Lesson 2: Administering Users and Groups
- Lesson 3: Configuring Permissions
- Lesson 4: Implementing File Management
- Lesson 5: Authoring Text Files
- Lesson 6: Managing Software
- Lesson 7: Administering Storage
- Lesson 8: Managing Devices, Processes, Memory, and the Kernel
- Lesson 9: Managing Services
- Lesson 10: Configuring Network Settings
- Lesson 11: Configuring Network Security
- Lesson 12: Managing Linux Security
- Lesson 13: Implementing Simple Scripts
- Lesson 14: Using Infrastructure as Code
- Lesson 15: Managing Containers in Linux
- Lesson 16: Installing Linux

Labs included:

CompTIA Linux+ (63 hours) labs

1. Design Hard Disk Layout

2. Create Partitions and Filesystems
3. Using Various Disk Management Tools
4. Working with Kernel, Boot Modules, and Files
5. Working with Relative and Absolute Paths
6. Work with the Flow Control Constructs
7. Control Mounting and Unmounting of Filesystems
8. View the Hard Drive Details
9. Check and Repair Filesystems
10. Using RPM and YUM Package Management
11. Using Debian Package Management
12. Using Repositories
13. Managing User and Group Accounts and Related System Files
14. Run User Level Queries
15. Managing Disk Quotas
16. Working with Bash Profiles and Bash Scripts
17. Setup Host Security
18. Perform Basic File Editing Operations Using vi
19. Search Text Files using Regular Expressions
20. Using Shell Input and Output Redirections
21. Install and Configure a Web Server
22. Performing Basic File Management
23. Amending Hard and Symbolic Links
24. Find System Files and Place Files in the Correct Location
25. Use Systemctl and update-rc.d Utility to Manage Services
26. Configuring Host Names
27. Change Runlevels and Shutdown or Reboot System
28. Maintain System Time

29. Configure Client Side DNS
30. Configure System Logging
31. Mail Transfer Agent (MTA) Basics
32. Automate System Administration Tasks by Scheduling Jobs
33. Create, Monitor and Kill Processes
34. Manage Printers and Printing
35. Accessibility
36. Manage File Permissions and Ownership
37. Perform Security Administration Tasks
38. Working with Access Control List
39. Configure SELinux
40. Maintain the Integrity of Filesystems
41. Work with Pluggable Authentication Modules (PAM)
42. Secure Communication using SSH
43. Securing Data with Encryption
44. Work with TTY
45. Set up SFTP to Chroot Jail only for Specific Group
46. Secure a Linux Terminal and Implement Logging Services
47. Boot the System
48. Configure UFW and DenyHosts
49. Compress Data Using Various Tools and Utilities
50. Process Text Streams using Filters
51. Basic Network Troubleshooting
52. Use Streams Pipes and Redirects
53. Perform CPU Monitoring and Configuration
54. Perform Memory Monitoring and Configuration
55. Perform Process Monitoring

56. Modify Process Execution Priorities
57. Manage File and Directory Permissions
58. Access the Linux System
59. Configure Inheritance and Group Memberships
60. Patch the System
61. Working with the Environment Variables
62. Shells, Scripting and Data Management
63. Customize or Write Simple Scripts
64. Configure Permissions on Files and Directories
65. Work with PKI

CompTIA A+ (56 hours) labs

1. Operating System Types and Features
2. Implementing Different Boot Methods and Types of Operating System Installation
3. Disk Partitioning Methods and File Systems
4. Installing System Configuration Settings
5. Using Microsoft Command Line Tools
6. Using Microsoft Operating System Tools and Features
7. Microsoft Windows System Utilities
8. Using Microsoft Windows Control Panel Utilities
9. Using Microsoft Windows Control Panel's User Related Utilities
10. Application Software Installation and Configuration Methods
11. Features and Tools of Mac OS and Linux Desktop Operating System
12. Logical Security Concepts
13. Wi-fi Security Protocols and Authentication Methods
14. Working with Tools and Methods of Malware Prevention, Detection and Removal
15. Microsoft Windows OS Security Settings
16. Implementing Security Best Practices to Secure a Workstation

17. Using Data Destruction and Disposal Methods
18. Troubleshooting Microsoft Windows Issues
19. Troubleshooting PC Security Issues
20. Malware Removal Best Practices
21. Implementing Basic Change Management Best Practices
22. Implement Basic Disaster Prevention and Recovery Methods
23. Basics of Scripting
24. Working with Remote Access Technologies
25. Documentation and Licences Best Practices
26. Using Proper Communication Techniques and Professionalism
27. Using System Restore
28. Working with BitLocker
29. Identifying different Windows Operating System Editions
30. Managing a Windows device using the Command Line Interface
31. Managing a Windows device using the Graphical User Interface (GUI)
32. Configuring a Windows Device using the Control Panel
33. Configuring and Managing a Windows Device using Settings
34. Configuring Networking Settings on a Windows Device
35. Install and Configure Applications on a Windows Device
36. Identify different Operating Systems and functionality
37. Different Operating System Installation methods
38. Tools for Managing and Maintaining MAC Operating Systems
39. Tools for Managing and Maintaining Linux Operating Systems
40. Implementing Physical Security Measures
41. Implementing Network Security Measures
42. Authentication and Authorization Methods
43. Wireless Security Implementation

44. Malware and Social Engineering Prevention Methods
45. Security Implementation on a Windows Device
46. Password and Account Management on a Windows Device
47. Mobile Security Solutions
48. Secure Data Disposal Methods
49. Securing a SOHO Network
50. Securing Web Browsers on a Windows Device
51. Troubleshooting Windows Operating Systems
52. Troubleshooting Personal Computer Security Settings
53. Malware Removal and Remediating Best Practices
54. Troubleshooting Mobile Device Security Settings
55. Documentation Best Practices
56. Implementing Basic Change Management Best Practices
57. Backup and Recovery Implementation
58. Safety and Environmental Procedures
59. Privacy, Licensing & Policy Concepts
60. Using Proper Communication Techniques and Professionalism
61. Basic Scripting Techniques
62. Remote Access Methods

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA A+ (220-1101 and 220-1102) CertMaster Learn and Labs: CertMaster Learn for CompTIA A+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career. There is 40+ hours of training and A+ Core 1 and Core 2 have 190 (100 practice questions/90 final assessment questions) each.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario

- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Installing Motherboards and Connectors
- Lesson 2: Installing System Devices
- Lesson 3: Troubleshooting PC Hardware
- Lesson 4: Comparing Local Networking Hardware
- Lesson 5: Configuring Network Addressing and Internet Connections
- Lesson 6: Supporting Network Services
- Lesson 7: Summarizing Virtualization and Cloud Concepts
- Lesson 8: Supporting Mobile Devices
- Lesson 9: Supporting Print Devices
- Lesson 10: Configuring Windows
- Lesson 11: Managing Windows
- Lesson 12: Identifying OS Types and Features
- Lesson 13: Supporting Windows
- Lesson 14: Managing Windows Networking
- Lesson 15: Managing Linux and macOS
- Lesson 16: Configuring SOHO Network Security
- Lesson 17: Managing Security Settings
- Lesson 18: Supporting Mobile Software
- Lesson 19: Using Support and Scripting Tools
- Lesson 20: Implementing Operational Procedures

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Installing a Motherboard
- Assisted Lab: Installing Power Supplies
- Assisted Lab: Installing and Configuring System Memory
- Assisted Lab: Installing RAM
- Assisted Lab: Installing CPU and Cooler
- Assisted Lab: Upgrading and Installing GPU and Daisy-Chain Monitors
- Assisted Lab: Exploring the Virtual Machine Lab Environment
- Assisted Lab: Compare Networking Hardware
- Assisted Lab: Compare Wireless Network Technologies
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Compare Protocols and Ports
- Assisted Lab: Troubleshoot a Network #1
- Assisted Lab: Troubleshoot a Network #2
- APPLIED Lab: Troubleshoot a Network #1
- APPLIED Lab: Troubleshoot a Network #2
- Assisted Lab: Adding Expansion SSD in a Laptop
- Assisted Lab: Upgrading Laptop RAM
- Assisted Lab: Replacing Laptop Non-User Removable Battery
- Assisted Lab: Configuring Laptop Dock and External Peripherals
- Assisted Lab: Deploy a Printer
- Assisted Lab: Manage User Settings in Windows
- Assisted Lab: Support Windows 11
- Assisted Lab: Configure Windows System Settings
- Assisted Lab: Use Management Consoles
- Assisted Lab: Use Task Manager
- Assisted Lab: Monitor Performance and Event Logs

- Assisted Lab: Use Command-line Tools
- APPLIED Lab: Support Windows 10
- Assisted Lab: Perform Windows 10 OS Installation
- Assisted Lab: Perform Ubuntu Linux OS Installation
- Assisted Lab: Install and Configure an Application
- Assisted Lab: Troubleshoot a Windows OS Issue
- Assisted Lab: Configure Windows Networking
- Assisted Lab: Configure Folder Sharing in a Workgroup
- Assisted Lab: Manage Linux using Command-line Tools
- Assisted Lab: Manage Files using Linux Command-line Tools
- APPLIED Lab: Support and Troubleshoot Network Hosts
- Assisted Lab: Configure SOHO Router Security
- Assisted Lab: Configure Workstation Security
- Assisted Lab: Configure Browser Security
- Assisted Lab: Troubleshoot Security Issues Scenario #1
- APPLIED Lab: Troubleshoot Security Issues Scenario #2
- Assisted Lab: Use Remote Access Technologies
- Assisted Lab: Implement Backup and Recovery
- Assisted Lab: Implement a PowerShell Script
- Assisted Lab: Implement Bash Script
- Assisted Lab: Manage a Support Ticket
- Assisted Lab: Support Active Directory Domain Networking

CompTIA Linux+ (XK0-005) CertMaster Learn and Labs: CertMaster Learn for CompTIA Linux+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career. There are 40+ hours of training and there are 150 practice questions and a 90 question final assessment.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos

- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Introducing Linux
- Lesson 2: Administering Users and Groups
- Lesson 3: Configuring Permissions
- Lesson 4: Implementing File Management
- Lesson 5: Authoring Text Files
- Lesson 6: Managing Software
- Lesson 7: Administering Storage
- Lesson 8: Managing Devices, Processes, Memory, and the Kernel
- Lesson 9: Managing Services
- Lesson 10: Configuring Network Settings
- Lesson 11: Configuring Network Security
- Lesson 12: Managing Linux Security
- Lesson 13: Implementing Simple Scripts
- Lesson 14: Using Infrastructure as Code
- Lesson 15: Managing Containers in Linux
- Lesson 16: Installing Linux

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Basic Linux Interaction

- Assisted Lab: Manage User Accounts
- Assisted Lab: Manage Group Accounts
- Assisted Lab: Configure and troubleshoot privilege escalation
- Assisted Lab: Configure Standard Permissions
- Assisted Lab: Configure Special Permissions
- Assisted Lab: Configure ACLs
- Assisted Lab: Troubleshoot permissions
- APPLIED LAB: Identity and Access Control
- Assisted Lab: Manage File Links
- Assisted Lab: Use File Management Commands
- Assisted Lab: Search for Files
- Assisted Lab: Edit Text Files
- Assisted Lab: Backup, Restore, and Compress Files
- Assisted Lab: Manage RPM Packages
- Assisted Lab: Manage DEB Packages
- Assisted Lab: Compile a Program
- Assisted Lab: Download Files From a Web Server
- APPLIED LAB: File and software management
- Assisted Lab: Deploy Storage and LVM
- Assisted Lab: Manage Processes
- Assisted Lab: Manage Services
- Assisted Lab: Deploy Services
- Assisted Lab: Configure Network Settings
- Assisted Lab: Configure Remote Administration
- Assisted Lab: Troubleshoot Network Configurations
- APPLIED LAB: System Management
- Assisted Lab: Configure a Firewall

- Assisted Lab: Intercept Network Traffic
- Assisted Lab: Harden a Linux System
- Assisted Lab: Verify file integrity by using hashes.
- Assisted Lab: Configure SELinux
- APPLIED LAB: Security
- Assisted Lab: Manage Scripts
- Assisted Lab: Configure a System with Ansible
- Assisted Lab: Manage Version Control with Git
- Assisted Lab: Deploy Docker Containers
- Assisted Lab: Manage GRUB2
- Assisted Lab: Deploy a Linux System
- APPLIED LAB: Scripting, Orchestration, Installation

Product Information:

- One license provides access to CertMaster Learn for Linux+ (XK0-005) with CertMaster Labs integrated throughout the course and ITI courses and labs.
- Once activated, the license is valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee: This bundle includes an exam voucher and an exam pass guarantee for A+ and Linux+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with an additional exam voucher. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Cloud Admin Professional (Network+ / Cloud+) Bundle

ITI SKU: CompTIA-12

MSRP: $2499

Sales Price: $2199

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Cloud Admin Professional (Network+ / Cloud+) Bundle provides comprehensive training for individuals seeking to excel in cloud administration and networking. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Network+ and Cloud+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for Network+ and Cloud+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Network+ and Cloud+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Cloud Admin Professional (Network+ / Cloud+): Master cloud administration and networking with our comprehensive CompTIA Cloud Admin Professional course, designed to provide the skills needed to manage and troubleshoot various cloud and network systems effectively.

Course Highlights:

- Duration: 60+ hours
- Content: 335+ On-demand Videos
- Exam Prep: 275+ Prep Questions
- Certificate of Completion for CompTIA Cloud Admin Professional

Topics Areas Included:

CompTIA Network+ N10-008 Course Content

- Module 0: Course introduction
- Module 1: Networking Fundamentals
- Module 2: Cables and Connectors
- Module 3: Internet Protocol (IP)
- Module 4: Layer 7 Protocols
- Module 5: Network Services
- Module 6: Networking Devices
- Module 7: Networked Devices

- Module 8: Routing and Bandwidth Management
- Module 9: Ethernet Switching
- Module 10: Wireless Technologies
- Module 11: Network Performance
- Module 12: High Availability and Disaster Recovery
- Module 13: Organizational Documents
- Module 14: Network Security
- Module 15: Network Troubleshooting

CompTIA Cloud+ CV0-003 Course Content

- Lesson 1: Understanding Cloud Concepts
- Lesson 2: Analyzing System Requirements
- Lesson 3: Deploying a Pilot Project
- Lesson 4: Testing Pilot Project
- Lesson 5: Designing a Cloud Infrastructure
- Lesson 6: Monitoring Cloud Infrastructure
- Lesson 7: Securing Cloud Technologies
- Lesson 8: Securing Cloud Systems
- Lesson 9: Troubleshooting Cloud Issues
- Lesson 10: Preparing for Cloud Deployment

Labs included:

CompTIA Network+ (33 hours)

1. Introduction to the OSI Model
2. Networking Topologies and Characteristics
3. Internet Protocol Addressing Solutions
4. Cable and Connector Types
5. Cable Management Solutions
6. Virtual Network Concepts

7. Network Security Concept Fundamentals
8. General Network Attacks
9. Network Services and Protocols
10. Network Command Line Tools
11. Network Analysis Software
12. Configuring and Maintaining DNS Servers
13. DHCP Server Installation and Configuration
14. Remote Access and Management
15. Load Balancing and NIC Teaming
16. NTP Server Management
17. High Availability and Disaster Recovery Concepts
18. Configuring Switching Features
19. Routing Concepts and Protocols
20. Troubleshooting Common Networking Issues
21. Cloud Concepts
22. Network Architecture
23. Networking Device Monitoring
24. Network Troubleshooting Techniques
25. Networking Hardening Techniques and Best Practices
26. Physical Networking Tools
27. Defining Networking Devices
28. Troubleshooting Cable Connectivity
29. Wireless Configuration Techniques and Standards
30. Troubleshooting and Securing Wireless Networks
31. Physical Network Security Concepts
32. Organizational Documentation and Procedures
33. Organizational Networking Diagrams and Agreements

CompTIA Cloud+ (28 hours)

1. Cloud Deployment Models
2. Different Cloud Service Models
3. Cloud Resource Capacity Planning
4. High Availability and Scalability in the Cloud
5. Analyzing Business Requirements for a Cloud Solution
6. Configuring and Managing Cloud Identities
7. Cloud Networking Concepts
8. Securing Cloud Infrastructure Resources
9. Data Security and Compliance in the Cloud
10. Cloud Security Assessments and Tools
11. Incident Response Procedures
12. Cloud Solution Integration
13. Provisioning Cloud Resources
14. Provisioning Public Cloud Storage Solutions
15. Provisioning Private Cloud Storage Solutions
16. Deploying Cloud Networking Solutions
17. Virtualization Concepts and Platforms
18. Cloud Migration Techniques
19. Configuring Logging for Cloud Resources
20. Implementing Cloud Resource Monitoring Solutions
21. Implementing Cloud Resource Monitoring and Alert Solutions
22. Cloud Dashboards and Reporting
23. Cloud Patches, Upgrading and Lifecycle Management
24. Optimizing Cloud Solutions
25. Implementing Cloud Resource Automation Solutions
26. Implementing Cloud Backup and Restore Solutions

27. Cloud Disaster Recovery Concepts
28. Cloud Troubleshooting Methodologies
29. Security Troubleshooting Techniques
30. Troubleshooting Cloud Deployments
31. Cloud Networking Troubleshooting Concepts
32. Troubleshooting Cloud Resource Utilization
33. Automation and Orchestration Troubleshooting Methodologies

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Network+ (N10-008) CertMaster Learn and Labs: CertMaster Learn for CompTIA Network+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Installing Motherboards and Connectors
- Lesson 2: Installing System Devices
- Lesson 3: Troubleshooting PC Hardware
- Lesson 4: Comparing Local Networking Hardware
- Lesson 5: Configuring Network Addressing and Internet Connections
- Lesson 6: Supporting Network Services

- Lesson 7: Summarizing Virtualization and Cloud Concepts
- Lesson 8: Supporting Mobile Devices
- Lesson 9: Supporting Print Devices
- Lesson 10: Configuring Windows
- Lesson 11: Managing Windows
- Lesson 12: Identifying OS Types and Features
- Lesson 13: Supporting Windows
- Lesson 14: Managing Windows Networking
- Lesson 15: Managing Linux and macOS
- Lesson 16: Configuring SOHO Network Security
- Lesson 17: Managing Security Settings
- Lesson 18: Supporting Mobile Software
- Lesson 19: Using Support and Scripting Tools
- Lesson 20: Implementing Operational Procedures

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Installing a Motherboard
- Assisted Lab: Installing Power Supplies
- Assisted Lab: Installing and Configuring System Memory
- Assisted Lab: Installing RAM
- Assisted Lab: Installing CPU and Cooler
- Assisted Lab: Upgrading and Installing GPU and Daisy-Chain Monitors
- Assisted Lab: Exploring the Virtual Machine Lab Environment
- Assisted Lab: Compare Networking Hardware
- Assisted Lab: Compare Wireless Network Technologies
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Compare Protocols and Ports

- Assisted Lab: Troubleshoot a Network #1
- Assisted Lab: Troubleshoot a Network #2
- APPLIED Lab: Troubleshoot a Network #1
- APPLIED Lab: Troubleshoot a Network #2
- Assisted Lab: Adding Expansion SSD in a Laptop
- Assisted Lab: Upgrading Laptop RAM
- Assisted Lab: Replacing Laptop Non-User Removable Battery
- Assisted Lab: Configuring Laptop Dock and External Peripherals
- Assisted Lab: Deploy a Printer
- Assisted Lab: Manage User Settings in Windows
- Assisted Lab: Support Windows 11
- Assisted Lab: Configure Windows System Settings
- Assisted Lab: Use Management Consoles
- Assisted Lab: Use Task Manager
- Assisted Lab: Monitor Performance and Event Logs
- Assisted Lab: Use Command-line Tools
- APPLIED Lab: Support Windows 10
- Assisted Lab: Perform Windows 10 OS Installation
- Assisted Lab: Perform Ubuntu Linux OS Installation
- Assisted Lab: Install and Configure an Application
- Assisted Lab: Troubleshoot a Windows OS Issue
- Assisted Lab: Configure Windows Networking
- Assisted Lab: Configure Folder Sharing in a Workgroup
- Assisted Lab: Manage Linux using Command-line Tools
- Assisted Lab: Manage Files using Linux Command-line Tools
- APPLIED Lab: Support and Troubleshoot Network Hosts
- Assisted Lab: Configure SOHO Router Security

- Assisted Lab: Configure Workstation Security
- Assisted Lab: Configure Browser Security
- Assisted Lab: Troubleshoot Security Issues Scenario #1
- APPLIED Lab: Troubleshoot Security Issues Scenario #2
- Assisted Lab: Use Remote Access Technologies
- Assisted Lab: Implement Backup and Recovery
- Assisted Lab: Implement a PowerShell Script
- Assisted Lab: Implement Bash Script
- Assisted Lab: Manage a Support Ticket
- Assisted Lab: Support Active Directory Domain Networking

CompTIA Cloud+ (CV0-003) CertMaster Learn and Labs: CertMaster Learn for CompTIA Cloud+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Understanding Cloud Concepts
- Lesson 2: Planning and Designing a Cloud Environment
- Lesson 3: Administering Cloud Resources
- Lesson 4: Managing Cloud Storage

- Lesson 5: Managing Networks in the Cloud
- Lesson 6: Securing and Troubleshooting Networks in the Cloud
- Lesson 7: Managing Cloud Migrations and Troubleshooting Cloud Deployments
- Lesson 8: Managing Cloud Automation and Orchestration
- Lesson 9: Understanding Cloud Security Concepts
- Lesson 10: Managing Cloud Security
- Lesson 11: Managing Cloud Performance
- Lesson 12: Managing Maintenance in the Cloud
- Lesson 13: Implementing High Availability and Disaster Recovery in the Cloud

Labs Available:

- Assisted Lab: Explore the Lab Environment
- Assisted Lab: Plan and Design a Cloud Environment
- Assisted Lab: Deploy and Manage Cloud Resources
- Assisted Lab: Manage Compute Resources
- Assisted Lab: Manage Networks in the Cloud
- Assisted Lab: Secure Cloud Components
- APPLIED LAB: Deploy Cloud Resources
- Assisted Lab: Manage Cloud Automation
- Assisted Lab: Manage Baseline Configurations
- Assisted Lab: Deploy Patches
- Assisted Lab: Configure Monitoring
- Assisted Lab: Manage Backup and Restore Processes
- APPLIED LAB: Manage Cloud Resources

Product Information:

- One license provides access to CertMaster Learn for Network+ and Cloud+ with CertMaster Labs integrated throughout the courses and ITI courses and labs.
- Access keys must be redeemed within 12 months of purchase

- Once redeemed, Learn for Network+ and Cloud+ with CertMaster Labs integrated will be valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Network+ and Cloud+): This bundle includes an exam voucher and an exam pass guarantee for Network+ and Cloud+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Network Infrastructure Professional (Network+ / Server+) and Microsoft Bundle

ITI SKU: CompTIA-13

MSRP: $2,999

Sales Price: $2,499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Network Infrastructure Professional (Network+ / Server+) and Microsoft Bundle provides comprehensive training for individuals seeking to excel in networking and Microsoft system administration. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Network+ and Server+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for Network+ and Server+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Network+ and Server+, and Microsoft courses followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Network+ N10-008: Master networking with our comprehensive CompTIA Network+ course, designed to provide the skills needed to manage and troubleshoot various network systems effectively.

Course Highlights:

- Duration: 25 hours

- Content: 110 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Network+ N10-008

Topics Areas Included:

- Networking Fundamentals
- Network Implementations
- Network Operations
- Network Security
- Network Troubleshooting

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

CompTIA Network+ (33 hours)

1. Introduction to the OSI Model
2. Networking Topologies and Characteristics
3. Internet Protocol Addressing Solutions
4. Cable and Connector Types
5. Cable Management Solutions
6. Virtual Network Concepts
7. Network Security Concept Fundamentals
8. General Network Attacks
9. Network Services and Protocols
10. Network Command Line Tools
11. Network Analysis Software
12. Configuring and Maintaining DNS Servers
13. DHCP Server Installation and Configuration
14. Remote Access and Management
15. Load Balancing and NIC Teaming
16. NTP Server Management
17. High Availability and Disaster Recovery Concepts
18. Configuring Switching Features
19. Routing Concepts and Protocols
20. Troubleshooting Common Networking Issues
21. Cloud Concepts
22. Network Architecture
23. Networking Device Monitoring
24. Network Troubleshooting Techniques
25. Networking Hardening Techniques and Best Practices
26. Physical Networking Tools
27. Defining Networking Devices

28. Troubleshooting Cable Connectivity
29. Wireless Configuration Techniques and Standards
30. Troubleshooting and Securing Wireless Networks
31. Physical Network Security Concepts
32. Organizational Documentation and Procedures
33. Organizational Networking Diagrams and Agreements

Microsoft MTA 98-365 course and labs: This training provides valuable knowledge and skills necessary for server management, which is useful for preparing for the Server+ certification. This course offers comprehensive content delivered through engaging video lessons, quizzes, and hands-on labs. Once purchased, you have 12 months' access to the course.

Course Highlights:

- Duration: 5+ Training Hours
- Content: 35+ On-demand Videos, covering essential server management topics
- Preparation Questions: 74

Modules:

- Module 1 Introducing Windows Server 2016
- Module 2 Managing Windows Server 2016
- Module 3 Managing Storage
- Module 4 Monitoring and Troubleshooting Servers
- Module 5 Essential Services
- Module 6 Understanding File and Print Services
- Module 7 Windows Network Services and Applications
- Mod 8 Key Takeaways
- Mod 9 Terms to Know
- Mod 10 Hands on Labs

Labs included (30 hours)

1. Install and Configure Nano Server

2. Install and Configure Server Core
3. Configure Network Installation of Windows
4. Manage Windows Services
5. Working with Mail Servers
6. Configure Remote Assistance and Remote Server Admin Tools
7. Manage Remote Access with VPN
8. Configure Application Virtualization
9. Manage Active Directory Infrastructure - Part 1
10. Manage Active Directory Infrastructure - Part 2
11. Manage Active Directory Infrastructure - Part 3
12. Manage Virtual Hard Disks with Hyper-V
13. Enable Nested Virtualization
14. Manage Shared Storage using iSCSI
15. Manage Updates with Windows Server Update Services
16. Configure Group Policy Settings
17. Configure Disk Types
18. Configure Distributed File System
19. Manage Disk Redundancy
20. Manage File System Security
21. Manage Windows Event Logs
22. Configure Audit Policies
23. Administer OUs and Containers
24. Administer User and Group Accounts
25. Implement Group Nesting
26. Backup and Restore Active Directory
27. Install and Configure a Database Server
28. Install and Configure a Failover Cluster

29. Configure User Profiles
30. Implement Folder Redirection
31. Implement Performance Monitor
32. Install and Configure Web Services
33. Working with Collaboration Software
34. Install and Configure Threat Management Software
35. Manage Remote Desktop Services

CompTIA Server+ labs: The Server+ Practice Lab's primary focus is the practical application of the CompTIA exam objectives, providing a 19-hour hands-on practical lab experience. Once purchased, you have 12 months' access to the labs.

Labs included (19 hours):

- Server Operating Systems Installation Methods
- Server Network Infrastructure Configuration
- Installing and Configuring Server Roles and Features
- Server Identity and Access Management
- Deploying and Managing Server Storage
- Implementing a Backup and Restore Solution
- Automation of Server Administration using Scripts
- Server Virtualization Concepts
- Configuring Server High Availability
- Server and Application Hardening Techniques
- Server Hardware Components
- Securing a Physical Server Infrastructure
- Server Hardware Maintenance
- Server Licensing Concepts
- Data Security Concepts
- Troubleshooting Server Storage Related Issues
- Server Operating Systems Troubleshooting Techniques

- Troubleshooting Network Connectivity Issues

AZ-104 Microsoft Azure Administrator Certification: Prepare for the Microsoft AZ-104 Azure Administrator certification with this comprehensive course. This course covers advanced Azure administration, including managing Azure identities and governance, implementing and managing storage, and configuring and managing virtual networks.

Course Highlights:

- Duration: 35+ Training Hours
- Content: 85+ On-demand Videos, covering Azure administration topics
- Preparation Questions: 200

Modules:

- Module 1 – Overview: Azure Essentials for Success
- Module 2 – Tools: Navigating the Azure Ecosystem
- Module 3 – Identities and Governance: Secure and Efficient Identity Management
- Module 4 – Master Data Storage and Security
- Module 5 – Compute Resources: Unlock the Power of Azure Compute
- Module 6 – Virtual Networks: Connect and Secure Your Resources
- Module 7 – Monitoring and Backup: Ensure Stability and Recovery

Labs included (8 hours):

- Azure Management Concepts Lab (3 Hours):
    - Azure Service Level Agreements (SLAs)
    - Management Tools
    - Monitoring Tools
    - The Azure Marketplace
- Azure Storage Management Lab (2 Hours):
    - Azure Storage Services
    - Working with Blobs
    - Azure SQL Databases
    - Azure Cosmos Databases

- Azure Security Concepts Lab (3 Hours):
    - Using Azure Key Vault
    - Security Tools
    - Network Security

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Network+ (N10-008) CertMaster Learn and Labs: CertMaster Learn for CompTIA Network+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Comparing OSI Model Network Functions
- Lesson 2: Deploying Ethernet Cabling
- Lesson 3: Deploying Ethernet Switching
- Lesson 4: Troubleshooting Ethernet Networks
- Lesson 5: Explaining IPv4 Addressing
- Lesson 6: Supporting IPv4 and IPv6 Networks
- Lesson 7: Configuring and Troubleshooting Routers
- Lesson 8: Explaining Network Topologies and Types
- Lesson 9: Explaining Transport Layer Protocols

- Lesson 10: Explaining Network Services
- Lesson 11: Explaining Network Applications
- Lesson 12: Ensuring Network Availability
- Lesson 13: Explaining Common Security Concepts
- Lesson 14: Supporting and Troubleshooting Secure Networks
- Lesson 15: Deploying and Troubleshooting Wireless Networks
- Lesson 16: Comparing WAN Links and Remote Access Methods
- Lesson 17: Explaining Organizational and Physical Security Concepts
- Lesson 18: Explaining Disaster Recovery and High Availability Concepts
- Lesson 19: Applying Network Hardening Techniques
- Lesson 20: Summarizing Cloud and Datacenter Architecture

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Capture Network Traffic
- Assisted Lab: Configure Interface Settings
- Assisted Lab: Configure IPv4 Static Addressing
- Assisted Lab: Analyze ARP Traffic
- Assisted Lab: Use Tools to Test IP Configuration
- Assisted Lab: Configure IPv6 Static Addressing
- Assisted Lab: Configure Static Routing
- Assisted Lab: Configure Dynamic Routing
- APPLIED Lab: Troubleshoot IP Networks
- Assisted Lab: Use Network Scanners
- Assisted Lab: Analyze a DHCP Server Configuration
- Assisted Lab: Analyze a DNS Server Configuration
- Assisted Lab: Analyze Application Security Configurations
- Assisted Lab: Configure Secure Access Channels

- Assisted Lab: Configure SNMP and Syslog Collection
- Assisted Lab: Analyze Network Performance
- APPLIED Lab: Verify Service and Application Configuration
- Assisted Lab: Configure a NAT Firewall
- Assisted Lab: Configure Remote Access
- APPLIED Lab: Troubleshoot Service and Security Issues
- Assisted Lab: Develop Network Documentation
- Assisted Lab: Backup and Restore Network Device Configurations
- Assisted Lab: Analyze an On-Path Attack
- Assisted Lab: Configure Port Security

Sever+ CertMaster Learn with Labs:

Server+ CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow. Easy-to-use course management tools provide a comprehensive suite of instructor resources alongside a reporting dashboard, making course preparation and progress tracking simple and efficient.

Topics Covered:

- Lesson 1: Understanding Server Administration Concepts
- Lesson 2: Understanding Virtualization and Cloud Computing
- Lesson 3: Understanding Physical and Network Security Concepts
- Lesson 4: Managing Physical Assets
- Lesson 5: Managing Server Hardware
- Lesson 6: Configuring Storage Management
- Lesson 7: Installing and Configuring an Operating System
- Lesson 8: Troubleshooting OS, Application, and Network Configurations

- Lesson 9: Managing Post-Installation Administrative Tasks
- Lesson 10: Managing Data Security
- Lesson 11: Managing Service and Data Availability
- Lesson 12: Decommissioning Servers

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Reporting Windows Server Specifications
- Assisted Lab: Reporting Linux Server Specifications
- Assisted Lab: Deploying a Hyper-V VM
- Assisted Lab: Deploying a Docker Container
- Assisted Lab: Auditing Network Services
- Assisted Lab: Securing Network Traffic with IPSec
- Assisted Lab: Managing System Inventories
- Assisted Lab: Monitoring Performance in Windows
- Assisted Lab: Monitoring Performance in Linux
- APPLIED LAB: Deploying and Monitoring Servers
- Assisted Lab: Managing Event Logs in Windows
- Assisted Lab: Managing Event Logs in Linux
- Assisted Lab: Configuring RAID Storage in Windows
- Assisted Lab: Provisioning iSCSI Storage
- Assisted Lab: Deploying a Linux Application Server
- Assisted Lab: Configuring Volumes in Linux
- Assisted Lab: Managing Network Configurations
- Assisted Lab: Developing Network Documentation
- Assisted Lab: Developing Administrative Bash Scripts
- Assisted Lab: Developing Administrative PowerShell Scripts
- APPLIED LAB: Managing Storage and Networks
- Assisted Lab: Troubleshooting a Network Issue
- Assisted Lab: Auditing Accounts and Permissions in Windows
- Assisted Lab: Configuring Server Roles
- Assisted Lab: Configuring Administrative Interfaces
- Assisted Lab: Managing Virtual Memory
- Assisted Lab: Configuring Group Policy Objects
- Assisted Lab: Analyzing Configuration Baselines
- APPLIED LAB A: Troubleshooting Servers Scenario #1
- APPLIED LAB B: Troubleshooting Servers Scenario #2
- APPLIED LAB C: Troubleshooting Servers Scenario #3
- Assisted Lab: Configuring EFS and BitLocker
- Assisted Lab: Troubleshooting a Security Issue

- Assisted Lab: Configuring Backup Solutions on Windows Server
- Assisted Lab: Configuring Backup Solutions on Linux
- Assisted Lab: Configuring a File Server Cluster
- Assisted Lab: Decommissioning a Domain Controller
- APPLIED LAB A: Troubleshooting Server Security Scenario #1
- APPLIED LAB B: Troubleshooting Server Security Scenario #2

TestOut Hybrid Server Pro: Core

Hybrid Server Pro: Core is a high-quality, easy-to-use curriculum where you will gain the knowledge and skills you need to configure and manage both on-premise and cloud based servers. Hosted on the online TestOut learning platform, LabSim, it provides a comprehensive experience for gaining knowledge and practical skills through interactive learning modules like video lessons and lab simulations.

LabSim is ideal for learning server technology in a self-paced engaging way. Instructional lessons are combined with instructor-led videos, demonstrations, quizzes, practice exams, and performance-based lab simulations to provide hours of content to prepare you for the ***Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure*** certification exam.

- Engaging video lessons and text lessons teach you key on-premise and cloud concepts and skills
- Section quizzes help you gauge how well you're retaining what you've learned
- Performance-based labs simulations let you apply what you've learned in real-world scenarios and provide detailed feedback reports and scores
- Exam practice for Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure certification exam includes Readiness Reports, Domain Exams, and full-length exams that emulate the real certification exam

Topics and Integrated Labs Covered

- Chapter 1: Course Introduction
- Chapter 2: On-Premises Windows Server
- Chapter 3: Cloud and Azure
- Chapter 4: Manage IP Addressing
- Chapter 5: Implement DNS
- Chapter 6: Active Directory
- Chapter 7: Active Directory Objects
- Chapter 8: Group Policy
- Chapter 9: Manage Servers and Workloads in a Hybrid Environment
- Chapter 10: Manage Storage Devices

- Chapter 11: Manage File Services
- Chapter 12: Virtualization and Containers
- Chapter 13: On-Premises and Hybrid Network Connectivity
- Appendix A: TestOut Hybrid Server Pro: Core - Practice Exams
- Appendix B: Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure - Practice Exams

License Information

- One license provides access to CertMaster Learn for Server+ (SK0-005) with CertMaster Labs integrated throughout the course, TestOut, as well as ITI custom courses and labs.
- Once activated, the license is valid for 12 months

How to Access Courses and Labs

An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Network+ and Server+ only): This bundle includes an exam voucher and an exam pass guarantee for Network+ and Server+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Linux Network Professional (Network+ / Linux+) Bundle

ITI SKU: CompTIA-14

MSRP: $2,499

Sales Price: $2,199

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Linux Network Professional (Network+ / Linux+) Bundle provides comprehensive training for individuals seeking to excel in networking and Linux system administration. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Network+ and Linux+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for Network+ and Linux+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Network+ and Linux+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Network+ N10-008: Master networking with our comprehensive CompTIA Network+ course, designed to provide the skills needed to manage and troubleshoot various network systems effectively.

Course Highlights:

- Duration: 25 hours
- Content: 110 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Network+ N10-008

Topics Areas Included:

- Networking Fundamentals
- Network Implementations
- Network Operations
- Network Security
- Network Troubleshooting

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management

- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

CompTIA Linux+ XK0-004: Gain expertise in Linux system administration with our CompTIA Linux+ course. This has not been updated for the current exam but is still highly relevant and is coupled with the official **CompTIA Linux+ XK0-005.**

Course Highlights:

- Duration: 30+ hours
- Content: 120+ On-demand Videos
- Exam Prep: 400+ Prep Questions
- Certificate of Completion for CompTIA Linux+ XK0-004

Topics Areas Included:

- Introduction to Linux
- Administering Users and Groups
- Configuring Permissions
- Implementing File Management
- Managing Software and Storage
- Configuring Network Settings
- Securing Linux Systems
- Scripting and Automation

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors

- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

Labs Included:

CompTIA Network+ (33 hours)

1. Introduction to the OSI Model
2. Networking Topologies and Characteristics
3. Internet Protocol Addressing Solutions
4. Cable and Connector Types
5. Cable Management Solutions
6. Virtual Network Concepts
7. Network Security Concept Fundamentals
8. General Network Attacks
9. Network Services and Protocols
10. Network Command Line Tools
11. Network Analysis Software
12. Configuring and Maintaining DNS Servers

13. DHCP Server Installation and Configuration
14. Remote Access and Management
15. Load Balancing and NIC Teaming
16. NTP Server Management
17. High Availability and Disaster Recovery Concepts
18. Configuring Switching Features
19. Routing Concepts and Protocols
20. Troubleshooting Common Networking Issues
21. Cloud Concepts
22. Network Architecture
23. Networking Device Monitoring
24. Network Troubleshooting Techniques
25. Networking Hardening Techniques and Best Practices
26. Physical Networking Tools
27. Defining Networking Devices
28. Troubleshooting Cable Connectivity
29. Wireless Configuration Techniques and Standards
30. Troubleshooting and Securing Wireless Networks
31. Physical Network Security Concepts
32. Organizational Documentation and Procedures
33. Organizational Networking Diagrams and Agreements

CompTIA Linux+ (63 hours)

1. Design Hard Disk Layout
2. Create Partitions and Filesystems
3. Using Various Disk Management Tools
4. Working with Kernel, Boot Modules, and Files
5. Working with Relative and Absolute Paths

6. Work with the Flow Control Constructs
7. Control Mounting and Unmounting of Filesystems
8. View the Hard Drive Details
9. Check and Repair Filesystems
10. Using RPM and YUM Package Management
11. Using Debian Package Management
12. Using Repositories
13. Managing User and Group Accounts and Related System Files
14. Run User Level Queries
15. Managing Disk Quotas
16. Working with Bash Profiles and Bash Scripts
17. Setup Host Security
18. Perform Basic File Editing Operations Using vi
19. Search Text Files using Regular Expressions
20. Using Shell Input and Output Redirections
21. Install and Configure a Web Server
22. Performing Basic File Management
23. Amending Hard and Symbolic Links
24. Find System Files and Place Files in the Correct Location
25. Use Systemctl and update-rc.d Utility to Manage Services
26. Configuring Host Names
27. Change Runlevels and Shutdown or Reboot System
28. Maintain System Time
29. Configure Client Side DNS
30. Configure System Logging
31. Mail Transfer Agent (MTA) Basics
32. Automate System Administration Tasks by Scheduling Jobs

33. Create, Monitor and Kill Processes
34. Manage Printers and Printing
35. Accessibility
36. Manage File Permissions and Ownership
37. Perform Security Administration Tasks
38. Working with Access Control List
39. Configure SELinux
40. Maintain the Integrity of Filesystems
41. Work with Pluggable Authentication Modules (PAM)
42. Secure Communication using SSH
43. Securing Data with Encryption
44. Work with TTY
45. Set up SFTP to Chroot Jail only for Specific Group
46. Secure a Linux Terminal and Implement Logging Services
47. Boot the System
48. Configure UFW and DenyHosts
49. Compress Data Using Various Tools and Utilities
50. Process Text Streams using Filters
51. Basic Network Troubleshooting
52. Use Streams Pipes and Redirects
53. Perform CPU Monitoring and Configuration
54. Perform Memory Monitoring and Configuration
55. Perform Process Monitoring
56. Modify Process Execution Priorities
57. Manage File and Directory Permissions
58. Access the Linux System
59. Configure Inheritance and Group Memberships

60. Patch the System
61. Working with the Environment Variables
62. Shells, Scripting and Data Management
63. Customize or Write Simple Scripts
64. Configure Permissions on Files and Directories
65. Work with PKI

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Network+ (N10-008) CertMaster Learn and Labs: CertMaster Learn for CompTIA Network+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Comparing OSI Model Network Functions
- Lesson 2: Deploying Ethernet Cabling
- Lesson 3: Deploying Ethernet Switching
- Lesson 4: Troubleshooting Ethernet Networks
- Lesson 5: Explaining IPv4 Addressing
- Lesson 6: Supporting IPv4 and IPv6 Networks
- Lesson 7: Configuring and Troubleshooting Routers

- Lesson 8: Explaining Network Topologies and Types
- Lesson 9: Explaining Transport Layer Protocols
- Lesson 10: Explaining Network Services
- Lesson 11: Explaining Network Applications
- Lesson 12: Ensuring Network Availability
- Lesson 13: Explaining Common Security Concepts
- Lesson 14: Supporting and Troubleshooting Secure Networks
- Lesson 15: Deploying and Troubleshooting Wireless Networks
- Lesson 16: Comparing WAN Links and Remote Access Methods
- Lesson 17: Explaining Organizational and Physical Security Concepts
- Lesson 18: Explaining Disaster Recovery and High Availability Concepts
- Lesson 19: Applying Network Hardening Techniques
- Lesson 20: Summarizing Cloud and Datacenter Architecture

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Capture Network Traffic
- Assisted Lab: Configure Interface Settings
- Assisted Lab: Configure IPv4 Static Addressing
- Assisted Lab: Analyze ARP Traffic
- Assisted Lab: Use Tools to Test IP Configuration
- Assisted Lab: Configure IPv6 Static Addressing
- Assisted Lab: Configure Static Routing
- Assisted Lab: Configure Dynamic Routing
- APPLIED Lab: Troubleshoot IP Networks
- Assisted Lab: Use Network Scanners
- Assisted Lab: Analyze a DHCP Server Configuration
- Assisted Lab: Analyze a DNS Server Configuration

- Assisted Lab: Analyze Application Security Configurations
- Assisted Lab: Configure Secure Access Channels
- Assisted Lab: Configure SNMP and Syslog Collection
- Assisted Lab: Analyze Network Performance
- APPLIED Lab: Verify Service and Application Configuration
- Assisted Lab: Configure a NAT Firewall
- Assisted Lab: Configure Remote Access
- APPLIED Lab: Troubleshoot Service and Security Issues
- Assisted Lab: Develop Network Documentation
- Assisted Lab: Backup and Restore Network Device Configurations
- Assisted Lab: Analyze an On-Path Attack
- Assisted Lab: Configure Port Security

CompTIA Linux+ (XK0-005) CertMaster Learn and Labs: CertMaster Learn for CompTIA Linux+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Introducing Linux
- Lesson 2: Administering Users and Groups
- Lesson 3: Configuring Permissions

- Lesson 4: Implementing File Management
- Lesson 5: Authoring Text Files
- Lesson 6: Managing Software
- Lesson 7: Administering Storage
- Lesson 8: Managing Devices, Processes, Memory, and the Kernel
- Lesson 9: Managing Services
- Lesson 10: Configuring Network Settings
- Lesson 11: Configuring Network Security
- Lesson 12: Managing Linux Security
- Lesson 13: Implementing Simple Scripts
- Lesson 14: Using Infrastructure as Code
- Lesson 15: Managing Containers in Linux
- Lesson 16: Installing Linux

Integrated Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Basic Linux Interaction
- Assisted Lab: Manage User Accounts
- Assisted Lab: Manage Group Accounts
- Assisted Lab: Configure and troubleshoot privilege escalation
- Assisted Lab: Configure Standard Permissions
- Assisted Lab: Configure Special Permissions
- Assisted Lab: Configure ACLs
- Assisted Lab: Troubleshoot permissions
- APPLIED LAB: Identity and Access Control
- Assisted Lab: Manage File Links
- Assisted Lab: Use File Management Commands
- Assisted Lab: Search for Files

- Assisted Lab: Edit Text Files
- Assisted Lab: Backup, Restore, and Compress Files
- Assisted Lab: Manage RPM Packages
- Assisted Lab: Manage DEB Packages
- Assisted Lab: Compile a Program
- Assisted Lab: Download Files From a Web Server
- APPLIED LAB: File and software management
- Assisted Lab: Deploy Storage and LVM
- Assisted Lab: Manage Processes
- Assisted Lab: Manage Services
- Assisted Lab: Deploy Services
- Assisted Lab: Configure Network Settings
- Assisted Lab: Configure Remote Administration
- Assisted Lab: Troubleshoot Network Configurations
- APPLIED LAB: System Management
- Assisted Lab: Configure a Firewall
- Assisted Lab: Intercept Network Traffic
- Assisted Lab: Harden a Linux System
- Assisted Lab: Verify file integrity by using hashes.
- Assisted Lab: Configure SELinux
- APPLIED LAB: Security
- Assisted Lab: Manage Scripts
- Assisted Lab: Configure a System with Ansible
- Assisted Lab: Manage Version Control with Git
- Assisted Lab: Deploy Docker Containers
- Assisted Lab: Manage GRUB2
- Assisted Lab: Deploy a Linux System

- APPLIED LAB: Scripting, Orchestration, Installation

Product and License Information:

- One license provides access to CertMaster Learn for Network+ and Linux+ with CertMaster Labs integrated throughout the courses
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses are valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Network+ and Linux+): This bundle includes an exam voucher and an exam pass guarantee for Network+ and Linux+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Network+ Bundle

ITI SKU: CompTIA-15

MSRP: $1999

Sale Price: 1499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Network+ Bundle provides comprehensive training for individuals seeking to excel in networking. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Network+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Network+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Network+ N10-008: Master networking with our comprehensive CompTIA Network+ course, designed to provide the skills needed to manage and troubleshoot various network systems effectively.

Course Highlights:

- Duration: 25 hours
- Content: 110 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Network+ N10-008

Topics Areas Included:

- Networking Fundamentals
- Network Implementations
- Network Operations
- Network Security
- Network Troubleshooting

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security

- Module 15 Network Troubleshooting

Engage in over 33+ hours of labs that reinforce the material learned and prepare you for real-world networking scenarios:

- Introduction to the OSI Model
- Networking Topologies and Characteristics
- Internet Protocol Addressing Solutions
- Cable and Connector Types
- Cable Management Solutions
- Virtual Network Concepts
- Network Security Concept Fundamentals
- General Network Attacks
- Network Services and Protocols
- Network Command Line Tools
- Network Analysis Software
- Configuring and Maintaining DNS Servers
- DHCP Server Installation and Configuration
- Remote Access and Management
- Load Balancing and NIC Teaming
- NTP Server Management
- High Availability and Disaster Recovery Concepts
- Configuring Switching Features
- Routing Concepts and Protocols
- Troubleshooting Common Networking Issues
- Cloud Concepts
- Network Architecture
- Networking Device Monitoring
- Network Troubleshooting Techniques

- Networking Hardening Techniques and Best Practices
- Physical Networking Tools
- Defining Networking Devices
- Troubleshooting Cable Connectivity
- Wireless Configuration Techniques and Standards
- Troubleshooting and Securing Wireless Networks
- Physical Network Security Concepts
- Organizational Documentation and Procedures
- Organizational Networking Diagrams and Agreements

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Network+ (N10-008) CertMaster Learn and Labs: CertMaster Learn for CompTIA Network+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Comparing OSI Model Network Functions
- Lesson 2: Deploying Ethernet Cabling
- Lesson 3: Deploying Ethernet Switching
- Lesson 4: Troubleshooting Ethernet Networks

- Lesson 5: Explaining IPv4 Addressing
- Lesson 6: Supporting IPv4 and IPv6 Networks
- Lesson 7: Configuring and Troubleshooting Routers
- Lesson 8: Explaining Network Topologies and Types
- Lesson 9: Explaining Transport Layer Protocols
- Lesson 10: Explaining Network Services
- Lesson 11: Explaining Network Applications
- Lesson 12: Ensuring Network Availability
- Lesson 13: Explaining Common Security Concepts
- Lesson 14: Supporting and Troubleshooting Secure Networks
- Lesson 15: Deploying and Troubleshooting Wireless Networks
- Lesson 16: Comparing WAN Links and Remote Access Methods
- Lesson 17: Explaining Organizational and Physical Security Concepts
- Lesson 18: Explaining Disaster Recovery and High Availability Concepts
- Lesson 19: Applying Network Hardening Techniques
- Lesson 20: Summarizing Cloud and Datacenter Architecture

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Capture Network Traffic
- Assisted Lab: Configure Interface Settings
- Assisted Lab: Configure IPv4 Static Addressing
- Assisted Lab: Analyze ARP Traffic
- Assisted Lab: Use Tools to Test IP Configuration
- Assisted Lab: Configure IPv6 Static Addressing
- Assisted Lab: Configure Static Routing
- Assisted Lab: Configure Dynamic Routing

- APPLIED Lab: Troubleshoot IP Networks
- Assisted Lab: Use Network Scanners
- Assisted Lab: Analyze a DHCP Server Configuration
- Assisted Lab: Analyze a DNS Server Configuration
- Assisted Lab: Analyze Application Security Configurations
- Assisted Lab: Configure Secure Access Channels
- Assisted Lab: Configure SNMP and Syslog Collection
- Assisted Lab: Analyze Network Performance
- APPLIED Lab: Verify Service and Application Configuration
- Assisted Lab: Configure a NAT Firewall
- Assisted Lab: Configure Remote Access
- APPLIED Lab: Troubleshoot Service and Security Issues
- Assisted Lab: Develop Network Documentation
- Assisted Lab: Backup and Restore Network Device Configurations
- Assisted Lab: Analyze an On-Path Attack
- Assisted Lab: Configure Port Security

Product Information:

- One license provides access to CertMaster Learn for Network+ with CertMaster Labs integrated throughout the course and the ITI custom course and labs.
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, Learn for Network+ with CertMaster Labs integrated will be valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Network+): This bundle includes an exam voucher and an exam pass guarantee for Network+: if you don't pass the exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Secure Infrastructure Specialist (A+ / Network+ / Security+) Bundle

ITI SKU: CompTIA-16

MSRP: $2,999

Sales Price: $2,799

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Secure Infrastructure Specialist (A+ / Network+ / Security+) Bundle provides comprehensive training for individuals seeking to excel in IT infrastructure and security. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA A+, Network+, and Security+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for A+, Network+, and Security+, followed by the integrated CompTIA CertMaster Learn and Labs.

Recommended prerequisites: While there are no prerequisites for CompTIA Security+, it is recommended that students have at least two years of IT administration experience with a security focus and hold the CompTIA Network+ or similar certification.

CTI Custom Online Self-Paced ILT Description:

CompTIA A+ 220-1101 and 220-1102: Master IT operations and troubleshooting with our comprehensive CompTIA A+ course, designed to provide the skills needed to support and manage various IT systems effectively.

Course Highlights:

- Duration: 35 hours
- Content: 200 On-demand Videos
- Exam Prep: 400 Prep Questions
- Certificate of Completion for CompTIA A+ 220-1101 and 220-1102

Topics Areas Included:

- Devices, Setups, and Installs
- Displays and Multimedia Devices

- Supporting Multiple Drive Types
- Accounting for CPUs and Internal Components
- Network Theories, Operations, and Diagnostics
- Cloud and Virtualization Computing
- Laptop Features and Troubleshooting
- Syncing and Setup of Mobile Devices
- Printing
- Operating System Management, Installation, and Troubleshooting
- Network Management Tools and Security Measures

CompTIA A+ 220-1101 (Core 1) Course Content

- Module 1: Devices, Setups, and Installs
- Module 2: Displays and Multimedia Devices
- Module 3: Supporting Multiple Drive Types
- Module 4: Accounting for CPUs and Internal Components
- Module 5: All About Network Theories
- Module 6: Network Operations and Diagnostics
- Module 7: Cloud and Virtualization Computing
- Module 8: Laptop Features and Troubleshooting
- Module 9: Syncing and Setup of Mobile Devices
- Module 10: All Things Printing
- Module 11: Resources and Testing

CompTIA A+ 220-1102 (Core 2) Course Content

- Module 1: Operating System Management
- Module 2: Configuring and installing the OS
- Module 3: Tools to Troubleshoot and Maintain the OS
- Module 4: Network Management Tools
- Module 5: Sharing Resources and Wrights Management

- Module 6: Threats and Security Measures
- Module 7: Policies to Protect Data
- Module 8: Prevent Malware and Security Threats
- Module 9: Supporting and Troubleshooting Mobile Devices
- Module 10: Implementing Operational Procedures
- Module 11: Resources and Testing

Labs for Core 2 (220-1102) (32+ hours):

- Identifying different Windows Operating System Editions
- Managing a Windows device using the Command Line Interface
- Managing a Windows device using the Graphical User Interface (GUI)
- Configuring a Windows Device using the Control Panel
- Configuring and Managing a Windows Device using Settings
- Configuring Networking Settings on a Windows Device
- Install and Configure Applications on a Windows Device
- Identify different Operating Systems and functionality
- Different Operating System Installation methods
- Tools for Managing and Maintaining MAC Operating Systems
- Tools for Managing and Maintaining Linux Operating Systems
- Implementing Physical Security Measures
- Implementing Network Security Measures
- Authentication and Authorization Methods
- Wireless Security Implementation
- Malware and Social Engineering Prevention Methods
- Security Implementation on a Windows Device
- Password and Account Management on a Windows Device
- Mobile Security Solutions
- Secure Data Disposal Methods

- Securing a SOHO Network
- Securing Web Browsers on a Windows Device
- Troubleshooting Windows Operating Systems
- Troubleshooting Personal Computer Security Settings
- Malware Removal and Remediating Best Practices
- Troubleshooting Mobile Device Security Settings
- Documentation Best Practices
- Implementing Basic Change Management Best Practices
- Backup and Recovery Implementation
- Safety and Environmental Procedures
- Privacy, Licensing & Policy Concepts
- Using Proper Communication Techniques and Professionalism
- Basic Scripting Techniques
- Remote Access Methods

CompTIA Network+ N10-008: Master networking with our comprehensive CompTIA Network+ course, designed to provide the skills needed to manage and troubleshoot various network systems effectively.

Course Highlights:

- Duration: 25 hours
- Content: 110 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Network+ N10-008

Topics Areas Included:

- Networking Fundamentals
- Network Implementations
- Network Operations
- Network Security
- Network Troubleshooting

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

Labs included (33 hours):

- Introduction to the OSI Model
- Networking Topologies and Characteristics
- Internet Protocol Addressing Solutions
- Cable and Connector Types
- Cable Management Solutions
- Virtual Network Concepts
- Network Security Concept Fundamentals
- General Network Attacks
- Network Services and Protocols

- Network Command Line Tools
- Network Analysis Software
- Configuring and Maintaining DNS Servers
- DHCP Server Installation and Configuration
- Remote Access and Management
- Load Balancing and NIC Teaming
- NTP Server Management
- High Availability and Disaster Recovery Concepts
- Configuring Switching Features
- Routing Concepts and Protocols
- Troubleshooting Common Networking Issues
- Cloud Concepts
- Network Architecture
- Networking Device Monitoring
- Network Troubleshooting Techniques
- Networking Hardening Techniques and Best Practices
- Physical Networking Tools
- Defining Networking Devices
- Troubleshooting Cable Connectivity
- Wireless Configuration Techniques and Standards
- Troubleshooting and Securing Wireless Networks
- Physical Network Security Concepts
- Organizational Documentation and Procedures
- Organizational Networking Diagrams and Agreements

CompTIA Security+ SY0-701: Develop critical security skills with our CompTIA Security+ course, designed to provide the knowledge needed to secure and protect networks and systems.

Course Highlights:

- Duration: 30+ hours
- Content: 110+ On-demand Videos
- Exam Prep: 290+ Prep Questions
- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules:

- Module 1: General Security Concepts
- Module 2: Threats, Vulnerabilities, and Mitigations
- Module 3: Security Architecture
- Module 4: Security Operations
- Module 5: Security Program Management and Oversight

Labs Included (17 hours):

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Mitigation Techniques
7. Security Architecture Models
8. Securing Enterprise Infrastructures
9. Data Protection Strategies
10. Resilience in Security Architecture
11. Securing Computing Resources
12. Asset Management Techniques
13. Vulnerability Management
14. Monitoring Computing Resources
15. Enhancing Enterprise Security
16. Implement Identity & Access Management
17. Implementation of Automation & Orchestration for Security Operations
18. Investigative Data Sources

CompTIA A+ (220-1101 and 220-1102) CertMaster Learn and Labs: CertMaster Learn for CompTIA A+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks

- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Installing Motherboards and Connectors
- Lesson 2: Installing System Devices
- Lesson 3: Troubleshooting PC Hardware
- Lesson 4: Comparing Local Networking Hardware
- Lesson 5: Configuring Network Addressing and Internet Connections
- Lesson 6: Supporting Network Services
- Lesson 7: Summarizing Virtualization and Cloud Concepts
- Lesson 8: Supporting Mobile Devices
- Lesson 9: Supporting Print Devices
- Lesson 10: Configuring Windows
- Lesson 11: Managing Windows
- Lesson 12: Identifying OS Types and Features
- Lesson 13: Supporting Windows
- Lesson 14: Managing Windows Networking
- Lesson 15: Managing Linux and macOS
- Lesson 16: Configuring SOHO Network Security
- Lesson 17: Managing Security Settings
- Lesson 18: Supporting Mobile Software
- Lesson 19: Using Support and Scripting Tools
- Lesson 20: Implementing Operational Procedures

Labs Available:

- Assisted Lab: Exploring the Lab Environment

- Assisted Lab: Installing a Motherboard
- Assisted Lab: Installing Power Supplies
- Assisted Lab: Installing and Configuring System Memory
- Assisted Lab: Installing RAM
- Assisted Lab: Installing CPU and Cooler
- Assisted Lab: Upgrading and Installing GPU and Daisy-Chain Monitors
- Assisted Lab: Exploring the Virtual Machine Lab Environment
- Assisted Lab: Compare Networking Hardware
- Assisted Lab: Compare Wireless Network Technologies
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Compare Protocols and Ports
- Assisted Lab: Troubleshoot a Network #1
- Assisted Lab: Troubleshoot a Network #2
- APPLIED Lab: Troubleshoot a Network #1
- APPLIED Lab: Troubleshoot a Network #2
- Assisted Lab: Adding Expansion SSD in a Laptop
- Assisted Lab: Upgrading Laptop RAM
- Assisted Lab: Replacing Laptop Non-User Removable Battery
- Assisted Lab: Configuring Laptop Dock and External Peripherals
- Assisted Lab: Deploy a Printer
- Assisted Lab: Manage User Settings in Windows
- Assisted Lab: Support Windows 11
- Assisted Lab: Configure Windows System Settings
- Assisted Lab: Use Management Consoles
- Assisted Lab: Use Task Manager
- Assisted Lab: Monitor Performance and Event Logs
- Assisted Lab: Use Command-line Tools

- APPLIED Lab: Support Windows 10
- Assisted Lab: Perform Windows 10 OS Installation
- Assisted Lab: Perform Ubuntu Linux OS Installation
- Assisted Lab: Install and Configure an Application
- Assisted Lab: Troubleshoot a Windows OS Issue
- Assisted Lab: Configure Windows Networking
- Assisted Lab: Configure Folder Sharing in a Workgroup
- Assisted Lab: Manage Linux using Command-line Tools
- Assisted Lab: Manage Files using Linux Command-line Tools
- APPLIED Lab: Support and Troubleshoot Network Hosts
- Assisted Lab: Configure SOHO Router Security
- Assisted Lab: Configure Workstation Security
- Assisted Lab: Configure Browser Security
- Assisted Lab: Troubleshoot Security Issues Scenario #1
- APPLIED Lab: Troubleshoot Security Issues Scenario #2
- Assisted Lab: Use Remote Access Technologies
- Assisted Lab: Implement Backup and Recovery
- Assisted Lab: Implement a PowerShell Script
- Assisted Lab: Implement Bash Script
- Assisted Lab: Manage a Support Ticket
- Assisted Lab: Support Active Directory Domain Networking

CompTIA Network+ (N10-008) CertMaster Learn and Labs: CertMaster Learn for CompTIA Network+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge

- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Comparing OSI Model Network Functions
- Lesson 2: Deploying Ethernet Cabling
- Lesson 3: Deploying Ethernet Switching
- Lesson 4: Troubleshooting Ethernet Networks
- Lesson 5: Explaining IPv4 Addressing
- Lesson 6: Supporting IPv4 and IPv6 Networks
- Lesson 7: Configuring and Troubleshooting Routers
- Lesson 8: Explaining Network Topologies and Types
- Lesson 9: Explaining Transport Layer Protocols
- Lesson 10: Explaining Network Services
- Lesson 11: Explaining Network Applications
- Lesson 12: Ensuring Network Availability
- Lesson 13: Explaining Common Security Concepts
- Lesson 14: Supporting and Troubleshooting Secure Networks
- Lesson 15: Deploying and Troubleshooting Wireless Networks
- Lesson 16: Comparing WAN Links and Remote Access Methods
- Lesson 17: Explaining Organizational and Physical Security Concepts
- Lesson 18: Explaining Disaster Recovery and High Availability Concepts
- Lesson 19: Applying Network Hardening Techniques
- Lesson 20: Summarizing Cloud and Datacenter Architecture

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Capture Network Traffic
- Assisted Lab: Configure Interface Settings
- Assisted Lab: Configure IPv4 Static Addressing
- Assisted Lab: Analyze ARP Traffic
- Assisted Lab: Use Tools to Test IP Configuration
- Assisted Lab: Configure IPv6 Static Addressing
- Assisted Lab: Configure Static Routing
- Assisted Lab: Configure Dynamic Routing
- APPLIED Lab: Troubleshoot IP Networks
- Assisted Lab: Use Network Scanners
- Assisted Lab: Analyze a DHCP Server Configuration
- Assisted Lab: Analyze a DNS Server Configuration
- Assisted Lab: Analyze Application Security Configurations
- Assisted Lab: Configure Secure Access Channels
- Assisted Lab: Configure SNMP and Syslog Collection
- Assisted Lab: Analyze Network Performance
- APPLIED Lab: Verify Service and Application Configuration
- Assisted Lab: Configure a NAT Firewall
- Assisted Lab: Configure Remote Access
- APPLIED Lab: Troubleshoot Service and Security Issues
- Assisted Lab: Develop Network Documentation
- Assisted Lab: Backup and Restore Network Device Configurations
- Assisted Lab: Analyze an On-Path Attack
- Assisted Lab: Configure Port Security

CompTIA Security+ (SY0-701) CertMaster Learn and Labs:

CertMaster Learn for CompTIA Security+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Summarize Fundamental Security Concepts
- Lesson 2: Compare Threat Types
- Lesson 3: Explain Cryptographic Solutions
- Lesson 4: Implement Identity and Access Management
- Lesson 5: Secure Enterprise Network Architecture
- Lesson 6: Secure Cloud Network Architecture
- Lesson 7: Explain Resiliency and Site Security Concepts
- Lesson 8: Explain Vulnerability Management
- Lesson 9: Evaluate Network Security Capabilities
- Lesson 10: Assess Endpoint Security Capabilities
- Lesson 11: Enhance Application Security Capabilities
- Lesson 12: Explain Incident Response and Monitoring Concepts
- Lesson 13: Analyze Indicators of Malicious Activity

- Lesson 14: Summarize Security Governance Concepts
- Lesson 15: Explain Risk Management Processes
- Lesson 16: Summarize Data Protection and Compliance Concepts

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Perform System Configuration Gap Analysis
- Assisted Lab: Configuring Examples of Security Control Types
- Assisted Lab: Finding Open Service Ports
- Assisted Lab: Using SET to Perform Social Engineering
- Applied Lab: Using Storage Encryption
- Assisted Lab: Using Hashing and Salting
- Assisted Lab: Managing Password Security
- Assisted Lab: Managing Permissions
- Assisted Lab: Setting up Remote Access
- Assisted Lab: Using TLS Tunneling
- Assisted Lab: Using Containers
- Assisted Lab: Using Virtualization
- Assisted Lab: Implement Backups
- Assisted Lab: Performing Drive Sanitization
- Assisted Lab: Exploiting and Detecting SQLi
- Assisted Lab: Working with Threat Feeds
- Assisted Lab: Performing Vulnerability Scans
- Assisted Lab: Understanding Security Baselines
- Applied Lab: Implementing a Firewall
- Assisted Lab: Using Group Policy
- Applied Lab: Hardening
- Assisted Lab: Performing DNS Filtering

- Assisted Lab: Configuring System Monitoring
- Applied Lab: Incident Response: Detection
- Applied Lab: Performing Digital Forensics
- Assisted Lab: Performing Root Cause Analysis
- Assisted Lab: Detecting and Responding to Malware
- Assisted Lab: Understanding On-Path Attacks
- Adaptive Lab: Using a Playbook
- Assisted Lab: Implementing Allow Lists and Deny Lists
- Assisted Lab: Performing Reconnaissance
- Assisted Lab: Performing Penetration Testing
- Assisted Lab: Training and Awareness through Simulation
- Capstone Lab: Discovering Anomalous Behavior
- Assisted Lab: Use Cases of Automation and Scripting
- Applied Lab: Using Network Sniffers

Product Information:

- One license provides access to CertMaster Learn for A+, Network+, and Security+ with CertMaster Labs integrated throughout the courses and ITI courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (A+, Network+, and Security+): This bundle includes an exam voucher and an exam pass guarantee for A+, Network+, and Security+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Secure Cloud Professional (Security+ / Cloud+) Bundle

ITI SKU: CompTIA-17

MSRP: $2499

Sales Price: $2199

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Secure Cloud Professional (Security+ / Cloud+) Bundle provides comprehensive training for individuals seeking to excel in cloud security and administration. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Security+ and Cloud+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Security+ and Cloud+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Security+ SY0-701: Develop critical security skills with our CompTIA Security+ course, designed to provide the knowledge needed to secure and protect networks and systems.

Course Highlights:

- Duration: 30+ hours
- Content: 110+ On-demand Videos
- Exam Prep: 300 Prep Questions
- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security

- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules:

- Module 1: General Security Concepts
- Module 2: Threats, Vulnerabilities, and Mitigations
- Module 3: Security Architecture
- Module 4: Security Operations
- Module 5: Security Program Management and Oversight

Labs included (17 hours):

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Mitigation Techniques
7. Security Architecture Models
8. Securing Enterprise Infrastructures
9. Data Protection Strategies
10. Resilience in Security Architecture
11. Securing Computing Resources

12. Asset Management Techniques
13. Vulnerability Management
14. Monitoring Computing Resources
15. Enhancing Enterprise Security
16. Implement Identity & Access Management
17. Implementation of Automation & Orchestration for Security Operations
18. Investigative Data Sources

CompTIA Cloud+ CV0-003: Master cloud infrastructure and services with our CompTIA Cloud+ course, covering essential cloud computing skills.

Course Highlights:

- Duration: 8+ hours
- Content: 130+ On-demand Videos
- Exam Prep: 45+ Prep Questions
- Certificate of Completion for CompTIA Cloud+ CV0-003

Topics Areas Included:

- Cloud Architecture and Design
- Cloud Security
- Cloud Deployment
- Operations and Support
- Troubleshooting

Modules:

- Module 1: CompTIA Cloud+ CV0-003 Course Overview
- Module 2: General Cloud Knowledge
- Module 3: Cloud Security
- Module 4: Cloud Deployment
- Module 5: Operations and Support
- Module 6: Troubleshooting
- Module 7: Course Closeout

Labs included (28 hours):

1. Cloud Deployment Models
2. Different Cloud Service Models
3. Cloud Resource Capacity Planning
4. High Availability and Scalability in the Cloud
5. Analyzing Business Requirements for a Cloud Solution
6. Configuring and Managing Cloud Identities
7. Cloud Networking Concepts
8. Securing Cloud Infrastructure Resources
9. Data Security and Compliance in the Cloud
10. Cloud Security Assessments and Tools
11. Incident Response Procedures
12. Cloud Solution Integration
13. Provisioning Cloud Resources
14. Provisioning Public Cloud Storage Solutions
15. Provisioning Private Cloud Storage Solutions
16. Deploying Cloud Networking Solutions
17. Virtualization Concepts and Platforms
18. Cloud Migration Techniques
19. Configuring Logging for Cloud Resources
20. Implementing Cloud Resource Monitoring Solutions
21. Implementing Cloud Resource Monitoring and Alert Solutions
22. Cloud Dashboards and Reporting
23. Cloud Patches, Upgrading and Lifecycle Management
24. Optimizing Cloud Solutions
25. Implementing Cloud Resource Automation Solutions
26. Implementing Cloud Backup and Restore Solutions

27. Cloud Disaster Recovery Concepts
28. Cloud Troubleshooting Methodologies
29. Security Troubleshooting Techniques
30. Troubleshooting Cloud Deployments
31. Cloud Networking Troubleshooting Concepts
32. Troubleshooting Cloud Resource Utilization
33. Automation and Orchestration Troubleshooting Methodologies

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Security+ (SY0-701) CertMaster Learn and Labs: CertMaster Learn is a self-paced, comprehensive online learning experience that helps you gain the knowledge and practical skills necessary to be successful on your CompTIA certification exam, and in your IT career. A Learning Plan helps you stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for you to practice and apply your skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on inputs.

When purchased with CertMaster Learn in a bundle, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Comparing Security Roles and Security Controls

- Explaining Threat Actors and Threat Intelligence
- Performing Security Assessments
- Identifying Social Engineering and Malware
- Summarizing Basic Cryptographic Concepts
- Implementing Public Key Infrastructure
- Implementing Authentication Controls
- Implementing Identity and Account Management Controls
- Implementing Secure Network Designs
- Implementing Network Security Appliances
- Implementing Secure Network Protocols
- Implementing Host Security Solutions
- Implementing Secure Mobile Solutions
- Summarizing Secure Application Concepts
- Implementing Secure Cloud Solutions
- Explaining Data Privacy and Protection Concepts
- Performing Incident Response
- Explaining Digital Forensics
- Summarizing Risk Management Concepts
- Implementing Cybersecurity Resilience
- Explaining Physical Security

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Scanning and Identifying Network Nodes
- Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
- Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- APPLIED LAB: Performing Network Reconnaissance and Vulnerability Scanning

- Assisted Lab: Managing the Lifecycle of a Certificate
- Assisted Lab: Managing Certificates with OpenSSL
- Assisted Lab: Auditing Passwords with a Password Cracking Utility
- Assisted Lab: Managing Centralized Authentication
- Assisted Lab: Managing Access Controls in Windows Server
- Assisted Lab: Configuring a System for Auditing Policies
- Assisted Lab: Managing Access Controls in Linux
- APPLIED LAB: Configuring Identity and Access Management Controls
- Assisted Lab: Implementing a Secure Network Design
- Assisted Lab: Configuring a Firewall
- Assisted Lab: Configuring an Intrusion Detection System
- Assisted Lab: Implementing Secure Network Addressing Services
- Assisted Lab: Implementing a Virtual Private Network
- Assisted Lab: Implementing a Secure SSH Server
- Assisted Lab: Implementing Endpoint Protection
- APPLIED LAB: Securing the Network Infrastructure
- Assisted Lab: Identifying Application Attack Indicators
- Assisted Lab: Identifying a Browser Attack
- Assisted Lab: Implementing PowerShell Security
- Assisted Lab: Identifying Malicious Code
- APPLIED LAB: Identifying Application Attacks
- Assisted Lab: Managing Data Sources for Incident Response
- Assisted Lab: Configuring Mitigation Controls
- Assisted Lab: Acquiring Digital Forensics Evidence
- Assisted Lab: Backing Up and Restoring Data in Windows and Linux
- APPLIED LAB: Managing Incident Response, Mitigation and Recovery

CompTIA Cloud+ (CV0-003) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and

practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow. Easy-to-use course management tools provide a comprehensive suite of instructor resources alongside a reporting dashboard, making course preparation and progress tracking simple and efficient.

Topics Covered:

- Understanding Cloud Concepts
- Planning and Designing a Cloud Environment
- Administering Cloud Resources
- Managing Cloud Storage
- Managing Networks in the Cloud
- Securing and Troubleshooting Networks in the Cloud
- Managing Cloud Migrations and Troubleshooting Cloud Deployments
- Managing Cloud Automation and Orchestration
- Understanding Cloud Security Concepts
- Managing Cloud Security
- Managing Cloud Performance
- Managing Maintenance in the Cloud
- Implementing High Availability and Disaster Recovery in the Cloud

Labs Available:

- Assisted Lab: Explore the Lab Environment
- Assisted Lab: Plan and Design a Cloud Environment
- Assisted Lab: Deploy and Manage Cloud Resources

- Assisted Lab: Manage Compute Resources
- Assisted Lab: Manage Networks in the Cloud
- Assisted Lab: Secure Cloud Components
- APPLIED LAB: Deploy Cloud Resources
- Assisted Lab: Manage Cloud Automation
- Assisted Lab: Manage Baseline Configurations
- Assisted Lab: Deploy Patches
- Assisted Lab: Configure Monitoring
- Assisted Lab: Manage Backup and Restore Processes
- APPLIED LAB: Manage Cloud Resources

Product and License Information:

- One license provides access to CertMaster Learn for Security+ and Cloud+ with CertMaster Labs integrated throughout the courses and ITI courses and labs.
- Access keys must be redeemed within 12 months of purchase.
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Security+ and Cloud+): This bundle includes an exam voucher and an exam pass guarantee for Security+ and Cloud+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Security Analytics Professional (Security+ / CySA+) Bundle

ITI SKU: CompTIA-18

MSRP: $2499

Sales Price: $2199

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Security Analytics Professional (Security+ / CySA+) Bundle provides comprehensive training for individuals seeking to excel in

security analytics. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Security+ and CySA+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Security+ and CySA+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Security+ SY0-701: Develop critical security skills with our CompTIA Security+ course, designed to provide the knowledge needed to secure and protect networks and systems.

Course Highlights:

- Duration: 35 hours
- Content: 130 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring

- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules:

- Module 1: General Security Concepts
- Module 2: Threats, Vulnerabilities, and Mitigations
- Module 3: Security Architecture
- Module 4: Security Operations
- Module 5: Security Program Management and Oversight

Labs Included (17 hours):

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Mitigation Techniques
7. Security Architecture Models
8. Securing Enterprise Infrastructures
9. Data Protection Strategies
10. Resilience in Security Architecture
11. Securing Computing Resources
12. Asset Management Techniques
13. Vulnerability Management
14. Monitoring Computing Resources
15. Enhancing Enterprise Security
16. Implement Identity & Access Management

17. Implementation of Automation & Orchestration for Security Operations
18. Investigative Data Sources

CompTIA CySA+ CS0-003: Gain expertise in cybersecurity analytics with our CompTIA CySA+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 6+ hours
- Content: 80+ On-demand Videos
- Exam Prep: 100Prep Questions
- Certificate of Completion for CompTIA CySA+ CS0-003

Topics Areas Included:

- Threat and Vulnerability Management
- Software and Systems Security
- Security Operations and Monitoring
- Incident Response
- Compliance and Assessment

Modules:

- Module 1 - CompTIA CySA+ CS0-003 Basics
- Module 2 - CompTIA CySA+ CS0-003 Domain 1 - Security Operations
- Module 3 - CompTIA CySA+ CS0-003 Domain 2 - Vulnerability Management
- Module 4 - CompTIA CySA+ CS0-003 Domain 3 - Incident Response and Management
- Module 5 - CompTIA CySA+ CS0-003 Domain 4 - Reporting and Communication
- Module 6 - CompTIA CySA+ CS0-003 - Course Closeout

Labs Included (12 hours):

- System & Network Security Implementation Concepts
- Threat Intelligence & Threat Gathering Concepts
- Techniques to Determine Malicious Activity
- Vulnerability Scanning Tools & Techniques

- Identifying & Analyzing Malicious Activity
- Tools for Identifying Malicious Activity
- Attack Methodology Frameworks
- Vulnerability Data Analysis and Prioritization
- Incident Response Management Techniques
- Incident Response Communication & Reporting
- Vulnerability Reporting Concepts
- Vulnerability Patching & Attack Surface Management

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Security+ (SY0-701) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam

- The Learning Plan keeps you on track with your studies

Topics Covered:

- Comparing Security Roles and Security Controls
- Explaining Threat Actors and Threat Intelligence
- Performing Security Assessments
- Identifying Social Engineering and Malware
- Summarizing Basic Cryptographic Concepts
- Implementing Public Key Infrastructure
- Implementing Authentication Controls
- Implementing Identity and Account Management Controls
- Implementing Secure Network Designs
- Implementing Network Security Appliances
- Implementing Secure Network Protocols
- Implementing Host Security Solutions
- Implementing Secure Mobile Solutions
- Summarizing Secure Application Concepts
- Implementing Secure Cloud Solutions
- Explaining Data Privacy and Protection Concepts
- Performing Incident Response
- Explaining Digital Forensics
- Summarizing Risk Management Concepts
- Implementing Cybersecurity Resilience
- Explaining Physical Security

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Scanning and Identifying Network Nodes
- Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools

- Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
- Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- APPLIED LAB: Performing Network Reconnaissance and Vulnerability Scanning
- Assisted Lab: Managing the Lifecycle of a Certificate
- Assisted Lab: Managing Certificates with OpenSSL
- Assisted Lab: Auditing Passwords with a Password Cracking Utility
- Assisted Lab: Managing Centralized Authentication
- Assisted Lab: Managing Access Controls in Windows Server
- Assisted Lab: Configuring a System for Auditing Policies
- Assisted Lab: Managing Access Controls in Linux
- APPLIED LAB: Configuring Identity and Access Management Controls
- Assisted Lab: Implementing a Secure Network Design
- Assisted Lab: Configuring a Firewall
- Assisted Lab: Configuring an Intrusion Detection System
- Assisted Lab: Implementing Secure Network Addressing Services
- Assisted Lab: Implementing a Virtual Private Network
- Assisted Lab: Implementing a Secure SSH Server
- Assisted Lab: Implementing Endpoint Protection
- APPLIED LAB: Securing the Network Infrastructure
- Assisted Lab: Identifying Application Attack Indicators
- Assisted Lab: Identifying a Browser Attack
- Assisted Lab: Implementing PowerShell Security
- Assisted Lab: Identifying Malicious Code
- APPLIED LAB: Identifying Application Attacks
- Assisted Lab: Managing Data Sources for Incident Response
- Assisted Lab: Configuring Mitigation Controls
- Assisted Lab: Acquiring Digital Forensics Evidence

- Assisted Lab: Backing Up and Restoring Data in Windows and Linux
- APPLIED LAB: Managing Incident Response, Mitigation and Recovery

CompTIA CySA+ (CS0-003) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Understanding Vulnerability Response, Handling, and Management
- Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts
- Lesson 3: Explaining Important System and Network Architecture Concepts
- Lesson 4: Understanding Process Improvement in Security Operations
- Lesson 5: Implementing Vulnerability Scanning Methods

- Lesson 6: Performing Vulnerability Analysis
- Lesson 7: Communicating Vulnerability Information
- Lesson 8: Explaining Incident Response Activities
- Lesson 9: Demonstrating Incident Response Communication
- Lesson 10: Applying Tools to Identify Malicious Activity
- Lesson 11: Analyzing Potentially Malicious Activity
- Lesson 12: Understanding Application Vulnerability Assessment
- Lesson 13: Exploring Scripting Tools and Analysis Concepts
- Lesson 14: Understanding Application Security and Attack Mitigation Best Practices

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configuring Controls
- Assisted Lab: Reviewing IoC and Threat Intelligence Sources
- Assisted Lab: Performing Threat Hunting
- Assisted Lab: Configuring Centralized Logging
- APPLIED LAB: Performing System Hardening
- Assisted Lab: Assess Time Synch Errors
- Assisted Lab: Configuring Automation
- Assisted Lab: Performing Asset Discovery
- Assisted Lab: Performing Vulnerability Scanning
- Assisted Lab: Performing Passive Scanning
- Assisted Lab: Establishing Context Awareness
- Assisted Lab: Analyzing Vulnerability Reports
- Assisted Lab: Detecting Legacy Systems
- APPLIED LAB: Performing Post-Incident Forensic Analysis
- APPLIED LAB: Performing IoC Detection and Analysis
- ADAPTIVE LAB: Performing Playbook Incident Response

- APPLIED LAB: Collecting Forensic Evidence
- Assisted Lab: Performing Root Cause Analysis
- APPLIED LAB: Using Network Sniffers
- APPLIED LAB: Researching DNS and IP Reputation
- Assisted Lab: Using File Analysis Techniques
- Assisted Lab: Analyzing Potentially Malicious Files
- Assisted Lab: Using Nontraditional Vulnerability Scanning Tools
- APPLIED LAB: Performing Web Vulnerability Scanning
- Assisted Lab: Exploiting Weak Cryptography
- Assisted Lab: Performing and Detecting Directory Traversal and Command Injection
- Assisted Lab: Performing and Detecting Privilege Escalation
- Assisted Lab: Performing and Detecting XSS
- Assisted Lab: Performing and Detecting LFI/RFI
- Assisted Lab: Performing and Detecting SQLi
- Assisted Lab: Performing and Detecting CSRF
- APPLIED LAB: Detecting and Exploiting Security Misconfiguration

Product and License Information:

- One license provides access to CertMaster Learn for Security+ and CySA+ with CertMaster Labs integrated throughout the courses
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, Learn for Security+ and CySA+ with CertMaster Labs integrated will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Security+ and CySA+): This bundle includes an exam voucher and an exam pass guarantee for Security+ and CySA+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the

exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+) Bundle

ITI SKU: CompTIA-19

MSRP: $2499

Sales Price: $2199

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+) Bundle provides comprehensive training for individuals seeking to excel in network vulnerability assessment. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Security+ and PenTest+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Security+ and PenTest+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Security+ SY0-701: Develop critical security skills with our CompTIA Security+ course, designed to provide the knowledge needed to secure and protect networks and systems.

Course Highlights:

- Duration: 35 hours
- Content: 130 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison

- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules:

- Module 1: General Security Concepts
- Module 2: Threats, Vulnerabilities, and Mitigations
- Module 3: Security Architecture
- Module 4: Security Operations
- Module 5: Security Program Management and Oversight

Labs Included (17 hours):

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Mitigation Techniques
7. Security Architecture Models

8. Securing Enterprise Infrastructures
9. Data Protection Strategies
10. Resilience in Security Architecture
11. Securing Computing Resources
12. Asset Management Techniques
13. Vulnerability Management
14. Monitoring Computing Resources
15. Enhancing Enterprise Security
16. Implement Identity & Access Management
17. Implementation of Automation & Orchestration for Security Operations
18. Investigative Data Sources

CompTIA PenTest+: Gain expertise in penetration testing and vulnerability management with our CompTIA PenTest+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 34+ hours
- Content: 200+ On-demand Videos
- Exam Prep: 240+ Prep Questions
- Certificate of Completion for CompTIA PenTest+

Topics Areas Included:

- Penetration Test Engagement
- Passive Reconnaissance:
- Active Reconnaissance
- Physical Security
- Social Engineering
- Vulnerability Scan Analysis
- Password Cracking
- Network Penetration Testing

- Exploitation of Windows and Linux Systems
- Web Application Testing

Modules:

- Module 1 - The Pen Test Engagement
- Module 2 - Passive Reconnaissance
- Module 3 - Active Reconnaissance
- Module 4 - Physical Security
- Module 5 - Social Engineering
- Module 6 - Vulnerability Scan Analysis
- Module 7 - Password Cracking
- Module 8 - Penetrating Wired Networks
- Module 9 - Penetrating Wireless Networks
- Module 10 - Windows Exploits
- Module 11 - Linux Exploits
- Module 12 - Mobile Devices
- Module 13 - Specialized Systems
- Module 14 - Scripts
- Module 15 - Application Testing
- Module 16 - Web App Exploits
- Module 17 - Lateral Movement
- Module 18 - Persistence
- Module 19 - Cover Your Tracks
- Module 20 - The Report
- Module 21 - Post Engagement Cleanup

Labs included (15 hours):

- Planning and Preparing for a Penetration Test Engagement
- Using the Metasploit Framework

- Performing Social Engineering
- Conducting Passive Reconnaissance for Vulnerabilities in a Network
- Conducting Active Reconnaissance for Vulnerabilities in a Network
- Perform Vulnerability Scan and Analyze Vulnerability Scan Results
- Exploiting the Network Vulnerabilities
- Exploiting Desktop Systems Vulnerabilities
- Exploit Web Application Vulnerabilities
- Performing Password Attacks
- Exploiting Discovered Vulnerabilities
- Work with Various Tools
- Performing Physical Security
- Working with Scripts
- Complete Post Exploit Tasks
- Analyzing and Reporting the Pen Test Results

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Security+ (SY0-701) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos

- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Comparing Security Roles and Security Controls
- Explaining Threat Actors and Threat Intelligence
- Performing Security Assessments
- Identifying Social Engineering and Malware
- Summarizing Basic Cryptographic Concepts
- Implementing Public Key Infrastructure
- Implementing Authentication Controls
- Implementing Identity and Account Management Controls
- Implementing Secure Network Designs
- Implementing Network Security Appliances
- Implementing Secure Network Protocols
- Implementing Host Security Solutions
- Implementing Secure Mobile Solutions
- Summarizing Secure Application Concepts
- Implementing Secure Cloud Solutions
- Explaining Data Privacy and Protection Concepts
- Performing Incident Response
- Explaining Digital Forensics
- Summarizing Risk Management Concepts

- Implementing Cybersecurity Resilience
- Explaining Physical Security

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Scanning and Identifying Network Nodes
- Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
- Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- APPLIED LAB: Performing Network Reconnaissance and Vulnerability Scanning
- Assisted Lab: Managing the Lifecycle of a Certificate
- Assisted Lab: Managing Certificates with OpenSSL
- Assisted Lab: Auditing Passwords with a Password Cracking Utility
- Assisted Lab: Managing Centralized Authentication
- Assisted Lab: Managing Access Controls in Windows Server
- Assisted Lab: Configuring a System for Auditing Policies
- Assisted Lab: Managing Access Controls in Linux
- APPLIED LAB: Configuring Identity and Access Management Controls
- Assisted Lab: Implementing a Secure Network Design
- Assisted Lab: Configuring a Firewall
- Assisted Lab: Configuring an Intrusion Detection System
- Assisted Lab: Implementing Secure Network Addressing Services
- Assisted Lab: Implementing a Virtual Private Network
- Assisted Lab: Implementing a Secure SSH Server
- Assisted Lab: Implementing Endpoint Protection
- APPLIED LAB: Securing the Network Infrastructure
- Assisted Lab: Identifying Application Attack Indicators
- Assisted Lab: Identifying a Browser Attack

- Assisted Lab: Implementing PowerShell Security
- Assisted Lab: Identifying Malicious Code
- APPLIED LAB: Identifying Application Attacks
- Assisted Lab: Managing Data Sources for Incident Response
- Assisted Lab: Configuring Mitigation Controls
- Assisted Lab: Acquiring Digital Forensics Evidence
- Assisted Lab: Backing Up and Restoring Data in Windows and Linux
- APPLIED LAB: Managing Incident Response, Mitigation and Recovery

CompTIA PenTest+ (PT0-002) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Scoping Organization/Customer Requirements
- Lesson 2: Defining the Rules of Engagement
- Lesson 3: Footprinting and Gathering Intelligence
- Lesson 4: Evaluating Human and Physical Vulnerabilities
- Lesson 5: Preparing the Vulnerability Scan
- Lesson 6: Scanning Logical Vulnerabilities
- Lesson 7: Analyzing Scanning Results
- Lesson 8: Avoiding Detection and Covering Tracks
- Lesson 9: Exploiting the LAN and Cloud
- Lesson 10: Testing Wireless Networks
- Lesson 11: Targeting Mobile Devices
- Lesson 12: Attacking Specialized Systems
- Lesson 13: Web Application-Based Attacks
- Lesson 14: Performing System Hacking
- Lesson 15: Scripting and Software Development
- Lesson 16: Leveraging the Attack: Pivot and Penetrate
- Lesson 17: Communicating During the PenTesting Process
- Lesson 18: Summarizing Report Components
- Lesson 19: Recommending Remediation
- Lesson 20: Performing Post-Report Delivery Activities

Labs Available:

- Assisted Lab: Gathering Intelligence
- Assisted Lab: Performing Social Engineering using SET
- Assisted Lab: Discovering Information using Nmap
- Assisted Lab: Performing Vulnerability Scans and Analysis
- Assisted Lab: Penetrating an Internal Network

- Assisted Lab: Exploiting Web Authentication
- Assisted Lab: Exploiting Weaknesses in a Website
- Assisted Lab: Exploiting Weaknesses in a Database
- Assisted Lab: Using SQL Injection
- Assisted Lab: Performing an AitM Attack
- Assisted Lab: Performing Password Attacks
- Assisted Lab: Using Reverse and Bind Shells
- Assisted Lab: Performing Post-Exploitation Activities
- Assisted Lab: Establishing Persistence
- Assisted Lab: Performing Lateral Movement

Product and License Information:

- One license provides access to CertMaster Learn for Security+ and PenTest+ with CertMaster Labs integrated throughout the courses
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, Learn for Security+ and PenTest+ with CertMaster Labs integrated will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Security+ and PenTest+): This bundle includes an exam voucher and an exam pass guarantee for Security+ and PenTest+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Network Security Professional (Security+ / PenTest+ / CySA+) Bundle

ITI SKU: CompTIA-20

MSRP: $2999

Sales Price: $2799

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Network Security Professional (Security+ / PenTest+ / CySA+) Bundle provides comprehensive training for individuals seeking to excel in network security. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Security+, PenTest+, and CySA+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Security+, PenTest+, and CySA+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Security+ SY0-701: Develop critical security skills with our CompTIA Security+ course, designed to provide the knowledge needed to secure and protect networks and systems.

Course Highlights:

- Duration: 35 hours
- Content: 130 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities

- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules:

- Module 1: General Security Concepts
- Module 2: Threats, Vulnerabilities, and Mitigations
- Module 3: Security Architecture
- Module 4: Security Operations
- Module 5: Security Program Management and Oversight

Labs Included (17 hours):

- Security Concept Fundamentals
- Cryptographic Solutions
- Threat Vectors and Attack Surfaces
- Identifying Security Vulnerabilities
- Analyze Malicious Activity
- Mitigation Techniques
- Security Architecture Models
- Securing Enterprise Infrastructures
- Data Protection Strategies
- Resilience in Security Architecture
- Securing Computing Resources
- Asset Management Techniques
- Vulnerability Management
- Monitoring Computing Resources

- Enhancing Enterprise Security
- Implement Identity & Access Management
- Implementation of Automation & Orchestration for Security Operations
- Investigative Data Sources

CompTIA PenTest+: Gain expertise in penetration testing and vulnerability management with our CompTIA PenTest+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 34+ hours
- Content: 200+ On-demand Videos
- Exam Prep: 240+ Prep Questions
- Certificate of Completion for CompTIA PenTest+

Topics Areas Included:

- Penetration Test Engagement
- Passive Reconnaissance:
- Active Reconnaissance
- Physical Security
- Social Engineering
- Vulnerability Scan Analysis
- Password Cracking
- Network Penetration Testing
- Exploitation of Windows and Linux Systems
- Web Application Testing

Modules:

- Module 1 - The Pen Test Engagement
- Module 2 - Passive Reconnaissance
- Module 3 - Active Reconnaissance
- Module 4 - Physical Security

- Module 5 - Social Engineering
- Module 6 - Vulnerability Scan Analysis
- Module 7 - Password Cracking
- Module 8 - Penetrating Wired Networks
- Module 9 - Penetrating Wireless Networks
- Module 10 - Windows Exploits
- Module 11 - Linux Exploits
- Module 12 - Mobile Devices
- Module 13 - Specialized Systems
- Module 14 - Scripts
- Module 15 - Application Testing
- Module 16 - Web App Exploits
- Module 17 - Lateral Movement
- Module 18 - Persistence
- Module 19 - Cover Your Tracks
- Module 20 - The Report
- Module 21 - Post Engagement Cleanup

Labs included (15 hours):

- Planning and Preparing for a Penetration Test Engagement
- Using the Metasploit Framework
- Performing Social Engineering
- Conducting Passive Reconnaissance for Vulnerabilities in a Network
- Conducting Active Reconnaissance for Vulnerabilities in a Network
- Perform Vulnerability Scan and Analyze Vulnerability Scan Results
- Exploiting the Network Vulnerabilities
- Exploiting Desktop Systems Vulnerabilities
- Exploit Web Application Vulnerabilities

- Performing Password Attacks
- Exploiting Discovered Vulnerabilities
- Work with Various Tools
- Performing Physical Security
- Working with Scripts
- Complete Post Exploit Tasks
- Analyzing and Reporting the Pen Test Results

CompTIA CySA+ CS0-003: Gain expertise in cybersecurity analytics with our CompTIA CySA+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 6+ hours
- Content: 80+ On-demand Videos
- Exam Prep: 100Prep Questions
- Certificate of Completion for CompTIA CySA+ CS0-003

Topics Areas Included:

- Threat and Vulnerability Management
- Software and Systems Security
- Security Operations and Monitoring
- Incident Response
- Compliance and Assessment

Modules:

- Module 1 - CompTIA CySA+ CS0-003 Basics
- Module 2 - CompTIA CySA+ CS0-003 Domain 1 - Security Operations
- Module 3 - CompTIA CySA+ CS0-003 Domain 2 - Vulnerability Management
- Module 4 - CompTIA CySA+ CS0-003 Domain 3 - Incident Response and Management
- Module 5 - CompTIA CySA+ CS0-003 Domain 4 - Reporting and Communication
- Module 6 - CompTIA CySA+ CS0-003 - Course Closeout

Labs Included (12 hours):

- System & Network Security Implementation Concepts
- Threat Intelligence & Threat Gathering Concepts
- Techniques to Determine Malicious Activity
- Vulnerability Scanning Tools & Techniques
- Identifying & Analyzing Malicious Activity
- Tools for Identifying Malicious Activity
- Attack Methodology Frameworks
- Vulnerability Data Analysis and Prioritization
- Incident Response Management Techniques
- Incident Response Communication & Reporting
- Vulnerability Reporting Concepts
- Vulnerability Patching & Attack Surface Management

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Security+ (SY0-701) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge

- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Comparing Security Roles and Security Controls
- Explaining Threat Actors and Threat Intelligence
- Performing Security Assessments
- Identifying Social Engineering and Malware
- Summarizing Basic Cryptographic Concepts
- Implementing Public Key Infrastructure
- Implementing Authentication Controls
- Implementing Identity and Account Management Controls
- Implementing Secure Network Designs
- Implementing Network Security Appliances
- Implementing Secure Network Protocols
- Implementing Host Security Solutions
- Implementing Secure Mobile Solutions
- Summarizing Secure Application Concepts
- Implementing Secure Cloud Solutions
- Explaining Data Privacy and Protection Concepts
- Performing Incident Response
- Explaining Digital Forensics
- Summarizing Risk Management Concepts
- Implementing Cybersecurity Resilience

- Explaining Physical Security

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Scanning and Identifying Network Nodes
- Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
- Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- APPLIED LAB: Performing Network Reconnaissance and Vulnerability Scanning
- Assisted Lab: Managing the Lifecycle of a Certificate
- Assisted Lab: Managing Certificates with OpenSSL
- Assisted Lab: Auditing Passwords with a Password Cracking Utility
- Assisted Lab: Managing Centralized Authentication
- Assisted Lab: Managing Access Controls in Windows Server
- Assisted Lab: Configuring a System for Auditing Policies
- Assisted Lab: Managing Access Controls in Linux
- APPLIED LAB: Configuring Identity and Access Management Controls
- Assisted Lab: Implementing a Secure Network Design
- Assisted Lab: Configuring a Firewall
- Assisted Lab: Configuring an Intrusion Detection System
- Assisted Lab: Implementing Secure Network Addressing Services
- Assisted Lab: Implementing a Virtual Private Network
- Assisted Lab: Implementing a Secure SSH Server
- Assisted Lab: Implementing Endpoint Protection
- APPLIED LAB: Securing the Network Infrastructure
- Assisted Lab: Identifying Application Attack Indicators
- Assisted Lab: Identifying a Browser Attack
- Assisted Lab: Implementing PowerShell Security

- Assisted Lab: Identifying Malicious Code
- APPLIED LAB: Identifying Application Attacks
- Assisted Lab: Managing Data Sources for Incident Response
- Assisted Lab: Configuring Mitigation Controls
- Assisted Lab: Acquiring Digital Forensics Evidence
- Assisted Lab: Backing Up and Restoring Data in Windows and Linux
- APPLIED LAB: Managing Incident Response, Mitigation, and Recovery

CompTIA PenTest+ (PT0-002) CertMaster Learn and Labs: CertMaster Learn for PenTest+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary for success in the field of penetration testing. It includes a Learning Plan to help keep track of progress, along with robust analytics to identify strengths and weaknesses. CertMaster Labs enable practical, hands-on experience with real equipment and software, guiding learners through job tasks in preparation for the certification exam.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Scoping Organization/Customer Requirements
- Lesson 2: Defining the Rules of Engagement
- Lesson 3: Footprinting and Gathering Intelligence
- Lesson 4: Evaluating Human and Physical Vulnerabilities
- Lesson 5: Preparing the Vulnerability Scan

- Lesson 6: Scanning Logical Vulnerabilities
- Lesson 7: Analyzing Scanning Results
- Lesson 8: Avoiding Detection and Covering Tracks
- Lesson 9: Exploiting the LAN and Cloud
- Lesson 10: Testing Wireless Networks
- Lesson 11: Targeting Mobile Devices
- Lesson 12: Attacking Specialized Systems
- Lesson 13: Web Application-Based Attacks
- Lesson 14: Performing System Hacking
- Lesson 15: Scripting and Software Development
- Lesson 16: Leveraging the Attack: Pivot and Penetrate
- Lesson 17: Communicating During the PenTesting Process
- Lesson 18: Summarizing Report Components
- Lesson 19: Recommending Remediation
- Lesson 20: Performing Post-Report Delivery Activities

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Gathering Intelligence
- Assisted Lab: Performing Social Engineering using SET
- Assisted Lab: Discovering Information using Nmap
- Assisted Lab: Performing Vulnerability Scans and Analysis
- Assisted Lab: Penetrating an Internal Network
- Assisted Lab: Exploiting Web Authentication
- Assisted Lab: Exploiting Weaknesses in a Website
- Assisted Lab: Exploiting Weaknesses in a Database
- Assisted Lab: Using SQL Injection
- Assisted Lab: Performing an AitM Attack

- Assisted Lab: Performing Password Attacks
- Assisted Lab: Using Reverse and Bind Shells
- Assisted Lab: Performing Post-Exploitation Activities
- Assisted Lab: Establishing Persistence
- Assisted Lab: Performing Lateral Movement

CompTIA CySA+ (CS0-003) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Understanding Vulnerability Response, Handling, and Management
- Exploring Threat Intelligence and Threat Hunting Concepts

- Explaining Important System and Network Architecture Concepts
- Understanding Process Improvement in Security Operations
- Implementing Vulnerability Scanning Methods
- Performing Vulnerability Analysis
- Communicating Vulnerability Information
- Explaining Incident Response Activities
- Demonstrating Incident Response Communication
- Applying Tools to Identify Malicious Activity
- Analyzing Potentially Malicious Activity
- Understanding Application Vulnerability Assessment
- Exploring Scripting Tools and Analysis Concepts
- Understanding Application Security and Attack Mitigation Best Practices

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configuring Controls
- Assisted Lab: Reviewing IoC and Threat Intelligence Sources
- Assisted Lab: Performing Threat Hunting
- Assisted Lab: Configuring Centralized Logging
- APPLIED LAB: Performing System Hardening
- Assisted Lab: Assess Time Synch Errors
- Assisted Lab: Configuring Automation
- Assisted Lab: Performing Asset Discovery
- Assisted Lab: Performing Vulnerability Scanning
- Assisted Lab: Performing Passive Scanning
- Assisted Lab: Establishing Context Awareness
- Assisted Lab: Analyzing Vulnerability Reports
- Assisted Lab: Detecting Legacy Systems

- APPLIED LAB: Performing Post-Incident Forensic Analysis
- APPLIED LAB: Performing IoC Detection and Analysis
- ADAPTIVE LAB: Performing Playbook Incident Response
- APPLIED LAB: Collecting Forensic Evidence
- Assisted Lab: Performing Root Cause Analysis
- APPLIED LAB: Using Network Sniffers
- APPLIED LAB: Researching DNS and IP Reputation
- Assisted Lab: Using File Analysis Techniques
- Assisted Lab: Analyzing Potentially Malicious Files
- Assisted Lab: Using Nontraditional Vulnerability Scanning Tools
- APPLIED LAB: Performing Web Vulnerability Scanning
- Assisted Lab: Exploiting Weak Cryptography
- Assisted Lab: Performing and Detecting Directory Traversal and Command Injection
- Assisted Lab: Performing and Detecting Privilege Escalation
- Assisted Lab: Performing and Detecting XSS
- Assisted Lab: Performing and Detecting LFI/RFI
- Assisted Lab: Performing and Detecting SQLi
- Assisted Lab: Performing and Detecting CSRF
- APPLIED LAB: Detecting and Exploiting Security Misconfiguration

Product Information:

- One license provides access to CertMaster Learn for Security+, PenTest+, and CySA+ with CertMaster Labs integrated throughout the courses
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, Learn for Security+, PenTest+, and CySA+ with CertMaster Labs integrated will be valid for 12 months

Exam Voucher and Exam Pass Guarantee (Security+, PenTest+, and CySA+): This bundle includes an exam voucher and an exam pass guarantee for Security+, PenTest+, and CySA+: if you don't pass the exams on the first try, we will provide another 12

months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Security Analytics Expert (Security+ / CySA+ / CASP+) Bundle

ITI SKU: CompTIA-21

MSRP: $2999

Sales Price: $2799

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Security Analytics Expert (Security+ / CySA+ / CASP+) Bundle provides comprehensive training for individuals seeking to excel in security analytics. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Security+, CySA+, and CASP+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Security+, CySA+, and CASP+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Security+ SY0-701: Develop critical security skills with our CompTIA Security+ course, designed to provide the knowledge needed to secure and protect networks and systems.

Course Highlights:

- Duration: 35 hours
- Content: 130 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts

- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules:

- Module 1: General Security Concepts
- Module 2: Threats, Vulnerabilities, and Mitigations
- Module 3: Security Architecture
- Module 4: Security Operations
- Module 5: Security Program Management and Oversight

Labs Included (17 hours):

19. Security Concept Fundamentals
20. Cryptographic Solutions
21. Threat Vectors and Attack Surfaces
22. Identifying Security Vulnerabilities
23. Analyze Malicious Activity
24. Mitigation Techniques

25. Security Architecture Models
26. Securing Enterprise Infrastructures
27. Data Protection Strategies
28. Resilience in Security Architecture
29. Securing Computing Resources
30. Asset Management Techniques
31. Vulnerability Management
32. Monitoring Computing Resources
33. Enhancing Enterprise Security
34. Implement Identity & Access Management
35. Implementation of Automation & Orchestration for Security Operations
36. Investigative Data Sources

CompTIA CySA+ CS0-003: Gain expertise in cybersecurity analytics with our CompTIA CySA+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 6+ hours
- Content: 80+ On-demand Videos
- Exam Prep: 100Prep Questions
- Certificate of Completion for CompTIA CySA+ CS0-003

Topics Areas Included:

- Threat and Vulnerability Management
- Software and Systems Security
- Security Operations and Monitoring
- Incident Response
- Compliance and Assessment

Modules:

- Module 1 - CompTIA CySA+ CS0-003 Basics
- Module 2 - CompTIA CySA+ CS0-003 Domain 1 - Security Operations

- Module 3 - CompTIA CySA+ CS0-003 Domain 2 - Vulnerability Management
- Module 4 - CompTIA CySA+ CS0-003 Domain 3 - Incident Response and Management
- Module 5 - CompTIA CySA+ CS0-003 Domain 4 - Reporting and Communication
- Module 6 - CompTIA CySA+ CS0-003 - Course Closeout

Labs Included (12 hours):

- System & Network Security Implementation Concepts
- Threat Intelligence & Threat Gathering Concepts
- Techniques to Determine Malicious Activity
- Vulnerability Scanning Tools & Techniques
- Identifying & Analyzing Malicious Activity
- Tools for Identifying Malicious Activity
- Attack Methodology Frameworks
- Vulnerability Data Analysis and Prioritization
- Incident Response Management Techniques
- Incident Response Communication & Reporting
- Vulnerability Reporting Concepts
- Vulnerability Patching & Attack Surface Management

CompTIA CASP+: Gain expertise in advanced security practices with our CompTIA CASP+ course, covering essential concepts and practices for enterprise security.

Course Highlights:

- Duration: 28+ hours
- Content: 85+ On-demand Videos
- Exam Prep: 250 Prep Questions
- Certificate of Completion for CompTIA CASP+

Topics Areas Included:

- Risk Management: Understanding and applying risk management frameworks and methodologies.

- Enterprise Security Architecture: Designing and implementing secure network architectures.
- Security Operations: Conducting security assessments and implementing advanced security measures.
- Technical Integration: Integrating security controls and technologies in enterprise environments.
- Incident Response: Developing and implementing effective incident response strategies.
- Cryptography: Applying cryptographic techniques to secure communications and data.
- Threat Intelligence: Gathering and analyzing threat intelligence to protect against advanced threats.

Modules:

- Module 1: Enterprise Security Architecture
- Module 2: Enterprise Security Operations
- Module 3: Technical Integration of Enterprise Security
- Module 4: Research, Development, and Collaboration
- Module 5: Risk Management
- Module 6: Security Operations and Monitoring
- Module 7: Incident Response
- Module 8: Security Controls for Hosts
- Module 9: Network Security
- Module 10: Cloud and Virtualization Security
- Module 11: Identity and Access Management
- Module 12: Application Security

Labs included (30 hours):

- With Remote Connectivity
- Perform digital forensics
- Security and Risk Management Support Materials
- Configuring SCCM Configuration Items and Baselines
- Integrate Network and Security Components
- Install and Configure Network Load Balancing
- Perform Firewall Rule-based Management

- Implement SSL VPN using ASA Device Manager
- Configure Verify and Troubleshoot Port Security
- Scanning and Remediating Vulnerabilities with OpenVAS
- Configure and Verify IPv4 and IPv6 Access Lists for Traffic Filtering
- Analyze network traffic with Wireshark
- Configuring Endpoint Security
- Configuring Advanced Authentication and Authorization
- Encryption and Hashing
- Performing security assessment using various tools
- Using various tools for security assessments
- Perform Security Assessment Using MBSA
- Compliance Patching
- Mapping Networks
- Install and Configure ManageEngine OpManager
- Implementing DNSSEC
- Implementing AD Federation Services
- Performing Offline Attacks
- Configure Verify and Troubleshoot GRE Tunnel Connectivity
- Implement OpenPGP
- PKI Concepts
- Perform Banner Grabbing
- Using Password Cracking Tools
- Upgrading and Securing SSH Connection
- Configure Two Factor Authentication
- Using Encryption and Steganography

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Security+ (SY0-701) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Comparing Security Roles and Security Controls
- Explaining Threat Actors and Threat Intelligence
- Performing Security Assessments
- Identifying Social Engineering and Malware
- Summarizing Basic Cryptographic Concepts
- Implementing Public Key Infrastructure
- Implementing Authentication Controls
- Implementing Identity and Account Management Controls
- Implementing Secure Network Designs
- Implementing Network Security Appliances
- Implementing Secure Network Protocols
- Implementing Host Security Solutions
- Implementing Secure Mobile Solutions
- Summarizing Secure Application Concepts
- Implementing Secure Cloud Solutions

- Explaining Data Privacy and Protection Concepts
- Performing Incident Response
- Explaining Digital Forensics
- Summarizing Risk Management Concepts
- Implementing Cybersecurity Resilience
- Explaining Physical Security

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Scanning and Identifying Network Nodes
- Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
- Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- APPLIED LAB: Performing Network Reconnaissance and Vulnerability Scanning
- Assisted Lab: Managing the Lifecycle of a Certificate
- Assisted Lab: Managing Certificates with OpenSSL
- Assisted Lab: Auditing Passwords with a Password Cracking Utility
- Assisted Lab: Managing Centralized Authentication
- Assisted Lab: Managing Access Controls in Windows Server
- Assisted Lab: Configuring a System for Auditing Policies
- Assisted Lab: Managing Access Controls in Linux
- APPLIED LAB: Configuring Identity and Access Management Controls
- Assisted Lab: Implementing a Secure Network Design
- Assisted Lab: Configuring a Firewall
- Assisted Lab: Configuring an Intrusion Detection System
- Assisted Lab: Implementing Secure Network Addressing Services
- Assisted Lab: Implementing a Virtual Private Network
- Assisted Lab: Implementing a Secure SSH Server

- Assisted Lab: Implementing Endpoint Protection
- APPLIED LAB: Securing the Network Infrastructure
- Assisted Lab: Identifying Application Attack Indicators
- Assisted Lab: Identifying a Browser Attack
- Assisted Lab: Implementing PowerShell Security
- Assisted Lab: Identifying Malicious Code
- APPLIED LAB: Identifying Application Attacks
- Assisted Lab: Managing Data Sources for Incident Response
- Assisted Lab: Configuring Mitigation Controls
- Assisted Lab: Acquiring Digital Forensics Evidence
- Assisted Lab: Backing Up and Restoring Data in Windows and Linux
- APPLIED LAB: Managing Incident Response, Mitigation, and Recovery

CompTIA CySA+ (CS0-003) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks

- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Understanding Vulnerability Response, Handling, and Management
- Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts
- Lesson 3: Explaining Important System and Network Architecture Concepts
- Lesson 4: Understanding Process Improvement in Security Operations
- Lesson 5: Implementing Vulnerability Scanning Methods
- Lesson 6: Performing Vulnerability Analysis
- Lesson 7: Communicating Vulnerability Information
- Lesson 8: Explaining Incident Response Activities
- Lesson 9: Demonstrating Incident Response Communication
- Lesson 10: Applying Tools to Identify Malicious Activity
- Lesson 11: Analyzing Potentially Malicious Activity
- Lesson 12: Understanding Application Vulnerability Assessment
- Lesson 13: Exploring Scripting Tools and Analysis Concepts
- Lesson 14: Understanding Application Security and Attack Mitigation Best Practices

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configuring Controls
- Assisted Lab: Reviewing IoC and Threat Intelligence Sources
- Assisted Lab: Performing Threat Hunting
- Assisted Lab: Configuring Centralized Logging
- APPLIED LAB: Performing System Hardening
- Assisted Lab: Assess Time Synch Errors

- Assisted Lab: Configuring Automation
- Assisted Lab: Performing Asset Discovery
- Assisted Lab: Performing Vulnerability Scanning
- Assisted Lab: Performing Passive Scanning
- Assisted Lab: Establishing Context Awareness
- Assisted Lab: Analyzing Vulnerability Reports
- Assisted Lab: Detecting Legacy Systems
- APPLIED LAB: Performing Post-Incident Forensic Analysis
- APPLIED LAB: Performing IoC Detection and Analysis
- ADAPTIVE LAB: Performing Playbook Incident Response
- APPLIED LAB: Collecting Forensic Evidence
- Assisted Lab: Performing Root Cause Analysis
- APPLIED LAB: Using Network Sniffers
- APPLIED LAB: Researching DNS and IP Reputation
- Assisted Lab: Using File Analysis Techniques
- Assisted Lab: Analyzing Potentially Malicious Files
- Assisted Lab: Using Nontraditional Vulnerability Scanning Tools
- APPLIED LAB: Performing Web Vulnerability Scanning
- Assisted Lab: Exploiting Weak Cryptography
- Assisted Lab: Performing and Detecting Directory Traversal and Command Injection
- Assisted Lab: Performing and Detecting Privilege Escalation
- Assisted Lab: Performing and Detecting XSS
- Assisted Lab: Performing and Detecting LFI/RFI
- Assisted Lab: Performing and Detecting SQLi
- Assisted Lab: Performing and Detecting CSRF
- APPLIED LAB: Detecting and Exploiting Security Misconfiguration

CompTIA CASP+ (CAS-004) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Performing Risk Management Activities
- Lesson 2: Summarizing Governance & Compliance Strategies
- Lesson 3: Implementing Business Continuity & Disaster Recovery
- Lesson 4: Identifying Infrastructure Services
- Lesson 5: Performing Software Integration
- Lesson 6: Explain Virtualization, Cloud and Emerging Technology
- Lesson 7: Exploring Secure Configurations and System Hardening

- Lesson 8: Understanding Security Considerations of Cloud and Specialized Platforms
- Lesson 9: Implementing Cryptography
- Lesson 10: Implementing Public Key Infrastructure (PKI)
- Lesson 11: Understanding Threat and Vulnerability Management
- Lesson 12: Developing Incident Response Capabilities

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Using Automation to Identify Sensitive Data
- Assisted Lab: Understanding DR Capabilities in the Cloud
- Assisted Lab: Implementing a Web Application Firewall
- Assisted Lab: Understanding the Role of SPF Records and DNSSEC
- Assisted Lab: Using Security Incident and Event Management Features
- Assisted Lab: Performing Static Code Analysis
- Assisted Lab: Exploiting Web Applications – Stored XSS, SQL Injection
- APPLIED LAB: Analyzing Web Application Vulnerabilities
- Assisted Lab: Implementing a VNet in Azure
- Assisted Lab: Deploying a Virtual Private Cloud in Amazon Web Services
- Assisted Lab: Implementing and Updating Containers on Windows Server 2019
- APPLIED LAB: Performing Container Update Tasks
- Assisted Lab: Understanding DNS over HTTPS (DoH)
- Assisted Lab: Deploying a Hardened Server Image in the Cloud
- Assisted Lab: Implementing an Application Blocklist Policy
- Assisted Lab: Configuring Monitoring in the Cloud
- Assisted Lab: Implementing Data Protection using Symmetric Encryption
- Assisted Lab: Exploring Cryptography and Cryptanalysis using Visual Tools
- Assisted Lab: Implementing HTTP Server Certificates
- APPLIED LAB: Troubleshooting HTTP Server Certificates
- Assisted Lab: Exploring MITRE ATT&CK Navigator

- Assisted Lab: Exploring and Interpreting Intrusion Detection System Alerts
- APPLIED LAB: Analyzing Intrusion Detection System Logs
- Assisted Lab: Exploiting the Server Message Block Protocol
- Assisted Lab: Analyzing SMB Vulnerabilities
- Assisted Lab: Analyzing Firmware using Binary Analysis and Hardware Emulation
- Assisted Lab: Analyzing and Attack Wireless Network Protections

Product and License Information:

- One license provides access to CertMaster Learn for Security+, CySA+, and CASP+ with CertMaster Labs integrated throughout the courses
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, Learn for Security+, CySA+, and CASP+ with CertMaster Labs integrated will be valid for 12 months

Exam Voucher and Exam Pass Guarantee (Security+, CySA+, and CASP+): This bundle includes an exam voucher and an exam pass guarantee for Security+, CySA+, and CASP+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Secure Infrastructure Expert (Security+ / CySA+ / PenTest+ / CASP+) and CompTIA Security Analytics Expert Dual Bundle

ITI SKU: CompTIA-22

MSRP: $3699

Sales Price: $3499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Secure Infrastructure Expert (Security+ / CySA+ / PenTest+ / CASP+) Bundle provides comprehensive training for individuals seeking to excel in secure infrastructure management. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Security+, CySA+, PenTest+, and CASP+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass

the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Security+, CySA+, PenTest+, and CASP+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Security+ SY0-701: Develop critical security skills with our CompTIA Security+ course, designed to provide the knowledge needed to secure and protect networks and systems.

Course Highlights:

- Duration: 35 hours
- Content: 130 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes

- Data Protection and Compliance Concepts

Modules:

- Module 1: General Security Concepts
- Module 2: Threats, Vulnerabilities, and Mitigations
- Module 3: Security Architecture
- Module 4: Security Operations
- Module 5: Security Program Management and Oversight

Labs Included (17 hours):

- Security Concept Fundamentals
- Cryptographic Solutions
- Threat Vectors and Attack Surfaces
- Identifying Security Vulnerabilities
- Analyze Malicious Activity
- Mitigation Techniques
- Security Architecture Models
- Securing Enterprise Infrastructures
- Data Protection Strategies
- Resilience in Security Architecture
- Securing Computing Resources
- Asset Management Techniques
- Vulnerability Management
- Monitoring Computing Resources
- Enhancing Enterprise Security
- Implement Identity & Access Management
- Implementation of Automation & Orchestration for Security Operations
- Investigative Data Sources

CompTIA CySA+ CS0-003: Gain expertise in cybersecurity analytics with our CompTIA CySA+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 6+ hours
- Content: 80+ On-demand Videos
- Exam Prep: 100Prep Questions
- Certificate of Completion for CompTIA CySA+ CS0-003

Topics Areas Included:

- Threat and Vulnerability Management
- Software and Systems Security
- Security Operations and Monitoring
- Incident Response
- Compliance and Assessment

Modules:

- Module 1 - CompTIA CySA+ CS0-003 Basics
- Module 2 - CompTIA CySA+ CS0-003 Domain 1 - Security Operations
- Module 3 - CompTIA CySA+ CS0-003 Domain 2 - Vulnerability Management
- Module 4 - CompTIA CySA+ CS0-003 Domain 3 - Incident Response and Management
- Module 5 - CompTIA CySA+ CS0-003 Domain 4 - Reporting and Communication
- Module 6 - CompTIA CySA+ CS0-003 - Course Closeout

Labs Included (12 hours):

- System & Network Security Implementation Concepts
- Threat Intelligence & Threat Gathering Concepts
- Techniques to Determine Malicious Activity
- Vulnerability Scanning Tools & Techniques
- Identifying & Analyzing Malicious Activity
- Tools for Identifying Malicious Activity

- Attack Methodology Frameworks
- Vulnerability Data Analysis and Prioritization
- Incident Response Management Techniques
- Incident Response Communication & Reporting
- Vulnerability Reporting Concepts
- Vulnerability Patching & Attack Surface Management

CompTIA PenTest+: Gain expertise in penetration testing with our CompTIA PenTest+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 34+ hours
- Content: 200+ On-demand Videos
- Exam Prep: 240+ Prep Questions
- Certificate of Completion for CompTIA PenTest+

Topics Areas Included:

- Penetration Test Engagement
- Passive Reconnaissance:
- Active Reconnaissance
- Physical Security
- Social Engineering
- Vulnerability Scan Analysis
- Password Cracking
- Network Penetration Testing
- Exploitation of Windows and Linux Systems
- Web Application Testing

Modules:

- Module 1 - The Pen Test Engagement
- Module 2 - Passive Reconnaissance

- Module 3 - Active Reconnaissance
- Module 4 - Physical Security
- Module 5 - Social Engineering
- Module 6 - Vulnerability Scan Analysis
- Module 7 - Password Cracking
- Module 8 - Penetrating Wired Networks
- Module 9 - Penetrating Wireless Networks
- Module 10 - Windows Exploits
- Module 11 - Linux Exploits
- Module 12 - Mobile Devices
- Module 13 - Specialized Systems
- Module 14 - Scripts
- Module 15 - Application Testing
- Module 16 - Web App Exploits
- Module 17 - Lateral Movement
- Module 18 - Persistence
- Module 19 - Cover Your Tracks
- Module 20 - The Report
- Module 21 - Post Engagement Cleanup

Labs included (15 hours):

- Planning and Preparing for a Penetration Test Engagement
- Using the Metasploit Framework
- Performing Social Engineering
- Conducting Passive Reconnaissance for Vulnerabilities in a Network
- Conducting Active Reconnaissance for Vulnerabilities in a Network
- Perform Vulnerability Scan and Analyze Vulnerability Scan Results
- Exploiting the Network Vulnerabilities

- Exploiting Desktop Systems Vulnerabilities
- Exploit Web Application Vulnerabilities
- Performing Password Attacks
- Exploiting Discovered Vulnerabilities
- Work with Various Tools
- Performing Physical Security
- Working with Scripts
- Complete Post Exploit Tasks
- Analyzing and Reporting the Pen Test Results

CompTIA CASP+: Gain expertise in advanced security practices with our CompTIA CASP+ course, covering essential concepts and practices for enterprise security.

Course Highlights:

- Duration: 28+ hours
- Content: 85+ On-demand Videos
- Exam Prep: 250 Prep Questions
- Certificate of Completion for CompTIA CASP+

Topics Areas Included:

- Risk Management: Understanding and applying risk management frameworks and methodologies.
- Enterprise Security Architecture: Designing and implementing secure network architectures.
- Security Operations: Conducting security assessments and implementing advanced security measures.
- Technical Integration: Integrating security controls and technologies in enterprise environments.
- Incident Response: Developing and implementing effective incident response strategies.
- Cryptography: Applying cryptographic techniques to secure communications and data.
- Threat Intelligence: Gathering and analyzing threat intelligence to protect against advanced threats.

Modules:

- Module 1: Enterprise Security Architecture
- Module 2: Enterprise Security Operations
- Module 3: Technical Integration of Enterprise Security
- Module 4: Research, Development, and Collaboration
- Module 5: Risk Management
- Module 6: Security Operations and Monitoring
- Module 7: Incident Response
- Module 8: Security Controls for Hosts
- Module 9: Network Security
- Module 10: Cloud and Virtualization Security
- Module 11: Identity and Access Management
- Module 12: Application Security

Labs included (30 hours):

- With Remote Connectivity
- Perform digital forensics
- Security and Risk Management Support Materials
- Configuring SCCM Configuration Items and Baselines
- Integrate Network and Security Components
- Install and Configure Network Load Balancing
- Perform Firewall Rule-based Management
- Implement SSL VPN using ASA Device Manager
- Configure Verify and Troubleshoot Port Security
- Scanning and Remediating Vulnerabilities with OpenVAS
- Configure and Verify IPv4 and IPv6 Access Lists for Traffic Filtering
- Analyze network traffic with Wireshark
- Configuring Endpoint Security
- Configuring Advanced Authentication and Authorization
- Encryption and Hashing
- Performing security assessment using various tools
- Using various tools for security assessments
- Perform Security Assessment Using MBSA
- Compliance Patching
- Mapping Networks
- Install and Configure ManageEngine OpManager

- Implementing DNSSEC
- Implementing AD Federation Services
- Performing Offline Attacks
- Configure Verify and Troubleshoot GRE Tunnel Connectivity
- Implement OpenPGP
- PKI Concepts
- Perform Banner Grabbing
- Using Password Cracking Tools
- Upgrading and Securing SSH Connection
- Configure Two Factor Authentication
- Using Encryption and Steganography

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Security+ (SY0-701) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Comparing Security Roles and Security Controls
- Lesson 2: Explaining Threat Actors and Threat Intelligence
- Lesson 3: Performing Security Assessments
- Lesson 4: Identifying Social Engineering and Malware
- Lesson 5: Summarizing Basic Cryptographic Concepts
- Lesson 6: Implementing Public Key Infrastructure
- Lesson 7: Implementing Authentication Controls
- Lesson 8: Implementing Identity and Account Management Controls
- Lesson 9: Implementing Secure Network Designs
- Lesson 10: Implementing Network Security Appliances
- Lesson 11: Implementing Secure Network Protocols
- Lesson 12: Implementing Host Security Solutions
- Lesson 13: Implementing Secure Mobile Solutions
- Lesson 14: Summarizing Secure Application Concepts
- Lesson 15: Implementing Secure Cloud Solutions
- Lesson 16: Explaining Data Privacy and Protection Concepts
- Lesson 17: Performing Incident Response
- Lesson 18: Explaining Digital Forensics
- Lesson 19: Summarizing Risk Management Concepts
- Lesson 20: Implementing Cybersecurity Resilience
- Lesson 21: Explaining Physical Security

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Scanning and Identifying Network Nodes
- Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan

- Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- APPLIED LAB: Performing Network Reconnaissance and Vulnerability Scanning
- Assisted Lab: Managing the Lifecycle of a Certificate
- Assisted Lab: Managing Certificates with OpenSSL
- Assisted Lab: Auditing Passwords with a Password Cracking Utility
- Assisted Lab: Managing Centralized Authentication
- Assisted Lab: Managing Access Controls in Windows Server
- Assisted Lab: Configuring a System for Auditing Policies
- Assisted Lab: Managing Access Controls in Linux
- APPLIED LAB: Configuring Identity and Access Management Controls
- Assisted Lab: Implementing a Secure Network Design
- Assisted Lab: Configuring a Firewall
- Assisted Lab: Configuring an Intrusion Detection System
- Assisted Lab: Implementing Secure Network Addressing Services
- Assisted Lab: Implementing a Virtual Private Network
- Assisted Lab: Implementing a Secure SSH Server
- Assisted Lab: Implementing Endpoint Protection
- APPLIED LAB: Securing the Network Infrastructure
- Assisted Lab: Identifying Application Attack Indicators
- Assisted Lab: Identifying a Browser Attack
- Assisted Lab: Implementing PowerShell Security
- Assisted Lab: Identifying Malicious Code
- APPLIED LAB: Identifying Application Attacks
- Assisted Lab: Managing Data Sources for Incident Response
- Assisted Lab: Configuring Mitigation Controls
- Assisted Lab: Acquiring Digital Forensics Evidence
- Assisted Lab: Backing Up and Restoring Data in Windows and Linux
- APPLIED LAB: Managing Incident Response, Mitigation and Recovery

CompTIA CySA+ CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Understanding Vulnerability Response, Handling, and Management
- Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts
- Lesson 3: Explaining Important System and Network Architecture Concepts
- Lesson 4: Understanding Process Improvement in Security Operations
- Lesson 5: Implementing Vulnerability Scanning Methods
- Lesson 6: Performing Vulnerability Analysis
- Lesson 7: Communicating Vulnerability Information
- Lesson 8: Explaining Incident Response Activities
- Lesson 9: Demonstrating Incident Response Communication

- Lesson 10: Applying Tools to Identify Malicious Activity
- Lesson 11: Analyzing Potentially Malicious Activity
- Lesson 12: Understanding Application Vulnerability Assessment
- Lesson 13: Exploring Scripting Tools and Analysis Concepts
- Lesson 14: Understanding Application Security and Attack Mitigation Best Practices

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configuring Controls
- Assisted Lab: Reviewing IoC and Threat Intelligence Sources
- Assisted Lab: Performing Threat Hunting
- Assisted Lab: Configuring Centralized Logging
- APPLIED LAB: Performing System Hardening
- Assisted Lab: Assess Time Synch Errors
- Assisted Lab: Configuring Automation
- Assisted Lab: Performing Asset Discovery
- Assisted Lab: Performing Vulnerability Scanning
- Assisted Lab: Performing Passive Scanning
- Assisted Lab: Establishing Context Awareness
- Assisted Lab: Analyzing Vulnerability Reports
- Assisted Lab: Detecting Legacy Systems
- APPLIED LAB: Performing Post-Incident Forensic Analysis
- APPLIED LAB: Performing IoC Detection and Analysis
- ADAPTIVE LAB: Performing Playbook Incident Response
- APPLIED LAB: Collecting Forensic Evidence
- Assisted Lab: Performing Root Cause Analysis
- APPLIED LAB: Using Network Sniffers

- APPLIED LAB: Researching DNS and IP Reputation
- Assisted Lab: Using File Analysis Techniques
- Assisted Lab: Analyzing Potentially Malicious Files
- Assisted Lab: Using Nontraditional Vulnerability Scanning Tools
- APPLIED LAB: Performing Web Vulnerability Scanning
- Assisted Lab: Exploiting Weak Cryptography
- Assisted Lab: Performing and Detecting Directory Traversal and Command Injection
- Assisted Lab: Performing and Detecting Privilege Escalation
- Assisted Lab: Performing and Detecting XSS
- Assisted Lab: Performing and Detecting LFI/RFI
- Assisted Lab: Performing and Detecting SQLi
- Assisted Lab: Performing and Detecting CSRF
- APPLIED LAB: Detecting and Exploiting Security Misconfiguration

CompTIA PenTest+ CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow. Easy-to-use course management tools provide a comprehensive suite of instructor resources alongside a reporting dashboard, making course preparation and progress tracking simple and efficient.

Topics Covered:

- Lesson 1: Scoping Organization/Customer Requirements
- Lesson 2: Defining the Rules of Engagement

- Lesson 3: Footprinting and Gathering Intelligence
- Lesson 4: Evaluating Human and Physical Vulnerabilities
- Lesson 5: Preparing the Vulnerability Scan
- Lesson 6: Scanning Logical Vulnerabilities
- Lesson 7: Analyzing Scanning Results
- Lesson 8: Avoiding Detection and Covering Tracks
- Lesson 9: Exploiting the LAN and Cloud
- Lesson 10: Testing Wireless Networks
- Lesson 11: Targeting Mobile Devices
- Lesson 12: Attacking Specialized Systems
- Lesson 13: Web Application-Based Attacks
- Lesson 14: Performing System Hacking
- Lesson 15: Scripting and Software Development
- Lesson 16: Leveraging the Attack: Pivot and Penetrate
- Lesson 17: Communicating During the PenTesting Process
- Lesson 18: Summarizing Report Components
- Lesson 19: Recommending Remediation
- Lesson 20: Performing Post-Report Delivery Activities

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Gathering Intelligence
- Assisted Lab: Performing Social Engineering using SET
- Assisted Lab: Discovering Information using Nmap
- Assisted Lab: Performing Vulnerability Scans and Analysis
- Assisted Lab: Penetrating an Internal Network
- Assisted Lab: Exploiting Web Authentication
- Assisted Lab: Exploiting Weaknesses in a Website
- Assisted Lab: Exploiting Weaknesses in a Database
- Assisted Lab: Using SQL Injection

- Assisted Lab: Performing an AitM Attack
- Assisted Lab: Performing Password Attacks
- Assisted Lab: Using Reverse and Bind Shells
- Assisted Lab: Performing Post-Exploitation Activities
- Assisted Lab: Establishing Persistence
- Assisted Lab: Performing Lateral Movement

CompTIA CASP+ CertMaster Learn and Labs: Add CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow. Easy-to-use course management tools provide a comprehensive suite of instructor resources alongside a reporting dashboard, making course preparation and progress tracking simple and efficient.

Topics Covered:

- Lesson 1: Performing Risk Management Activities
- Lesson 2: Summarizing Governance & Compliance Strategies
- Lesson 3: Implementing Business Continuity & Disaster Recovery
- Lesson 4: Identifying Infrastructure Services
- Lesson 5: Performing Software Integration
- Lesson 6: Explain Virtualization, Cloud and Emerging Technology
- Lesson 7: Exploring Secure Configurations and System Hardening
- Lesson 8: Understanding Security Considerations of Cloud and Specialized Platforms
- Lesson 9: Implementing Cryptography

- Lesson 10: Implementing Public Key Infrastructure (PKI)
- Lesson 11: Understanding Threat and Vulnerability Management
- Lesson 12: Developing Incident Response Capabilities

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Using Automation to Identify Sensitive Data
- Assisted Lab: Understanding DR Capabilities in the Cloud
- Assisted Lab: Implementing a Web Application Firewall
- Assisted Lab: Understanding the Role of SPF Records and DNSSEC
- Assisted Lab: Using Security Incident and Event Management Features
- Assisted Lab: Performing Static Code Analysis
- Assisted Lab: Exploiting Web Applications – Stored XSS, SQL Injection
- APPLIED LAB: Analyzing Web Application Vulnerabilities
- Assisted Lab: Implementing a VNet in Azure
- Assisted Lab: Deploying a Virtual Private Cloud in Amazon Web Services
- Assisted Lab: Implementing and Updating Containers on Windows Server 2019
- APPLIED LAB: Performing Container Update Tasks
- Assisted Lab: Understanding DNS over HTTPS (DoH)
- Assisted Lab: Deploying a Hardened Server Image in the Cloud
- Assisted Lab: Implementing an Application Blocklist Policy
- Assisted Lab: Configuring Monitoring in the Cloud
- Assisted Lab: Implementing Data Protection using Symmetric Encryption
- Assisted Lab: Exploring Cryptography and Cryptanalysis using Visual Tools
- Assisted Lab: Implementing HTTP Server Certificates
- APPLIED LAB: Troubleshooting HTTP Server Certificates
- Assisted Lab: Exploring MITRE ATT&CK Navigator
- Assisted Lab: Exploring and Interpreting Intrusion Detection System Alerts
- APPLIED LAB: Analyzing Intrusion Detection System Logs
- Assisted Lab: Exploiting the Server Message Block Protocol

- Assisted Lab: Analyzing SMB Vulnerabilities
- Assisted Lab: Analyzing Firmware using Binary Analysis and Hardware Emulation
- Assisted Lab: Analyzing and Attack Wireless Network Protections

Product Information:

- One license provides access to CertMaster Learn for Security+, CySA+, PenTest+, and CASP+ with CertMaster Labs integrated throughout the courses and ITI courses and labs.
- Access keys must be redeemed within 12 months of purchase.
- Once redeemed, licenses will be valid for 12 months.

Exam Voucher and Exam Pass Guarantee (Security+, CySA+, PenTest+, and CASP+): This bundle includes an exam voucher and an exam pass guarantee for Security+, CySA+, PenTest+, and CASP+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA A+ (Core 1 & Core 2) Bundle

ITI SKU: CompTIA-23

MSRP: $1999

Sales Price: $1799

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA A+ (Core 1 & Core 2) Bundle provides comprehensive training for individuals seeking to excel in foundational IT skills. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102), combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for A+ Core 1 and Core 2, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA A+ 220-1101 (Core 1): Develop critical IT skills with our CompTIA A+ Core 1 course, designed to provide the knowledge needed to manage and troubleshoot various IT systems effectively.

Course Highlights:

- Duration: 30 hours
- Content: 100 On-demand Videos
- Exam Prep: 300 Prep Questions
- Certificate of Completion for CompTIA A+ Core 1

Topics Areas Included:

- Devices, Setups, and Installs
- Displays and Multimedia Devices
- Supporting Multiple Drive Types
- Accounting for CPUs and Internal Components
- All About Network Theories
- Network Operations and Diagnostics
- Cloud and Virtualization Computing
- Laptop Features and Troubleshooting
- Syncing and Setup of Mobile Devices
- All Things Printing

Modules:

- Module 1: Devices, Setups, and Installs
- Module 2: Displays and Multimedia Devices
- Module 3: Supporting Multiple Drive Types
- Module 4: Accounting for CPUs and Internal Components
- Module 5: All About Network Theories
- Module 6: Network Operations and Diagnostics
- Module 7: Cloud and Virtualization Computing

- Module 8: Laptop Features and Troubleshooting
- Module 9: Syncing and Setup of Mobile Devices
- Module 10: All Things Printing

CompTIA A+ 220-1102 (Core 2): Enhance your IT skills with our CompTIA A+ Core 2 course, designed to provide advanced knowledge needed for IT support and troubleshooting.

Course Highlights:

- Duration: 30 hours
- Content: 100 On-demand Videos
- Exam Prep: 300 Prep Questions
- Certificate of Completion for CompTIA A+ Core 2

Topics Areas Included:

- Operating System Management
- Configuring and installing the OS
- Tools to Troubleshoot and Maintain the OS
- Network Management Tools
- Sharing Resources and Rights Management
- Threats and Security Measures
- Policies to Protect Data
- Prevent Malware and Security Threats
- Supporting and Troubleshooting Mobile Devices
- Implementing Operational Procedures

Modules:

- Module 1: Operating System Management
- Module 2: Configuring and installing the OS
- Module 3: Tools to Troubleshoot and Maintain the OS
- Module 4: Network Management Tools
- Module 5: Sharing Resources and Rights Management

- Module 6: Threats and Security Measures
- Module 7: Policies to Protect Data
- Module 8: Prevent Malware and Security Threats
- Module 9: Supporting and Troubleshooting Mobile Devices
- Module 10: Implementing Operational Procedures

Labs included (56 hours):

1. Operating System Types and Features
2. Implementing Different Boot Methods and Types of Operating System Installation
3. Disk Partitioning Methods and File Systems
4. Installing System Configuration Settings
5. Using Microsoft Command Line Tools
6. Using Microsoft Operating System Tools and Features
7. Microsoft Windows System Utilities
8. Using Microsoft Windows Control Panel Utilities
9. Using Microsoft Windows Control Panel's User Related Utilities
10. Application Software Installation and Configuration Methods
11. Features and Tools of Mac OS and Linux Desktop Operating System
12. Logical Security Concepts
13. Wi-fi Security Protocols and Authentication Methods
14. Working with Tools and Methods of Malware Prevention, Detection and Removal
15. Microsoft Windows OS Security Settings
16. Implementing Security Best Practices to Secure a Workstation
17. Using Data Destruction and Disposal Methods
18. Troubleshooting Microsoft Windows Issues
19. Troubleshooting PC Security Issues
20. Malware Removal Best Practices
21. Implementing Basic Change Management Best Practices

22. Implement Basic Disaster Prevention and Recovery Methods
23. Basics of Scripting
24. Working with Remote Access Technologies
25. Documentation and Licenses Best Practices
26. Using Proper Communication Techniques and Professionalism
27. Using System Restore
28. Working with BitLocker
29. Identifying different Windows Operating System Editions
30. Managing a Windows device using the Command Line Interface
31. Managing a Windows device using the Graphical User Interface (GUI)
32. Configuring a Windows Device using the Control Panel
33. Configuring and Managing a Windows Device using Settings
34. Configuring Networking Settings on a Windows Device
35. Install and Configure Applications on a Windows Device
36. Identify different Operating Systems and functionality
37. Different Operating System Installation methods
38. Tools for Managing and Maintaining MAC Operating Systems
39. Tools for Managing and Maintaining Linux Operating Systems
40. Implementing Physical Security Measures
41. Implementing Network Security Measures
42. Authentication and Authorization Methods
43. Wireless Security Implementation
44. Malware and Social Engineering Prevention Methods
45. Security Implementation on a Windows Device
46. Password and Account Management on a Windows Device
47. Mobile Security Solutions
48. Secure Data Disposal Methods

49. Securing a SOHO Network
50. Securing Web Browsers on a Windows Device
51. Troubleshooting Windows Operating Systems
52. Troubleshooting Personal Computer Security Settings
53. Malware Removal and Remediating Best Practices
54. Troubleshooting Mobile Device Security Settings
55. Documentation Best Practices
56. Implementing Basic Change Management Best Practices
57. Backup and Recovery Implementation
58. Safety and Environmental Procedures
59. Privacy, Licensing & Policy Concepts
60. Using Proper Communication Techniques and Professionalism
61. Basic Scripting Techniques
62. Remote Access Methods

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA A+ (220-1101 and 220-1102) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge

- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Installing Motherboards and Connectors
- Installing System Devices
- Troubleshooting PC Hardware
- Comparing Local Networking Hardware
- Configuring Network Addressing and Internet Connections
- Supporting Network Services
- Summarizing Virtualization and Cloud Concepts
- Supporting Mobile Devices
- Supporting Print Devices
- Configuring Windows
- Managing Windows
- Identifying OS Types and Features
- Supporting Windows
- Managing Windows Networking
- Managing Linux and macOS
- Configuring SOHO Network Security
- Managing Security Settings
- Supporting Mobile Software
- Using Support and Scripting Tools
- Implementing Operational Procedures

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Installing a Motherboard
- Assisted Lab: Installing Power Supplies
- Assisted Lab: Installing and Configuring System Memory
- Assisted Lab: Installing RAM
- Assisted Lab: Installing CPU and Cooler
- Assisted Lab: Upgrading and Installing GPU and Daisy-Chain Monitors
- Assisted Lab: Exploring the Virtual Machine Lab Environment
- Assisted Lab: Compare Networking Hardware
- Assisted Lab: Compare Wireless Network Technologies
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Compare Protocols and Ports
- Assisted Lab: Troubleshoot a Network #1
- Assisted Lab: Troubleshoot a Network #2
- APPLIED Lab: Troubleshoot a Network #1
- APPLIED Lab: Troubleshoot a Network #2
- Assisted Lab: Adding Expansion SSD in a Laptop
- Assisted Lab: Upgrading Laptop RAM
- Assisted Lab: Replacing Laptop Non-User Removable Battery
- Assisted Lab: Configuring Laptop Dock and External Peripherals
- Assisted Lab: Deploy a Printer
- Assisted Lab: Manage User Settings in Windows
- Assisted Lab: Support Windows 11
- Assisted Lab: Configure Windows System Settings
- Assisted Lab: Use Management Consoles
- Assisted Lab: Use Task Manager

- Assisted Lab: Monitor Performance and Event Logs
- Assisted Lab: Use Command-line Tools
- APPLIED Lab: Support Windows 10
- Assisted Lab: Perform Windows 10 OS Installation
- Assisted Lab: Perform Ubuntu Linux OS Installation
- Assisted Lab: Install and Configure an Application
- Assisted Lab: Troubleshoot a Windows OS Issue
- Assisted Lab: Configure Windows Networking
- Assisted Lab: Configure Folder Sharing in a Workgroup
- Assisted Lab: Manage Linux using Command-line Tools
- Assisted Lab: Manage Files using Linux Command-line Tools
- APPLIED Lab: Support and Troubleshoot Network Hosts
- Assisted Lab: Configure SOHO Router Security
- Assisted Lab: Configure Workstation Security
- Assisted Lab: Configure Browser Security
- Assisted Lab: Troubleshoot Security Issues Scenario #1
- APPLIED Lab: Troubleshoot Security Issues Scenario #2
- Assisted Lab: Use Remote Access Technologies
- Assisted Lab: Implement Backup and Recovery
- Assisted Lab: Implement a PowerShell Script
- Assisted Lab: Implement Bash Script
- Assisted Lab: Manage a Support Ticket
- Assisted Lab: Support Active Directory Domain Networking

Product Information:

- One license provides access to CertMaster Learn for A+ Core 1 & Core 2 (220-1101 & 220-1102) with CertMaster Labs integrated throughout the course and ITI courses and labs.
- Access keys must be redeemed within 12 months of purchase.

- Once redeemed the license will be valid for 12 months.

Exam Voucher and Exam Pass Guarantee (A+ Core 1 & Core 2): This bundle includes an exam voucher and an exam pass guarantee for A+ Core 1 & Core 2: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA CASP+ Bundle

ITI SKU: CompTIA-24

MSRP: $1999

Sales Price: $1499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA CASP+ Bundle provides comprehensive training for individuals seeking to excel in advanced security practices and enterprise security. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA CASP+ (CAS-004), combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for CASP+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA CASP+: Gain expertise in advanced security practices with our CompTIA CASP+ course, covering essential concepts and practices for enterprise security.

Course Highlights:

- Duration: 28+ hours
- Content: 85+ On-demand Videos
- Exam Prep: 250 Prep Questions
- Certificate of Completion for CompTIA CASP+

Topics Areas Included:

- Risk Management: Understanding and applying risk management frameworks and methodologies.
- Enterprise Security Architecture: Designing and implementing secure network architectures.
- Security Operations: Conducting security assessments and implementing advanced security measures.
- Technical Integration: Integrating security controls and technologies in enterprise environments.
- Incident Response: Developing and implementing effective incident response strategies.
- Cryptography: Applying cryptographic techniques to secure communications and data.
- Threat Intelligence: Gathering and analyzing threat intelligence to protect against advanced threats.

Modules:

- Module 1: Enterprise Security Architecture
- Module 2: Enterprise Security Operations
- Module 3: Technical Integration of Enterprise Security
- Module 4: Research, Development, and Collaboration
- Module 5: Risk Management
- Module 6: Security Operations and Monitoring
- Module 7: Incident Response
- Module 8: Security Controls for Hosts
- Module 9: Network Security
- Module 10: Cloud and Virtualization Security
- Module 11: Identity and Access Management
- Module 12: Application Security

Labs included (30 hours):

- With Remote Connectivity
- Perform digital forensics
- Security and Risk Management Support Materials
- Configuring SCCM Configuration Items and Baselines
- Integrate Network and Security Components

- Install and Configure Network Load Balancing
- Perform Firewall Rule-based Management
- Implement SSL VPN using ASA Device Manager
- Configure Verify and Troubleshoot Port Security
- Scanning and Remediating Vulnerabilities with OpenVAS
- Configure and Verify IPv4 and IPv6 Access Lists for Traffic Filtering
- Analyze network traffic with Wireshark
- Configuring Endpoint Security
- Configuring Advanced Authentication and Authorization
- Encryption and Hashing
- Performing security assessment using various tools
- Using various tools for security assessments
- Perform Security Assessment Using MBSA
- Compliance Patching
- Mapping Networks
- Install and Configure ManageEngine OpManager
- Implementing DNSSEC
- Implementing AD Federation Services
- Performing Offline Attacks
- Configure Verify and Troubleshoot GRE Tunnel Connectivity
- Implement OpenPGP
- PKI Concepts
- Perform Banner Grabbing
- Using Password Cracking Tools
- Upgrading and Securing SSH Connection
- Configure Two Factor Authentication
- Using Encryption and Steganography

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA CASP+ (CAS-004) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Performing Risk Management Activities
- Summarizing Governance & Compliance Strategies
- Implementing Business Continuity & Disaster Recovery
- Identifying Infrastructure Services
- Performing Software Integration
- Explain Virtualization, Cloud, and Emerging Technology
- Exploring Secure Configurations and System Hardening
- Understanding Security Considerations of Cloud and Specialized Platforms
- Implementing Cryptography
- Implementing Public Key Infrastructure (PKI)
- Understanding Threat and Vulnerability Management
- Developing Incident Response Capabilities

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Using Automation to Identify Sensitive Data

- Assisted Lab: Understanding DR Capabilities in the Cloud
- Assisted Lab: Implementing a Web Application Firewall
- Assisted Lab: Understanding the Role of SPF Records and DNSSEC
- Assisted Lab: Using Security Incident and Event Management Features
- Assisted Lab: Performing Static Code Analysis
- Assisted Lab: Exploiting Web Applications – Stored XSS, SQL Injection
- APPLIED LAB: Analyzing Web Application Vulnerabilities
- Assisted Lab: Implementing a VNet in Azure
- Assisted Lab: Deploying a Virtual Private Cloud in Amazon Web Services
- Assisted Lab: Implementing and Updating Containers on Windows Server 2019
- APPLIED LAB: Performing Container Update Tasks
- Assisted Lab: Understanding DNS over HTTPS (DoH)
- Assisted Lab: Deploying a Hardened Server Image in the Cloud
- Assisted Lab: Implementing an Application Blocklist Policy
- Assisted Lab: Configuring Monitoring in the Cloud
- Assisted Lab: Implementing Data Protection using Symmetric Encryption
- Assisted Lab: Exploring Cryptography and Cryptanalysis using Visual Tools
- Assisted Lab: Implementing HTTP Server Certificates
- APPLIED LAB: Troubleshooting HTTP Server Certificates
- Assisted Lab: Exploring MITRE ATT&CK Navigator
- Assisted Lab: Exploring and Interpreting Intrusion Detection System Alerts
- APPLIED LAB: Analyzing Intrusion Detection System Logs
- Assisted Lab: Exploiting the Server Message Block Protocol
- Assisted Lab: Analyzing SMB Vulnerabilities
- Assisted Lab: Analyzing Firmware using Binary Analysis and Hardware Emulation
- Assisted Lab: Analyzing and Attack Wireless Network Protections

Product Information:

- One license provides access to CertMaster Learn for CASP+ (CAS-004) with CertMaster Labs integrated throughout the course.
- Access keys must be redeemed within 12 months of purchase.
- Once redeemed, Learn for CASP+ (CAS-004) with CertMaster Labs integrated will be valid for 12 months.

Exam Voucher and Exam Pass Guarantee (CASP+): This bundle includes an exam voucher and an exam pass guarantee for CASP+: if you don't pass the exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Cloud+ Bundle

ITI SKU: CompTIA-25

MSRP: $1999

Sales Price: $1499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Cloud + provides comprehensive training for individuals seeking to excel in cloud administration. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Cloud+ as well as labs, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for Cloud+.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Cloud+ and the labs, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

Course Highlights:

- Duration: 5+ hours
- Content: 42+ On-demand Videos
- Exam Prep: 60+ Prep Questions
- Certificate of Completion for CompTIA Cloud+

Topics Areas Included:

CompTIA Cloud+ CV0-003 Course Content

- Lesson 1: Understanding Cloud Concepts
- Lesson 2: Analyzing System Requirements
- Lesson 3: Deploying a Pilot Project
- Lesson 4: Testing Pilot Project
- Lesson 5: Designing a Cloud Infrastructure
- Lesson 6: Monitoring Cloud Infrastructure
- Lesson 7: Securing Cloud Technologies
- Lesson 8: Securing Cloud Systems
- Lesson 9: Troubleshooting Cloud Issues
- Lesson 10: Preparing for Cloud Deployment

Labs included: (28 hours)

1. Cloud Deployment Models
2. Different Cloud Service Models
3. Cloud Resource Capacity Planning
4. High Availability and Scalability in the Cloud
5. Analyzing Business Requirements for a Cloud Solution
6. Configuring and Managing Cloud Identities
7. Cloud Networking Concepts
8. Securing Cloud Infrastructure Resources
9. Data Security and Compliance in the Cloud
10. Cloud Security Assessments and Tools
11. Incident Response Procedures
12. Cloud Solution Integration
13. Provisioning Cloud Resources
14. Provisioning Public Cloud Storage Solutions
15. Provisioning Private Cloud Storage Solutions

16. Deploying Cloud Networking Solutions
17. Virtualization Concepts and Platforms
18. Cloud Migration Techniques
19. Configuring Logging for Cloud Resources
20. Implementing Cloud Resource Monitoring Solutions
21. Implementing Cloud Resource Monitoring and Alert Solutions
22. Cloud Dashboards and Reporting
23. Cloud Patches, Upgrading and Lifecycle Management
24. Optimizing Cloud Solutions
25. Implementing Cloud Resource Automation Solutions
26. Implementing Cloud Backup and Restore Solutions
27. Cloud Disaster Recovery Concepts
28. Cloud Troubleshooting Methodologies
29. Security Troubleshooting Techniques
30. Troubleshooting Cloud Deployments
31. Cloud Networking Troubleshooting Concepts
32. Troubleshooting Cloud Resource Utilization
33. Automation and Orchestration Troubleshooting Methodologies

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Cloud+ (CV0-003) CertMaster Learn and Labs: CertMaster Learn for CompTIA Cloud+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks

- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Understanding Cloud Concepts
- Lesson 2: Planning and Designing a Cloud Environment
- Lesson 3: Administering Cloud Resources
- Lesson 4: Managing Cloud Storage
- Lesson 5: Managing Networks in the Cloud
- Lesson 6: Securing and Troubleshooting Networks in the Cloud
- Lesson 7: Managing Cloud Migrations and Troubleshooting Cloud Deployments
- Lesson 8: Managing Cloud Automation and Orchestration
- Lesson 9: Understanding Cloud Security Concepts
- Lesson 10: Managing Cloud Security
- Lesson 11: Managing Cloud Performance
- Lesson 12: Managing Maintenance in the Cloud
- Lesson 13: Implementing High Availability and Disaster Recovery in the Cloud

Labs Available:

- Assisted Lab: Explore the Lab Environment
- Assisted Lab: Plan and Design a Cloud Environment
- Assisted Lab: Deploy and Manage Cloud Resources
- Assisted Lab: Manage Compute Resources
- Assisted Lab: Manage Networks in the Cloud
- Assisted Lab: Secure Cloud Components
- APPLIED LAB: Deploy Cloud Resources
- Assisted Lab: Manage Cloud Automation

- Assisted Lab: Manage Baseline Configurations
- Assisted Lab: Deploy Patches
- Assisted Lab: Configure Monitoring
- Assisted Lab: Manage Backup and Restore Processes
- APPLIED LAB: Manage Cloud Resources

Product Information:

- One license provides access to CertMaster Learn for Network+ and Cloud+ with CertMaster Labs integrated throughout the courses and ITI courses and labs.
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, Learn for Network+ and Cloud+ with CertMaster Labs integrated will be valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Cloud+): This bundle includes an exam voucher and an exam pass guarantee for Cloud+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA CySA+ Bundle

ITI SKU: CompTIA-27

MSRP: $1999

Sales Price: $1499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA CySA+ Bundle provides comprehensive training for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CySA+ plus labs, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for CySA+ and the labs, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA CySA+ CS0-003: Gain expertise in cybersecurity analytics with our CompTIA CySA+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 6+ hours
- Content: 80+ On-demand Videos
- Exam Prep: 100Prep Questions
- Certificate of Completion for CompTIA CySA+ CS0-003

Topics Areas Included:

- Threat and Vulnerability Management
- Software and Systems Security
- Security Operations and Monitoring
- Incident Response
- Compliance and Assessment

Modules:

- Module 1 - CompTIA CySA+ CS0-003 Basics
- Module 2 - CompTIA CySA+ CS0-003 Domain 1 - Security Operations
- Module 3 - CompTIA CySA+ CS0-003 Domain 2 - Vulnerability Management
- Module 4 - CompTIA CySA+ CS0-003 Domain 3 - Incident Response and Management
- Module 5 - CompTIA CySA+ CS0-003 Domain 4 - Reporting and Communication
- Module 6 - CompTIA CySA+ CS0-003 - Course Closeout

Labs Included (12 hours):

- System & Network Security Implementation Concepts
- Threat Intelligence & Threat Gathering Concepts
- Techniques to Determine Malicious Activity

- Vulnerability Scanning Tools & Techniques
- Identifying & Analyzing Malicious Activity
- Tools for Identifying Malicious Activity
- Attack Methodology Frameworks
- Vulnerability Data Analysis and Prioritization
- Incident Response Management Techniques
- Incident Response Communication & Reporting
- Vulnerability Reporting Concepts
- Vulnerability Patching & Attack Surface Management

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA CySA+ (CS0-003) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis

- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Understanding Vulnerability Response, Handling, and Management
- Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts
- Lesson 3: Explaining Important System and Network Architecture Concepts
- Lesson 4: Understanding Process Improvement in Security Operations
- Lesson 5: Implementing Vulnerability Scanning Methods
- Lesson 6: Performing Vulnerability Analysis
- Lesson 7: Communicating Vulnerability Information
- Lesson 8: Explaining Incident Response Activities
- Lesson 9: Demonstrating Incident Response Communication
- Lesson 10: Applying Tools to Identify Malicious Activity
- Lesson 11: Analyzing Potentially Malicious Activity
- Lesson 12: Understanding Application Vulnerability Assessment
- Lesson 13: Exploring Scripting Tools and Analysis Concepts
- Lesson 14: Understanding Application Security and Attack Mitigation Best Practices

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configuring Controls
- Assisted Lab: Reviewing IoC and Threat Intelligence Sources
- Assisted Lab: Performing Threat Hunting
- Assisted Lab: Configuring Centralized Logging
- APPLIED LAB: Performing System Hardening
- Assisted Lab: Assess Time Synch Errors
- Assisted Lab: Configuring Automation

- Assisted Lab: Performing Asset Discovery
- Assisted Lab: Performing Vulnerability Scanning
- Assisted Lab: Performing Passive Scanning
- Assisted Lab: Establishing Context Awareness
- Assisted Lab: Analyzing Vulnerability Reports
- Assisted Lab: Detecting Legacy Systems
- APPLIED LAB: Performing Post-Incident Forensic Analysis
- APPLIED LAB: Performing IoC Detection and Analysis
- ADAPTIVE LAB: Performing Playbook Incident Response
- APPLIED LAB: Collecting Forensic Evidence
- Assisted Lab: Performing Root Cause Analysis
- APPLIED LAB: Using Network Sniffers
- APPLIED LAB: Researching DNS and IP Reputation
- Assisted Lab: Using File Analysis Techniques
- Assisted Lab: Analyzing Potentially Malicious Files
- Assisted Lab: Using Nontraditional Vulnerability Scanning Tools
- APPLIED LAB: Performing Web Vulnerability Scanning
- Assisted Lab: Exploiting Weak Cryptography
- Assisted Lab: Performing and Detecting Directory Traversal and Command Injection
- Assisted Lab: Performing and Detecting Privilege Escalation
- Assisted Lab: Performing and Detecting XSS
- Assisted Lab: Performing and Detecting LFI/RFI
- Assisted Lab: Performing and Detecting SQLi
- Assisted Lab: Performing and Detecting CSRF
- APPLIED LAB: Detecting and Exploiting Security Misconfiguration

Product and License Information:

- One license provides access to CertMaster Learn for CySA+ with CertMaster Labs integrated throughout the courses as well as ITI's courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CySA+): This bundle includes an exam voucher and an exam pass guarantee for and CySA+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA ITF+ PRO Bundle

ITI SKU: CompTIA-28

MSRP: $1299

Sales Price: $999

Bundle Access Period: 12 months from purchase.

High-level description:

High-level description: The CompTIA ITF+ Bundle provides basic IT fundamental skills needed in this industry and is based on different areas of IT, including hardware, software, programming, security, and infrastructure. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for ITF+, and combines CompTIA ITF PRO engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for ITF+, followed by the integrated official CompTIA ITF Pro.

CTI Custom Online Self-Paced ILT Description:

CompTIA CySA+ CS0-003: Gain expertise in cybersecurity analytics with our CompTIA ITF+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 9+ hours

- Content: 50+ On-demand Videos
- Exam Prep: 150+ Prep Questions
- Certificate of Completion for CompTIA ITF+

Topics Areas Included:

- Basic database concepts
- Basic IT concepts
- Basic network connectivity
- Basics of network communication
- Fundamentals ITF+
- Common operating systems
- Basic computer maintenance

Modules:

Module 1 - IT Concepts and Terminology

Module 2 - Infrastructure

Module 3 - Applications and Software

Module 4 - Software Development

Module 5 - Database Fundamentals

Module 6 - Security

CompTIA official Training – ITF+ Pro:

What is IT Fundamentals Pro?

IT Fundamentals Pro is a high-quality, all-in-one e-learning curriculum that is easy to use and will provide instructors with the hands-on training needed to prepare students for an IT education. Hosted on the online TestOut learning platform, LabSim, it provides a comprehensive experience and hours of content for training practical skills through interactive learning modules. Instructional lessons are combined with instructor-led videos, demonstrations, quizzes, practice exams, and performance-based lab simulations to provide hours of content to prepare students for the CompTIA ITF+ (FC0-U61) certification exam.

LabSim is ideal for learning computer technology in a variety of classroom formats; self-paced, in person, online, hybrid, and flipped. As an online resource, it also works with PCs, Macs, laptops, and Chrome books.

When used in a classroom environment, LabSim empowers instructor and administrator success by providing easy-to-use course management tools, LMS integration, a comprehensive suite of instructor resources, and reporting and analytics options which make tracking student progress effective and efficient.

- Engaging video lessons and text lessons teach the essentials of software and hardware to networking and programming
- Section quizzes help gauge how well students retain what they have learned
- Performance-based labs simulations provide application to real-world scenarios such as configuring a wired network or programming images for a webpage
- Labs and assessments (custom and certification practice exams) provide detailed feedback reports and scores
- Automatic grading and teaching resources help guide the classroom experience
- Exam practice for CompTIA ITF+ (FC0-U61) includes Readiness Reports, Domain Exams, and full-length exams that emulate the real certification exam

Topics Covered

Chapter 1: Course Overview

Chapter 2: Information Technology Basics

Chapter 3: Computer Hardware

Chapter 4: Computer Software

Chapter 5: Internet Technology

Chapter 6: Networking

Chapter 7: Databases

Chapter 8: Programming

Chapter 9: Information Systems

Chapter 10: Cybersecurity

Chapter 11: IT Career Preparation

Appendix A: TestOut IT Fundamentals Pro - Practice Exams

Product and License Information:

- One license provides access to courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (ITF+): This bundle includes an exam voucher and an exam pass guarantee for and ITF+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Linux+ Bundle

ITI SKU: CompTIA-29

MSRP: $1999

Sales Price: $1499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Linux+ Bundle provides comprehensive training for individuals seeking to excel in Linux system administration. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Linux+, combined with engaging official CompTIA video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for Linux+.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Linux+ and labs, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Linux+: Gain expertise in Linux system administration with our CompTIA Linux+ course. This course will provide you with the knowledge and skills required to configure, manage, operate, and troubleshoot a Linux environment by using security best practices, scripting, and automation computing models.

Course Highlights:

- Duration: 30+ hours
- Content: 120+ On-demand Videos
- Exam Prep: 400+ Prep Questions
- Certificate of Completion for CompTIA Linux+

Topics Areas Included:

- Introduction to Linux
- Administering Users and Groups
- Configuring Permissions
- Implementing File Management
- Managing Software and Storage
- Configuring Network Settings
- Securing Linux Systems
- Scripting and Automation

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery

- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

CompTIA Linux+ labs included (63 hours):

1. Design Hard Disk Layout
2. Create Partitions and Filesystems
3. Using Various Disk Management Tools
4. Working with Kernel, Boot Modules, and Files
5. Working with Relative and Absolute Paths
6. Work with the Flow Control Constructs
7. Control Mounting and Unmounting of Filesystems
8. View the Hard Drive Details
9. Check and Repair Filesystems
10. Using RPM and YUM Package Management
11. Using Debian Package Management
12. Using Repositories
13. Managing User and Group Accounts and Related System Files
14. Run User Level Queries
15. Managing Disk Quotas
16. Working with Bash Profiles and Bash Scripts
17. Setup Host Security
18. Perform Basic File Editing Operations Using vi
19. Search Text Files using Regular Expressions
20. Using Shell Input and Output Redirections
21. Install and Configure a Web Server
22. Performing Basic File Management
23. Amending Hard and Symbolic Links

24. Find System Files and Place Files in the Correct Location
25. Use Systemctl and update-rc.d Utility to Manage Services
26. Configuring Host Names
27. Change Runlevels and Shutdown or Reboot System
28. Maintain System Time
29. Configure Client Side DNS
30. Configure System Logging
31. Mail Transfer Agent (MTA) Basics
32. Automate System Administration Tasks by Scheduling Jobs
33. Create, Monitor and Kill Processes
34. Manage Printers and Printing
35. Accessibility
36. Manage File Permissions and Ownership
37. Perform Security Administration Tasks
38. Working with Access Control List
39. Configure SELinux
40. Maintain the Integrity of Filesystems
41. Work with Pluggable Authentication Modules (PAM)
42. Secure Communication using SSH
43. Securing Data with Encryption
44. Work with TTY
45. Set up SFTP to Chroot Jail only for Specific Group
46. Secure a Linux Terminal and Implement Logging Services
47. Boot the System
48. Configure UFW and DenyHosts
49. Compress Data Using Various Tools and Utilities
50. Process Text Streams using Filters

51. Basic Network Troubleshooting
52. Use Streams Pipes and Redirects
53. Perform CPU Monitoring and Configuration
54. Perform Memory Monitoring and Configuration
55. Perform Process Monitoring
56. Modify Process Execution Priorities
57. Manage File and Directory Permissions
58. Access the Linux System
59. Configure Inheritance and Group Memberships
60. Patch the System
61. Working with the Environment Variables
62. Shells, Scripting and Data Management
63. Customize or Write Simple Scripts
64. Configure Permissions on Files and Directories
65. Work with PKI

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Linux+ (XK0-005) CertMaster Learn and Labs: CertMaster Learn for CompTIA Linux+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam

- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Introducing Linux
- Lesson 2: Administering Users and Groups
- Lesson 3: Configuring Permissions
- Lesson 4: Implementing File Management
- Lesson 5: Authoring Text Files
- Lesson 6: Managing Software
- Lesson 7: Administering Storage
- Lesson 8: Managing Devices, Processes, Memory, and the Kernel
- Lesson 9: Managing Services
- Lesson 10: Configuring Network Settings
- Lesson 11: Configuring Network Security
- Lesson 12: Managing Linux Security
- Lesson 13: Implementing Simple Scripts
- Lesson 14: Using Infrastructure as Code
- Lesson 15: Managing Containers in Linux
- Lesson 16: Installing Linux

Integrated Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Basic Linux Interaction
- Assisted Lab: Manage User Accounts
- Assisted Lab: Manage Group Accounts
- Assisted Lab: Configure and troubleshoot privilege escalation
- Assisted Lab: Configure Standard Permissions
- Assisted Lab: Configure Special Permissions
- Assisted Lab: Configure ACLs

- Assisted Lab: Troubleshoot permissions
- APPLIED LAB: Identity and Access Control
- Assisted Lab: Manage File Links
- Assisted Lab: Use File Management Commands
- Assisted Lab: Search for Files
- Assisted Lab: Edit Text Files
- Assisted Lab: Backup, Restore, and Compress Files
- Assisted Lab: Manage RPM Packages
- Assisted Lab: Manage DEB Packages
- Assisted Lab: Compile a Program
- Assisted Lab: Download Files From a Web Server
- APPLIED LAB: File and software management
- Assisted Lab: Deploy Storage and LVM
- Assisted Lab: Manage Processes
- Assisted Lab: Manage Services
- Assisted Lab: Deploy Services
- Assisted Lab: Configure Network Settings
- Assisted Lab: Configure Remote Administration
- Assisted Lab: Troubleshoot Network Configurations
- APPLIED LAB: System Management
- Assisted Lab: Configure a Firewall
- Assisted Lab: Intercept Network Traffic
- Assisted Lab: Harden a Linux System
- Assisted Lab: Verify file integrity by using hashes.
- Assisted Lab: Configure SELinux
- APPLIED LAB: Security
- Assisted Lab: Manage Scripts

- Assisted Lab: Configure a System with Ansible
- Assisted Lab: Manage Version Control with Git
- Assisted Lab: Deploy Docker Containers
- Assisted Lab: Manage GRUB2
- Assisted Lab: Deploy a Linux System
- APPLIED LAB: Scripting, Orchestration, Installation

Product and License Information:

- One license provides access to CertMaster Learn for Linux+ with CertMaster Labs integrated throughout the courses as well as ITI's course and labs.
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses are valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Linux+): This bundle includes an exam voucher and an exam pass guarantee for Linux+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Ethical Hacker - CEH Master with C|HFI Blended Bundle

SKU: EC-Council-38

MSRP: $3999

Sales Price: $3899

High-level description: The Certified Ethical Hacker (CEH) Master with Computer Hacking Forensic Investigator (CHFI) blended bundle is designed to equip IT professionals with advanced skills in ethical hacking and forensic investigation. This comprehensive training program combines theoretical knowledge with practical skills, ensuring participants are proficient in identifying vulnerabilities and conducting thorough investigations following security incidents. This bundle includes our ITI's custom Self-paced Online ILT and labs, as well as an official EC-Council live Online ILT CEH course (as well as their self-paced course) and an official Self-paced Online ILT CHFI course.

Course Delivery:

- **Official EC-Council CEH Master:** Live Online ILT
    - **Contact us to schedule.**
- **Official EC-Council CEH Master:** Self-paced Online ILT
- **Official EC-Council CHFI:** Self-paced Online ILT
- **ITI Custom CEH:** Self-paced Online ILT
- **ITI Custom CHFI:** Self-paced Online ILT

Duration:

- **Official EC-Council CEH Master (live):** 5 days
- **Official EC-Council CEH (self-paced):** 5 days
- **Official EC-Council CHFI:** 5 days
- **ITI Custom CEH: ~** 7 days (70+ hours)
- **ITI Custom CHFI: ~** 4 days (30+ hours)

Recommended Study Sequence: Begin with the Official CEH Master training then the ITI CEH training to understand the core concepts of ethical hacking. Follow this with the Official CHFI course and then the ITI CHFI training to gain expertise in forensic investigation techniques.

CTI Custom CEH Course Description: Our course offers CEH training to provide you the tools to research, discover and scan targets, analyze vulnerabilities and test attack methods and tools. The focus of this CEH online training course is to solve the challenge of breaking into a target network, collect evidence of success, and escape unnoticed.

Topics Covered:

- Introduction to the key concepts of ethical hacking and information security.
- Conducting footprinting and reconnaissance using advanced tools and techniques.
- Scanning networks and identifying vulnerabilities.
- Performing system hacking and exploiting operating systems.
- Understanding malware threats and implementing countermeasures.
- Utilizing social engineering techniques and tools.
- Executing Denial-of-Service (DoS) and session hijacking attacks.

- Evading IDS, firewalls, and honeypots.
- Hacking web servers and applications.
- Performing SQL injection and securing databases.
- Hacking wireless networks and mobile platforms.
- Exploring IoT and OT hacking methodologies.
- Securing cloud environments and implementing cryptographic techniques.

Labs included (15 hours):

- Footprinting and Reconnaissance Techniques
- Network Reconnaissance Techniques
- Enumeration Reconnaissance Techniques
- Vulnerability Analysis Tools & Techniques
- System Hacking Methodologies
- Malware Threat Concepts
- Network Sniffing Techniques
- Social Engineering Exploits
- Denial of Service Attacks
- Session Hijacking Concepts
- Compromising Web Servers
- Web Application Hacking
- SQL Injection Methodologies
- Introduction to Cloud Computing
- Cryptography Techniques

CTI Custom CHFI Course Description: Our CHFI course will cover the security discipline of computer forensics from a vendor-neutral perspective and work towards preparing students to become Forensic Investigators in Computer Hacking.

Topics Covered (18+ hours):

- Comprehensive understanding of computer forensics and the forensic investigation process.
- Techniques for searching and seizing digital evidence.
- Methods for analyzing and handling digital evidence.
- First responder procedures for incident management.
- Setup and operation of a forensic lab.
- Gain in-depth knowledge of hard disks, file systems, and Windows forensics.

- Data acquisition and duplication techniques.
- Recovering deleted files and partitions.
- Utilizing Access Data FTK and EnCase for forensic investigations.
- Understanding and applying steganography and password cracking techniques.
- Log correlation, network forensics, and analyzing wireless and web attacks.
- Investigating email crimes and conducting mobile investigations.
- Preparing investigative reports and serving as an expert witness.

Labs included (12+ hours):

- Understanding the Digital Forensics Profession and Investigations
- Data Acquisition
- Processing Crime and Incident Scenes
- Working with Windows and CLI Systems
- Current Digital Forensics Tools
- Linux and Macintosh File Systems
- Recovering Graphics Files
- Digital Forensics Analysis and Validation
- Virtual Machine Forensics, Live Acquisitions, and Network Forensics
- E-mail and Social Media Investigations
- Mobile Device Forensics
- Cloud Forensics
- Report Writing for High-Tech Investigations
- Expert Testimony in Digital Investigations
- Ethics for the Expert Witness

Official EC-Council CEH Master Course Description: Master ethical hacking with our CEH Master course, tailored for security professionals aiming to protect their organizations from cyber threats. This course includes 40 hours of content, delivered through engaging videos, quizzes, and hands-on labs. Participants will learn to think like hackers and use the same tools and techniques to identify and mitigate vulnerabilities.

Topics Covered (labs integrated):

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration

- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial of Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

Official EC-Council CHFI Course Description: Enhance your investigative skills with the CHFI course, which provides 30 hours of content focusing on digital forensics. This course covers the essentials of computer forensics, including the investigation process, tools, and techniques for analyzing digital evidence.

Topics Covered (labs integrated):

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-Forensics Techniques
- Operating System Forensics
- Network Forensics

- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigative Reports

Exam and exam pass guarantee information: All courses include an exam voucher and the CEH comes with a retake. Exams can be taken online through the EC-Council's remote proctoring service or at authorized testing centers. If you don't pass the CEH or CHFI exam, upon request you will be provided an additional 12 months of access to ITI's custom CEH and CHFI training.

License Information: One license provides access to both official EC-Council CEH and CHFI, ITI's CEH and CHFI courses and labs for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Link to brochure: https://www.eccouncil.org/wp-content/uploads/2022/09/CEH-brochure.pdf and https://www.eccouncil.org/wp-content/uploads/2023/03/CHFI-brochure.pdf

Certified Ethical Hacker - CEH Master with C|PENT and PenTest+ Blended Bundle

SKU: EC-Council-30

MSRP: $3,999

Sale Price: $3,899

High-level description: The Certified Ethical Hacker (CEH) Master with Certified Penetration Testing Professional (CPENT) blended bundle is designed to provide IT professionals with comprehensive training in ethical hacking and advanced penetration testing. This training program focuses on both defensive and offensive cybersecurity skills.

Course Delivery:

- **Official EC-Council CEH Master:** Live Online ILT
    - **Contact us to schedule.**
- **Official EC-Council CEH:** Self-paced Online ILT
- **Official EC-Council CPENT:** Self-paced Online ILT

- **ITI Custom CEH:** Self-paced Online ILT
- **ITI Custom PenTest+:** Self-paced Online ILT

Duration:

- **Official EC-Council CEH Master (live):** 5 days
- **Official EC-Council CEH Master (self-paced):** 5 days
- **Official EC-Council CPENT:** 5 days
- **ITI Custom CEH:** ~7+ days (70+ hours)
- **ITI Custom PenTest+:** ~6+ days (53+ hours)

Recommended Study Sequence: Begin with the Official CEH Master training then the ITI CEH training to understand the core concepts of ethical hacking. Follow this with the CPENT course to develop advanced penetration testing skills and then ITI's PenTest+ course and labs.

CTI Custom CEH Course Description: Our course offers CEH training to provide you the tools to research, discover and scan targets, analyze vulnerabilities and test attack methods and tools. The focus of this CEH online training course is to solve the challenge of breaking into a target network, collect evidence of success, and escape unnoticed.

Topics Covered:

- Introduction to the key concepts of ethical hacking and information security.
- Conducting footprinting and reconnaissance using advanced tools and techniques.
- Scanning networks and identifying vulnerabilities.
- Performing system hacking and exploiting operating systems.
- Understanding malware threats and implementing countermeasures.
- Utilizing social engineering techniques and tools.
- Executing Denial-of-Service (DoS) and session hijacking attacks.
- Evading IDS, firewalls, and honeypots.
- Hacking web servers and applications.
- Performing SQL injection and securing databases.
- Hacking wireless networks and mobile platforms.

- Exploring IoT and OT hacking methodologies.
- Securing cloud environments and implementing cryptographic techniques.

Labs included (15 hours):

- Footprinting and Reconnaissance Techniques
- Network Reconnaissance Techniques
- Enumeration Reconnaissance Techniques
- Vulnerability Analysis Tools & Techniques
- System Hacking Methodologies
- Malware Threat Concepts
- Network Sniffing Techniques
- Social Engineering Exploits
- Denial of Service Attacks
- Session Hijacking Concepts
- Compromising Web Servers
- Web Application Hacking
- SQL Injection Methodologies
- Introduction to Cloud Computing
- Cryptography Techniques

CTI CompTIA PenTest+: Gain expertise in penetration testing with our CompTIA PenTest+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 34+ hours
- Content: 200+ On-demand Videos
- Exam Prep: 240+ Prep Questions
- Certificate of Completion for CompTIA PenTest+

Topics Areas Included:

- Penetration Test Engagement
- Passive Reconnaissance:
- Active Reconnaissance
- Physical Security
- Social Engineering
- Vulnerability Scan Analysis

- Password Cracking
- Network Penetration Testing
- Exploitation of Windows and Linux Systems
- Web Application Testing

Modules:

- Module 1 - The Pen Test Engagement
- Module 2 - Passive Reconnaissance
- Module 3 - Active Reconnaissance
- Module 4 - Physical Security
- Module 5 - Social Engineering
- Module 6 - Vulnerability Scan Analysis
- Module 7 - Password Cracking
- Module 8 - Penetrating Wired Networks
- Module 9 - Penetrating Wireless Networks
- Module 10 - Windows Exploits
- Module 11 - Linux Exploits
- Module 12 - Mobile Devices
- Module 13 - Specialized Systems
- Module 14 - Scripts
- Module 15 - Application Testing
- Module 16 - Web App Exploits
- Module 17 - Lateral Movement
- Module 18 - Persistence
- Module 19 - Cover Your Tracks
- Module 20 - The Report
- Module 21 - Post Engagement Cleanup

Labs included (15 hours):

- Planning and Preparing for a Penetration Test Engagement
- Using the Metasploit Framework
- Performing Social Engineering
- Conducting Passive Reconnaissance for Vulnerabilities in a Network
- Conducting Active Reconnaissance for Vulnerabilities in a Network
- Perform Vulnerability Scan and Analyze Vulnerability Scan Results
- Exploiting the Network Vulnerabilities
- Exploiting Desktop Systems Vulnerabilities
- Exploit Web Application Vulnerabilities
- Performing Password Attacks
- Exploiting Discovered Vulnerabilities
- Work with Various Tools
- Performing Physical Security
- Working with Scripts
- Complete Post Exploit Tasks
- Analyzing and Reporting the Pen Test Results

Official EC-Council CEH Master Course Description: Master ethical hacking with our CEH Master course, designed for security professionals aiming to protect their organizations from cyber threats. This course includes 40 hours of content, delivered through engaging videos, quizzes, and hands-on labs.

Topics Covered:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats

- Sniffing
- Social Engineering
- Denial of Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

Official EC-Council CPENT Course Description: Advance your penetration testing skills with the CPENT course, which provides 40 hours of content focused on real-world penetration testing scenarios. This course covers advanced topics such as IoT hacking, binary exploitation, and writing exploits.

Topics Covered:

- Advanced Windows Attacks
- Attacking IoT Systems
- Writing Exploits: Advanced Binary Exploitation
- Bypassing a Filtered Network
- Pentesting Operational Technology (OT)
- Accessing Hidden Networks with Pivoting
- Double Pivoting
- Privilege Escalation
- Evading Defense Mechanisms
- Reporting and Documentation

Exam Information: All courses, except for the PenTest+, include an exam voucher. Exams can be taken online through the EC-Council's remote proctoring service or at authorized testing centers. The CEH course comes with one exam retake. A PenTest+ exam voucher can be purchased at a 20% discount.

License Information: One license provides access to all course's for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Link to brochure: https://www.eccouncil.org/wp-content/uploads/2022/09/CEH-brochure.pdf and https://www.eccouncil.org/wp-content/uploads/2023/02/CPENT-brochure.pdf

DUAL CISO Bundle - EC-Council Certified Chief Information Security Officer (CCISO) and PECB CISO

SKU: EC-Council-32

MSRP: $3999

Sale Price: $3799

High-level description: Chief Information Security Officer training programs are designed for executives who want to advance their careers in information security management. This bundle covers the EC-Council five domains of the CCISO Body of Knowledge, focusing on governance, security risk management, controls, audit management, security program management, and operations, as well as the PECB CISO learning objectives; Explain the fundamental principles and concepts of information security; Comprehend the roles and responsibilities of the CISO and the ethical considerations involved, and address the challenges associated with the role;

Design and develop an effective information security program, tailored to the needs of the organization; Adopt applicable frameworks, laws, and regulations and effectively communicate and implement policies to ensure information security compliance; and Identify, analyze, evaluate, and treat information security risks, using a systematic and effective approach.

Course Delivery:

- **EC-Council CCISO:** Self-Paced ILT
- **PECB CISO:** Self-Paced ILT

Duration:

- **EC-Council CCISO:** 5 days

- **PECB CISO:** 5 days

EC-Council CCISO Description: The CCISO course is designed for current and aspiring information security executives. This program includes 40 hours of content, combining theoretical knowledge with practical skills required to establish and maintain an information security program.

Topics Covered:

Domain 1: Governance and Risk Management

1. Define, Implement, Manage, and Maintain an Information Security Governance Program

1.1. Form of Business Organization

1.2. Industry

1.3. Organizational Maturity

2. Information Security Drivers

3. Establishing an information security management structure

3.1. Organizational Structure

3.2. Where does the CISO fit within the organizational structure

3.3. The Executive CISO

3.4. Nonexecutive CISO

4. Laws/Regulations/Standards as drivers of Organizational Policy/Standards/Procedures

5. Managing an enterprise information security compliance program

5.1. Security Policy

5.1.1. Necessity of a Security Policy

5.1.2. Security Policy Challenges

5.2. Policy Content

5.2.1. Types of Policies

5.2.2. Policy Implementation

5.3. Reporting Structure

5.4. Standards and best practices

5.5. Leadership and Ethics

5.6. EC-Council Code of Ethics

6. Introduction to Risk Management

3.1. Organizational Structure

3.2. Where does the CISO fit within the organizational structure

3.3. The Executive CISO

3.4. Nonexecutive CISO

PECB CISO Description: By obtaining the PECB Chief Information Security Officer certification, you will develop the professional knowledge to plan and oversee the implementation of an information security program, and, in turn, ensure that an organization's confidential information is protected from disclosure.

Topics Covered:

1. **Day 1 Fundamentals of information security and the role of a CISO**
   - Training course objectives and structure
   - Fundamentals of information security
   - Chief information security officer (CISO)
   - Information security program
2. **Day 2 Information security compliance program, risk management, and security architecture and design**
   - Information security compliance program
   - Analysis of the existing information security capabilities
   - Information security risk management
   - Security architecture and design
3. **Day 3 Security controls, incident management, and change management**
   - Information security controls
   - Information security incident management
   - Change management
4. **Day 4 Information security awareness, monitoring and measurement, and continual improvement**
   - Awareness and training programs
   - Monitoring and measurement h
   - Assurance program
   - Continual improvement
   - Closing of the training course
5. **Day 5 Certification Exam**

Exam Information: The CCISO course includes an exam voucher and one retake. The CCISO exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers. The PECB CISO course comes with the exam.

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course and taking the exams will be emailed after purchase.

Link to EC-Council Brochure: https://www.eccouncil.org/wp-content/uploads/2023/07/CCISO-brochure-V.11-1.pdf

Link to PECB Brochure: https://pecb.com/pdf/brochures/4/chief-information-security-officer-4p.pdf

Computer Hacking Forensics Investigator Blended Bundle

SKU: EC-Council-33

MSRP Bundle Price: $3,999

Sale Bundle Price: $3,899

High-level description: The Computer Hacking Forensics Investigator (CHFI) certification blended bundle program is designed to equip IT professionals with the skills to identify, track, and prosecute cybercriminals. This course covers the forensic investigation process, tools, and techniques used to gather and analyze digital evidence. It includes ITI's customer CHFI Self-Paced Online ILT course and labs, as well as EC-Council's official live and self-paced CHFI course, in addition to their online self-paced Mobile Forensics, Malware and Memory Forensics, and Dark Web courses:

Course Delivery:

- **Official EC-Council CHFI:** Live Online ILT
    - **Contact us to schedule.**
- **Official EC-Council CHFI:** Self-paced Online ILT
- **Official EC-Council Certified Incident Handler (ECIH):** Self-paced Online ILT
- **Official EC-Council Mobile Forensics:** Self-paced Online ILT
- **Official EC-Council Malware and Memory Forensics:** Self-paced Online ILT
- **Official EC-Council Dark Web:** Self-paced Online ILT
- **ITI Custom CHFI:** Self-paced Online ILT

Duration:

- **Official EC-Council CHFI (Live):** 5 Days
- **Official EC-Council CHFI (Self-paced):** 5 Days
- **Official EC-Council Certified Incident Handler:** 3 Days
- **Official EC-Council Mobile Forensics:** 1 Day
- **Official EC-Council Malware and Memory Forensics:** 1 Day
- **Official EC-Council Dark Web:** 1 Day
- **ITI Custom CHFI: ~**4 days (30+ hours)
- **ITI Custom CEH:** ~7 days (70+ hours**)**

ITI Custom CHFI Course Description: Our CHFI course will cover the security discipline of computer forensics from a vendor-neutral perspective and work towards preparing students to become Forensic Investigators in Computer Hacking.

Topics Covered (18+ hours):

- Comprehensive understanding of computer forensics and the forensic investigation process.
- Techniques for searching and seizing digital evidence.
- Methods for analyzing and handling digital evidence.
- First responder procedures for incident management.
- Setup and operation of a forensic lab.
- Gain in-depth knowledge of hard disks, file systems, and Windows forensics.
- Data acquisition and duplication techniques.
- Recovering deleted files and partitions.
- Utilizing Access Data FTK and EnCase for forensic investigations.
- Understanding and applying steganography and password cracking techniques.
- Log correlation, network forensics, and analyzing wireless and web attacks.
- Investigating email crimes and conducting mobile investigations.
- Preparing investigative reports and serving as an expert witness.

Labs included (12+ hours):

- Understanding the Digital Forensics Profession and Investigations
- Data Acquisition
- Processing Crime and Incident Scenes
- Working with Windows and CLI Systems
- Current Digital Forensics Tools
- Linux and Macintosh File Systems
- Recovering Graphics Files
- Digital Forensics Analysis and Validation
- Virtual Machine Forensics, Live Acquisitions, and Network Forensics
- E-mail and Social Media Investigations
- Mobile Device Forensics
- Cloud Forensics
- Report Writing for High-Tech Investigations
- Expert Testimony in Digital Investigations
- Ethics for the Expert Witness

ITI Custom CEH Course Description: Our course offers CEH training to provide you with the tools to research, discover and scan targets, analyze vulnerabilities and test attack methods and tools. The focus of this CEH online training course is to solve the challenge of breaking into a target network, collect evidence of success, and escape unnoticed.

Topics Covered:

- Introduction to the key concepts of ethical hacking and information security.
- Conducting footprinting and reconnaissance using advanced tools and techniques.
- Scanning networks and identifying vulnerabilities.
- Performing system hacking and exploiting operating systems.
- Understanding malware threats and implementing countermeasures.
- Utilizing social engineering techniques and tools.
- Executing Denial-of-Service (DoS) and session hijacking attacks.
- Evading IDS, firewalls, and honeypots.
- Hacking web servers and applications.
- Performing SQL injection and securing databases.
- Hacking wireless networks and mobile platforms.

- Exploring IoT and OT hacking methodologies.
- Securing cloud environments and implementing cryptographic techniques.

Labs included (15 hours):

- Footprinting and Reconnaissance Techniques
- Network Reconnaissance Techniques
- Enumeration Reconnaissance Techniques
- Vulnerability Analysis Tools & Techniques
- System Hacking Methodologies
- Malware Threat Concepts
- Network Sniffing Techniques
- Social Engineering Exploits
- Denial of Service Attacks
- Session Hijacking Concepts
- Compromising Web Servers
- Web Application Hacking
- SQL Injection Methodologies
- Introduction to Cloud Computing
- Cryptography Techniques

Official EC-Council CHFI Course Description: Enhance your investigative skills with the CHFI course, which provides 40 hours of content focusing on digital forensics. This course covers the essentials of computer forensics, including the investigation process, tools, and techniques for analyzing digital evidence.

Topics Covered:

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-Forensics Techniques
- Operating System Forensics
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics

- Malware Forensics
- Investigative Reports

Mobile Forensics:
Gain expertise in performing forensic investigations on mobile devices. This course covers data acquisition, analysis, and recovery techniques specific to mobile platforms, ensuring thorough and accurate investigations.

Topics Covered:

- Introduction to Mobile Forensics
- Understanding Mobile Device Architecture
- Data Acquisition from Mobile Devices
- Analyzing Mobile Device Data
- Mobile Forensics Tools and Techniques
- Recovering Deleted Data from Mobile Devices
- Mobile Application Forensics
- Reporting and Documentation

Malware and Memory Forensics:
Learn advanced techniques to analyze and investigate malware within system memory. This course provides deep insights into identifying malicious activities and understanding the impact of malware on system memory.

Topics Covered:

- Fundamentals of Malware Forensics
- Memory Acquisition and Analysis
- Identifying Malicious Code in Memory
- Techniques for Memory Forensics
- Analyzing Memory Artifacts
- Tools for Malware and Memory Forensics
- Investigating Memory-based Attacks
- Reporting and Documentation

Dark Web:
Understand the complexities of the Dark Web, including how to navigate, investigate,

and analyze activities within this hidden part of the internet. This course equips you with the skills needed to perform investigations and gather intelligence from the Dark Web.

Topics Covered:

- Introduction to the Dark Web
- Navigating the Dark Web
- Understanding Dark Web Marketplaces
- Tools and Techniques for Dark Web Investigations
- Collecting Intelligence from the Dark Web
- Analyzing Dark Web Activities
- Dark Web Forensics Tools
- Reporting and Documentation

Exam Information: The courses include exam voucher. The EC-Council exams can be taken online through the EC-Council's remote proctoring service or at authorized testing centers. The CHFI does come with an exam retake (additional voucher if needed)

License Information: One license provides access to all courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Certified Network Defender – CND and CEH Blended Bundle

SKU: EC-Council-105

MSRP: $3699

Sales Price: $3499

High-level description: The Certified Network Defender (CND) certification blended bundle program is designed to teach IT professionals the skills needed to protect, detect, and respond to network security threats. This course covers network security controls, protocols, perimeter appliances, secure VPN implementation, IDS/IPS, network traffic signature analysis, and vulnerability scanning. The Network Defender Program includes the complete Ethical Hacker Core Skills (EHCS) course, providing a solid security foundation, with detailed traffic analysis at the packet and binary level. The bundle also includes ITI's custom CEH Self-paced Online ILT course.

Course Delivery:

- Official EC-Council CND: Live Online ILT

    - Contact us to schedule
- Official EC-Council CND: Self-paced Online ILT
- Official EC-Council EHCS: Self-paced Online ILT
- ITI Custom CEH: Self-paced Online ILT

Duration:

- Official EC-Council CND: 5 Days
- Official EC-Council EHCS: 2 Days
- ITI Custom CEH: ~7 Days (70+ hours)

ITI Custom CEH Course Description:

Our course offers CEH training to provide you with the tools to research, discover, and scan targets, analyze vulnerabilities, and test attack methods and tools. The focus of this CEH online training course is to solve the challenge of breaking into a target network, collect evidence of success, and escape unnoticed.

Topics Covered:

- Introduction to the key concepts of ethical hacking and information security.
- Conducting footprinting and reconnaissance using advanced tools and techniques.
- Scanning networks and identifying vulnerabilities.
- Performing system hacking and exploiting operating systems.
- Understanding malware threats and implementing countermeasures.
- Utilizing social engineering techniques and tools.
- Executing Denial-of-Service (DoS) and session hijacking attacks.
- Evading IDS, firewalls, and honeypots.
- Hacking web servers and applications.
- Performing SQL injection and securing databases.
- Hacking wireless networks and mobile platforms.
- Exploring IoT and OT hacking methodologies.
- Securing cloud environments and implementing cryptographic techniques.

Labs included (15 hours):

- Footprinting and Reconnaissance Techniques
- Network Reconnaissance Techniques
- Enumeration Reconnaissance Techniques
- Vulnerability Analysis Tools & Techniques
- System Hacking Methodologies
- Malware Threat Concepts
- Network Sniffing Techniques
- Social Engineering Exploits
- Denial of Service Attacks
- Session Hijacking Concepts
- Compromising Web Servers
- Web Application Hacking
- SQL Injection Methodologies
- Introduction to Cloud Computing
- Cryptography Techniques

Official EC-Council CND Course Description:

Enhance your network defense skills with our CND course, which provides 40 hours of content focusing on network security. This course covers the essentials of network defense, from designing secure network architectures to implementing and managing security controls.

Topics Covered:

- Network Security Fundamentals
- Network Security Threats, Vulnerabilities, and Attacks
- Network Security Controls
- Network Security Policy Design and Implementation
- Physical Security
- Host Security
- Secure Firewall Configuration and Management

- Secure IDS Configuration and Management
- Secure VPN Configuration and Management
- Wireless Network Defense
- Network Traffic Monitoring and Analysis
- Network Incident Response and Management

Official EC-Council EHCS Course Description:

The Ethical Hacking Core Skills (EHCS) course provides the foundational skills required for advanced security training. This course includes hands-on exercises to master TCP/IP protocols, Unix/Linux survival skills, vulnerability assessment, and the hacking methodology.

Topics Covered:

- Foundations of Security
- In-depth TCP/IP Protocol Knowledge
- Packet Analysis
- Advanced Protocol Analysis Techniques
- Unix and Linux Skills
- Vulnerability Assessment
- Hacking Methodology
- Building Virtual Labs

Objectives:

- Explain security foundations
- Analyze network packets for irregularities
- Detect crafted packets
- Perform advanced protocol analysis
- Conduct vulnerability assessments
- Build and use virtual labs

Exam Information: The course includes an exam voucher and retake for the CND exam. The CND exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the CND course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Link to brochure: CND Brochure
Link to EHCS course: EHCS Course

Certified SOC and Incident Handling Bundle

SKU: EC-Council-106

MSRP: $3999

Sales Price: $3799

High-level description: The SOC and Incident Handling Bundle equips current and aspiring SOC analysts with the skills needed to excel in today's cybersecurity landscape. This comprehensive program includes the Certified SOC Analyst (CSA), Certified Threat Intelligence Analyst (CTIA), EC-Council Incident Handler (ECIH), and CompTIA CySA+ certifications. The bundle covers foundational concepts, SOC operations, log management, SIEM deployment, advanced incident detection, threat intelligence, and incident response, delivered through a blend of live online and self-paced training by industry experts.

Course Delivery:

- **Official EC-Council ECIH:** Live Online ILT
    - **Contact us to schedule**
- **Official EC-Council CSA:** Self-paced Online ILT
- **Official EC-Council CTIA:** Self-paced Online ILT
- **ITI Custom CompTIA CySA+:** Self-paced Online ILT
- **Official CompTIA CySA+:** Self-paced Online ILT

Duration:

- **Official EC-Council CSA (Live):** 3 Days
- **Official EC-Council CSA (Self-paced):** 3 Days
- **Official EC-Council CTIA (Self-paced):** 2 Days
- **ITI Custom CompTIA CySA+ (Self-paced):** ~ 2.5 days (18 hours)
- **Official CompTIA CySA+ (Self-paced):** ~ 3 days

ITI Custom CompTIA CySA+ : Gain expertise in cybersecurity analytics with our CompTIA CySA+ course, covering essential concepts and practices.

Course Highlights:

- Duration: 6+ hours
- Content: 80+ On-demand Videos
- Exam Prep: 100Prep Questions
- Certificate of Completion for CompTIA CySA+

Topics Areas Included:

- Threat and Vulnerability Management
- Software and Systems Security
- Security Operations and Monitoring
- Incident Response
- Compliance and Assessment

Modules:

- Module 1 - CompTIA CySA+ CS0-003 Basics
- Module 2 - CompTIA CySA+ CS0-003 Domain 1 - Security Operations
- Module 3 - CompTIA CySA+ CS0-003 Domain 2 - Vulnerability Management
- Module 4 - CompTIA CySA+ CS0-003 Domain 3 - Incident Response and Management
- Module 5 - CompTIA CySA+ CS0-003 Domain 4 - Reporting and Communication
- Module 6 - CompTIA CySA+ CS0-003 - Course Closeout

Labs Included (12 hours):

- System & Network Security Implementation Concepts
- Threat Intelligence & Threat Gathering Concepts
- Techniques to Determine Malicious Activity
- Vulnerability Scanning Tools & Techniques
- Identifying & Analyzing Malicious Activity
- Tools for Identifying Malicious Activity

- Attack Methodology Frameworks
- Vulnerability Data Analysis and Prioritization
- Incident Response Management Techniques
- Incident Response Communication & Reporting
- Vulnerability Reporting Concepts
- Vulnerability Patching & Attack Surface Management

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA CySA+ (CS0-003) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Understanding Vulnerability Response, Handling, and Management
- Lesson 2: Exploring Threat Intelligence and Threat Hunting Concepts
- Lesson 3: Explaining Important System and Network Architecture Concepts
- Lesson 4: Understanding Process Improvement in Security Operations
- Lesson 5: Implementing Vulnerability Scanning Methods
- Lesson 6: Performing Vulnerability Analysis
- Lesson 7: Communicating Vulnerability Information
- Lesson 8: Explaining Incident Response Activities
- Lesson 9: Demonstrating Incident Response Communication
- Lesson 10: Applying Tools to Identify Malicious Activity
- Lesson 11: Analyzing Potentially Malicious Activity
- Lesson 12: Understanding Application Vulnerability Assessment
- Lesson 13: Exploring Scripting Tools and Analysis Concepts
- Lesson 14: Understanding Application Security and Attack Mitigation Best Practices

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configuring Controls
- Assisted Lab: Reviewing IoC and Threat Intelligence Sources
- Assisted Lab: Performing Threat Hunting
- Assisted Lab: Configuring Centralized Logging
- APPLIED LAB: Performing System Hardening
- Assisted Lab: Assess Time Synch Errors
- Assisted Lab: Configuring Automation
- Assisted Lab: Performing Asset Discovery
- Assisted Lab: Performing Vulnerability Scanning
- Assisted Lab: Performing Passive Scanning
- Assisted Lab: Establishing Context Awareness

- Assisted Lab: Analyzing Vulnerability Reports
- Assisted Lab: Detecting Legacy Systems
- APPLIED LAB: Performing Post-Incident Forensic Analysis
- APPLIED LAB: Performing IoC Detection and Analysis
- ADAPTIVE LAB: Performing Playbook Incident Response
- APPLIED LAB: Collecting Forensic Evidence
- Assisted Lab: Performing Root Cause Analysis
- APPLIED LAB: Using Network Sniffers
- APPLIED LAB: Researching DNS and IP Reputation
- Assisted Lab: Using File Analysis Techniques
- Assisted Lab: Analyzing Potentially Malicious Files
- Assisted Lab: Using Nontraditional Vulnerability Scanning Tools
- APPLIED LAB: Performing Web Vulnerability Scanning
- Assisted Lab: Exploiting Weak Cryptography
- Assisted Lab: Performing and Detecting Directory Traversal and Command Injection
- Assisted Lab: Performing and Detecting Privilege Escalation
- Assisted Lab: Performing and Detecting XSS
- Assisted Lab: Performing and Detecting LFI/RFI
- Assisted Lab: Performing and Detecting SQLi
- Assisted Lab: Performing and Detecting CSRF
- APPLIED LAB: Detecting and Exploiting Security Misconfiguration

CSA Description: Prepare for a career in a Security Operations Center (SOC) with our CSA course, which provides 24 hours of content focusing on SOC operations. This course covers the essentials of working in a SOC, from understanding SOC infrastructure to performing advanced incident detection and response. The lab-intensive CSA program emphasizes the holistic approach to deliver advanced knowledge of how to identify and validate intrusion attempts.

Topics Covered:

- Introduction to SOC
- Understanding Cyber Threats, IoCs, and Attack Methodologies
- Incident Detection with SIEM
- Incident Response
- Threat Intelligence, Threat Modeling, and Threat Hunting
- Post Incident Response

Exam Information: The course includes an exam voucher. The CSA exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the CSA course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Link to brochure: And

CTIA Description: This course covers the fundamentals of threat intelligence, including its types, lifecycle, strategy, and frameworks. It explores various cybersecurity threats and attack frameworks such as APTs, Cyber Kill Chain, MITRE ATT&CK, and Diamond Model. Participants will learn the steps involved in planning a threat intelligence program, data collection methods, and processing techniques. The course also delves into threat data analysis, threat modeling, creating and sharing intelligence reports, threat hunting, and using Python scripting for automation and intelligence sharing in SOC operations and incident response.

Topics Covered:

- Introduction to Threat Intelligence
- Cyber Threats and Attack Frameworks
- Requirements, Planning, Direction, and Review
- Data Collection and Processing
- Data Analysis
- Intelligence Reporting and Dissemination
- Threat Hunting and Detection
- Threat Intelligence in SOC Operations, Incident Response, & Risk Management

Exam Information: The course includes an exam voucher. The CTIA exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the CTIA course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

ECIH Description: Prepare for effective incident handling with our ECIH course, which provides 24 hours of content focusing on incident management. This course covers the essentials of incident handling, from identifying security incidents to responding and recovering from them.

Topics Covered:

- Introduction to Incident Handling and Response
- Incident Handling and Response Process
- Forensic Readiness and First Response
- Incident Handling Tools and Techniques
- Incident Handling Policies and Laws
- Risk Assessment
- Handling Different Types of Incidents
- Incident Recovery Techniques

Exam Information: Each course includes an exam voucher. The EC-Council exams can be taken online through the EC-Council's remote proctoring service or at authorized testing centers and CompTIA exams can be taken online through Pearson VUE.

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Risk Management Approach and Practices – RM and PMI Risk Management Professional (PMI-RMP) Bundle

SKU: EC-Council-105

MSRP: $1499

Sales Price: $1299

High-level Description:
The Risk Management Certification Bundle combines the EC-Council Risk Management Approach and Practices (RM) course with the ITI Custom PMI-RMP course. This comprehensive bundle is designed to equip IT professionals and risk management professionals with the skills needed to effectively identify, assess, and manage risks within an organization. The program covers both IT-focused risk management strategies and broader project management risk practices.

EC-Council Risk Management Approach and Practices (RM) Course

Duration: 3 Days (24 Hours)

Course Description:
The Risk Management Approach and Practices (RM) certification offers a standardized framework for identifying, assessing, and managing risks within an organization. This course introduces participants to common risk management practices and frameworks used globally, focusing on comprehending potential threats, opportunities, their implications, and efficient management techniques.

Topics Covered:

- Introduction to Risk Management
- The Essentials of a Risk Management Program
- Risk Management Frameworks
- Risk Management Policies and Procedures
- Risk-Based Audits
- Third-Party Risk Management (TPRM)
- Risk Management Positions and Laws
- Procurement Risk Management
- Risk Culture
- Future of Risk Management

Learning Objectives:

1. Understand the fundamentals of risk management.
2. Learn various risk identification techniques.
3. Familiarize with risk assessment methods.
4. Develop skills in formulating risk mitigation strategies.

5. Gain insights into risk monitoring and control.
6. Understand the importance of risk communication and reporting.
7. Integrate risk management practices into strategic planning.
8. Apply risk management principles to real-world scenarios.
9. Prepare for the RM certification exam.

Exam Information:
The course includes an exam voucher and retake for the EC-Council RM exam. The exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information:
One license provides access to the RM course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access:
Instructions for accessing the course will be emailed after purchase.

ITI Custom PMI-RMP Course

Duration: 8+ hours
Content: 25+ videos, 10 lessons, 100 test prep questions

Course Description:
Our ITI Custom PMI-RMP course offers comprehensive training on project risk management, providing tools to identify, assess, and control project risks. The course covers risk management concepts, processes, and best practices to prepare participants for the PMI-RMP certification exam. This training is essential for project managers looking to enhance their risk management skills and improve project success rates.

Topics Covered:

- Introduction to Risk Management Concepts
- Risk Management Planning
- Risk Identification Techniques
- Qualitative Risk Analysis
- Quantitative Risk Analysis
- Risk Response Planning
- Risk Monitoring and Control

- Risk Management in Agile Projects
- Case Studies and Practical Applications
- Exam Preparation Strategies

Course Features:

- In-depth video lectures and interactive content
- Practical exercises and real-world scenarios
- Access to expert instructors for guidance and support
- Comprehensive test prep questions to ensure exam readiness

License Information:
Access to the ITI Custom PMI-RMP course is provided for 12 months.

How to Access:
Instructions for accessing the course will be emailed after purchase.

Combined Bundle Benefits:

- Comprehensive training on both IT-focused and project management risk management practices.
- Access to expert instructors and comprehensive exam preparation materials.
- Exam voucher and retake for the EC-Council RM certification.
- Flexible online learning formats to fit your schedule and learning style.

Enhance your risk management skills and prepare for certification with this comprehensive bundle.

Certified Blockchain Professional Bundle

SKU: EC-Council-39

MSRP: $2499

Sale Price: $2299

High-level description: The EC-Council Certified Blockchain Professional (CBP) certification program is designed to equip IT professionals with the knowledge and skills required to understand and implement blockchain technology. This course covers blockchain fundamentals, blockchain development, and blockchain security. The ITI custom Blockchain 3 course bundle is ideal for anyone looking to understand and effectively communicate blockchain technology concepts. As blockchain technologies have evolved from Proof of Concept to Production use cases, skills in this area are

increasingly essential for customer-facing technical experts, such as pre-sales engineers and software engineers, especially within large VARs, Vendors, and Integrators. The bootcamp includes three courses:

1. **Certified Blockchain Developer Hyperledger (CBDH)** - Designed for technology-focused engineers and developers, this course certifies participants through the Blockchain Training Alliance.
2. **Certified Blockchain Solutions Architect (CBSA)** - This course covers the basics of blockchain, including components, terminology, and ledgers, preparing participants for the Blockchain Training Alliance Certification.
3. **Enterprise Blockchain Bootcamp for Solutions Engineers** - This training provides a comprehensive understanding of blockchain fundamentals, exploring various enterprise blockchain platforms and their use cases.

Course Delivery:

- **EC-Council CBP:** Self-paced ILT
- **ITI Custom Course:** Self-paced ILT

Duration:

- **EC-Council CBP:** 3 days
- **ITI Custom Course:** ~ 2 days (12+ hours)

Official EC-Council CBP Description: Gain expertise in blockchain technology with our CBP course, which provides 24 hours of content focusing on the fundamentals of blockchain, blockchain development, and blockchain security. This course covers the essential concepts and techniques needed to understand and implement blockchain technology.

Topics Covered:

- Lesson 1 Introduction to Blockchain Technology
- Lesson 2 Crypto Assets
- Lesson 3 Blockchain Mining
- Lesson 4 Bitcoin
- Lesson 5 Sustainable Blockchain
- Lesson 6 Open Source Blockchain Frameworks
- Lesson 7 Ethereum

- Lesson 8 Decentralized Applications (DApps)
- Lesson 9 AI and Blockchain
- Lesson 10 Impact on Industry
- Lesson 11 Industry Use Cases
- Lesson 12 IoT and Blockchain (BoT)
- Lesson 13 Blockchain Project Implementation
- Lesson 14 Scalable Blockchain
- Lesson 15 Security in Blockchain
- Lesson 16 Blockchain as a Service
- Lesson 17 Open Research Problems in Blockchain

Exam Information: The course includes an exam voucher. The CBP exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the CBP course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

ITI custom Blockchain 3 course bundle: This three-course bundle includes the following topics:

- **Certified Blockchain Developer Hyperledger (CBDH) Course Content**
  - Module 1: Certified Blockchain Developer Hyperledger Overview
  - Module 2: Hyperledger Framework
  - Module 3: Hyperledger Fabric Blockchain
  - Module 4: Access Controls and Secure Chaincode
  - Module 5: Plan and Prepare Apps for Deployment
  - Module 6: Hyperledger Fabric Explorer
  - Module 7: Chaincode and Development
  - Module 8: Course Wrap Up
- Certified Blockchain Solutions Architect (CBSA) Course Content
  - Module 1: Certified Blockchain Solutions Architect Overview
  - Module 2: Blockchain 101 Terminology and Components
  - Module 3: Exam Objectives
  - Module 4: Hyperledger
  - Module 5: Ethereum
  - Module 6: Course Closeout

- Enterprise Blockchain Bootcamp for Solutions Engineers Course Content
  - Module 1: Course Overview
  - Module 2: Pre-Sales Activities
  - Module 3: Blockchain Fundamentals
  - Module 4: Enterprise Blockchains
  - Module 5: Use Cases
  - Module 6: Course Closeout

License Information: One license provides access to the bundle of ITI courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

EC-Council Certified Cloud Security Engineer and CompTIA Secure Cloud Professional Bundle

SKU: EC-Council-35

MSRP: $3999

Sales Price: $3799

High-level description: The EC-Council Certified Cloud Security Engineer (CCSE), CompTIA Secure Cloud Professional, AWS Cloud Practitioner and Azure Administrator Bundle is designed to equip IT and cybersecurity professionals with comprehensive skills to secure cloud environments. This program covers essential cloud security concepts, cloud architecture, cloud security operations, and cloud security compliance. The bundle includes both the EC-Council Certified Cloud Security Engineer (CCSE) certification course in Self-paced online format and the ITI custom CompTIA Secure Cloud Professional courses (Security+ and Cloud+) self-paced ILT online training and labs, as well as the official CompTIA CertMaster learning and integrated labs, providing a well-rounded education in cloud security. The bundle also includes ITI's custom self-paced ITL online AWS Cloud Practitioner and Azure Administrator courses and labs.

CCSE Description: Enhance your cloud security skills with our official EC-Council CCSE course, which provides 32 hours of content focusing on securing cloud environments. This course covers the essential components of cloud security, including architecture, operations, and compliance.

Topics Covered:

- Introduction to Cloud Security
- Cloud Security Architecture
- Cloud Security Operations

- Identity and Access Management in the Cloud
- Cloud Data Security
- Cloud Security Compliance
- Cloud Security Risk Management

Exam Information: The course includes an exam voucher and retake. The CCSE exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the CCSE course for 12 months.

High-level description: The CompTIA Secure Cloud Professional (Security+ / Cloud+) Bundle provides comprehensive training for individuals seeking to excel in cloud security and administration. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Security+ and Cloud+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Security+ and Cloud+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Security+ SY0-701: Develop critical security skills with our CompTIA Security+ course, designed to provide the knowledge needed to secure and protect networks and systems.

Course Highlights:

- Duration: 30+ hours
- Content: 110+ On-demand Videos
- Exam Prep: 300 Prep Questions
- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison

- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules:

- Module 1: General Security Concepts
- Module 2: Threats, Vulnerabilities, and Mitigations
- Module 3: Security Architecture
- Module 4: Security Operations
- Module 5: Security Program Management and Oversight

Labs included (17 hours):

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Mitigation Techniques
7. Security Architecture Models

8. Securing Enterprise Infrastructures
9. Data Protection Strategies
10. Resilience in Security Architecture
11. Securing Computing Resources
12. Asset Management Techniques
13. Vulnerability Management
14. Monitoring Computing Resources
15. Enhancing Enterprise Security
16. Implement Identity & Access Management
17. Implementation of Automation & Orchestration for Security Operations
18. Investigative Data Sources

CompTIA Cloud+ CV0-003: Master cloud infrastructure and services with our CompTIA Cloud+ course, covering essential cloud computing skills.

Course Highlights:

- Duration: 8+ hours
- Content: 130+ On-demand Videos
- Exam Prep: 45+ Prep Questions
- Certificate of Completion for CompTIA Cloud+ CV0-003

Topics Areas Included:

- Cloud Architecture and Design
- Cloud Security
- Cloud Deployment
- Operations and Support
- Troubleshooting

Modules:

- Module 1: CompTIA Cloud+ CV0-003 Course Overview
- Module 2: General Cloud Knowledge
- Module 3: Cloud Security

- Module 4: Cloud Deployment
- Module 5: Operations and Support
- Module 6: Troubleshooting
- Module 7: Course Closeout

Labs included (28 hours):

1. Cloud Deployment Models
2. Different Cloud Service Models
3. Cloud Resource Capacity Planning
4. High Availability and Scalability in the Cloud
5. Analyzing Business Requirements for a Cloud Solution
6. Configuring and Managing Cloud Identities
7. Cloud Networking Concepts
8. Securing Cloud Infrastructure Resources
9. Data Security and Compliance in the Cloud
10. Cloud Security Assessments and Tools
11. Incident Response Procedures
12. Cloud Solution Integration
13. Provisioning Cloud Resources
14. Provisioning Public Cloud Storage Solutions
15. Provisioning Private Cloud Storage Solutions
16. Deploying Cloud Networking Solutions
17. Virtualization Concepts and Platforms
18. Cloud Migration Techniques
19. Configuring Logging for Cloud Resources
20. Implementing Cloud Resource Monitoring Solutions
21. Implementing Cloud Resource Monitoring and Alert Solutions
22. Cloud Dashboards and Reporting

23. Cloud Patches, Upgrading and Lifecycle Management
24. Optimizing Cloud Solutions
25. Implementing Cloud Resource Automation Solutions
26. Implementing Cloud Backup and Restore Solutions
27. Cloud Disaster Recovery Concepts
28. Cloud Troubleshooting Methodologies
29. Security Troubleshooting Techniques
30. Troubleshooting Cloud Deployments
31. Cloud Networking Troubleshooting Concepts
32. Troubleshooting Cloud Resource Utilization
33. Automation and Orchestration Troubleshooting Methodologies

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Security+ (SY0-701) CertMaster Learn and Labs: CertMaster Learn is a self-paced, comprehensive online learning experience that helps you gain the knowledge and practical skills necessary to be successful on your CompTIA certification exam, and in your IT career. A Learning Plan helps you stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for you to practice and apply your skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on inputs.

When purchased with CertMaster Learn in a bundle, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis

- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Comparing Security Roles and Security Controls
- Explaining Threat Actors and Threat Intelligence
- Performing Security Assessments
- Identifying Social Engineering and Malware
- Summarizing Basic Cryptographic Concepts
- Implementing Public Key Infrastructure
- Implementing Authentication Controls
- Implementing Identity and Account Management Controls
- Implementing Secure Network Designs
- Implementing Network Security Appliances
- Implementing Secure Network Protocols
- Implementing Host Security Solutions
- Implementing Secure Mobile Solutions
- Summarizing Secure Application Concepts
- Implementing Secure Cloud Solutions
- Explaining Data Privacy and Protection Concepts
- Performing Incident Response
- Explaining Digital Forensics
- Summarizing Risk Management Concepts
- Implementing Cybersecurity Resilience
- Explaining Physical Security

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Scanning and Identifying Network Nodes

- Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
- Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- APPLIED LAB: Performing Network Reconnaissance and Vulnerability Scanning
- Assisted Lab: Managing the Lifecycle of a Certificate
- Assisted Lab: Managing Certificates with OpenSSL
- Assisted Lab: Auditing Passwords with a Password Cracking Utility
- Assisted Lab: Managing Centralized Authentication
- Assisted Lab: Managing Access Controls in Windows Server
- Assisted Lab: Configuring a System for Auditing Policies
- Assisted Lab: Managing Access Controls in Linux
- APPLIED LAB: Configuring Identity and Access Management Controls
- Assisted Lab: Implementing a Secure Network Design
- Assisted Lab: Configuring a Firewall
- Assisted Lab: Configuring an Intrusion Detection System
- Assisted Lab: Implementing Secure Network Addressing Services
- Assisted Lab: Implementing a Virtual Private Network
- Assisted Lab: Implementing a Secure SSH Server
- Assisted Lab: Implementing Endpoint Protection
- APPLIED LAB: Securing the Network Infrastructure
- Assisted Lab: Identifying Application Attack Indicators
- Assisted Lab: Identifying a Browser Attack
- Assisted Lab: Implementing PowerShell Security
- Assisted Lab: Identifying Malicious Code
- APPLIED LAB: Identifying Application Attacks
- Assisted Lab: Managing Data Sources for Incident Response
- Assisted Lab: Configuring Mitigation Controls

- Assisted Lab: Acquiring Digital Forensics Evidence
- Assisted Lab: Backing Up and Restoring Data in Windows and Linux
- APPLIED LAB: Managing Incident Response, Mitigation and Recovery

CompTIA Cloud+ (CV0-003) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow. Easy-to-use course management tools provide a comprehensive suite of instructor resources alongside a reporting dashboard, making course preparation and progress tracking simple and efficient.

Topics Covered:

- Understanding Cloud Concepts
- Planning and Designing a Cloud Environment
- Administering Cloud Resources
- Managing Cloud Storage
- Managing Networks in the Cloud
- Securing and Troubleshooting Networks in the Cloud
- Managing Cloud Migrations and Troubleshooting Cloud Deployments
- Managing Cloud Automation and Orchestration
- Understanding Cloud Security Concepts
- Managing Cloud Security
- Managing Cloud Performance
- Managing Maintenance in the Cloud

- Implementing High Availability and Disaster Recovery in the Cloud

Labs Available:

- Assisted Lab: Explore the Lab Environment
- Assisted Lab: Plan and Design a Cloud Environment
- Assisted Lab: Deploy and Manage Cloud Resources
- Assisted Lab: Manage Compute Resources
- Assisted Lab: Manage Networks in the Cloud
- Assisted Lab: Secure Cloud Components
- APPLIED LAB: Deploy Cloud Resources
- Assisted Lab: Manage Cloud Automation
- Assisted Lab: Manage Baseline Configurations
- Assisted Lab: Deploy Patches
- Assisted Lab: Configure Monitoring
- Assisted Lab: Manage Backup and Restore Processes
- APPLIED LAB: Manage Cloud Resources

Product and License Information:

- One license provides access to CertMaster Learn for Security+ and Cloud+ with CertMaster Labs integrated throughout the courses and ITI courses and labs.
- Access keys must be redeemed within 12 months of purchase.
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Security+ and Cloud+): This bundle includes an exam voucher and an exam pass guarantee for Security+ and Cloud+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

AZ-104 Microsoft Azure Administrator Certification: Prepare for the Microsoft AZ-104 Azure Administrator certification with this comprehensive course. This course covers

advanced Azure administration, including managing Azure identities and governance, implementing and managing storage, and configuring and managing virtual networks.

Course Highlights:

- Duration: 35+ Training Hours
- Content: 85+ On-demand Videos, covering Azure administration topics
- Preparation Questions: 200

Modules:

- Module 1 – Overview: Azure Essentials for Success
- Module 2 – Tools: Navigating the Azure Ecosystem
- Module 3 – Identities and Governance: Secure and Efficient Identity Management
- Module 4 – Master Data Storage and Security
- Module 5 – Compute Resources: Unlock the Power of Azure Compute
- Module 6 – Virtual Networks: Connect and Secure Your Resources
- Module 7 – Monitoring and Backup: Ensure Stability and Recovery

Labs included (8 hours):

- Azure Management Concepts Lab (3 Hours):
  - Azure Service Level Agreements (SLAs)
  - Management Tools
  - Monitoring Tools
  - The Azure Marketplace
- Azure Storage Management Lab (2 Hours):
  - Azure Storage Services
  - Working with Blobs
  - Azure SQL Databases
  - Azure Cosmos Databases
- Azure Security Concepts Lab (3 Hours):
  - Using Azure Key Vault

- Security Tools
- Network Security

AWS Certified Cloud Practitioner Course Description: Prepare for foundational knowledge of AWS Cloud concepts, services, and best practices, serving as a prep course for the AWS DevOps Engineering Course.

Course Highlights:

- Duration: 8+ hours
- Content: 130+ On-demand Videos
- Exam Prep: 45+ Prep Questions
- Certificate of Completion for AWS Certified Cloud Practitioner

Topics Areas Included:

- AWS Fundamentals
- AWS Security & Compliance Concepts
- AWS Security Services
- AWS Deployment Methods
- AWS Global Infrastructure
- AWS Computing Services
- AWS Storage Services
- AWS Networking Services
- AWS Database Services

Labs Included (8+ hours):

1. AWS Fundamentals
2. AWS Security & Compliance Concepts
3. AWS Security Services
4. AWS Deployment Methods
5. AWS Global Infrastructure
6. AWS Computing Services
7. AWS Storage Services

8. AWS Networking Services
9. AWS Database Services

EC-Council Certified DevSecOps Engineer (ECDE), AWS DevOps and Certified Kubernetes Bundle

SKU: EC-Council-36

MSRP: $3999

Sales Price: $3799

High-level Description: This Bundle is designed to equip IT and Cybersecurity professionals with comprehensive skills in integrating security into DevOps processes and leveraging AWS and Kubernetes for DevOps. This bundle includes the ECDE certification program, covering DevSecOps concepts, tools, and practices, the AWS Certified Cloud Practitioner course for foundational AWS knowledge, the AWS DevOps Engineering course focusing on deploying and managing applications on AWS with DevOps best practices, and a comprehensive Kubernetes training series covering key certifications and skills.

Course Delivery:

- **ECDE:**
  - Self-paced Online ILT
- **AWS Certified Cloud Practitioner:**
  - Self-paced Online ILT
- **AWS DevOps Engineering:**
  - Live Online ILT (Contact us to schedule)
- **Kubernetes Training Series:**
  - Self-paced Online ILT

Duration:

- **ECDE:** 3 Days
- **AWS Certified Cloud Practitioner:** 16+ hours (2 days)
- **AWS DevOps Engineering:** 24 Hours (3 Days)
- **Kubernetes Training Series:** 11+ hours (combined for ~1.5 Days))

EC-Council Certified DevSecOps Engineer (ECDE) Course Description:

Enhance your DevSecOps skills with our ECDE course, which provides 24 hours of content focusing on integrating security into DevOps processes. This course covers essential components of DevSecOps, including tools and practices for securing the development pipeline. This course is blended with both theoretical knowledge as well as the practical implementation of DevSecOps in your on-prem and cloud-native (AWS and Azure) environment. The course covers integration and automation of all the major and widely used tools, processes, and methodologies of DevSecOps that help organizations to build secure applications rapidly in a DevOps environment.

Topics Covered:

- Introduction to DevSecOps
- DevSecOps Frameworks
- Security as Code
- Continuous Integration and Continuous Deployment (CI/CD)
- Secure Coding Practices
- Monitoring and Logging
- Automated Security Testing
- Container Security
- Incident Response and Recovery

Exam Information: The course includes an exam voucher. The ECDE exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the ECDE course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

AWS Certified Cloud Practitioner Course Description:

Prepare for foundational knowledge of AWS Cloud concepts, services, and best practices, serving as a prep course for the AWS DevOps Engineering Course.

Course Highlights:

- Duration: 8+ hours
- Content: 130+ On-demand Videos
- Exam Prep: 45+ Prep Questions

- Certificate of Completion for AWS Certified Cloud Practitioner

Topics Areas Included:

- AWS Fundamentals
- AWS Security & Compliance Concepts
- AWS Security Services
- AWS Deployment Methods
- AWS Global Infrastructure
- AWS Computing Services
- AWS Storage Services
- AWS Networking Services
- AWS Database Services

Labs Included (8+ hours):

10. AWS Fundamentals
11. AWS Security & Compliance Concepts
12. AWS Security Services
13. AWS Deployment Methods
14. AWS Global Infrastructure
15. AWS Computing Services
16. AWS Storage Services
17. AWS Networking Services
18. AWS Database Services

AWS DevOps Engineering Course Description:

The AWS DevOps Engineering course is designed to teach IT professionals the skills needed to develop, deliver, and maintain applications and services at high velocity on AWS. This course focuses on Continuous Integration (CI), Continuous Delivery (CD), microservices, and more.

Course Highlights:

- Duration: 24 Hours of Live Interactive Trainer-Led Sessions

- Mentorship by Amazon Certified Trainers
- AWS Certified DevOps Engineer – Professional Exam Prep
- Master AWS Cloud9 to Write, Run, and Debug Code
- Build Infrastructure that Supports DevOps Projects
- Automate Building, Testing, and Packaging of Code

Topics Covered:

1. Introduction to DevOps on AWS
2. Implementing Continuous Integration and Continuous Delivery (CI/CD) Pipelines
3. Automating Infrastructure with AWS CloudFormation and AWS CLI
4. Deploying Applications using AWS Elastic Beanstalk, Amazon ECS, and Kubernetes
5. Monitoring and Logging using Amazon CloudWatch, AWS CloudTrail, and AWS X-Ray
6. Implementing Security and Compliance Automation
7. Managing Microservices with Docker and Kubernetes on AWS
8. Optimizing Infrastructure for Cost and Performance

Course Delivery:

- Live Online ILT (Contact us to schedule)

Kubernetes Training Series:

Gain in-depth knowledge on deploying, managing, and scaling containerized applications using Kubernetes. This training series includes three comprehensive courses:

Total Training: 11+ hours, 25+ topics, 200+ videos, and 60 exam prep questions.

1. **Certified Kubernetes Administrator (CKA): Topics Covered:**
    - Kubernetes Architecture
    - Installation and Configuration
    - Workloads and Scheduling
    - Services and Networking
    - Storage

- Troubleshooting

2. **Certified Kubernetes Application Developer (CKAD): Topics Covered:**
    - Kubernetes Fundamentals
    - Building and Managing Kubernetes Applications
    - Configuring Kubernetes Applications
    - Kubernetes Application Troubleshooting
    - Helm and Operators
3. **Kubernetes – Containerizing Applications in the Cloud: Topics Covered:**
    - Introduction to Containers
    - Container Orchestration
    - Managing Containerized Applications
    - Kubernetes and Cloud Integration
    - Advanced Kubernetes Features

Combined Bundle Benefits:

- Comprehensive training on DevSecOps, AWS Cloud Practitioner, AWS DevOps, and Kubernetes practices.
- Access to expert instructors and comprehensive exam preparation materials.
- Exam voucher and retake for the EC-Council ECDE certification.
- Flexible online learning formats to fit your schedule and learning style.

Enhance your DevOps and cloud security skills and prepare for certification with this comprehensive bundle.

EC-Council Certified DevSecOps Engineer and Microsoft Certified: DevOps Engineer Expert and Kubernetes Bundle

SKU: EC-Council-37

MSRP: $3999

Sales Price: $3799

High-level Description: This Bundle is designed to equip IT and Cybersecurity professionals with comprehensive skills in integrating security into DevOps processes and leveraging Azure and Kubernetes for DevOps. This comprehensive online course

bundle is designed for IT professionals seeking to enhance their skills in DevOps, cloud administration, and containerization. It includes self-paced EC-Council Certified DevSecOps Engineer training, equipping you with essential DevSecOps practices and methodologies. Additionally, you'll gain proficiency in managing and administering Azure environments through the self-paced Microsoft Azure Administrator course. The bundle also features a live, instructor-led course on Designing and Implementing Microsoft DevOps Solutions, offering hands-on experience in deploying DevOps strategies. Finally, you will master containerization with self-paced courses on Certified Kubernetes Administrator (CKA), Certified Kubernetes Application Developer (CKAD), and Kubernetes Container – Containerizing Apps in the Cloud, ensuring you are well-versed in deploying and managing containerized applications in cloud environments.

Course Delivery:

- **ECDE:**
  - Self-paced Online ILT
- **Azure Administrator:**
  - Self-paced Online ILT
- **Designing and Implementing Microsoft DevOps Solutions:**
  - Live Online ILT (Contact us to schedule)
- **Kubernetes Training Series:**
  - Self-paced Online ILT

Duration:

- **ECDE:** 3 Days
- **Azure Administrator (AZ-104):** 40+ hours (5 days)
- **Designing and Implementing Microsoft DevOps Solutions (AZ-400):** 40 Hours (5 Days)
- **Kubernetes Training Series:** 11+ hours (combined for ~1.5 Days))

EC-Council Certified DevSecOps Engineer (ECDE) Course Description:

Enhance your DevSecOps skills with our ECDE course, which provides 24 hours of content focusing on integrating security into DevOps processes. This course covers essential components of DevSecOps, including tools and practices for securing the development pipeline. This course is blended with both theoretical knowledge as well as the practical implementation of DevSecOps in your on-prem and cloud-native (AWS and Azure) environment. The course covers integration and automation of all the major

and widely used tools, processes, and methodologies of DevSecOps that help organizations to build secure applications rapidly in a DevOps environment.

Topics Covered:

- Introduction to DevSecOps
- DevSecOps Frameworks
- Security as Code
- Continuous Integration and Continuous Deployment (CI/CD)
- Secure Coding Practices
- Monitoring and Logging
- Automated Security Testing
- Container Security
- Incident Response and Recovery

Exam Information: The course includes an exam voucher. The ECDE exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the ECDE course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

AZ-104 Microsoft Azure Administrator Certification: Prepare for the Microsoft AZ-104 Azure Administrator certification with this comprehensive course. This course covers advanced Azure administration, including managing Azure identities and governance, implementing and managing storage, and configuring and managing virtual networks.

Course Highlights:

- Duration: 35+ Training Hours
- Content: 85+ On-demand Videos, covering Azure administration topics
- Preparation Questions: 200

Modules:

- Module 1 – Overview: Azure Essentials for Success
- Module 2 – Tools: Navigating the Azure Ecosystem

- Module 3 – Identities and Governance: Secure and Efficient Identity Management
- Module 4 – Master Data Storage and Security
- Module 5 – Compute Resources: Unlock the Power of Azure Compute
- Module 6 – Virtual Networks: Connect and Secure Your Resources
- Module 7 – Monitoring and Backup: Ensure Stability and Recovery

Labs included (8 hours):

- Azure Management Concepts Lab (3 Hours):
  - Azure Service Level Agreements (SLAs)
  - Management Tools
  - Monitoring Tools
  - The Azure Marketplace
- Azure Storage Management Lab (2 Hours):
  - Azure Storage Services
  - Working with Blobs
  - Azure SQL Databases
  - Azure Cosmos Databases
- Azure Security Concepts Lab (3 Hours):
  - Using Azure Key Vault
  - Security Tools
  - Network Security

Exam AZ-400: Designing and Implementing Microsoft DevOps Solutions Course Description:

The AWS DevOps Engineering course is designed to teach IT professionals the skills needed to develop, deliver, and maintain applications and services at high velocity on AWS. This course focuses on Continuous Integration (CI), Continuous Delivery (CD), microservices, and more.

Prerequisites: AZ-104 Microsoft Azure Administrator Certification or AZ-204 Microsoft Certified: Azure Developer Associate

Course Highlights:

- Coaching by the Best Microsoft Certified Trainers
- 40 Hours of Live, Instructor-Led Sessions
- Latest, Up-To-Date Curriculum, Approved by Microsoft
- Access to a Digital Library of Learning Resources
- Enhanced Knowledge of Core Azure Services
- Mix of Classroom Sessions and Hands-on Training

Topics Covered:

1. Planning for DevOps
2. Getting Started with Source Control
3. Managing Technical Debt
4. Working with Git for Enterprise DevOps
5. Configuring Azure Pipelines
6. Implementing Continuous Integration using Azure Pipelines
7. Managing Application Configuration and Secrets
8. Implementing Continuous Integration with GitHub Actions
9. Designing and Implementing a Dependency Management Strategy
10. Designing a Release Strategy
11. Implementing Continuous Deployment using Azure Pipelines
12. Implementing an Appropriate Deployment Pattern
13. Managing Infrastructure and Configuration using Azure Tools
14. Third Party Infrastructure as Code Tools Available with Azure
15. Managing Containers using Docker
16. Creating and Managing Kubernetes Service Infrastructure
17. Implementing Feedback for Development Teams
18. Implementing System Feedback Mechanisms
19. Implementing Security in DevOps Projects
20. Validating Code Bases for Compliance

Course Delivery:

- Live Online ILT (Contact us to schedule)

Kubernetes Training Series:

Gain in-depth knowledge on deploying, managing, and scaling containerized applications using Kubernetes. This training series includes three comprehensive courses:

Total Training: 11+ hours, 25+ topics, 200+ videos, and 60 exam prep questions.

1. **Certified Kubernetes Administrator (CKA): Topics Covered:**

- Kubernetes Architecture
- Installation and Configuration
- Workloads and Scheduling
- Services and Networking
- Storage
- Troubleshooting

2. **Certified Kubernetes Application Developer (CKAD): Topics Covered:**
   - Kubernetes Fundamentals
   - Building and Managing Kubernetes Applications
   - Configuring Kubernetes Applications
   - Kubernetes Application Troubleshooting
   - Helm and Operators
3. **Kubernetes – Containerizing Applications in the Cloud: Topics Covered:**
   - Introduction to Containers
   - Container Orchestration
   - Managing Containerized Applications
   - Kubernetes and Cloud Integration
   - Advanced Kubernetes Features

Combined Bundle Benefits:

- Comprehensive training on DevSecOps, AWS Cloud Practitioner, AWS DevOps, and Kubernetes practices.
- Access to expert instructors and comprehensive exam preparation materials.
- Exam voucher and retake for the EC-Council ECDE certification.
- Flexible online learning formats to fit your schedule and learning style.

Enhance your DevOps and cloud security skills and prepare for certification with this comprehensive bundle.

Exam Information: The Microsoft and Kubernetes courses do not include exam vouchers; to schedule a Microsoft exam, visit Microsoft's official certification page and follow the instructions to register through an authorized testing center, while

Kubernetes exams (like CKA or CKAD) are scheduled through the Linux Foundation's website, where candidates can select an online proctoring option.

License Information: One license provides access to the Azure Administrator and Kubernetes courses for 12 months. Access keys must be redeemed within 12 months of purchase. Contract us to schedule the **Exam AZ-400: Designing and Implementing Microsoft DevOps Solutions Course.**

How to Access: Instructions for accessing the course will be emailed after purchase.

Public Sector Training

Our Public Sector Training is an integral component of our Government Training Center of Excellence, dedicated to fostering a highly skilled workforce within government organizations. This center focuses on delivering comprehensive training programs aligned with industry standards and frameworks, ensuring that personnel are well-equipped to address the evolving challenges of cybersecurity and information assurance.

We enhance the skills and capabilities of government organizations through specialized training programs aligned with the National Initiative for Cybersecurity Education (NICE) and the Department of Defense Cyber Workforce Framework (DCWF). Our offerings encompass critical workforce elements, including Cybersecurity, Intelligence (Cyberspace), Cyberspace Enablers, Cyberspace Effects, Data/AI, Software Engineering, and IT (Cyberspace). Cyberspace enablers have 4 subcategories, Leadership, Training and Education, Legal/Law Enforcement and Acquisition. Each training module is designed to meet NICE competencies, ensuring relevance and applicability to real-world scenarios.

In addition to foundational training, we offer specialized courses in advanced areas such as Malware Analysis and Reverse Engineering, empowering cybersecurity professionals to proactively identify and respond to emerging threats. By focusing on advanced technical training, we equip government employees with the necessary skills to protect critical infrastructure and enhance national security.

Recognizing that effective training is vital to mission success, our programs foster a culture of continuous improvement and adaptation. Our commitment to staying ahead of emerging technologies ensures that our training programs evolve to meet the dynamic needs of the public sector.

The DoD categories their workforce roles into Workforce Elements, and the NICE framework puts them into Workforce Categories. Each one is described below and each of our corresponding courses is listed and link to the description within this catalog.

DoD Cyber Workforce Elements Overview

Most of the DCWF roles map to a NICE work role; however, the DCWF has released new work roles with no direct mapping to NICE currently. In terms of categories and elements, there are not one-to-one matches, but the table below shows how key DCWF elements align with corresponding NICE Framework categories to reflect overlapping functional areas and competencies.

DCWF Elements	NICE Categories
IT (Cyberspace)	Operate and Maintain, Securely Provision
Cybersecurity	Protect and Defend, Oversight and Governance
Cyberspace Effects	Collect and Operate, Analyze
Intelligence (Cyberspace)	Analyze, Investigate
Cyberspace Enablers	Operate and Maintain, Oversight and Governance
Software Engineering	Securely Provision, Design and Develop
Data / Artificial Intelligence (AI)	Analyze, Securely Provision, Investigate

The Cyberspace Effects workforce element is essential for understanding the operational impacts of cyber actions. Training in this area prepares professionals to manage and respond to cyber incidents effectively, ensuring that they can analyze threats and implement strategies to mitigate risks. Our offerings equip participants with the skills necessary to excel in various roles focused on cyber operations and threat management. By integrating practical exercises and real-world scenarios, we ensure that our training is relevant and applicable to the challenges faced in today's dynamic cyber landscape. Relevant Course Bundles and Applied Micro Degrees:

- Certified Cyberspace Operator™ (CCO™)
- Certified Cyber Operations Planner™ (CCOP™)
- Certified Exploitation and Penetration Analyst™ (CEPA™)
- Certified Mission Assessment and Assurance Specialist™ (CMAAS™)
- Certified Joint Targeting Analyst™ (CJTA™)
- Certified Target Developer™ (CTD™)
- Certified Target Digital Network Analyst™ (CTDNA™)
- Certified Digital Network Exploitation Analyst™ (CDNEA™)
- Certified Host Analyst™ (CHA™)
- Certified Network Analyst Professional™ (CNAP™)
- Certified Network Technician Professional™ (CNTP™)
- Certified Target Analyst Reporter™ (CTAR™)

The IT (Cyberspace) workforce element focuses on the foundational technologies that support cyberspace operations. This area encompasses a wide range of skills necessary for effective system administration, network management, and technical operations. Our training programs ensure that professionals are well-prepared to manage complex IT environments and safeguard critical information systems. By providing hands-on experience, we equip participants with the tools they need to excel in evolving technological landscapes. Relevant Course Bundles and Applied Micro Degrees:

- Certified Enterprise Security Architect™ (CESA™)
- Certified Systems Requirements Planner™ (CSRP™)
- Certified System Testing and Evaluation Specialist™ (CSTES™)
- Certified Research & Development Specialist™ (CRDS™)
- Certified Database Administrator Professional™ (CDAP™)
- Certified Secure Knowledge Manager™ (CSKM™)
- Certified Network Operations Specialist™ (CNOS™)
- Certified Secure System Administrator™ (CSSA™)
- Certified Technical Support Systems Specialist™ (CTSSS™)
- Certified Information Systems Developer™ (CISD™)
- Certified Site Reliability Engineer™ (CSRE™)

The **Cyberspace Enablers** workforce element encompasses essential skills and knowledge that facilitate effective cybersecurity operations. This area includes training in leadership, legal aspects, and project management, ensuring that professionals are equipped to navigate the complexities of cybersecurity within their organizations. Our offerings empower participants to drive initiatives and implement strategies that enhance cybersecurity frameworks and practices across the board. Subcategories include Leadership, Training and Education, Legal/Law Enforcement, and Acquisition. Relevant Course Bundles and Applied Micro Degrees:

- Chief Information Officer Certified™ (CIOC™)
- Certified Cyber Policy and Strategy Planner™ (CCPSP™)
- Certified Cyber Curriculum Developer™ (CCCD™)
- Certified Cyber Instructor™ (CCI™)
- Certified Cyber Legal Advisor™ (CCLA™)
- Certified Executive Cyber Leader™ (CECL™)
- Certified Privacy Compliance Manager™ (CPCM™)
- Certified Program Manager™ (CPM™)
- Certified IT Project Manager™ (CITPM™)
- Certified IT Portfolio Manager™ (CITPM™)
- Certified IT Program Auditor™ (CITPA™)
- Certified Intrusion Forensic Analyst ™ (CIFA™)
- Certified Cyber Crime Forensic Investigator™ (CCCFI™)
- Certified Malware Reverse Engineer™ (CMRE™)

The **Intelligence (Cyberspace)** workforce element focuses on the critical skills required for gathering, analyzing, and applying data to inform cybersecurity operations and decision-making processes. This area prepares professionals to leverage intelligence effectively, enabling them to anticipate threats and develop proactive strategies. Our training equips participants with the necessary tools and methodologies to enhance their analytical capabilities and support organizational objectives. Relevant Course Bundles and Applied Micro Degrees:

- Certified Insider Threat Professional - Investigative Analyst™ (CITP-IGA™)
  - Note there are several sub-disciplines for this certification track.
- Certified All-Source Analyst™ (CASA™)
- Certified All-Source Collection Manager™ (CASCM™)
- Certified All-Source Collection Requirements Manager™ (CASCRM™)

- Certified Cyber Intelligence Planner Professional™ (CCIPP™)

The **Cybersecurity** workforce element is essential for protecting information systems and networks from a wide range of cyber threats. This area focuses on equipping professionals with the necessary knowledge and skills to implement effective security measures, conduct risk assessments, and respond to incidents. Our training programs empower participants to understand and navigate the complexities of cybersecurity, ensuring they can safeguard critical assets and maintain organizational integrity. Relevant Course Bundles and Applied Micro Degrees:

- Certified COMSEC Manager™ (CCM™)
- Certified Cyber Workforce Developer™ (CCWD™)
- Certified Security Control Assessor™ (CSCA™)
- Certified Cyber Authorizing Official™ (CCAO™)
- Systems Certified Security Manager™ (SCSM™)
- Certified Security Architect™ (CSA™)
- Certified Information Systems Security Developer™ (CISSD™)
- Certified Secure Software Assessor™ (CSSA™)
- Certified Cyber Defense Analyst™ (CCDA™)
- Certified Cybersecurity Defense Forensics Analyst™ (CCDFA™)
- Certified Cyber Defense Incident Responder™ (CCDIR™)
- Certified Cyber Defense Infrastructure Support Specialist™ (CCDIS™)
- Certified Control Systems Security Specialist™ (CCSSS™)

The **Data/AI** workforce element emphasizes the critical use of data analytics and artificial intelligence in enhancing cybersecurity measures and decision-making processes. Training in this area equips professionals with the skills to analyze data effectively, implement AI solutions, and understand the ethical implications of these technologies. Our offerings provide participants with the tools needed to leverage data for actionable insights, fostering innovation and improving organizational security. Relevant Course Bundles and Applied Micro Degrees:

- Certified Data Analyst Professional™ (CDAP™)
- Certified AI Adoption Specialist™ (CAIAS™)
- Certified AI Innovation Leader™ (CAIL™)
- Certified AI Risk & Ethics Specialist™ (CARES™)

- Certified AI Test & Evaluation Specialist™ (CATES™)
- Certified AI/ML Specialist™ (CAIMLS™)
- Certified Data Architect™ (CDA™)
- Certified Data Officer™ (CDO™)
- Certified Data Operations Specialist™ (CDOS™) (Azure)
- Applied Data Scientist Certified Professional (ADSCP)
- Certified Expert in Data Science Expert™ (CEDS™) (Azure)
- Certified Data Steward Analyst™ (CDSA™)
- DevSecOps Specialist Certified™ (DSC™)

The **Software Engineering** workforce element emphasizes the development of secure and efficient software systems, focusing on best practices throughout the software development lifecycle. Training in this area equips professionals with the knowledge and skills necessary to design, implement, and test software solutions that meet stringent security standards. Our offerings prepare participants to tackle the complexities of software development in today's rapidly evolving technological landscape. Relevant Course Bundles and Applied Micro Degrees:

- Certified Product Support Manager™ (CPSM™)
- Certified Secure Software Development Professional™ (CSSDP™)
- Certified Systems Security Analyst™ (CSSA™)
- Certified Product Designer User Interface (UI)™ (CPDUI™)
- Certified Product Manager Professional™ (CPMP™)
- Certified Service Designer User Experience (UX)™ (CSDUX™)
- Certified Software Test & Evaluation Specialist™ (CSTES™)
- Certified Software/Cloud Architect™ (CSCA™)

Nice Categories Overview

The NICE "**Operate and Maintain**" workforce category focuses on jobs responsible for the day-to-day maintenance and protection of IT systems, infrastructure, and data. These roles involve monitoring network and system health, responding to issues, and implementing solutions that support organizational cybersecurity and operational standards. Key tasks include performing system diagnostics, applying patches and updates, managing incident response, and ensuring that all IT assets operate securely and efficiently within established protocols.

The NICE "**Investigate**" workforce category is dedicated to roles focused on examining cybersecurity events and incidents to determine their root causes, impact, and attribution. Professionals in this category use digital forensics, data analysis, and investigative techniques to uncover evidence of malicious activities, support law enforcement, and develop intelligence on cyber threats. Key responsibilities include collecting and preserving digital evidence, analyzing data from multiple sources, and providing findings that aid in the development of proactive cybersecurity strategies.

The NICE "**Oversight and Govern**" workforce category includes roles that develop, implement, and enforce cybersecurity policies, standards, and guidelines to ensure compliance with regulatory requirements and align cybersecurity initiatives with organizational goals. Professionals in this category are responsible for establishing governance frameworks, conducting audits, and managing cybersecurity risk by evaluating program effectiveness, ensuring policy adherence, and addressing any issues in organizational cyber readiness.

The NICE "**Protect and Defend**" workforce category includes roles responsible for identifying, analyzing, and mitigating threats to information systems and networks. Professionals in this category proactively defend against cyber incidents through continuous monitoring, threat detection, vulnerability assessment, and incident response. Key activities include managing security alerts, applying threat intelligence, performing security assessments, and implementing defensive measures to safeguard organizational assets and maintain cybersecurity posture.

The NICE "**Collect and Operate**" workforce category encompasses roles focused on specialized collection and operational capabilities for cybersecurity missions. These professionals apply technical tools and techniques to gather and exploit information or insights from systems and networks, supporting intelligence, counterintelligence, and other operational objectives. Key tasks involve data collection, conducting network reconnaissance, and implementing advanced operations to meet specific mission needs.

The NICE "**Analyze**" workforce category consists of roles that focus on interpreting data to support cybersecurity decision-making. Professionals in this category apply analytical techniques to detect threats, assess risks, and provide insights that enhance cybersecurity operations. Key responsibilities include evaluating security events, understanding patterns and trends in cyber threats, and producing actionable intelligence for security measures and strategic planning.

The NICE "**Securely Provision**" workforce category includes roles that focus on designing, developing, and implementing secure IT systems, software, and infrastructure. Professionals in this category are responsible for setting up cybersecurity measures from the beginning of the system lifecycle, including secure coding, risk management, and systems engineering to prevent vulnerabilities and ensure that security is integral to system design. Key tasks involve configuring secure environments, implementing controls, and verifying compliance with security requirements throughout the development process.

Training Pathways: Practitioner, Master, Expert

Practitioner

The **Practitioner Level** is the entry point for all personnel, designed to equip participants with foundational **Knowledge, Skills, Abilities, and Tasks (KSATs)** needed across technical roles in the public sector. Accessible to individuals at any stage of their career, the Practitioner Level provides essential training that lays the groundwork for future specialization and advanced skill development.

Each ITI certification at this level results in an **applied micro degree**, awarded upon completion of a curated bundle of courses. These bundles include multiple certification courses, along with labs and hands-on exercises that build practical skills in real-world settings. This approach ensures that personnel gain applied competencies, relevant certifications, and practical experience as they progress through the Practitioner Level.

Recommended for: All personnel looking to establish or strengthen a foundational competency in technical fields such as cybersecurity, infrastructure support, and IT operations.

Master Level

The **Master Level** is a specialized track that builds on the skills acquired in the Practitioner Level. To qualify for Master-level certification, personnel must first complete the Practitioner Level. Over a dedicated three-month period, participants undergo advanced training within the **Mission Readiness Range™**, where they apply their KSATs in structured, real-world simulations and task-based scenarios. This intensive, hands-on experience prepares personnel to take on more complex challenges and specialized roles.

Requirements: Completion of the Practitioner Level and successful demonstration of applied skills over a three-month assessment period.

Recommended for: Intermediate personnel who are ready to deepen their expertise through applied learning and practical assessments across various technical fields.

Expert Level

The **Expert Level** represents the highest achievement within the ITI training framework, designed for professionals who have demonstrated advanced technical skills, strategic insight, and leadership capabilities. To qualify for the Expert certification, personnel must complete **three Practitioner certifications** in relevant foundational areas, followed by **two Master designations as defined within that certification**. This progression ensures that Expert candidates possess a broad base of knowledge and advanced, specialized competencies before undertaking Expert-level tasks.

Requirements: Completion of three Practitioner certifications, and one or two Master designations depending on the program, which encompasses completion of intensive, applied assessments in the Mission Readiness Range™.

Recommended for: Experienced professionals and leaders who are responsible for overseeing and executing advanced technical and operational strategies within government and public sector roles. Recommend 5 years of experience within the given discipline or domain.

Applied Master Micro Degree: For those that pass the requirements and achieve the expert level certification, they will also be awarded an Applied Master Micro degree.

The Expert Series represents advanced training tracks tailored to five core functional areas essential to government and critical infrastructure security. These areas structure the path for public sector personnel to develop mission-critical KSATs, preparing them to respond effectively to evolving cyber and operational challenges:

- ✓ **Expert Defensive Cyber Operations™**
- ✓ **Expert Offensive Cyber Operations™**
- ✓ **Expert Technical Support Operations™**
- ✓ **Expert Counter-Insider Threat Operations™**
- ✓ **Expert Critical Infrastructure Operations™**

Each Expert Series area builds on practitioner and master training to provide personnel with specialized, in-depth expertise. Our Mission Readiness Range™ offers a hands-on validation platform where individuals and teams apply KSATs in realistic scenarios, while the Tech Pro Library supports continuous learning and skill reinforcement, with resources available on demand.

20 Expert Certifications by Functional Area and Specialty

Each Expert Certification consists of three specialized certification bundles and includes required Master Designations. The are grouped into one of the following functional areas:

- ✓ **Expert Defensive Cyber Operations™**
- ✓ **Expert Offensive Cyber Operations™**
- ✓ **Expert Technical Support Operations™**
- ✓ **Expert Counter-Insider Threat Operations™**
- ✓ **Expert Critical Infrastructure Operations™**

Below are the 17 Expert Certifications, organized by track:

Expert Defensive Cyber Operations™

- **Defensive Cyber Operations Expert – Cyber (Defense)™ (DCOE-CD™)**
  Includes: Certified Cyber Defense Analyst™ (CCDA™), Certified Cyber Forensics Analyst™ (CCFA™), Certified Cyber Defense Incident Responder™ (CCDIR™)
- **Defensive Cyber Operations Expert – Cyber (Infrastructure)™ (DCOE-CI™)**
  Includes: Certified Cyber Defense Analyst™ (CCDA™), Certified Information Systems Security Developer™ (CISSD™), Certified Security Architect™ (CSA™)

- **Defensive Cyber Operations Expert – Cyber (Management) ™ (DCOE-CM™)**
  Includes: Certified Cyber Workforce Developer™ (CCWD™), Certified Cyber Authorizing Official™ (CCAO™), Systems Certified Security Manager™ (SCSM™)
- **Defensive Cyber Operations Expert – Cyber (Assessments)™ (DCOE-CA™)**
  Includes: Certified Cyber Defense Analyst™ (CCDA™), Certified Security Control Assessor™ (CSCA™), Certified Secure Software Assessor™ (CSSA™) or Vulnerability Assessor Certified™ (VAC™)
- **Defensive Cyber Operations Expert – Cyber (Red Team) ™ (DCOE-CR™)**
  Includes: Certified Cyber Defense Analyst™ (CCDA™), Vulnerability Assessor Certified™ (VAC™), Certified Exploitation and Penetration Analyst™ (CEPA™)
- **Defensive Cyber Operations Expert – Investigations (Analytics)™ (DCOE-IA™)**
  Includes: Certified Cyber Defense Analyst™ (CCDA™), Certified Intrusion Forensics Analyst™ (CIFA™), Certified Malware Reverse Engineer™ (CMRE™)
- **Defensive Cyber Operations Expert – Intelligence (Cyberspace)™ (DCOE-IC™)**
  Includes: Certified All-Source Requirements Manager™ (CASRM™), Certified All-Source Analyst™ (CASA™), Certified Cyber Intelligence Planner Professional™ (CCIPP™)
- **Defensive Cyber Operations Expert – Cyber Enabler (Leaders)™ (DCOE-CL™)**
  Includes: Certified Cyber Policy and Strategy Planner™ (CCPSP™), Certified Executive Cyber Leader™ (CECL™), Chief Information Officer Certified™ (CIOC™)
- **Defensive Cyber Operations Expert – Cyber Enabler (Legal/LE)™ (DCOE-CLE™)**
  Includes: Certified Cyber Legal Advisor™ (CCLA™), Certified Intrusion Forensic Analyst™ (CIFA™), Certified Cyber Crime Forensic Investigator™ (CCCFI™)
- **Defensive Cyber Operations Expert – Cyber Enabler (Programs)™ (DCOE-PM™)**
  Includes: Certified Program Manager™ (CPM™), Certified IT Project Manager™ (CITPM™), Certified IT Program Auditor™ (CITPA™)
- **Defensive Cyber Operations Expert – Cyber Enabler (Training)™ (DCOE-TR™)**
  Includes: Certified Cyber Curriculum Developer™ (CCCD™), Certified Cyber Instructor™ (CCI™), Certified Secure System Administrator™ (CSSA™)

Expert Offensive Cyber Operations™

- **Offensive Cyber Operations Expert (OCOE) - Cyber Effects (CE)™ (OCOE-CE™)**
  Includes: Certified Exploitation and Penetration Analyst™ (CEPA™), Certified Joint Targeting Analyst™ (CJTA™), Certified Mission Assurance Specialist™ (CMAS™)

Expert Technical Support Operations™

- **Technical Support Operations Expert – IT (Cyberspace)™ (TSOE-IT™)**
  Includes: Certified Network Operations Specialist™ (CNOS™), Certified Secure System Administrator™ (CSSA™), Certified Enterprise Security Architect™ (CESA™)
- **Technical Support Operations Expert – Software Engineering™ (TSOE-SE™)**
  Includes: Certified Secure Software Development Professional™ (CSSDP™), Certified Product Support Manager™ (CPSM™), Certified Software Test & Evaluation Specialist™ (CSTES™)
- **Technical Support Operations Expert – Data/AI™ (TSOE-DA™)**
  Includes: Certified Data Analyst Professional™ (CDAP™), Applied Data Scientist Certified Professional™ (ADSCP™), DevSecOps Specialist Certified™ (DevSC™)

Expert Critical Infrastructure Operations™

- **Certified Critical Infrastructure Expert™ (CCIE™)**
  Includes: Certified Control Systems Security Specialist™ (CCSSS™), Certified Infrastructure Support Specialist™ (CISS™), Certified System Testing and Evaluation Specialist™ (CSTES™)

Expert Counter-Insider Threat Operations™

- **Certified Insider Threat Expert – Cyber™**
  Includes: Certified Insider Threat Professional - Cyber Analytics (CITP-CA), User Activity Monitoring (CITP-UAM™), Cyber Lead (CITP-CL)
- **Certified Insider Threat Expert – Infrastructure™ (CITE-I™)**
  Includes: Certified Insider Threat Professional – Infrastructure Operator™ (CITP-IO™), User Activity Monitoring™ (CITP-UAM™), Infrastructure Engineer™ (CITP-IE™)
- **Certified Insider Threat Expert – Data™ (CITE-D™)**
  Includes: Certified Insider Threat Professional – Data Analytics™ (CITP-DA™), Cyber Lead (CITP-CL) and Data Scientist™ (CITP-DS™)
- **Certified Insider Threat Expert – Operations™ (CITE-O™)**
  Includes: Certified Insider Threat Professional – Program Manager™ (CITP-PM™), Cyber Lead (CITP-CL) and Hub Chief™ (CITP-HC™)

Certified COMSEC Manager™ (CCM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-1

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Courses in bundle: Security+ (with exam), CISM, CISSP, EC-Council Certified Encryption Specialist, COMSEC Resources

8140 DCWF Work Role: COMSEC Manager (Work Role Code: 723)

NICE Work Role: Communications Security (COMSEC) Management (Nice Work Role ID: OG-WRL-001)

Combined Work Role Description: Responsible for managing the Communications Security (COMSEC) resources of an organization, including all aspects of COMSEC as outlined in CNSSI No. 4009.

High-level bundle description: This bundle was intricately designed to equip participants with the knowledge and skills necessary to develop the abilities to accomplish defined tasks (KSATs) associated with the NICE and 8140 DCWF Work Roles for Cybersecurity Policy and Strategic Planning. It Incorporates Online Self-Paced Instructor Led Training and labs, covering content for the CompTIA Security+, CISM, CISSP and EC-Council Certified Encryption Specialist (ECES) certifications.

Requirements for certification: To earn the ITI certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+, ISACA CISM or ISC2 CISSP and EC-Council ECES certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Specific COMSEC Resources: The COMSEC references included in this bundle are designed to enhance understanding and implementation of Communications Security (COMSEC) protocols, primarily based on the Department of the Navy, Marine Corps and Coast Guard requirements, but applicable to most federal positions. Students will be asked to take an open book exam based on these materials.

Topics Covered (estimated 24-32 hours to review and complete final exam):

1. **Introduction to COMSEC**
   - **Purpose and Scope:** Protect sensitive and classified information from unauthorized access.
   - **Key Elements:** Transmission Security (TRANSEC), Cryptographic Security, Physical Security, Emissions Security (TEMPEST).
2. **Transmission Security (TRANSEC)**
   - **Modes of Transmission:** Electromagnetic (radio, telephone, email) and non-electromagnetic (face-to-face, hand delivery).

- **Protection Measures:** Frequency changes, secure communications, authentication, use of authorized codes.

3. **Cryptographic Security**
   - **Crypto Systems:** Design and use of secure cryptographic systems.
   - **Best Practices:** Follow operating instructions, perform key changes, limit access, use approved key material.
4. **Physical Security**
   - **Storage and Handling:** Use GSA-approved containers, maintain surveillance during working hours, conduct end-of-day security checks.
   - **Control Access Areas (CAA):** Limit access to authorized personnel only, use identification methods like personal recognition, access lists, security badges.
5. **Emissions Security (TEMPEST)**
   - **Purpose:** Prevent unauthorized access to information through electromagnetic emanations.
   - **Countermeasures:** Implement TEMPEST standards, use appropriate physical security, apply specific countermeasures based on system vulnerability analysis.
6. **Information and Classifications**
   - **Types of Information:** Top Secret, Secret, Confidential, For Official Use Only (FOUO), Sensitive but Unclassified (SBU).
   - **Handling:** Ensure proper marking, storage, and dissemination procedures to prevent unauthorized disclosure.
7. **Security Incidents**
   - **Types:** Personnel, physical, and cryptographic insecurities.
   - **Reporting:** Immediate reporting of suspected incidents, use of secure communication channels, follow documented reporting procedures.
8. **COMSEC Custodian Responsibilities**
   - **Role:** Handle and safeguard COMSEC materials, manage inventories, ensure proper storage.
   - **Key Tasks:** Conduct regular inventories, oversee the destruction of unneeded materials, manage access control, report incidents.
9. **COMSEC Incident Management**
   - **Types of Incidents:** Unauthorized disclosure, physical insecurities, cryptographic insecurities.
   - **Response Procedures:** Notify the Responsible COMSEC Officer, document the incident, secure compromised materials, conduct investigations, implement corrective actions.
10. **Common Fill Device (CFD)**
    - **Purpose:** Securely load cryptographic keys into communication equipment.
    - **Significance:** Ensures secure exchange of encrypted information.
11. **Responsible COMSEC Officer (RCO)**
    - **Role:** Oversee the implementation and management of the COMSEC program.

- **Responsibilities:** Ensure compliance with policies, address security incidents, manage overall COMSEC operations.

CTI CISSP Description: The Certified Information Systems Security Professional (CISSP) course is designed to provide comprehensive training in the field of cybersecurity. This course covers key concepts such as Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security. Each module delves deep into the principles and practices necessary for securing and managing information systems effectively. This course includes 19+ hours of ILT broken up into over 45 videos and 8 topics and provides over 250 exam preparation questions, as well as 25 hours of labs.

Topics Covered (19+ hours):

- Module 1: Security and Risk Management
- Module 2: Asset Security
- Module 3: Security Architecture and Engineering
- Module 4: Communication and Network Security
- Module 5: Identity and Access Management (IAM)
- Module 6: Security Assessment and Testing
- Module 7: Security Operations
- Module 8: Software Development Security

Labs Included (25 hours):

- Introduction to CISSP
- Security and Risk Management
- Encryption and Hashing
- SCCM Configuration Items and Baselines
- Implement OpenPGP
- Two factor Authentication with SSH
- Implement SSL VPN using ASA Device Manager
- Configure and Verify IPv4 and IPv6 Access Lists for Traffic Filtering
- Configuring IPtables
- Windows Command Line Tools
- Administering and Deploying Endpoint Protection
- Bitlocker on Portable Media
- Managing Remote Desktop
- Manage Role-based Security
- Configuring MBSA Scanner
- Compliance Patching

- Passive Topology Discovery
- Scanning and Remediating Vulnerabilities with OpenVAS
- Installing Kali
- Implement Backup and Recovery
- Installation and Verification of Snort
- Configuring and Securing IIS
- Upgrading and Securing SSH Connection
- DVWA - Manual SQL Injection and Password Cracking

CTI Custom Online Self-Paced Security+ ILT with Labs Description: Master cybersecurity with our Security+ 701 Online, Self-Paced ILT Course, designed for aspiring security specialists, network administrators, and IT auditors. This course covers essential cybersecurity principles and practices, aligning with the latest trends and techniques. Gain the core skills necessary to protect against digital threats and excel in today's dynamic IT security landscape. Included in this course is 30 hours of content, delivered over 100+ short easily digestible videos, covering 5 topic areas, and providing more than 250 prep practice questions. Once purchased, you have 12 months' access to the course.

- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules include (30 hours):

- Module 1 - SY0-701 General Security Concepts
- Module 2 - SY0-701 Threats, Vulnerabilities, and Mitigations
- Module 3 - SY0-701 Security Architecture
- Module 4 - SY0-701 Security Operations

- Module 5 - SY0-701 Security Program Management and Oversight

Labs Included (17 hours):

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Mitigation Techniques
7. Security Architecture Models
8. Securing Enterprise Infrastructures
9. Data Protection Strategies
10. Resilience in Security Architecture
11. Securing Computing Resources
12. Asset Management Techniques
13. Vulnerability Management
14. Monitoring Computing Resources
15. Enhancing Enterprise Security
16. Implement Identity & Access Management
17. Implementation of Automation & Orchestration for Security Operations
18. Investigative Data Sources

Official CompTIA CertMaster Learn with Integrated CertMaster Labs Description

Security+ CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis

- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered

- Lesson 1: Summarize Fundamental Security Concepts
- Lesson 2: Compare Threat Types
- Lesson 3: Explain Cryptographic Solutions
- Lesson 4: Implement Identity and Access Management
- Lesson 5: Secure Enterprise Network Architecture
- Lesson 6: Secure Cloud Network Architecture
- Lesson 7: Explain Resiliency and Site Security Concepts
- Lesson 8: Explain Vulnerability Management
- Lesson 9: Evaluate Network Security Capabilities
- Lesson 10: Assess Endpoint Security Capabilities
- Lesson 11: Enhance Application Security Capabilities
- Lesson 12: Explain Incident Response and Monitoring Concepts
- Lesson 13: Analyze Indicators of Malicious Activity
- Lesson 14: Summarize Security Governance Concepts
- Lesson 15: Explain Risk Management Processes
- Lesson 16: Summarize Data Protection and Compliance Concepts

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Perform System Configuration Gap Analysis
- Assisted Lab: Configuring Examples of Security Control Types
- Assisted Lab: Finding Open Service Ports
- Assisted Lab: Using SET to Perform Social Engineering
- Applied Lab: Using Storage Encryption
- Assisted Lab: Using Hashing and Salting
- Assisted Lab: Managing Password Security
- Assisted Lab: Managing Permissions
- Assisted Lab: Setting up Remote Access
- Assisted Lab: Using TLS Tunneling
- Assisted Lab: Using Containers
- Assisted Lab: Using Virtualization
- Assisted Lab: Implement Backups
- Assisted Lab: Performing Drive Sanitization
- Assisted Lab: Exploiting and Detecting SQLi
- Assisted Lab: Working with Threat Feeds

- Assisted Lab: Performing Vulnerability Scans
- Assisted Lab: Understanding Security Baselines
- Applied Lab: Implementing a Firewall
- Assisted Lab: Using Group Policy
- Applied Lab: Hardening
- Assisted Lab: Performing DNS Filtering
- Assisted Lab: Configuring System Monitoring
- Applied Lab: Incident Response: Detection
- Applied Lab: Performing Digital Forensics
- Assisted Lab: Performing Root Cause Analysis
- Assisted Lab: Detecting and Responding to Malware
- Assisted Lab: Understanding On-Path Attacks
- Adaptive Lab: Using a Playbook
- Assisted Lab: Implementing Allow Lists and Deny Lists
- Assisted Lab: Performing Reconnaissance
- Assisted Lab: Performing Penetration Testing
- Assisted Lab: Training and Awareness through Simulation
- Capstone Lab: Discovering Anomalous Behavior
- Assisted Lab: Use Cases of Automation and Scripting
- Applied Lab: Using Network Sniffers

License Information

One license provides access to CertMaster Learn for Security+ (SY0-701) with CertMaster Labs integrated throughout the course and ITU custom Security+ training and labs.

Once activated, the license is valid for 12 months

How to Access the training and labs

An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee

This bundle includes an Security+ exam voucher and an exam pass guarantee: if you don't pass the exam on the first try, we will provide a second voucher and another 12 months of access to our custom online self-paced ILT. In order to qualify for the exam pass guarantee, you have to show proof that you completed all training materials, to include course content, labs and practice prep questions prior to taking your exam.

CTI CISM Course Description: This intensive training course is tailored for professionals looking to excel in information security management. It covers essential topics such as information security governance, risk management, program

development, and incident management, equipping participants with the skills to develop and enforce robust security frameworks and best practices within their organizations. Participants will engage in practical applications and in-depth studies of security architecture, risk assessment, and incident response, all aimed at preparing them for the CISM certification exam and advancing their careers in information security management. This course includes over 17 hours of ILT covered over 45+ videos and 6 topic areas and provides 100 exam preparation questions.

Course Outline (17 hours):

- Module 1: Introduction
  - Instructor Introduction
  - Course Introduction
  - Exam Overview
- Module 2: Information Security Governance
  - Module Overview
  - InfoSec Strategic Context Part 1
  - InfoSec Strategic Context Part 2
  - GRC Strategy and Assurance
  - Roles and Responsibilities
  - GMA Tasks Knowledge and Metrics
  - IS Strategy Overview
  - Strategy Implemenation
  - Strategy Development Support
  - Architecture and Controls
  - Considerations and Action Plan
  - InfoSec Prog Objectives and Wrap-Up
- Module 3: Information Security Risk Management
  - Module Overview
  - Risk Identification Task and Knowledge
  - Risk Management Strategy
  - Additional Considerations
  - Risk Analysis and Treatment Tasks & Knowledge
  - Leveraging Frameworks
  - Assessment Tools and Analysis
  - Risk Scenario Development
  - Additional Risk Factors
  - Asset Classification and Risk Management
  - Risk Monitoring and Communication
  - Information Risk Management Summary
- Module 4: InfoSec Prog Development and Management
  - Module Overview
  - Alignment and Resource Management - Task and Knowledge
  - Key Relationships
  - Standards Awareness and Training - Tasks and Knowledge

    - Awareness and Training
    - Building Security into Process and Practices - Tasks and Knowledge
    - Additional Technology Infrastructure Concerns
    - Security monitoring and reporting Overview Tasks and Knowledge
    - Metrics and Monitoring
    - Summary
- Module 5: Information Security Incident Management
    - Module Overview
    - Planning and Integration Overview Task and Knowledge
    - Incident Response Concepts and Process
    - Forensics and Recovery
    - Readiness and Assessment - Overview Tasks and Knowledge
    - Identification and Response Overview Tasks and Knowledge
    - Incident Processes
- Module 6: Exam Prep
    - Case Study - Security On a Shoestring Budget
    - Case Study - APT In Action
    - Summary
- Exam Prep

Official Online Self-Paced EC-Council Certified Encryption Specialist (ECES): The EC-Council Certified Encryption Specialist (ECES) program introduces professionals and students to the field of cryptography. The participants will learn the foundations of modern symmetric and key cryptography including the details of algorithms such as Feistel Functions, DES, and AES. ECES provides necessary skills to perform effective deployment of encryption technologies. It is a comprehensive course covering various algorithms and the key concepts behind those algorithms.

Course Outline (20 hours over 3 days):

Module 01: Introduction and History of Cryptography

- **Overview:** What is Cryptography?, History of Cryptography
- **Ciphers:** Mono-Alphabet Substitution (e.g., Caesar Cipher, Atbash Cipher), Multi-Alphabet Substitution (e.g., Vigenère Cipher, Playfair Cipher), Homophonic Substitution, Null and Book Ciphers, Rail Fence Ciphers
- **Tools and Machines:** The Enigma Machine, CrypTool

Module 02: Symmetric Cryptography and Hashes

- **Fundamentals:** Symmetric Cryptography, Information Theory, Kerckhoffs's Principle, Substitution and Transposition, Binary Math

- **Algorithms:** Block vs. Stream Ciphers, Symmetric Block Ciphers (e.g., DES, AES, Blowfish, Twofish), Symmetric Stream Ciphers (e.g., RC4), Hash Functions (e.g., MD5, SHA, RIPEMD-160)
- **Tools:** CryptoBench

Module 03: Number Theory and Asymmetric Cryptography

- **Basics:** Asymmetric Encryption, Number Theory, Birthday Theorem, Random Number Generators
- **Key Algorithms:** Diffie-Hellman, RSA, Digital Signature Algorithm, Elliptic Curve, Elgamal
- **Tools:** CrypTool

Module 04: Applications of Cryptography

- **Standards and Certificates:** FIPS Standards, Digital Signatures, Public Key Infrastructure (PKI), Digital Certificate Management, Trust Models
- **Encryption in Practice:** Wi-Fi Encryption, SSL/TLS, VPNs, File and Disk Encryption (e.g., BitLocker, VeraCrypt), Steganography
- **Common Mistakes and Best Practices:** Common Cryptography Mistakes, Unbreakable Encryption, Steganalysis Tools

Module 05: Cryptanalysis

- **Techniques:** Breaking Ciphers, Frequency Analysis, Kasiski Examination, Linear and Differential Cryptanalysis, Integral Cryptanalysis
- **Tools and Successes:** Cryptanalysis Resources, Rainbow Tables, Password Cracking

License Information

One license provides access to the course.

Once activated, the license is valid for 12 months

How to Access the training and labs

An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee

This bundle includes EC-Council Certified Encryption Specialist exam voucher and one retake. The exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

Certified Cyber Policy and Strategy Planner™ (CCPSP™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-2

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Courses in bundle: Security+ (with exam), CISM, CISSP, EC-Council CCISO (with exam)

8140 DCWF Work Role: Cyber Policy and Strategy Planner (Work Role Code: 752)

NICE Work Role: Cybersecurity Policy and Planning (Nice Work Role ID: OG-WRL-002)

Combined Work Role Description: Responsible for developing and maintaining cybersecurity and cyberspace plans, strategies, and policies to support and align with organizational missions, initiatives, and regulatory compliance.

High-level bundle description: This bundle was intricately designed to equip participants with the knowledge and skills necessary to develop the abilities to accomplish defined tasks (KSATs) associated with the NICE and 8140 DCWF Work Roles for Cybersecurity Policy and Strategic Planning. It Incorporates Online Self-Paced Instructor Led Training and labs, covering content for the CompTIA Security+, CISM, CISSP and CCISO certifications, covering all three DoD 8140 Qualification proficiency levels (Basic, Intermediate and Advanced).

Requirements for certification: To earn the ITI certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the ComptTIA Security+ and EC-Council CCISO certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

CTI Custom Online Self-Paced ILT with Labs Description: Master cybersecurity with our Security+ 701 Online, Self-Paced ILT Course, designed for aspiring security specialists, network administrators, and IT auditors. This course covers essential cybersecurity principles and practices, aligning with the latest trends and techniques. Gain the core skills necessary to protect against digital threats and excel in today's dynamic IT security landscape. Included in this course is 30 hours of content, delivered over 100+ short easily digestible videos, covering 5 topic areas, and providing more than 250 prep practice questions. Once purchased, you have 12 months' access to the course.

- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules include:

- Module 1 - SY0-701 General Security Concepts
- Module 2 - SY0-701 Threats, Vulnerabilities, and Mitigations
- Module 3 - SY0-701 Security Architecture
- Module 4 - SY0-701 Security Operations
- Module 5 - SY0-701 Security Program Management and Oversight

Labs Included (17 hours):

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Mitigation Techniques
7. Security Architecture Models
8. Securing Enterprise Infrastructures
9. Data Protection Strategies
10. Resilience in Security Architecture
11. Securing Computing Resources
12. Asset Management Techniques
13. Vulnerability Management
14. Monitoring Computing Resources
15. Enhancing Enterprise Security
16. Implement Identity & Access Management
17. Implementation of Automation & Orchestration for Security Operations
18. Investigative Data Sources

Official CompTIA CertMaster Learn with Integrated CertMaster Labs Description

CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered

- Lesson 1: Summarize Fundamental Security Concepts
- Lesson 2: Compare Threat Types
- Lesson 3: Explain Cryptographic Solutions
- Lesson 4: Implement Identity and Access Management
- Lesson 5: Secure Enterprise Network Architecture
- Lesson 6: Secure Cloud Network Architecture
- Lesson 7: Explain Resiliency and Site Security Concepts
- Lesson 8: Explain Vulnerability Management
- Lesson 9: Evaluate Network Security Capabilities
- Lesson 10: Assess Endpoint Security Capabilities
- Lesson 11: Enhance Application Security Capabilities
- Lesson 12: Explain Incident Response and Monitoring Concepts
- Lesson 13: Analyze Indicators of Malicious Activity
- Lesson 14: Summarize Security Governance Concepts
- Lesson 15: Explain Risk Management Processes
- Lesson 16: Summarize Data Protection and Compliance Concepts

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Perform System Configuration Gap Analysis
- Assisted Lab: Configuring Examples of Security Control Types
- Assisted Lab: Finding Open Service Ports
- Assisted Lab: Using SET to Perform Social Engineering
- Applied Lab: Using Storage Encryption
- Assisted Lab: Using Hashing and Salting
- Assisted Lab: Managing Password Security
- Assisted Lab: Managing Permissions
- Assisted Lab: Setting up Remote Access
- Assisted Lab: Using TLS Tunneling
- Assisted Lab: Using Containers
- Assisted Lab: Using Virtualization
- Assisted Lab: Implement Backups
- Assisted Lab: Performing Drive Sanitization
- Assisted Lab: Exploiting and Detecting SQLi
- Assisted Lab: Working with Threat Feeds
- Assisted Lab: Performing Vulnerability Scans
- Assisted Lab: Understanding Security Baselines
- Applied Lab: Implementing a Firewall
- Assisted Lab: Using Group Policy
- Applied Lab: Hardening
- Assisted Lab: Performing DNS Filtering
- Assisted Lab: Configuring System Monitoring
- Applied Lab: Incident Response: Detection
- Applied Lab: Performing Digital Forensics
- Assisted Lab: Performing Root Cause Analysis
- Assisted Lab: Detecting and Responding to Malware
- Assisted Lab: Understanding On-Path Attacks
- Adaptive Lab: Using a Playbook
- Assisted Lab: Implementing Allow Lists and Deny Lists
- Assisted Lab: Performing Reconnaissance
- Assisted Lab: Performing Penetration Testing
- Assisted Lab: Training and Awareness through Simulation
- Capstone Lab: Discovering Anomalous Behavior
- Assisted Lab: Use Cases of Automation and Scripting
- Applied Lab: Using Network Sniffers

License Information

One license provides access to CertMaster Learn for Security+ (SY0-701) with CertMaster Labs integrated throughout the course and ITU custom Security+ training and labs.

Once activated, the license is valid for 12 months

How to Access the training and labs

An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee

This bundle includes an Security+ exam voucher and an exam pass guarantee: if you don't pass the exam on the first try, we will provide a second voucher and another 12 months of access to our custom online self-paced ILT. In order to qualify for the exam pass guarantee, you have to show proof that you completed all training materials, to include course content, labs and practice prep questions prior to taking your exam.

CTI CISM Course Description: This intensive training course is tailored for professionals looking to excel in information security management. It covers essential topics such as information security governance, risk management, program development, and incident management, equipping participants with the skills to develop and enforce robust security frameworks and best practices within their organizations. Participants will engage in practical applications and in-depth studies of security architecture, risk assessment, and incident response, all aimed at preparing them for the CISM certification exam and advancing their careers in information security management. This course includes over 17 hours of ILT covered over 45+ videos and 6 topic areas and provides 100 exam preparation questions.

Course Outline:

- Module 1: Introduction
  - Instructor Introduction
  - Course Introduction
  - Exam Overview
- Module 2: Information Security Governance
  - Module Overview
  - InfoSec Strategic Context Part 1
  - InfoSec Strategic Context Part 2
  - GRC Strategy and Assurance
  - Roles and Responsibilities
  - GMA Tasks Knowledge and Metrics
  - IS Strategy Overview
  - Strategy Implemenation
  - Strategy Development Support
  - Architecture and Controls

    - Considerations and Action Plan
    - InfoSec Prog Objectives and Wrap-Up
- Module 3: Information Security Risk Management
    - Module Overview
    - Risk Identification Task and Knowledge
    - Risk Management Strategy
    - Additional Considerations
    - Risk Analysis and Treatment Tasks & Knowledge
    - Leveraging Frameworks
    - Assessment Tools and Analysis
    - Risk Scenario Development
    - Additional Risk Factors
    - Asset Classification and Risk Management
    - Risk Monitoring and Communication
    - Information Risk Management Summary
- Module 4: InfoSec Prog Development and Management
    - Module Overview
    - Alignment and Resource Management - Task and Knowledge
    - Key Relationships
    - Standards Awareness and Training - Tasks and Knowledge
    - Awareness and Training
    - Building Security into Process and Practices - Tasks and Knowledge
    - Additional Technology Infrastructure Concerns
    - Security monitoring and reporting Overview Tasks and Knowledge
    - Metrics and Monitoring
    - Summary
- Module 5: Information Security Incident Management
    - Module Overview
    - Planning and Integration Overview Task and Knowledge
    - Incident Response Concepts and Process
    - Forensics and Recovery
    - Readiness and Assessment - Overview Tasks and Knowledge
    - Identification and Response Overview Tasks and Knowledge
    - Incident Processes
- Module 6: Exam Prep
    - Case Study - Security On a Shoestring Budget
    - Case Study - APT In Action
    - Summary
- Exam Prep

License Information:
One license provides access to the CISM course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access:
Instructions for accessing the course will be emailed after purchase.

EC-Council CCISO Description: The CCISO course is designed for current and aspiring information security executives. This program includes 40 hours of content, combining theoretical knowledge with practical skills required to establish and maintain an information security program.

Topics Covered:

Domain 1: Governance and Risk Management

1. Define, Implement, Manage, and Maintain an Information Security Governance Program
2. Information Security Drivers
3. Establishing an information security management structure
4. Laws/Regulations/Standards as drivers of Organizational Policy/Standards/Procedures
5. Managing an enterprise information security compliance program
6. Introduction to Risk Management

Domain 2: Information Security Controls, Compliance, and Audit Management

1. Information Security Controls
2. Compliance Management
3. Guidelines, Good and Best Practices
4. Audit Management
5. Summary

Domain 3: Security Program Management & Operations

1. Program Management
2. Operations Management
3. Summary

Domain 4: Information Security Core Competencies

1. Access Control
2. Physical Security
3. Network Security
4. Certified Chief
5. Endpoint Protection

6. Application Security
7. Encryption Technologies
8. Virtualization Security
9. Cloud Computing Security
10. Transformative Technologies
11. Summary

Domain 5: Strategic Planning, Finance, Procurement and Vendor Management

1. Strategic Planning
2. Designing, Developing, and Maintaining an Enterprise Information Security Program
3. Understanding the Enterprise Architecture (EA)
4. Finance
5. Procurement
6. Vendor Management
7. Summary

Exam Information:
The course includes an exam voucher and retake for the EC-Council exam. The exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information:
One license provides access to the course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access:
Instructions for accessing the course will be emailed after purchase.

CTI CISSP Description: The Certified Information Systems Security Professional (CISSP) 2020 course is designed to provide comprehensive training in the field of cybersecurity. This course covers key concepts such as Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security. Each module delves deep into the principles and practices necessary for securing and managing information systems effectively. This course includes 19+ hours of ILT broken up into over 45 videos and 8 topics and provides over 250 exam preparation questions.

Topics Covered (19+ hours):

- Module 1: Security and Risk Management
- Module 2: Asset Security
- Module 3: Security Architecture and Engineering
- Module 4: Communication and Network Security
- Module 5: Identity and Access Management (IAM)
- Module 6: Security Assessment and Testing
- Module 7: Security Operations
- Module 8: Software Development Security

Labs Included (25 hours):

- Introduction to CISSP
- Security and Risk Management
- Encryption and Hashing
- SCCM Configuration Items and Baselines
- Implement OpenPGP
- Two factor Authentication with SSH
- Implement SSL VPN using ASA Device Manager
- Configure and Verify IPv4 and IPv6 Access Lists for Traffic Filtering
- Configuring IPtables
- Windows Command Line Tools
- Administering and Deploying Endpoint Protection
- Bitlocker on Portable Media
- Managing Remote Desktop
- Manage Role-based Security
- Configuring MBSA Scanner
- Compliance Patching
- Passive Topology Discovery
- Scanning and Remediating Vulnerabilities with OpenVAS
- Installing Kali
- Implement Backup and Recovery
- Installation and Verification of Snort
- Configuring and Securing IIS
- Upgrading and Securing SSH Connection
- DVWA - Manual SQL Injection and Password Cracking

License Information

One license provides access to CTI custom CISSP training and labs.

Once activated, the license is valid for 12 months.

How to Access the training and labs

An access key and instructions will be sent via email after your purchase is complete.

Certified Cyber Workforce Developer™ (CCWD™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-3

Courses in bundle: CompTIA Security+ (with exam), Project+ (with exam) and PMP Bundle, CISM and CISSP bundle, HDI-SCL (with exam), CCSP

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Cyber Workforce Developer and Manager (Work Role Code: 751)

NICE Work Role: Cybersecurity Workforce Management (Nice Work Role ID: OG-WRL-003)

Combined Work Role Description: Responsible for developing cybersecurity and cyberspace workforce plans, assessments, strategies, and guidance, including staff training, education, and hiring processes. This role involves making adjustments in response to or in anticipation of changes to cybersecurity and cyberspace policy, technology, doctrine, materiel, force structure, and staffing needs and requirements. It also includes authoring mandated workforce planning strategies to maintain compliance with legislation, regulation, and policy, and supporting manpower, personnel, training, and education requirements.

High-level bundle description: This bundle was intricately designed to equip participants with the knowledge and skills necessary to develop the abilities to accomplish defined tasks (KSATs) associated with the applicable NICE and 8140 DCWF Work Roles. It Incorporates Online Self-Paced Instructor Led Training and labs, covering content for the CompTIA Security+, ISACA CISM, ISC2 CISSP, HDI Support Center Led (HDI-SCL) and the ISC2 Certified Cloud Security Professional (CCSP). Additionally, this bundle strengthens project management acumen with the CompTIA Project+ and PMP training, ensuring readiness to lead teams and initiatives in dynamic cybersecurity environments.

Requirements for certification: To earn the ITI certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+ and Project+, either CISM or CISSP, and HDI-SCL certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Certification/Micro degree renewals: The ITI's Certification is good for three years. This certification is considered ever green and will renew every three years if the certification holders enter into and maintain a subscription to ITI's annual "Tech Pro" library for $749 a year. The "Tech Pro" library allows the student to benefit for the latest training and tools designed to equip participants with the knowledge and skills necessary to develop the abilities to accomplish defined tasks (KSATs) associated with the applicable NICE and 8140 DCWF Work Roles. The Tech Pro library includes access to all of our partner CTI's custom ILT, in addition to EC-Council's Annual Pro subscription. All other non-ITI certifications are subject to their vendors terms and policies for certification renewals. Micro degrees do not expire.

Bundled Course Links

CISM and CISSP

Project+ and PMP bundle

CTI Custom Online Self-Paced ILT with Labs Description: Master cybersecurity with our Security+ 701 Online, Self-Paced ILT Course, designed for aspiring security specialists, network administrators, and IT auditors. This course covers essential cybersecurity principles and practices, aligning with the latest trends and techniques. Gain the core skills necessary to protect against digital threats and excel in today's dynamic IT security landscape. Included in this course is 30 hours of content, delivered over 100+ short easily digestible videos, covering 5 topic areas, and providing more than 250 prep practice questions. Once purchased, you have 12 months' access to the course.

- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules include:

- Module 1 - SY0-701 General Security Concepts

- Module 2 - SY0-701 Threats, Vulnerabilities, and Mitigations
- Module 3 - SY0-701 Security Architecture
- Module 4 - SY0-701 Security Operations
- Module 5 - SY0-701 Security Program Management and Oversight

Labs Included (17 hours):

1. Security Concept Fundamentals
2. Cryptographic Solutions
3. Threat Vectors and Attack Surfaces
4. Identifying Security Vulnerabilities
5. Analyze Malicious Activity
6. Mitigation Techniques
7. Security Architecture Models
8. Securing Enterprise Infrastructures
9. Data Protection Strategies
10. Resilience in Security Architecture
11. Securing Computing Resources
12. Asset Management Techniques
13. Vulnerability Management
14. Monitoring Computing Resources
15. Enhancing Enterprise Security
16. Implement Identity & Access Management
17. Implementation of Automation & Orchestration for Security Operations
18. Investigative Data Sources

ITI's Official CompTIA CertMaster Learn with Integrated CertMaster Labs Description

Security+ CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge

- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered

- Lesson 1: Summarize Fundamental Security Concepts
- Lesson 2: Compare Threat Types
- Lesson 3: Explain Cryptographic Solutions
- Lesson 4: Implement Identity and Access Management
- Lesson 5: Secure Enterprise Network Architecture
- Lesson 6: Secure Cloud Network Architecture
- Lesson 7: Explain Resiliency and Site Security Concepts
- Lesson 8: Explain Vulnerability Management
- Lesson 9: Evaluate Network Security Capabilities
- Lesson 10: Assess Endpoint Security Capabilities
- Lesson 11: Enhance Application Security Capabilities
- Lesson 12: Explain Incident Response and Monitoring Concepts
- Lesson 13: Analyze Indicators of Malicious Activity
- Lesson 14: Summarize Security Governance Concepts
- Lesson 15: Explain Risk Management Processes
- Lesson 16: Summarize Data Protection and Compliance Concepts

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Perform System Configuration Gap Analysis
- Assisted Lab: Configuring Examples of Security Control Types
- Assisted Lab: Finding Open Service Ports
- Assisted Lab: Using SET to Perform Social Engineering
- Applied Lab: Using Storage Encryption
- Assisted Lab: Using Hashing and Salting
- Assisted Lab: Managing Password Security
- Assisted Lab: Managing Permissions
- Assisted Lab: Setting up Remote Access
- Assisted Lab: Using TLS Tunneling

- Assisted Lab: Using Containers
- Assisted Lab: Using Virtualization
- Assisted Lab: Implement Backups
- Assisted Lab: Performing Drive Sanitization
- Assisted Lab: Exploiting and Detecting SQLi
- Assisted Lab: Working with Threat Feeds
- Assisted Lab: Performing Vulnerability Scans
- Assisted Lab: Understanding Security Baselines
- Applied Lab: Implementing a Firewall
- Assisted Lab: Using Group Policy
- Applied Lab: Hardening
- Assisted Lab: Performing DNS Filtering
- Assisted Lab: Configuring System Monitoring
- Applied Lab: Incident Response: Detection
- Applied Lab: Performing Digital Forensics
- Assisted Lab: Performing Root Cause Analysis
- Assisted Lab: Detecting and Responding to Malware
- Assisted Lab: Understanding On-Path Attacks
- Adaptive Lab: Using a Playbook
- Assisted Lab: Implementing Allow Lists and Deny Lists
- Assisted Lab: Performing Reconnaissance
- Assisted Lab: Performing Penetration Testing
- Assisted Lab: Training and Awareness through Simulation
- Capstone Lab: Discovering Anomalous Behavior
- Assisted Lab: Use Cases of Automation and Scripting
- Applied Lab: Using Network Sniffers

License Information

One license provides access to CertMaster Learn for Security+ (SY0-701) with CertMaster Labs integrated throughout the course and ITU custom Security+ training and labs.

Once activated, the license is valid for 12 months

How to Access the training and labs

An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee

This bundle includes an Security+ exam voucher and an exam pass guarantee: if you don't pass the exam on the first try, we will provide a second voucher and another 12 months of access to our custom online self-paced ILT. In order to qualify for the exam

pass guarantee, you have to show proof that you completed all training materials, to include course content, labs and practice prep questions prior to taking your exam.

HDI Support Center Lead (HDI-SCL) description: Support center team leads serve as the communication link between the team and the manager as well as the first point of internal escalation for the customer.

HDI Support Center Team Lead training ensures that participants learn how to deliver exceptional customer support, promote process improvement, coach for success, and take charge of the day-to-day operational activities of a team. This course is designed for support professionals who need to develop fundamental management and leadership skills. Online, self-paced training allows student to train at their own speed, permitting them to concentrate on areas of specific need. Students can train from any computer with Internet access, and the course takes about 10-12 hours to complete.

Course Outline:

- **Unit 1: Support Center Overview**
  - Evolution of Service & Support
  - Successful Service & Support
- **Unit 2: Role of the Support Center Team Lead**
  - Role of the Team Lead
  - Effective Leadership
  - Emotional Intelligence
  - Managing Relationships
- **Unit 3: Business Planning and Strategy**
  - Strategic Perspective
  - Building a Strategy
  - Service Level Management
  - SOPs
  - Alignment
- **Unit 4: Support Center Processes**
  - Best Practices for Support
  - Service Operations
  - Additional Processes
  - Knowledge Management
- **Unit 5: Service Delivery Methods & Technology**
  - Systems Thinking Approach
  - Support Tools & Tech
  - Service Delivery Methods
  - Social Media
- **Unit 6: Workforce Management and Training**
  - Workforce Management
  - Sourcing and Recruitment
  - Training

- **Unit 7: Communication and Coaching**
  - Communication Skills
  - Cross-Cultural Communication
  - Managing Conflict
  - Coaching
- **Unit 8: Teamwork**
  - Motivation, Rewards, Recognition
  - Performance Management
  - Retention
- **Unit 9: Metrics and Quality Assurance**
  - Metrics
  - Quality Assurance
  - Using Surveys
  - Performance Reporting
  - Promoting the Support Center

Product Information:

- Once registered for an online course, you have 12 weeks to access the course. A 28-day extension is available for an online course for a fee of $50. Exam retakes are available for a $99 fee

CTI Custom Online Self-Paced Certified Cloud Security Professional (CCSP): this course This course covers key concepts, tools, technologies, and best practices for securing cloud environments. Students will learn about cloud architecture, legal and compliance issues, data security, platform and infrastructure security, application security, and security operations. The curriculum is designed to provide practical skills and real-world applications, ensuring that learners can effectively protect cloud-based assets and data.

Topics include:

- **Module 1 - Cloud Concepts, Architecture and Design**
  - Course Intro
  - Cloud Concepts, Architecture and Design - Part 1
  - Cloud Concepts, Architecture and Design - Part 2
  - Cloud Concepts, Architecture and Design - Part 3
  - Cloud Concepts, Architecture and Design - Part 4
  - Cloud Concepts, Architecture and Design - Part 5
  - Cloud Concepts, Architecture and Design - Part 6
  - Cloud Concepts, Architecture and Design - Part 7
  - Cloud Concepts, Architecture and Design - Part 8
  - Cloud Concepts, Architecture and Design - Part 9
- **Module 2 - Legal, Risk and Compliance**
  - Legal, Risk and Compliance Part 1
  - Legal, Risk and Compliance Part 2

  - Legal, Risk and Compliance Part 3
  - Legal, Risk and Compliance Part 4
  - Legal, Risk and Compliance Part 5
  - Legal, Risk and Compliance Part 6
  - Legal, Risk and Compliance Part 7
- **Module 3 - Cloud Data Security**
  - Cloud Data Security - Part 1
  - Cloud Data Security - Part 2
  - Cloud Data Security - Part 3
  - Cloud Data Security - Part 4
  - Cloud Data Security - Part 5
  - Cloud Data Security - Part 6
  - Cloud Data Security - Part 7
- **Module 4 - Cloud Platform and Infrastructure Security**
  - Cloud Platform and Infrastructure Security - Part 1
  - Cloud Platform and Infrastructure Security - Part 2
  - Cloud Platform and Infrastructure Security - Part 3
  - Cloud Platform and Infrastructure Security - Part 4
  - Cloud Platform and Infrastructure Security - Part 5
  - Cloud Platform and Infrastructure Security - Part 6
  - Cloud Platform and Infrastructure Security - Part 7
  - Cloud Platform and Infrastructure Security - Part 8
- **Module 5 - Cloud Application Security**
  - Cloud Application Security - Part 1
  - Cloud Application Security - Part 2
  - Cloud Application Security - Part 3
  - Cloud Application Security - Part 4
  - Cloud Application Security - Part 5
  - Cloud Application Security - Part 6
  - Cloud Application Security - Part 7
  - Cloud Application Security - Part 8
  - Cloud Application Security - Part 9
- **Module 6 - Cloud Security Operations**
  - Cloud Security Operations - Part 1
  - Cloud Security Operations - Part 2
  - Cloud Security Operations - Part 3
  - Cloud Security Operations - Part 4
  - Cloud Security Operations - Part 5
  - Cloud Security Operations - Part 6
  - Cloud Security Operations - Part 7
  - Cloud Security Operations - Part 8
  - Cloud Security Operations - Part 9
  - Cloud Security Operations - Part 10
  - Cloud Security Operations - Part 11

- Course Conclusion

Product Information:

- One license provides access to courses and labs.
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee: This bundle includes an exam vouchers and an exam pass guarantee for Security+, Cloud+, PenTest+ and CASP+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Cyber Curriculum Developer™ (CCCD™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-4

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CASP+

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Cyber Instructional Curriculum Developer (Work Role Code: 711)

NICE Work Role: Cybersecurity Curriculum Development (Nice Work Role ID: OG-WRL-004)

Combined Work Role Description: Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, and education courses, methods, and techniques based on instructional needs and requirements.

High-level bundle description: This bundle was intricately designed to equip participants with the knowledge and skills necessary to develop the abilities to accomplish defined tasks (KSATs) associated with the NICE and 8140 DCWF Work Roles. It Incorporates The CompTIA Secure Cloud Professional (Security+ / Cloud+) Bundle which provides comprehensive training for individuals seeking to excel in cloud

security and administration. It also includes The CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+) Bundle which provides comprehensive training for individuals seeking to excel in network vulnerability assessments and penetration testing. Finally, this bundle includes the CompTIA CASP+ course, covering essential concepts and practices for enterprise security. The bundle also includes an exam voucher and an exam pass guarantee for each certification.

Requirements for certification: To earn the ITI CCCD™ and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Certification/Micro degree renewals: The ITI's Certification is good for three years. This certification is considered ever green and will renew every three years if the certification holders enter into and maintain a subscription to ITI's annual "Tech Pro" library for $749 a year. The "Tech Pro" library allows the student to benefit for the latest training and tools designed to equip participants with the knowledge and skills necessary to develop the abilities to accomplish defined tasks (KSATs) associated with the applicable NICE and 8140 DCWF Work Roles. The Tech Pro library includes access to all of our partner CTI's custom ILT, in addition to EC-Council's Annual Pro subscription. All other non-ITI certifications are subject to their vendors terms and policies for certification renewals. Micro degrees do not expire.

Bundled Course Links

Security+

CASP+

Pentest+

Cloud+

Product Information:

- One license provides access to CertMaster Learn for Security+, Cloud+, PenTest+ and CASP+ with CertMaster Labs integrated throughout the courses and ITI courses and labs.
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee: This bundle includes an exam vouchers and an exam pass guarantee for Security+, Cloud+, PenTest+ and CASP+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Cyber Instructor™ (CCI™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-5

Courses in bundle: CompTIA Secure Infrastructure Expert and CompTIA Security Analytics Expert (official Security+ / CySA+ / PenTest+ / CASP+) with labs and exam vouchers and the following ITI custom courses and labs only: Cloud+, Server+, Linux+

MSRP: $4,499

Sales Price: $3,899

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Cyber Instructor (Work Role Code: 712)

NICE Work Role: Cybersecurity Instruction (Nice Work Role ID: OG-WRL-005)

Combined Work Role Description: Responsible for developing, planning, coordinating, and evaluating cybersecurity awareness, training, and education courses, methods, and techniques based on instructional needs and requirements.

High-level bundle description: This bundle was intricately designed to equip participants with the knowledge and skills necessary to develop the abilities to accomplish defined tasks (KSATs) associated with the NICE and 8140 DCWF Work Roles. It incorporates CTI custom Online Self-Paced Instructor Led Training and labs, covering content for the CompTIA Security+, CySA+, PenTest+, CASP+, Cloud+, Server+ (labs only), and Linux+ certifications. It also covers official CompTIA CertMaster learn and labs for Security+, CySA+, PenTest+, and CASP+. This is the best overall value bundle in our catalog.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, CySA+, PenTest+ and CASP+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

Security+

CySA+

PenTest+

CASP+

Cloud+

Server+

Linux+

Product Information:

- One license provides access to CertMaster Learn for Security+, CySA+, PenTest+ and CASP+ with CertMaster Labs integrated throughout the courses and ITI courses and labs. Once license provides access to ITI custom course and labs only for Cloud+, Server+, Linux+
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee: This bundle includes an exam vouchers and an exam pass guarantee for Security+, CySA+, PenTest+ and CASP+ only: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam. Exam vouchers for Cloud+, Server+, Linux+ are available at a 20% discount off of MSRP.

Certified Cyber Legal Advisor™ (CCLA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-6

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CISM and CISSP bundle, CCSP, CISA and PECB Forensics Examiner

8140 DCWF Work Role: Cyber Legal Advisor (Work Role Code: 751)

NICE Work Role: Cybersecurity Legal Advice (Nice Work Role ID: OG-WRL-006)

Combined Work Role Description: Responsible for providing legal advice and recommendations on topics related to cyber law, including monitoring related legislation and regulations.

High-level bundle description: This bundle equips participants with essential skills in cybersecurity, compliance, cloud security, and digital forensics, forming a comprehensive foundation for cyber law advisory roles. CompTIA Secure Cloud Professional (Security+ / Cloud+) establishes core skills in security and cloud fundamentals, helping advisors understand the specific security and legal implications of cloud environments. The CISM and CISSP bundle delivers in-depth training on security management and governance, supporting advisors in establishing and interpreting organizational security frameworks and policies. ISC2 Certified Cloud Security Professional (CCSP) focuses on cloud security architecture and regulatory compliance, essential for addressing legal considerations within cloud systems. Certified Information Systems Auditor (CISA) provides knowledge of IT auditing and control standards, enabling advisors to interpret audit requirements and ensure regulatory compliance. PECB Certified Forensics Examiner teaches digital forensics skills, from evidence handling to investigation, supporting legal advisory roles in managing cyber incidents and related legal protocols.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for Security+, Cloud+ and PECB Forensic Examiner certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Certification/Micro degree renewals: The ITI's Certification is good for three years. This certification is considered ever green and will renew every three years if the certification holders enter into and maintain a subscription to ITI's annual "Tech Pro" library for $749 a year. The "Tech Pro" library allows the student to benefit for the latest training and tools designed to equip participants with the knowledge and skills necessary to develop the abilities to accomplish defined tasks (KSATs) associated with the applicable NICE and 8140 DCWF Work Roles. The Tech Pro library includes access to all of our partner CTI's custom ILT, in addition to EC-Council's Annual Pro subscription. All other non-ITI certifications are subject to their vendors terms and policies for certification renewals. Micro degrees do not expire.

Bundled Course Links

Security+

Cloud+

CISSP and CISM

Product Information:

- One license provides access to CertMaster Learn for Cloud+, and Security+ with CertMaster Labs integrated throughout the courses and ITI courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee: This bundle includes an exam voucher and an exam pass guarantee for Cloud+, and Security+ only: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Executive Cyber Leader™ (CECL™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-7

Courses in bundle: CTI CISSP and CISM bundle (courses and labs only), Cloud+ (course and exam), HDI Support Center Lead (HDI-SCL) (with exam), CISSP-ISSMP (FedVTE (now CISA Learning) (now CISA Learning) Course only) and PECB CISO

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Executive Cyber Leader (Work Role Code: 901)

NICE Work Role: Executive Cybersecurity Leadership (Nice Work Role ID: OG-WRL-007)

Combined Work Role Description: Responsible for developing and maintaining cybersecurity and cyberspace plans, strategies, and policies to support and align with organizational missions, initiatives, and regulatory compliance.

High-level bundle description: This This bundle is designed to provide leaders with the cybersecurity knowledge and executive skills needed to effectively manage an organization's cybersecurity strategy, compliance, and risk management. The CTI CISSP and CISM bundle provides comprehensive training on security management and governance, equipping leaders with frameworks to develop and enforce security policies. CompTIA Cloud+ focuses on secure cloud implementation and management,

essential for overseeing cloud security in an executive role. HDI Support Center Lead (HDI-SCL) develops customer support and service management skills, preparing leaders to manage critical IT support functions. The CISSP-ISSMP course (available via FedVTE (now CISA Learning) (now CISA Learning)) covers strategic planning for cybersecurity program management, aligning with executive responsibilities. PECB Certified Information Security Officer (CISO) adds expertise in implementing high-level information security governance and risk management, rounding out the executive's skill set with a focus on compliance, leadership, and security strategy.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Cloud+, and HDI Support Center Manager (HDI-SCM) certifications and either the CISSP or CISM.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

Cloud+

CISSP and CISM

FedVTE (now CISA Learning) (now CISA Learning) CISSP-ISSMP

HDI Support Center Lead (HDI-SCL)

PECB CISO

See each of the other course links for how to access the material and exam information.

Certified Privacy Compliance Manager™ (CPCM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-8

Courses in bundle: CISM and CISSP Bundle, EC-Council CCISO, PECB ISO/IEC 27701 Implementer (Privacy Information Management System (PIMS) and EC-Council NIST SP 800-53 Controls Mastery Bundle and EC-Council OPSEC Demystified: Strategies for Secure Operations.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Privacy Compliance Manager (Work Role Code: 732)

NICE Work Role: Privacy Compliance (Nice Work Role ID: OG-WRL-008)

Combined Work Role Description: Responsible for developing and overseeing an organization's privacy compliance program and staff. This includes establishing and managing privacy-related governance, policy, and incident response, while supporting the privacy compliance needs of privacy and security executives and their teams.

High-level bundle description: This bundle provides advanced training for cybersecurity professionals focused on privacy management and compliance. The CISM and CISSP Bundle builds a strong foundation in security management and governance, while EC-Council's CCISO program equips leaders with executive skills for high-level security operations. PECB's ISO/IEC 27701 Implementer course focuses on establishing a Privacy Information Management System (PIMS) aligned with international privacy standards, and the EC-Council NIST SP 800-53 Controls Mastery course delves into critical federal security controls for compliance. Rounding out the bundle, EC-Council's OPSEC Demystified course offers strategies for secure operations, ensuring that professionals can safeguard sensitive information within complex environments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the EC-Council CCISO and PECB ISO/IEC 27701 Implementer certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links:

- CISM and CISSP
- CCISO Online Self-Paced
- EC-Council NIST SP 800-53 Controls Mastery Bundle
- EC-Council OPSEC Demystified: Strategies for Secure Operations

ISO/IEC 27701 Implementer Course Description: Add The ISO/IEC 27701 Lead Implementer training course enables you to develop the necessary expertise to assist an organization to establish, implement, maintain and continually improve a Privacy Information Management System (PIMS) based on ISO/IEC 27701 by enhancing an existing ISMS based on ISO/IEC 27001 and the guidance of ISO/IEC 27002. After mastering the implementation and management of a Privacy Information Management System (PIMS), you can sit for the exam and apply for a "PECB Certified ISO/IEC 27701 Lead Implementer" credential. The internationally recognized PECB Lead Implementer Certificate proves that you have the practical knowledge and professional capabilities to implement the ISO/IEC 27701 requirements in an organization.

Course outline:

- **Day 1:** Introduction to ISO/IEC 27701 and initiation of a PIMS
- **Day 2:** Planning the implementation of a PIMS
- **Day 3:** Implementing a PIMS
- **Day 4:** PIMS monitoring, continual improvement and preparation for the certification audit
- **Day 5:** Certification exam

For additional outline and agenda details, see the Brochure:
https://pecb.com/pdf/brochures/4/iso-iec-27701-lead-implementer_4p.pdf

Product Information:

- One license provides access to each course
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months
- Access keys and instructions will be sent via email after your purchase is complete.

Exam Information: Each course comes with the exam (one voucher). For the PECB exam, it will be provided to you after you complete the course. See the CCISO course link for CCISO exam information.

Certified Product Support Manager™ (CPSM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-9

Courses in bundle: ITI Security+ course and labs, HDI-SCL, CompTIA Project+ and PMP Bundle, Certified Scrum Product Owner (CSPO) Certification (course and exam)

MSRP: $4,499
Sales Price: $3,999
Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Product Support Manager (Work Role Code: 803)

NICE Work Role: Product Support Management (Nice Work Role ID: OG-WRL-009)

Combined Work Role Description: Responsible for managing the comprehensive package of support functions required to field and maintain the readiness and operational capability of systems and components. This role involves planning,

estimating costs, budgeting, and developing and implementing product support strategies to ensure sustained operational effectiveness. The position requires a strategic approach to managing product support, encompassing both technical and managerial aspects to achieve optimal system performance and reliability.

High-level bundle description: Elevate your career in product support management with the Certified Product Support Manager™ (CPSM™) and Applied Micro Degree Bundle. This extensive bundle includes online self-paced ITI Security+ course, labs and exam, HDI Support Center Leadership (HDI-SCL) course and exam, CompTIA Project+ (with course, lab and exam) and PMP (course) Bundle, and the online live Certified Scrum Product Owner (CSPO) certification course and exam (contact us to schedule). Designed to provide a comprehensive skill set for managing and supporting products in a dynamic environment, this bundle equips you with essential knowledge in security, support center leadership, information security management, and agile product ownership.

With this bundle, you will gain expertise in securing and managing product support, leading support teams, implementing effective information security practices, and driving product development through agile methodologies. Whether you are preparing for a new role or enhancing your current capabilities, the CPSM™ and Applied Micro Degree Bundle offers a robust foundation to excel in the ever-evolving field of product support management.

Requirements for certification: To earn the ITI CPSM™and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, HDI-SCL, Project+ and CSPO.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- Security+
- Project+ and PMP Bundle
- HDI-SCL
- Certified Scrum Product Owner

See each of the other course links for how to access the material and exam information.

Certified Program Manager™ (CPM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-10

Courses in bundle: CompTIA Security+, CISM and CISSP bundle, Project+ and PMP bundle, HDI-SCL

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Program Manager (Work Role Code: 801)

NICE Work Role: Program Management (Nice Work Role ID: OG-WRL-010)

Combined Work Role Description: Responsible for leading, coordinating, communicating, and integrating activities to ensure the overall success of a defined program. This role is accountable for aligning the program with critical agency or organizational priorities, effectively managing all aspects to meet strategic objectives and ensure compliance with relevant standards.

High-level bundle description: This bundle was intricately designed to equip participants with the knowledge and skills necessary to develop the abilities to accomplish defined tasks (KSATs) associated with the NICE and 8140 DCWF Work Roles for Program Manager and Program Management. It Incorporates Online Self-Paced Instructor Led Training and labs, covering content for the CompTIA Security+ and Project+, PMP, CISM, and CISSP.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CISM, Security+ and Project+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

Security+

CISM and CISSP

Project+ and PMP

HDI-SCL

Product Information:

- One license provides access to CertMaster Learn for Project+, and Security+ with CertMaster Labs integrated throughout the courses and ITI courses and labs

- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Security+ and Project+): This bundle includes an exam voucher and an exam pass guarantee for Security+ and Project+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified IT Project Manager™ (CITPM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-11

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CSM, CISA, Project+ and PMP Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: IT Project Manager (Work Role Code: 802)

NICE Work Role: Secure Project Management (Nice Work Role ID: OG-WRL-011)

Combined Work Role Description: Responsible for directly managing information technology projects to deliver unique services or products. This role oversees and coordinates all aspects of technology projects, ensuring that cybersecurity measures are integrated from the outset to protect the organization's critical infrastructure and assets, minimize risks, and align with organizational objectives. The role involves tracking and communicating project status effectively, demonstrating the project's value to the organization, and ensuring that each project outcome meets the required specifications and quality standards.

High-level bundle description: The Certified IT Project Manager™ (CITPM™) and Applied Micro Degree Bundle provides a well-rounded blend of IT project management and security-focused certifications, preparing participants to lead complex IT initiatives while addressing key cybersecurity considerations in support of the DCWF and NICE work roles. The bundle integrates a comprehensive range of certifications including CompTIA Secure Cloud Professional (Security+ / Cloud+), which equips learners with cloud management and security expertise, and Certified ScrumMaster (CSM), which

focuses on Agile methodologies and team leadership. The CISA certification develops skills in auditing, control, and assurance, while CompTIA Project+ and PMP provide a deep foundation in project planning, execution, and risk management. Together, these certifications ensure participants are equipped to manage IT projects securely and efficiently, meeting both organizational and cybersecurity objectives.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CSM, Security+, Cloud+ and Project+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional

Project+ and PMP

CISA

ITI Partner Delivered Course Description for CSM: The Certified ScrumMaster (CSM) Certification course equips participants with the skills necessary to lead Agile teams and effectively implement the Scrum framework. The training is designed to help professionals master Scrum practices and principles, preparing them for the CSM exam and for real-world project environments.

Key Areas Covered:

1. **Agile Principles and Scrum Framework**
    - Overview of Agile methodologies and the values behind the Agile Manifesto.
    - Detailed explanation of the **Scrum framework**, including its roles, events, and artifacts.
    - Understanding how Scrum differs from traditional project management and the benefits it provides in an Agile environment.
2. **Scrum Roles and Responsibilities**
    - **ScrumMaster**: Responsibilities in facilitating the process, protecting the team, and enabling progress.
    - **Product Owner**: Managing the product backlog, prioritizing features, and ensuring value delivery.

- **Development Team**: Understanding the dynamics of self-organizing, cross-functional teams and their role in delivering increments of work.

3. **Scrum Events (Ceremonies)**
    - **Sprint Planning**: How to plan a successful Sprint, set clear goals, and determine the work to be completed.
    - **Daily Scrum (Stand-ups)**: Facilitating daily team meetings to track progress and identify impediments.
    - **Sprint Review**: Gathering feedback from stakeholders and reviewing the product increment.
    - **Sprint Retrospective**: Encouraging continuous improvement by reflecting on the team's performance and processes.
4. **Scrum Artifacts**
    - **Product Backlog**: How to create and manage a dynamic list of product requirements.
    - **Sprint Backlog**: Breaking down the Product Backlog into actionable tasks during Sprint planning.
    - **Increment**: Delivering potentially shippable increments at the end of each Sprint.
    - Defining the **"Definition of Done"**: Establishing clear criteria for when a product increment is considered complete.
5. **Facilitating and Coaching Agile Teams**
    - Best practices for facilitating Scrum ceremonies and ensuring productive meetings.
    - The role of the ScrumMaster in **coaching the team**, resolving conflicts, and fostering a culture of collaboration.
    - Techniques for **servant leadership**, guiding teams to self-organization, and empowering team members.
6. **Scaling Scrum for Large Projects**
    - How to scale Scrum for large organizations and manage multiple Scrum teams.
    - Introduction to concepts like **Scrum of Scrums**, used for coordinating efforts across multiple teams.

7. **Agile Metrics and Performance Tracking**
    - Using metrics like **velocity**, **burn-down charts**, and **burn-up charts** to measure progress and ensure transparency.
    - Tracking team performance and productivity while ensuring continuous improvement.
8. **Risk Management and Removing Impediments**
    - Identifying potential risks and managing uncertainties within the Scrum process.
    - Techniques for **removing impediments** and obstacles that block progress, and creating a high-performing team environment.
9. **Practical Scrum Simulations and Case Studies**
    - Real-world case studies and practical exercises to simulate Scrum implementations.
    - Hands-on activities that help participants practice creating backlogs, planning Sprints, conducting reviews and retrospectives, and more.
10. **Exam Preparation for CSM Certification**
    - Review of key concepts and Scrum practices.
    - Sample test questions and strategies to successfully pass the **Certified ScrumMaster (CSM) exam**.

Product Information:

- One license provides access to CertMaster Learn for Cloud+, Project+ and Security+ with CertMaster Labs integrated throughout the courses and ITI/partner courses and labs.
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Cloud+, Security+, Project+): This bundle includes an exam voucher and an exam pass guarantee for Cloud+, Security+, Project+; if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials,

including course content, labs, and practice prep questions, before taking your exam. The CSM exam is included with the CSM course.

Certified Security Control Assessor™ (CSCA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-12

Courses in bundle: CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CISA, CySA+, Fundamentals of Cyber Risk Management (FedVTE (now CISA Learning) (now CISA Learning))
MSRP: $4,499
Sales Price: $3,999
Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Security Control Assessor (Work Role Code: 612)

NICE Work Role: Security Control Assessment (Nice Work Role ID: OG-WRL-012)

Combined Work Role Description: Responsible for conducting independent, comprehensive assessments of management, operational, and technical security controls, as well as control enhancements employed within or inherited by an information technology (IT) system. These assessments are carried out to determine the overall effectiveness of the controls, in alignment with NIST 800-37 guidelines, ensuring both inherited and system-specific controls are robust and meet security standards.

High-level bundle description: The Certified Security Control Assessor™ (CSCA™) and Applied Micro Degree Bundle is designed to provide professionals with the comprehensive skills needed to assess and validate security controls within IT systems. The bundle integrates multiple industry-recognized certifications, including CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), and CISA. Additionally, participants benefit from the Fundamentals of Cyber Risk Management (FedVTE (now CISA Learning)) course, focusing on risk management frameworks, vulnerability assessment, and system security engineering. This program ensures learners develop expertise in conducting assessments aligned with NIST standards, particularly NIST 800-37, preparing them to effectively assess, manage, and secure IT infrastructures.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CySA+, Security+ and PenTest+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)

CySA+

CISA

Fundamentals of Cyber Risk Management (FedVTE (now CISA Learning) (now CISA Learning)) course description: This online, self-paced program is designed to introduce participants to key concepts and methodologies in cyber risk management. The course covers essential topics such as identifying critical assets, performing risk assessments, analyzing threats and vulnerabilities, and implementing effective mitigation strategies. Participants will also learn about various risk management frameworks, including standards like OCTAVE and CERT Resilience Management, along with security controls and response and recovery mechanisms.

Course Outline:

- **Introduction to Cyber Risk Management**: Overview of key concepts and importance of managing cyber risks.
- **Risk Management Framework**: Standards for risk management, OCTAVE framework, and the CERT Resilience Model.
- **Critical Assets and Operations**: Identifying critical assets and ensuring operational continuity.
- **Threats and Vulnerabilities**: Understanding and identifying threats and vulnerabilities, along with developing threat scenarios.
- **Risk Analysis and Mitigation**: Performing risk and impact analyses and developing mitigation strategies.
- **Security Controls**: Overview of control methods, types of security controls, and their assessment.
- **Mitigation Strategy Maintenance**: Ensuring continuous effectiveness of mitigation strategies, and conducting security testing and assessments.
- **Response and Recovery**: Incident response phases, business continuity plans, and disaster recovery strategies.

Product Information:

- One license provides access to CertMaster Learn for CompTIA courses with CertMaster Labs integrated throughout the courses and ITI/Partner courses and labs

- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

How to access FedVTE (now CISA Learning) (now CISA Learning): Register for an account and search for and sign up for the course.

Exam Voucher and Exam Pass Guarantee: This bundle includes an exam voucher and an exam pass guarantee for the CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Cyber Authorizing Official™ (CCAO™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-13

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+) and Project+ and PMP Bundle, CTI CISSP and CISM bundle, and FedVTE (now CISA Learning) (now CISA Learning) ISC CAP.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Authorizing Official/Designating Representative (Work Role Code: 611)

NICE Work Role: Systems Authorization (Nice Work Role ID: OG-WRL-013)

Combined Work Role Description: Responsible for developing and maintaining cybersecurity and cyberspace plans, strategies, and policies to support and align with organizational missions, initiatives, and regulatory compliance.

High-level bundle description: This This bundle prepares professionals for the Cyber Authorizing Official role, focusing on risk management, compliance, and security authorization within federal frameworks. The CompTIA Secure Cloud Professional (Security+ / Cloud+) and Project+ courses equip participants with foundational cloud security, project management, and multitier project planning (MPM) skills essential for overseeing authorization processes in cloud environments. The CTI CISSP and CISM bundle provides a robust understanding of security management, governance, and risk

mitigation, while the FedVTE (now CISA Learning) (now CISA Learning) ISC CAP course delivers targeted training on the Risk Management Framework (RMF), emphasizing assessment, authorization, and compliance with NIST standards. Together, these courses develop the skills needed to assess, authorize, and manage security programs within complex IT infrastructures.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, Project+ and Cloud+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud)

CISM and CISSP

Project+ and PMP bundle

FedVTE (now CISA Learning) (now CISA Learning) CAP course description: The Certified Authorization Professional (CAP) course provides in-depth training on implementing and managing the Risk Management Framework (RMF) as outlined by NIST. This course focuses on each RMF step, from categorization and control selection to continuous monitoring, giving participants the knowledge needed to authorize and oversee secure information systems in alignment with federal compliance standards. CAP covers key NIST publications, including SP 800-37 and SP 800-53, and emphasizes the skills required to evaluate, document, and enforce security controls across federal IT environments, ensuring ongoing compliance and effective risk management.

Course Outline (11+ hours)

- CAP Course Introduction
- Risk Management Approach to Security Authorization
- Risk Management Framework Steps
- Risk Management Framework Phases
- RMF Roles and Responsibilities
- Organization Wide Risk Management
- Managing Risk
- Assessor Independence and External Environments

- System Development Life Cycle
- Alignment of RMF with SDLC Review
- RMF Legal and Regulatory Requirements
- NIST Publications
- Continuous Monitoring Strategies
- RMF Guidance Review
- Defining Categorization
- Categorization Examples
- Categorization Process
- Security Plans and Registration
- Categorize
- Selection Step Tasks
- Selection Step Definitions
- Security Controls Guidance
- Privacy and Security Controls
- Control Selection and Supplemental Guidance
- Tailoring Security Controls
- Control Assurance and Monitoring
- Control Assurance and Monitoring - Continued
- Select
- Implementing Security Controls Overview
- Integrating Implementation
- Implement
- Preparing for Control Assessments
- Conducting Control Assessments
- Security Assessment Report
- Remediation Actions and Process Review

- Assess
- Authorization Documentation
- Risk Determination and Acceptance Part 1 of 3
- Risk Determination and Acceptance Part 2 of 3
- Risk Determination and Acceptance Part 3 of 3
- Authorization Decisions
- Prioritized Risk Mitigation and Authorization Review
- Authorize
- Assessments and Configuration Management
- Ongoing Security Control Assessments
- Monitor
- CAP Certification Prep Practice Exam

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs and other courses: An access key and instructions will be sent via email after your purchase is complete. To access the FedVTE (now CISA Learning) (now CISA Learning) ISC2 CAP course, users must register for a FedVTE (now CISA Learning) (now CISA Learning) account, available to U.S. government employees, military personnel, and veterans. Once registered, simply log in to FedVTE (now CISA Learning) (now CISA Learning) and use the search function to locate "ISC2 CAP" in the course catalog.

Exam Voucher and Exam Pass Guarantee (Cloud+, and Security+): This bundle includes an exam voucher and an exam pass guarantee for Cloud+, Project+ and Security+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Systems Certified Security Manager™ (SCSM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-14

Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), CompTIA CASP+, CISM and CISSP bundle, CISSP-ISSMP (FedVTE (now CISA Learning))

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Information Systems Security Manager (Work Role Code: 722)

NICE Work Role: Systems Security Management (Nice Work Role ID: OG-WRL-014)

Combined Work Role Description: Responsible for managing the cybersecurity of a program, organization, system, or enclave.

High-level bundle description: This bundle is a comprehensive program designed to equip cybersecurity professionals with both hands-on and management skills essential for securing and overseeing complex IT systems. It includes certifications such as CompTIA Security Analytics Professional (Security+ / CySA+), CompTIA CASP+, CISM, CISSP, and CISSP-ISSMP (FedVTE (now CISA Learning)), providing expertise in both practical security analytics and strategic governance. Participants will gain advanced competencies in threat detection, incident response, and risk management, as well as leadership skills for aligning cybersecurity practices with organizational goals and compliance frameworks. This program prepares professionals for senior roles in cybersecurity management with a balanced focus on technical application and executive oversight.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, CySA+, and CASP+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

CISM and CISSP

CompTIA CASP+

CISSP-ISSMP (FedVTE (now CISA Learning)) Course Description: This course equips participants with advanced knowledge in security management, risk management, leadership, governance, business continuity, and legal compliance. This training is intended for professionals in leadership positions responsible for developing, implementing, and overseeing security policies and programs.

Course Outline:

1. **Leadership and Business Management**: Managing information security programs to align with business goals.
2. **Risk Management**: Identifying, assessing, and mitigating security risks across enterprise environments.
3. **Governance and Legal Compliance**: Navigating legal requirements and ensuring compliance with various standards.
4. **Business Continuity Planning**: Developing and managing disaster recovery and continuity plans.
5. **Incident Management**: Leading incident response efforts and breach mitigation strategies.

This self-paced course includes interactive study materials, practice assessments, and 24/7 availability for learners. It prepares candidates for the CISSP-ISSMP certification by covering these five key domains comprehensively.

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs and other courses: An access key and instructions will be sent via email after your purchase is complete. To access the FedVTE (now CISA Learning) course, users must register for a FedVTE (now CISA Learning) account, available to U.S. government employees, military personnel, and veterans. Once registered, simply log in to FedVTE (now CISA Learning) and use the search function to locate the course catalog.

Exam Voucher and Exam Pass Guarantee (CompTIA) This bundle includes an exam voucher and an exam pass guarantee for CompTIA: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam, pass guarantee, you

must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified IT Portfolio Manager™ (CITPM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-15

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CISM, CISSP, CCSP, Project+ and PMP.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: IT Investment/Portfolio Manager (Work Role Code: 804)

NICE Work Role: Technology Portfolio Management (Nice Work Role ID: OG-WRL-015)

Combined Work Role Description: Manages a portfolio of IT capabilities and technology investments that align with the overall needs of mission and business enterprise priorities.

High-level bundle description: This bundle is designed to equip professionals with the essential skills and knowledge needed to effectively manage technology investments and align them with mission-critical enterprise priorities. This comprehensive bundle includes key courses such as CompTIA Secure Cloud Professional, CISM, CISSP, and CCSP, which cover critical areas of cloud security, risk management, and information systems security. By integrating these foundational and advanced topics, participants will be prepared to oversee IT portfolios strategically, ensuring optimal performance and alignment with organizational goals.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, Cloud+, Project+ and CISM certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

CISM and CISSP

Project+ and PMP

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Project+, Clout+ and Security+): This bundle includes an exam voucher and an exam pass guarantee for **Project+, Clout+ and Security+):**: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified IT Program Auditor™ (CITPA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-16

Courses in bundle: CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CISA, PECB ISO/IEC 20000 Auditor

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: IT Program Auditor (Work Role Code: 805)

NICE Work Role: Technology Program Auditing (Nice Work Role ID: OG-WRL-016)

Combined Work Role Description: Responsible for conducting comprehensive evaluations of technology and IT programs or their individual components to determine compliance with established standards. This includes assessing both technical and operational aspects to ensure adherence to published standards, policies, and best practices, with a focus on identifying areas for improvement and ensuring alignment with organizational objectives.

High-level bundle description: This comprehensive bundle is designed to equip IT professionals with the skills and certifications necessary to excel in auditing IT programs and ensuring compliance with industry standards. It includes the CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), the globally recognized CISA certification, and the PECB ISO/IEC 20000 Auditor credential. Through a blend of theoretical knowledge and hands-on labs, this bundle prepares participants

to identify vulnerabilities, assess risk, and audit IT systems and services effectively, all while earning an Applied Micro Degree.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, PenTest+ and PECB ISO/IEC 20000 Auditor certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)

CISA

PECB ISO/IEC 20000 Auditor Course Description: Add The ISO/IEC 20000 Lead Auditor course provides participants with the expertise to audit IT Service Management Systems (ITSMS) in accordance with the ISO/IEC 20000-1 standard. This comprehensive 5-day course covers the key principles of service management system auditing, including planning, conducting, and closing audits. Participants will gain hands-on experience in interpreting the standard's requirements, leading an audit team, and preparing audit reports. Upon passing the final exam, participants can apply for the prestigious "PECB Certified ISO/IEC 20000 Lead Auditor" credential, demonstrating their ability to audit and ensure compliance with ITSMS best practices.

Course Outline

Day 1: Introduction to IT Service Management Systems (ITSMS) and ISO/IEC 20000

- Course objectives and structure
- Overview of ISO/IEC 20000 standards and regulatory framework
- The certification process and audit standards (ISO 17021-1, ISO 19011)
- Fundamental concepts of IT service management (SMS)
- ISO/IEC 20000-1 requirements for an ITSMS (Clauses 4-10)

Day 2: Audit Principles and Preparation

- Fundamental audit concepts and principles
- Evidence-based auditing and risk-based auditing
- The impact of emerging trends and technology in auditing
- Audit planning and initiation (Stage 1 audit)

- Preparing the audit test plans

Day 3: On-site Audit Activities

- Preparing for the Stage 2 audit
- Conducting on-site audit activities and communication techniques
- Application of audit procedures and evidence collection
- Developing audit test plans

Day 4: Closing the Audit

- Drafting audit findings and nonconformity reports
- Audit documentation and quality review
- Evaluating corrective actions and audit closure
- Managing an internal audit program beyond the initial audit

Day 5: Final Examination

- Certification exam (PECB Certified ISO/IEC 20000 Lead Auditor exam)
- Review of key topics for the final exam
- Practical application scenarios and mock exam discussions

Product Information:

- One license provides access to CertMaster Learn for CompTIA courses with CertMaster Labs integrated throughout the courses and ITI and PECB courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA Security+ and PenTest+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

The PECB course comes with the exam and will be administered at the end of the course.

Certified Security Architect™ (CSA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-17

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CISM and CISSP bundle, CompTIA Server+ and Microsoft Bundle, CCSP, CASP+

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Security Architect (Work Role Code: 652)

NICE Work Role: Cybersecurity Architecture (Nice Work Role ID: DD-WRL-001)

Combined Work Role Description: Responsible for developing and maintaining cybersecurity and cyberspace plans, strategies, and policies to support and align with organizational missions, initiatives, and regulatory compliance.

High-level bundle description: Responsible for ensuring that security requirements are thoroughly integrated into all aspects of enterprise architecture, including reference models, segment and solution architectures, and the systems that protect and support organizational missions and business processes. This role involves designing security measures across the system development lifecycle, translating technology, environmental conditions, laws, and regulations into robust security designs and processes that align with organizational goals.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, Cloud+, Server+, and CASP+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

CISM and CISSP

CASP+

CompTIA Server+ and Microsoft Bundle

CCSP

CTI Custom Online Self-Paced Certified Cloud Security Professional (CCSP): This course This course covers key concepts, tools, technologies, and best practices for securing cloud environments. Students will learn about cloud architecture, legal and compliance issues, data security, platform and infrastructure security, application security, and security operations. The curriculum is designed to provide practical skills and real-world applications, ensuring that learners can effectively protect cloud-based assets and data.

Topics include:

- **Module 1 - Cloud Concepts, Architecture and Design**
  - Course Intro
  - Cloud Concepts, Architecture and Design - Part 1
  - Cloud Concepts, Architecture and Design - Part 2
  - Cloud Concepts, Architecture and Design - Part 3
  - Cloud Concepts, Architecture and Design - Part 4
  - Cloud Concepts, Architecture and Design - Part 5
  - Cloud Concepts, Architecture and Design - Part 6
  - Cloud Concepts, Architecture and Design - Part 7
  - Cloud Concepts, Architecture and Design - Part 8
  - Cloud Concepts, Architecture and Design - Part 9
- **Module 2 - Legal, Risk and Compliance**
  - Legal, Risk and Compliance Part 1
  - Legal, Risk and Compliance Part 2
  - Legal, Risk and Compliance Part 3
  - Legal, Risk and Compliance Part 4
  - Legal, Risk and Compliance Part 5
  - Legal, Risk and Compliance Part 6
  - Legal, Risk and Compliance Part 7
- **Module 3 - Cloud Data Security**
  - Cloud Data Security - Part 1
  - Cloud Data Security - Part 2
  - Cloud Data Security - Part 3
  - Cloud Data Security - Part 4
  - Cloud Data Security - Part 5
  - Cloud Data Security - Part 6
  - Cloud Data Security - Part 7
- **Module 4 - Cloud Platform and Infrastructure Security**
  - Cloud Platform and Infrastructure Security - Part 1
  - Cloud Platform and Infrastructure Security - Part 2
  - Cloud Platform and Infrastructure Security - Part 3
  - Cloud Platform and Infrastructure Security - Part 4
  - Cloud Platform and Infrastructure Security - Part 5
  - Cloud Platform and Infrastructure Security - Part 6
  - Cloud Platform and Infrastructure Security - Part 7

    - Cloud Platform and Infrastructure Security - Part 8
- **Module 5 - Cloud Application Security**
    - Cloud Application Security - Part 1
    - Cloud Application Security - Part 2
    - Cloud Application Security - Part 3
    - Cloud Application Security - Part 4
    - Cloud Application Security - Part 5
    - Cloud Application Security - Part 6
    - Cloud Application Security - Part 7
    - Cloud Application Security - Part 8
    - Cloud Application Security - Part 9
- **Module 6 - Cloud Security Operations**
    - Cloud Security Operations - Part 1
    - Cloud Security Operations - Part 2
    - Cloud Security Operations - Part 3
    - Cloud Security Operations - Part 4
    - Cloud Security Operations - Part 5
    - Cloud Security Operations - Part 6
    - Cloud Security Operations - Part 7
    - Cloud Security Operations - Part 8
    - Cloud Security Operations - Part 9
    - Cloud Security Operations - Part 10
    - Cloud Security Operations - Part 11

Product Information:

- One license provides access to CertMaster Learn for CompTIA courses with CertMaster Labs integrated throughout the courses and ITI and CTI courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA) This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses; if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Enterprise Security Architect™ (CESA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-18

Courses in bundle: CompTIA Cloud Admin Professional (Network+ / Cloud+), CompTIA CASP+, CTI CISSP and CISM bundle, CISSP-ISSEP (FedVTE (now CISA Learning)) and EC-Council Mastering Microsoft Sentinel and Cisco Certified CyberOps Associate (200-201)

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Enterprise Architect (Work Role Code: 651)

NICE Work Role: Enterprise Architecture (Nice Work Role ID: DD-WRL-002)

Combined Work Role Description: Develops and maintains business, systems, and information processes to support enterprise mission needs. This role involves creating IT and technology rules and requirements that define both baseline and target architectures, ensuring alignment with organizational goals and objectives. The architect is responsible for translating mission requirements into comprehensive IT solutions that support efficient and effective operations across the enterprise.

High-level bundle description: This bundle is a comprehensive program designed to prepare professionals for architecting secure, resilient enterprise systems. This bundle includes courses such as CompTIA Cloud Admin Professional (Network+ / Cloud+), CompTIA CASP+, CTI CISSP and CISM bundle, CISSP-ISSEP (FedVTE (now CISA Learning)), EC-Council Mastering Microsoft Sentinel, and Cisco Certified CyberOps Associate (200-201), providing expertise in network, cloud, and system security, as well as centralized monitoring and incident response. Participants will gain advanced skills in threat detection, infrastructure development, and compliance with security standards, equipping them to oversee and secure complex IT environments. Completing this program awards an Applied Micro Degree and multiple industry-recognized certifications, ideal for professionals tasked with developing and managing enterprise-level security architectures.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Network+, Cloud+ and CASP+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Cloud Admin Professional (Network+ / Cloud+)

CASP+

CISSP and CISM

EC-Council Mastering Microsoft Sentinel

EC-Council Cisco Certified CyberOps Associate (200-201)

CISSP-ISSEP

See each of the other course links for how to access the material and exam information.

Certified Secure Software Development Professional™ (CSSDP™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-19

Courses in bundle: DevOps Fundamentals, Agile Scrum Master – Master the Principles, Introduction to Python, Introduction to Programming Using Python (lab), Certified Kubernetes Administrator (CKA), Certified Kubernetes Application Developer (CKAD), Kubernetes - Containerizing Applications in the Cloud, CompTIA Secure Cloud Professional (Security+ / Cloud+)

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Software Developer (Work Role Code: 621)

NICE Work Role: Secure Software Development (Nice Work Role ID: DD-WRL-003)

Combined Work Role Description: Responsible for the complete lifecycle of software development, including planning, requirements gathering, risk management, design, development, architecture, and testing. This role focuses on creating, modifying, and maintaining secure computer applications, software, and specialized utility programs. Secure Software Developers implement software development methodologies, architectural structures, design decisions, and frameworks across all lifecycle phases while ensuring software security and quality standards are met. Key responsibilities include configuration management, modeling, estimation, and conducting security assessments to safeguard against vulnerabilities throughout the software development process.

High-level bundle description: This bundle offers a robust learning path for IT professionals seeking expertise in secure cloud-based software development and DevOps practices. This bundle covers key areas such as DevOps fundamentals, Agile Scrum methodologies, and Python programming, with both theoretical and hands-on labs. It includes advanced cloud-native skills with Kubernetes through Certified Kubernetes Administrator (CKA), Certified Kubernetes Application Developer (CKAD), and containerization in the cloud. The program is enhanced with CompTIA Secure Cloud Professional (Security+ / Cloud+), preparing participants to master secure, agile, and scalable development in cloud environments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Cloud+, Security+, and either Certified Kubernetes Administrator (CKA) or Certified Kubernetes Application Developer (CKAD) certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

DevOps Fundamentals and Introduction to Agile and Scrum

Introduction to Python Programming with Lab

Kubernetes Training Series

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI/CTI courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA) This bundle includes an exam voucher and an exam pass guarantee for CompTIA certifications: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Information Systems Security Developer™ (CISSD™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-20

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CCSP and FedVTE (now CISA Learning) CISSP-ISSEP

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Information Systems Security Developer (Work Role Code: 631)

NICE Work Role: Secure Systems Development (Nice Work Role ID: DD-WRL-004)

Combined Work Role Description: Designs, develops, tests, and evaluates secure information systems across the entire systems development lifecycle. This role focuses on ensuring that security is integrated into every phase, from initial design to deployment, with responsibilities that include secure coding, system vulnerability testing, and evaluating system security post-deployment. The developer also ensures that security requirements are met, continuously assesses risks, and incorporates best practices for maintaining robust system protection throughout the lifecycle.

High-level bundle description: This bundle prepares IT professionals to develop secure systems through a combination of critical cloud and network security skills. This bundle includes CompTIA Secure Cloud Professional (Security+ / Cloud+), CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CCSP, and FedVTE (now CISA Learning) CISSP-ISSEP. It focuses on secure systems design, vulnerability assessment, and cloud security, ensuring learners gain expertise in safeguarding systems from vulnerabilities throughout the development lifecycle. This program is ideal for professionals seeking to secure both on-premises and cloud environments, with a strong focus on hands-on security testing and compliance.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, Cloud+ and PenTest+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

The CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)

CCSP

FedVTE (now CISA Learning) CISSP-ISSEP

See each of the other course links for how to access the material and exam information.

Certified Secure Software Assessor™ (CSSA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-21

Courses in bundle: CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), Software Testing Fundamentals, CySA+, CISA and FedVTE (now CISA Learning) CISSP-ISSEP and Static Code Analysis and Supply Chain Assurance using Sonatype Nexus

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Secure Software Assessor (Work Role Code: 622)

NICE Work Role: Software Security Assessment (Nice Work Role ID: DD-WRL-005)

Combined Work Role Description: Responsible for analyzing the security of new or existing computer applications, software, or specialized utility programs. This role evaluates systems for vulnerabilities, assesses their security posture, and provides actionable recommendations to improve security measures. The assessor ensures that both current and newly developed software meet security standards throughout the development lifecycle, delivering results that mitigate risks and enhance system protection.

High-level bundle description: This bundle is designed to equip IT professionals with advanced skills in secure software assessment, vulnerability management, and code analysis. It includes key certifications such as CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), Software Testing Fundamentals, CompTIA CySA+, CISA, and FedVTE (now CISA Learning) CISSP-ISSEP, along with specialized training in Static Code Analysis using HPE Fortify and Synopsis Coverity and Supply Chain Assurance using Sonatype Nexus. Focused on securing software throughout its lifecycle, this program covers critical areas like vulnerability testing, cybersecurity analytics, and automated code review. Ideal for professionals seeking to specialize in software security, this comprehensive bundle ensures learners are equipped to identify risks and maintain stringent security standards across all development phases.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, PenTest+ and CySA+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)

CISA

FedVTE (now CISA Learning) CISSP-ISSEP

CySA+

Static Code Analysis and Supply Chain Assurance

Software Testing Fundamentals Lab Description: This 15-hour Practice Lab will provide you with the necessary platform to gain hands on skills in Microsoft Visual Studio. By completing the lab tasks you will improve your practical skills in creating software tests, automating software testing, testing fundamentals and methodologies, managing software testing projects and working with bugs.

Labs included:

- Fundamentals of Software Programming
- Unit and Integration Testing
- Performance Testing and Testing Tools
- Creating Use Case Diagrams
- Implementing Test Driven Development
- Exploratory Testing
- Log Bugs
- Define Test Automation Strategies
- Implement Test Automation
- Testing Methodologies
- Manage Software Testing Projects
- Manage Test Scripts

- Detecting Software Defects
- Manage Bugs

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Systems Requirements Planner™ (CSRP™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-22

Courses in bundle: CompTIA Network Infrastructure Professional (Network+ / Server+) with Microsoft bundle, Security+, CASP+, CCSP

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Systems Requirements Planner (Work Role Code: 641)

NICE Work Role: Systems Requirements Planning (Nice Work Role ID: DD-WRL-006)

Combined Work Role Description: Consults with customers (internal and external) to evaluate functional requirements and translate functional requirements and integrating security policies into technical solutions.

High-level bundle description: This comprehensive bundle is designed to equip IT professionals with the skills required to excel as a Systems Requirements Planner under the NICE and DoD 8140 frameworks. It includes key courses such as CompTIA Network Infrastructure Professional (Network+ / Server+), Security+, CASP+, and

Certified Cloud Security Professional (CCSP). Participants will develop expertise in network infrastructure, cybersecurity fundamentals, and advanced security practices, preparing them to evaluate functional requirements and integrate security policies into technical solutions. With a focus on translating customer needs into secure, effective architectures, this bundle is ideal for professionals aiming to master the Knowledge, Skills, Abilities, and Tasks (KSATs) essential for Systems Requirements Planning.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Network+, Server+, Security+, and CASP+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CompTIA Network Infrastructure Professional (Network+ / Server+)
- Security+
- CASP+
- CCSP

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified System Testing and Evaluation Specialist™ (CSTES™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-23

Courses in bundle: CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), Cloud+, CCSP, CISA, Software Testing Fundamentals

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: System Testing and Evaluation Specialist (Work Role Code: 671)

NICE Work Role: Systems Testing and Evaluation (Nice Work Role ID: DD-WRL-007)

Combined Work Role Description: The System Testing and Evaluation Specialist is responsible for planning, preparing, and executing tests of systems to ensure they meet specified requirements and standards. This role involves conducting thorough evaluations of test results against defined specifications, analyzing data to assess performance, and reporting findings. The specialist plays a critical role in verifying that systems function as intended and that they comply with security, performance, and technical specifications. Their responsibilities include not only executing the tests but also providing in-depth analysis and documentation of the outcomes to inform system improvements and validate overall system readiness.

High-level bundle description: This bundle is designed to equip IT professionals with advanced skills in **system testing**, vulnerability assessment, and cloud security through targeted certifications and specialized training. It includes comprehensive courses like CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), Cloud+, Certified Cloud Security Professional (CCSP), Certified Information Systems Auditor (CISA), and Software Testing Fundamentals. These courses provide essential expertise in areas such as vulnerability management, cloud security, and software testing. Participants will develop the skills needed to plan, prepare, and execute system tests, ensuring systems meet performance and security standards across their lifecycle. This bundle is ideal for professionals focused on safeguarding system integrity and ensuring compliance with technical and operational requirements.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the (Security+, PenTest+ and Cloud+, certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

- CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)
- CISA

- Cloud+
- CCSP

Software Testing Fundamentals Lab Description: This 15-hour Practice Lab will provide you with the necessary platform to gain hands on skills in Microsoft Visual Studio. By completing the lab tasks you will improve your practical skills in creating software tests, automating software testing, testing fundamentals and methodologies, managing software testing projects and working with bugs.

Labs included:

- Fundamentals of Software Programming
- Unit and Integration Testing
- Performance Testing and Testing Tools
- Creating Use Case Diagrams
- Implementing Test Driven Development
- Exploratory Testing
- Log Bugs
- Define Test Automation Strategies
- Implement Test Automation
- Testing Methodologies
- Manage Software Testing Projects
- Manage Test Scripts
- Detecting Software Defects
- Manage Bugs

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Research & Development Specialist™ (CRDS™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-24

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CASP+, CompTIA Linux Network Professional (Network+ / Linux+) and CEH

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Research & Development Specialist (Work Role Code: 661)

NICE Work Role: Technology Research and Development (Nice Work Role ID: DD-WRL-008)

Combined Work Role Description: The Research & Development Specialist is responsible for conducting software and systems engineering, along with software systems research, to develop new capabilities that integrate cybersecurity from the outset. This role involves conducting comprehensive technology research to evaluate and address potential vulnerabilities in cyberspace systems. The specialist plays a crucial role in advancing system capabilities while ensuring robust cybersecurity measures are embedded throughout the development process, helping organizations stay ahead of emerging threats and technological advancements.

High-level bundle description: This bundle is designed to equip IT professionals with advanced skills in cybersecurity, cloud security, and network and system vulnerability assessment through targeted certifications and specialized training. It includes key courses such as CompTIA Secure Cloud Professional (Security+ / Cloud+), CASP+, CompTIA Linux Network Professional (Network+ / Linux+), and Certified Ethical Hacker (CEH). These courses provide essential expertise in cloud security, penetration testing, networking, and cybersecurity defense, enabling participants to conduct comprehensive research, evaluate potential vulnerabilities, and develop new capabilities with cybersecurity fully integrated. Ideal for professionals in Research & Development, this bundle ensures learners are well-prepared to advance system capabilities while maintaining robust security across the development lifecycle.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Network+, CASP+ and Linux+, certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

- CompTIA Secure Cloud Professional (Security+ / Cloud+)
- CASP+
- CompTIA Linux Network Professional (Network+ / Linux+)
- CEH (CTI course and lab only)

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Data Analyst Professional™ (CDAP™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-25

Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), CompTIA Data+ and Data Analyst Bundle.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Data Analyst (Work Role Code: 422)

NICE Work Role: Data Analysis (Nice Work Role ID: IO-WRL-001)

Combined Work Role Description: The Data Analyst is responsible for analyzing and interpreting data from multiple disparate sources to provide actionable insights into cybersecurity and privacy. This role involves designing and implementing custom algorithms, workflow processes, and layouts for large-scale enterprise data sets used in modeling, data mining, and research. Additionally, the Data Analyst builds visualizations and dashboards to effectively communicate findings, enabling organizations to make data-driven decisions while addressing complex cybersecurity challenges.

High-level bundle description: This bundle is designed to equip aspiring data analysts with advanced skills in data collection, cybersecurity analytics, data visualization, and analysis techniques. It includes comprehensive courses such as CompTIA Security Analytics Professional (Security+ / CySA+), CompTIA Data+, and the CTI Custom Data Analyst Online Self-Paced ILT, which covers tools like Microsoft Power BI, Excel, and SQL Server. Participants will gain expertise in analyzing data from multiple sources, building custom dashboards, and applying advanced data analytics to support cybersecurity and privacy decision-making. Ideal for professionals looking to specialize in data analysis for cybersecurity, this bundle ensures they are well-prepared to interpret complex data sets and provide valuable insights across various enterprise environments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, CySA+ and CompTIA Data+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

CompTIA Data+ and the CTI Custom Data Analyst

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Database Admin Professional™ (CDAP™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-26

Courses in bundle: CompTIA DataSys+, Security+, CASP+, Microsoft SQL Server 2019 Administration and Microsoft SQL Server 2019 Database Design, Oracle Database 12c Certification (1Z0-061 & 1Z0-062)

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Database Administrator (Work Role Code: 421)

NICE Work Role: Database Administration (Nice Work Role ID: IO-WRL-002)

Combined Work Role Description: The Database Administrator is responsible for administering databases and data management systems that enable the secure storage, querying, protection, and utilization of data. This role ensures that databases are properly maintained, optimized, and safeguarded to support data integrity, confidentiality, and availability. The Database Administrator plays a key role in managing access controls, monitoring performance, and ensuring the overall security of data systems to meet organizational needs.

High-level bundle description: This bundle is designed to provide IT professionals with the essential skills needed for database administration, including secure data management and advanced database operations. It includes comprehensive courses such as CompTIA DataSys+, Security+, CASP+, Microsoft SQL Server 2019 Administration and Database Design, and Oracle Database 12c Certification (1Z0-061 & 1Z0-062). Participants will gain expertise in managing and securing databases, optimizing performance, and ensuring data integrity and availability. Ideal for those looking to specialize in database administration, this bundle equips learners with the knowledge and skills required to support secure, efficient database environments across various platforms.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the DataSys+, Security+, and CASP+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

DataSys+, Microsoft and Oracle Bundle

Security+

CASP+

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Secure Knowledge Manager™ (CSKM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-27

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), Network+, HDI KCS Principles Certification, Microsoft 365 Fundamentals – MS-900

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Knowledge Manager (Work Role Code: 431)

NICE Work Role: Knowledge Management (Nice Work Role ID: IO-WRL-003)

Combined Work Role Description: The Knowledge Manager is responsible for managing and administering the processes and tools that enable an organization to effectively identify, document, and access its intellectual capital and information content. This role involves ensuring that knowledge management systems and practices are aligned with organizational goals, making critical information accessible while maintaining security and compliance. By overseeing the implementation of these processes, the Knowledge Manager supports knowledge sharing, collaboration, and decision-making across the enterprise.

High-level bundle description: The Certified Secure Knowledge Manager™ (CSKM™) and Applied Micro Degree Bundle provides a complete learning path for professionals aiming to enhance their secure knowledge management capabilities. This bundle integrates key principles of Knowledge-Centered Service (KCS) and advanced cybersecurity strategies, equipping learners to manage sensitive information securely while improving knowledge capture, organization, and reuse. Ideal for individuals in IT service and security management roles, this bundle prepares participants for leadership in secure knowledge management environments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+, Cloud+, HDI KCS Principles certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional

Network+

ITI Partner Delivered KCS Principles Course Description: The KCS Principles course teaches the Knowledge-Centered Service (KCS) methodology, designed to enhance organizational efficiency by effectively managing and sharing knowledge. Participants will learn to capture, structure, and reuse knowledge, improving the speed and quality of service delivery. The course covers key topics such as knowledge capture, search optimization, and continuous improvement strategies. By the end of the course, participants will be well-prepared to implement KCS methodologies within their organizations. Online, self-paced training allows student to train at their own speed, permitting them to concentrate on areas of specific need. Students can train from any computer with Internet access, and the course takes about 10-12 hours to complete.

Course outline

- Unit 1: What Is Knowledge-Centered Service (KCS)?
    - What Is Knowledge-Centered Service?
    - What Led to the Development of KCS?
    - KCS Principles
    - Why Do You Need KCS?
    - What Are the Benefits of KCS?
- Unit 2: The KCS Principles and Core Concepts
    - KCS Principles
    - KCS Core Concepts
- Unit 3: The KCS Practices
    - The KCS Practices
    - Understanding KCS
    - The KCS Methodologies
- Unit 4: Aligning KCS with the Business
    - Aligning Business Goals and Objectives
    - Providing Additional Value with KCS
    - KCS Benefits and ROI
- Unit 5: Content Health
    - The Content Standard
    - KCS Article State
    - Developing A Content Standard
    - Creating Evolve Loop Articles
    - Archiving Old Articles
    - Dealing with Legacy Data
    - Priming the Knowledge Base
    - Global Support Considerations
    - Knowledge Domain Analysis

- Content Health Indicators
- Self-Service Success
- Self-Service Measures

- Unit 6: KCS Roles and Responsibilities
  - KCS Roles and Licensing Model
  - The KCS Licensing Model
  - Defining Roles and Competencies

- Unit 7: Process Integration
  - Process Integration
  - Structured Problem Solving
  - Seamless Technology Integration
  - Search Technology for KCS
  - Closed Loop Feedback
  - KCS Process Integration Indicators
  - Unit 8: Performance Assessment
  - Assessing the Creation of Value
  - Feedback and Reputation Model
- Unit 9: Leadership
  - Leadership
  - Tap into Internal Motivators
  - Recognition Programs
  - Compelling Purpose
  - Promote Teamwork
- Unit 10: Communication
  - Communication
  - Key Messaging and Elevator Pitches
  - Handling Questions and Objections

    - Programs for Social Engagement
- Unit 11: Technology
    - Functional Requirements
    - Technology Selection
    - KCS Verified
- Unit 12: The KCS Adoption Roadmap
    - The KCS Adoption Program
    - Adoption Phases
    - Adoption Roles
    - KCS Implementation Strategy
    - KCS Investment
    - Critical Success Factors

CTI Course Description for Microsoft 365 Fundamentals: This course introduces key concepts of Microsoft 365 which includes services and tools that are essential for secure knowledge management, collaboration, and data sharing in enterprise environments. This course covers Microsoft Teams, SharePoint, and OneDrive, emphasizing their role in facilitating secure communication and document management across organizations. Participants can explore and envision how these tools support effective knowledge sharing, while ensuring compliance, privacy, and data protection. In addition to collaborative tools, the course provides an overview of cloud computing concepts, Microsoft 365 security solutions, and the licensing and support models available. This foundational knowledge prepares learners to manage Microsoft 365 environments efficiently and supports the attainment of the MS-900 certification.

Course Outline (3+ hours):

- Module 1: Introduction to Cloud Concepts
    - Module 1.1 - Course Introduction
    - Module 1.2 - Introduction to Cloud Computing
    - Module 1.3 - Microsoft SaaS, PaaS, IaaS Offerings
    - Module 1.4 - Cloud, Hybrid, On-Premises Models - Benefits and Considerations
    - Module 1.5 - Exploring Public, Private and Hybrid Cloud Models

- Module 1.6 - Cost Benefit of Cloud Solutions
- Module 1.7 - The Hybrid Work and Flexible Work Concept
- Module 1.8 - Introducing Microsoft Co-Pilot
- Module 1.9 - Microsoft 365 Tenant

- Module 2: Microsoft 365 Apps and Services
  - Module 2.1 - Core Productivity Solutions
  - Module 2.2 - Work Management in Microsoft 365
  - Module 2.3 - Collaboration Solutions
  - Module 2.4 - Microsoft Teams and Teams Phone Deep Dive
  - Module 2.5 - Extending Teams with Collaborative Apps
  - Module 2.6 - Endpoint Management with Microsoft Intune
  - Module 2.7 - Windows 365 vs. Azure Virtual Desktop
  - Module 2.8 - Deployment and Update Channels for Microsoft 365
  - Module 2.9 - Analytics in Microsoft 365
- Module 3: Security, Compliance, Privacy, and Trust in Microsoft 365
  - Module 3.1 - Identity and Access Management with Microsoft Entra
  - Module 3.2 - Threat Protection - Defender Suite Overview
  - Module 3.3 - Zero Trust Model and Compliance Solutions
  - Module 3.4 - Information Protection and Data Residency
- Module 4: Microsoft 365 Pricing, Licensing, and Support
  - Module 4.1 - Understanding Microsoft 365 Pricing and Billing
  - Module 4.2 - Licensing Options and Management
  - Module 4.3 - Microsoft 365 Support, SLAs and Monitoring Service
  - Module 4.4 - Microsoft 365 Fundamentals Course Closeout

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase

- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam. The HDI KCS Principles certification exam is included and must be completed within 12 weeks of purchase. For KCS, A 28-day extension is available for an online exam for a fee of $50, an Exam retake can be purchased for a fee of $99 and practice test can be purchased for $79.

Certified Network Operations Specialist™ (CNOS™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-28

Courses in bundle: CompTIA Cloud Admin Professional (Network+ / Cloud+), CASP+, MTA 98-365-r1, Azure Administrator, Linux+, Windows Server 2019 - Administration Concepts, CCNA

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Network Operations Specialist (Work Role Code: 441)

NICE Work Role: Network Operations (Nice Work Role ID: IO-WRL-004)

Combined Work Role Description: Responsible for developing and maintaining cybersecurity and cyberspace plans, strategies, and policies to support and align with organizational missions, initiatives, and regulatory compliance.

High-level bundle description: This bundle is designed to equip IT professionals with the essential skills to manage and maintain secure network operations across various environments. The Certified Network Operations Specialist™ (CNOS™) and Applied Micro Degree Bundle includes comprehensive training through courses such as CompTIA Secure Cloud Professional (Security+ / Cloud+), CompTIA Linux Network Professional (Network+ / Linux+), CompTIA Cloud Admin Professional (Network+ / Cloud+), and CCNA. These courses provide participants with key competencies in network infrastructure, cloud security, and cybersecurity defense. Focusing on developing the abilities required to align network operations with organizational missions and regulatory compliance, this bundle prepares learners to

excel in cybersecurity planning and network administration. Ideal for professionals pursuing advanced proficiency in network operations, this bundle ensures that learners are equipped to design, maintain, and secure complex network environments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Network+, Cloud+ and Security+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Linux Network Professional (Network+ / Linux+)

CompTIA Cloud Admin Professional (Network+ / Cloud+)

CompTIA Secure Cloud Professional (Security+ / Cloud+)

CCNA Bundle

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Secure System Administrator™ (CSSA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-29

Courses in bundle: CompTIA Linux Network Professional (Network+ / Linux+), CASP+, CompTIA Server+ and Microsoft Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: System Administrator (Work Role Code: 451)

NICE Work Role: Systems Administration (Nice Work Role ID: IO-WRL-005)

Combined Work Role Description: The System Administrator is responsible for installing, configuring, troubleshooting, and maintaining both hardware and software systems in alignment with organizational security policies and procedures. This includes managing system accounts, performing backups and recovery, applying updates, and implementing security controls to ensure the stability and security of systems. The role encompasses setting up and maintaining specific components of a system to ensure optimal performance and compliance with security standards.

High-level bundle description: This bundle is designed to equip IT professionals with the essential skills for managing and securing complex IT systems and server environments. The Certified Secure System Administrator™ (CSSA™) and Applied Micro Degree Bundle includes CompTIA Linux Network Professional (Network+ / Linux+), CASP+, and the CompTIA Server+ and Microsoft Bundle, providing in-depth training in server management, network administration, and hybrid cloud environments. Participants will benefit from a blended learning approach that includes self-paced instructor-led training, hands-on lab simulations, and comprehensive exam preparation. This bundle prepares learners with the expertise to manage secure, high-performance system infrastructures while adhering to industry best practices. It is ideal for professionals focused on securing and maintaining servers and networked systems in diverse environments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Linux+, CASP+, CompTIA Server+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Linux Network Professional (Network+ / Linux+)

CASP+

CompTIA Server+ and Microsoft Bundle

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs

- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Systems Security Analyst™ (CSSA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-30

Courses in bundle: CompTIA Security Analytics Expert (Security+ / CySA+ / CASP+) and Linux+ (course and labs only) and EC-Council NIST SP 800-53 Controls Mastery Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Systems Security Analyst (Work Role Code: 461)

NICE Work Role: Systems Security Analysis (Nice Work Role ID: IO-WRL-006)

Combined Work Role Description: The Systems Security Analyst is responsible for developing and analyzing the security of systems and software throughout their entire lifecycle. This includes integration, testing, operations, and maintenance. The role involves managing and implementing security measures during system setup and ensuring ongoing security during operation. The Systems Security Analyst plays a key role in preparing, performing, and overseeing the security aspects of system implementation and daily operations, ensuring that security controls are effectively integrated and maintained.

High-level bundle description: This bundle is designed to equip IT professionals with the skills necessary to secure and analyze systems across their lifecycle. The Certified Systems Security Analyst™ (CSSA™) and Applied Micro Degree Bundle includes comprehensive courses like CompTIA Security Analytics Expert (Security+ / CySA+ / CASP+) and Linux+, providing a strong foundation in systems security analysis,

advanced cybersecurity practices, and Linux-based environments. Participants will gain expertise in security analytics, incident response, threat detection, and system hardening, preparing them for roles in developing and maintaining secure systems. This bundle is ideal for professionals focused on integrating, testing, and maintaining robust security throughout the operations and maintenance phases of system management.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for Security+ CySA+, and CASP+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Expert (Security+ / CySA+ / CASP+)

Linux+ (course and labs only)

EC-Council NIST SP 800-53 Controls Mastery Bundle

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Technical Support Technician™ (CTST™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-31

Courses in bundle: CompTIA Secure Infrastructure Specialist (A+ / Network+ / Security+), CompTIA Systems Support Specialist (A+ / Linux+), CompTIA IT Operations

Specialist (A+ / Network+), CompTIA Linux Network Professional (Network+ / Linux+), HDI-SCA

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Technical Support Specialist (Work Role Code: 411)

NICE Work Role: Technical Support (Nice Work Role ID: IO-WRL-007)

Combined Work Role Description: The Technical Support Specialist is responsible for providing technical assistance to customers who need help with client-level hardware and software. This includes troubleshooting, resolving issues, and guiding users in accordance with established organizational policies and processes, such as incident management plans. The specialist ensures that users can effectively utilize their technology, while adhering to company procedures and maintaining system integrity.

High-level bundle description: This bundle is designed to provide IT professionals with the comprehensive skills needed to deliver effective technical support across client-level hardware and software environments. The Certified Technical Support Technician™ (CTST™) and Applied Micro Degree Bundle includes stackable courses such as CompTIA Secure Infrastructure Specialist, CompTIA Systems Support Specialist, CompTIA IT Operations Specialist, and, CompTIA Linux Network Professional, as well as HDI Support Center Analyst (HDI-SCA), offering a robust foundation in both soft skills (e.g., communications, critical thinking, contact handling procedures) and hard skills (e.g., troubleshooting, system administration, and network operations). Participants will gain practical expertise in diagnosing and resolving technical issues, managing secure IT infrastructures, and supporting users in accordance with organizational policies and incident management plans. Ideal for individuals focused on technical support roles, this bundle prepares learners for multiple industry-recognized certifications and provides the tools needed to deliver high-quality, secure support services.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the A+, Network+, and Security+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Infrastructure Specialist (A+ / Network+ / Security+)

CompTIA Systems Support Specialist (A+ / Linux+)

HDI-SCA

Product Information:

- One license provides access to CertMaster Learn for CompTIA with CertMaster Labs integrated throughout the courses and ITI and partner courses and labs
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (CompTIA): This bundle includes an exam voucher and an exam pass guarantee for CompTIA courses: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

Certified Cyber Defense Analyst™ (CCDA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-32

Courses in bundle: EC-Council ECIH, CSA, CTIA, and CEH (Course and Labs only) and CompTIA CySA+

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Cyber Defense Analyst (Work Role Code: 511)

NICE Work Role: Defensive Cybersecurity (Nice Work Role ID: PD-WRL-001)

Combined Work Role Description: The Cyber Defense Analyst is responsible for using data collected from various cybersecurity defense tools, such as intrusion detection systems (IDS), firewalls, and network traffic logs, to analyze events within their environment. This analysis is aimed at identifying, mitigating, and responding to potential threats. The role involves monitoring security systems, detecting vulnerabilities, and ensuring the organization's networks and systems remain protected from cyberattacks.

High-level bundle description: This bundle is designed to provide IT professionals with advanced skills in cybersecurity defense and threat analysis. The Certified Cyber Defense Analyst™ (CCDA™) and Applied Micro Degree Bundle includes courses such as EC-Council's ECIH (Incident Handler), CSA (Certified SOC Analyst), CTIA (Certified Threat Intelligence Analyst), and CompTIA CySA+. These courses offer a comprehensive foundation in incident response, threat intelligence, and cyber defense. Participants will learn how to analyze and respond to security incidents, mitigate threats using real-time data from various defense tools, and enhance their ability to protect organizational networks. Ideal for those seeking to specialize in cyber defense, this bundle prepares learners for key industry certifications and equips them with the skills needed to identify, analyze, and respond to cybersecurity threats effectively.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the EC-Council ECIH, CSA, and CTIA, and CompTIA CySA+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- SOC and Incident Handling Bundle
- CompTIA CySA+
- CTI CEH (Course and Labs only)

Certified Cyber Forensics Analyst™ (CCFA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-33

Courses in bundle: CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CHFI (course and lab only), CySA+, PECB Certified Forensic Examiner

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Cyber Defense Forensics Analyst (Work Role Code: 212)

NICE Work Role: Digital Forensics (Nice Work Role ID: PD-WRL-002)

Combined Work Role Description: The Cyber Defense Forensics Analyst is responsible for analyzing digital evidence from computer security incidents to uncover useful information that supports system and network vulnerability mitigation. This role

involves conducting investigations, gathering evidence, and using forensic tools and techniques to help identify security weaknesses, assess the impact of incidents, and support broader cybersecurity efforts aimed at preventing future breaches

High-level bundle description: This bundle is designed to equip IT professionals with specialized skills in digital forensics, vulnerability assessment, and incident response. The Certified Cyber Forensics Analyst™ (CCFA™) and Applied Micro Degree Bundle includes courses such as CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), EC-Council's CHFI (Computer Hacking Forensic Investigator) course and lab, and CompTIA CySA+. These courses provide a comprehensive foundation in investigating security incidents, analyzing digital evidence, and identifying system vulnerabilities. Participants will learn how to conduct forensic investigations, analyze compromised systems, and support cybersecurity efforts through vulnerability mitigation. This bundle is ideal for professionals seeking to develop expertise in digital forensics and cyber incident analysis, preparing them for key certifications and advanced roles in cybersecurity defense.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CySA+, Security+ and PenTest+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)
- CTI CHFI (course and lab only)
- CySA+
- PECB Certified Forensic Examiner

See each course link for how to access the material and exam information.

Certified Cyber Incident Responder™ (CCIR™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-34

Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), Cloud+, EC-Council ECIH

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Cyber Defense Incident Responder (Work Role Code: 531)

NICE Work Role: Incident Response (Nice Work Role ID: PD-WRL-003)

Combined Work Role Description: The Cyber Defense Incident Responder is responsible for investigating, analyzing, and responding to cybersecurity incidents within a network environment or enclave. This role involves identifying the source and impact of security breaches, containing threats, and mitigating vulnerabilities to prevent future incidents. The incident responder plays a key role in maintaining network security by using a range of tools and techniques to detect and address potential risks in real time.

High-level bundle description: This bundle is designed to provide IT professionals with the skills needed to secure, monitor, and respond to cyber threats in cloud and network environments. The CompTIA Security Analytics Professional bundle includes Security+, CySA+, Cloud+, and EC-Council's ECIH (Certified Incident Handler). These courses offer a comprehensive foundation in cybersecurity analytics, incident response, and cloud security, focusing on threat detection, incident handling, and vulnerability management. Participants will learn to analyze security events, implement cloud security solutions, and respond effectively to cybersecurity incidents. This bundle is ideal for professionals looking to develop expertise in both security operations and incident response, preparing them for key industry certifications and advanced roles in cybersecurity.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+, CySA+, and EC-Council ECIH certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

Cloud+

Official EC-Council ECIH

See each course link for how to access the material and exam information.

Certified Infrastructure Support Specialist™ (CISS™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-35

Courses in bundle: Certified Network Defender – EC-Council CND and CEH Blended Bundle, CISSP-ISSEP (FedVTE (now CISA Learning)), CTI Linux+ (course and lab only) and CASP+

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Cyber Defense Infrastructure Support Specialist (Work Role Code: 521)

NICE Work Role: Infrastructure Support (Nice Work Role ID: PD-WRL-004)

Combined Work Role Description: The Cyber Defense Infrastructure Support Specialist is responsible for testing, implementing, deploying, maintaining, and administering the infrastructure hardware and software that supports cybersecurity operations. This role involves ensuring the reliability and security of the systems by managing infrastructure components and providing ongoing support to protect against cyber threats. The specialist ensures that the infrastructure is maintained according to security protocols and operational requirements.

High-level bundle description: This bundle is designed to equip IT professionals with the skills needed to support and secure network infrastructure in complex environments. The Certified Infrastructure Support Specialist™ (CISS™) and Applied Micro Degree Bundle includes courses such as Certified Network Defender (CND) and Certified Ethical Hacker (CEH), CISSP-ISSEP (FedVTE (now CISA Learning)), CompTIA Linux+ (course and lab), and CASP+. These courses provide a comprehensive foundation in defending, maintaining, and administering infrastructure systems, with a focus on cybersecurity, ethical hacking, and advanced network defense strategies. Participants will learn to test, implement, deploy, and maintain secure infrastructure, ensuring compliance with industry standards and protecting networks from emerging threats. This bundle is ideal for professionals looking to strengthen their expertise in infrastructure support, preparing them for key certifications and advanced roles in cybersecurity infrastructure management.

Requirements for certification: To earn the ITI Certification™ and be awarded the applied micro degree, the student must complete all courses and pass the exams for the EC-Council CND and CompTIA CASP+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CND a CEH bundle
- CISSP-ISSEP (FedVTE (now CISA Learning))

- CASP+
- Linux+ (Course and labs only)

See each course link for how to access the material and exam information.

Certified Threat Warning Analyst™ (CTWA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-36

Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), EC-Council CTIA, CTI CEH with Labs, and EC-Council Master Threat Intelligence Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Warning Analyst (Work Role Code: 141)

NICE Work Role: Threat Analysis (Nice Work Role ID: PD-WRL-006)

Combined Work Role Description: Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment. Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.

High-level bundle description: This bundle is designed to equip IT professionals with advanced skills in threat detection, analysis, and response. The Bundle includes courses such as CompTIA Security Analytics Professional (Security+ / CySA+), EC-Council Certified Threat Intelligence Analyst (CTIA), and Certified Ethical Hacker (CEH) with labs. These courses provide a strong foundation in cybersecurity analytics, threat intelligence, and ethical hacking, focusing on detecting and mitigating potential cyber threats before they materialize. Participants will develop the expertise needed to analyze security data, identify emerging threats, and implement effective warning systems to protect organizational networks. This bundle is ideal for professionals in roles that involve monitoring and analyzing cybersecurity threats, preparing them for certifications and roles in threat analysis and defense.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, CySA+ and EC-Council CTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

EC-Council CTIA

CTI CEH with Labs (course and labs only, no exam)

EC-Council Master Threat Intelligence Bundle

See each course link for how to access the material and exam information.

Certified Insider Threat Program™ – Insider Threat Core

SKU: CITPCORE

Price: Free (with access to FedVTE (now CISA Learning) and purchase of Certified Insider Threat Professional Bundle)

High-level Description: The Certified Insider Threat Program™ – Insider Threat Core (CITPCORE) serves as the foundational curriculum for all Certified Insider Threat Professional™ (CITP™) certifications. While this core curriculum provides essential knowledge, each certification also includes additional specialized course requirements unique to its focus area.

All CITP™ certifications map to and meet the NICE Workforce Category for Insider Threat Analysis and align with at least one additional work role defined by the National Initiative for Cybersecurity Education (NICE) or the DoD Cyber Workforce Framework (DCWF/8140). This alignment ensures that participants gain the necessary knowledge, skills, and abilities (KSAs) to fulfill multiple operational roles.

The curriculum is designed to meet the highest federal standards, including EO 13587, DoD 8140, and NITTF guidelines, ensuring students are prepared to manage insider threats effectively across federal, state, and private-sector environments.

Core Components

Publicly Accessible CDSE Courses (https://securityawareness.usalearning.gov)

These courses provide a baseline understanding of insider threat awareness, program development, and related security measures.

- **Insider Threat Awareness (60 Min)** – Covers the basics of recognizing and reporting insider threats. This foundational course is essential for all personnel, helping them identify behaviors that may indicate risks and emphasizing proactive reporting of suspicious activities.
- **Establishing an Insider Threat Program (60 Min)** – Teaches strategies for building and managing insider threat programs in alignment with federal standards. This course provides a foundational understanding for developing comprehensive programs that detect and mitigate risks effectively.

- Maximizing Organizational Trust (60 Min) – Promotes early detection through trust-building strategies. Highlights trust-building strategies as a critical element in early threat detection. By fostering trust, organizations can encourage employees to report concerns more openly, aiding in quicker identification of potential threats.
- OPSEC Awareness (30 Min) – Teaches operational security measures to protect critical information. Focuses on operational security measures to protect critical information, a core element in preventing insider threats. This course emphasizes the need for employees to safeguard sensitive information, reducing unintentional or malicious disclosures.
- Counterintelligence Awareness and Reporting (60 Min) – Provides tools to identify and report counterintelligence threats, key to mitigating insider risks. This training equips individuals to recognize espionage indicators, strengthening defense against insider actions harmful to U.S. interests.
- Counterintelligence Awareness and Security Brief (30 Min) - Although designed primarily for defense contractors, this course is relevant for government roles where insider threat awareness is critical. It educates employees on spotting suspicious activities that could lead to data leaks or espionage.
- Thwarting the Enemy: Counterintelligence and Threat Awareness Information to the Defense Industrial Base (30 Min) - Although designed primarily for defense contractors, this course is relevant for government roles where insider threat awareness is critical. It covers threats to U.S. technology and the importance of reporting suspicious activities. This training is essential for employees in defense sectors, reinforcing the importance of vigilance against unauthorized access and leaks.
- Unauthorized Disclosure of Classified Information and Controlled Unclassified Information (60 Min) – This course discusses the risks and consequences of unauthorized information disclosures, a primary insider threat concern. Understanding these risks helps prevent leaks and equips employees to recognize potential security breaches.
- Introduction to the Risk Management Framework (RMF) (30 Min) - This course Provides an overview of RMF, highlighting its role in risk mitigation within IT environments. RMF processes help prevent vulnerabilities that insiders could exploit, supporting proactive threat management.

FedVTE (now CISA Learning) Courses

Free, self-paced courses for government employees, contractors, and veterans:

- Insider Threat Program Manager: Implementation and Operations– Develops skills to build and manage insider threat programs. (need more detail)

- **Insider Threat Analysis**– Focuses on multi-source data analysis to detect and mitigate insider threats. (need more detail)

FEMA Independent Study Courses

These courses focus on security awareness and insider threat mitigation with built-in assessments:

- IS-906: Workplace Security Awareness - Enhances workplace security awareness, encouraging employees to identify and report insider risks. A foundational course that supports a culture of vigilance organization-wide
- IS-907: Active Shooter: – Provides guidance on responding to active shooter situations. While focused on emergency preparedness, it also promotes awareness of unusual behaviors that could indicate insider threats.
- IS-912: Retail Security Awareness: – Teaches situational awareness skills in high-traffic environments, which can help employees identify insider threats in similar settings.
- IS-914: Surveillance Awareness: – Provides tools for recognizing suspicious surveillance activities. This awareness is vital in identifying early signs of insider risk behaviors, especially in sensitive environments.
- IS-915: Protecting Critical Infrastructure Against Insider Threats – Focuses on safeguarding critical infrastructure from insider threats. This course emphasizes the importance of reporting vulnerabilities that could be exploited internally.
- IS-916: Critical Infrastructure Security: Theft and Diversion – Addresses theft and diversion risks, teaching employees to recognize and report insider activities that may disrupt critical operations.

EC-Council Learning Courses

Advanced skills training provided through EC-Council Learning:

- **Mastering Threat Intelligence** (14 hours) - Teaches skills to collect, analyze, and act on threat intelligence, supporting proactive insider threat mitigation. By understanding threat intelligence, analysts can anticipate and counter potential insider actions
- **Master Open-Source Intelligence (OSINT)** (14 hours) – Provides expertise in gathering OSINT, useful for detecting insider threats through public information sources. This enables analysts to identify early indicators of insider threats, enhancing preventive measures.
- **OSINT for Ethical Hackers (Instagram & Facebook)** (9 hours) – Focuses on OSINT techniques for social media platforms. Social media can be a source of critical information regarding insider intent; this course equips analysts to identify potential risk behaviors online.
- **OPSEC Demystified: Strategies for Secure Operations** (5 hours) – Provides an understanding of nation-state tactics, supporting defense strategies against

insider collusion. This course helps employees recognize threats that may be indirectly linked to nation-state actors.

- **Cyber Warfare: Defense Against Nation-State Threats** (5 hours) (we need a short description and need to add the so what how is this important from an Insider Threat/Risk Perspective?)
- **Linux Crash Course for Beginners (6 hours)** – Introduces Linux, which many cybersecurity tools are built on. Familiarizing analysts with Linux-based tools aids in effective monitoring and analysis of insider threats.

Optional Capstone and Master Designation: Mission Readiness Range

Students can complete a 3-month capstone project through the Mission Readiness Range, applying KSAs in realistic insider threat scenarios. This hands-on experience prepares participants for advanced operational roles and the Master Certification.

Certification-Specific Requirements and Mapping to NICE/DCWF Work Roles

While the Insider Threat Core Curriculum forms the foundation, each CITP™ certification maps to one or more specific NICE or DCWF/8140 work roles. The core curriculum meets the requirements of the NICE Workforce Category for Insider Threat Analysis, ensuring participants are prepared to analyze, detect, and mitigate insider threats. Additionally, each certification aligns with at least one other NICE or DCWF work role.

Recommended Course Sequence and Duration

The following sequence ensures participants acquire foundational knowledge before advancing to specialized topics. The courses are ordered to provide logical progression from awareness to program management and technical and operational expertise.

Order	Course Name	Duration
1	Insider Threat Awareness (CDSE)	60 min
2	OPSEC Awareness (CDSE)	30 min
3	Counterintelligence Awareness and Reporting (CDSE)	60 min
4	Counterintelligence (CI) Security Brief	30 min
5	Thwarting the Enemy: Counterintelligence and Threat Awareness	30 min
6	Establishing an Insider Threat Program (CDSE)	60 min
7	Maximizing Organizational Trust (CDSE)	60 min
8	Unauthorized Disclosure of Classified and Controlled Unclassified Information	60 min
9	Introduction to the Risk Management Framework (RMF)	30 min
10	IS-906: Workplace Security Awareness (FEMA)	1.5 hours
11	IS-907: Active Shooter: What You Can Do (FEMA)	1.5 hours
12	IS-912: Retail Security Awareness: Understanding Hazards (FEMA)	1.5 hours
13	IS-914: Surveillance Awareness: What You Can Do (FEMA)	1.5 hours

Order	Course Name	Duration
14	IS-915: Protecting Critical Infrastructure (FEMA)	1.5 hours
15	IS-916: Critical Infrastructure Security: Theft & Diversion (FEMA)	1.5 hours
16	Insider Threat Program Manager: Implementation and Operations (FedVTE (now CISA Learning))	8 hours
17	Insider Threat Analysis (FedVTE (now CISA Learning))	8 hours
18	Mastering Threat Intelligence (EC-Council)	14 hours
19	Master Open-Source Intelligence (OSINT) (EC-Council)	14 hours
20	OSINT for Ethical Hackers (Instagram & Facebook) (EC-Council)	9 hours
21	OPSEC Demystified: Strategies for Secure Operations (EC-Council)	5 hours
22	Cyber Warfare: Defense Against Nation-State Threats (EC-Council)	5 hours
23	Linux Crash Course for Beginners (EC-Council)	6 hours
	Total: Approximately 85 Hours or 11 days	

Certified Insider Threat Professional - Investigative Analyst™ (CITP-IGA™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-37

Courses in bundle: Insider Threat Core Curriculum, CompTIA Security Analytics Professional Stackable Certification (Security+ / CySA+) and HDI-SCA.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: All-Source Analyst (Work Role Code: 111) and Cyber Crime Investigator (Work Role Code: 221)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005) and All-Source Analysis (Nice Work Role ID: CI-WRL-001) and Digital Evidence Analysis (Nice Work Role ID: CI-WRL-002)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. Within the All-Source Analyst specialty, the Insider Threat Professional is responsible for analyzing data and information from one or multiple sources to prepare the operational environment, respond to requests for information, and submit intelligence collection and production requirements. This role

supports planning and operations by conducting comprehensive all-source analysis to inform intelligence planning and operational decisions. Within the investigator analyst specialty, the Insider Threat Professional identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

High-level bundle description: This bundle provides focused training in insider threat detection, investigation, and all-source analysis. It includes the Insider Threat Core Curriculum, CompTIA Security Analytics Professional Stackable Certification (Security+ / CySA+), and HDI-SCA. Security+ establishes a strong foundation in essential security concepts, while CySA+ hones advanced threat detection, analysis, and response skills. The HDI-SCA certification emphasizes key support center competencies, including effective communication, problem-solving, and other soft skills critical for incident management and stakeholder interaction. This bundle equips participants to manage insider risks, conduct investigations, and support cybersecurity and intelligence operations. As part of the Certified Insider Threat Professional program, this bundle includes the Insider Threat Core Curriculum.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, CySA+, and HDI-SCA certifications.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links (or descriptions)

- Security+
- CySA+
- HDI-SCA

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional - Cyber Analytics™ (CITP-CA™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-38

Courses in bundle: CompTIA Security Analytics Professional Stackable Certification (Security+ / CySA+), Linux+ (course and labs only), EC-Council CSA.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Cyber Defense Analyst (Work Role Code: 511)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005) and Defensive Cybersecurity (Nice Work Role ID: PD-WRL-001)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. Within the Cyber Defense Analyst specialty, responsible for using data collected from a variety of cyber defense tools, including IDS alerts, firewalls, and network traffic logs, to analyze events and mitigate risks within their environments. This role focuses on the analysis of cybersecurity events to effectively address and reduce threats by leveraging comprehensive data gathered from diverse security technologies.

High-level bundle description: This bundle delivers advanced training in cyber analytics and insider threat detection. It equips insider threat analysts to detect, analyze, and mitigate internal risks using cyber tools and advanced analytics. It includes the CompTIA Security Analytics Professional Stack (Security+ / CySA+), Linux+ (labs only), and EC-Council CSA to develop SOC monitoring and analytical skills. The Wireshark for Hacking and Network Forensics Bundle provides hands-on network analysis techniques for identifying suspicious activity. This bundle ensures participants are prepared to monitor insider activities, analyze behavior patterns, and support investigations with effective data-driven insights. As part of the Certified Insider Threat Professional program, this bundle includes the Insider Threat Core Curriculum.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses, and pass the exams for the Security+, CySA+, and EC-Council CSA certifications.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+) Bundle

EC-Council CTIA

EC-Council CSA

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional - Infrastructure Engineer™ (CITP-IE™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-40

Courses in bundle: CompTIA Linux Network Professional and CompTIA Network Infrastructure Professional (Network+ / Server+ / Linux+), CompTIA CASP+ and Microsoft Bundle, NIST SP 800-53 Controls Mastery Bundle.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Security Architect (Work Role Code: 652)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005) and Cybersecurity Architecture (Nice Work Role ID: DD-WRL-001)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. The Security Architect specialty role requires the engineer to design enterprise and systems security throughout the development lifecycle, ensuring that security requirements are adequately addressed in all aspects of enterprise architecture. This includes translating technology and environmental conditions (e.g., law and regulation) into security designs and processes. The role involves the creation and maintenance of security reference models, segment and solution architectures, and the resulting systems that protect and support organizational mission and business processes. Responsibilities also encompass the continuous assessment and enhancement of security measures to adapt to evolving threats and regulatory requirements.

High-level bundle description: This online self-paced equips infrastructure engineers with the skills to design, manage, and secure enterprise systems that support insider threat detection and response operations. This bundle features the CompTIA Linux

Network Professional and Network Infrastructure Professional certifications (Network+ / Server+ / Linux+), CompTIA CASP+, and a Microsoft bundle. Network+ and Server+ build core competencies in managing secure networks and server environments, while CASP+ focuses on advanced enterprise-level security. The Microsoft courses enhance proficiency in implementing enterprise solutions, and the NIST Master Controls course to align projects with RMF and governance frameworks. Together, these certifications prepare participants to architect resilient cybersecurity infrastructures, integrate tools and systems for continuous monitoring, and support operational efforts to identify, mitigate, and respond to insider threats efficiently.

Requirements for certification: To earn the ITI certification and be awarded the applied micro degree, the student must complete all courses and pass the CompTIA exams.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CompTIA Linux Network Professional
- CompTIA Network Infrastructure Professional
- CompTIA Server+ and Microsoft Bundle
- CompTIA CASP+ (bundle)

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional - Data Analytics™ (CITP-DA™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-39

Courses in bundle: CompTIA Security+, Data+ and DataSys+, Linux+ (course and labs only), ITI's custom Data Analyst bundle, and HDI-SCA.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Data Analyst (Work Role Code: 422)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005) and Data Analysis (Nice Work Role ID: IO-WRL-001)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. The Data Analyst specialty role involves analyzing and interpreting data from multiple disparate sources to provide cybersecurity and privacy insights. The analyst designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. Additionally, this role includes building visualizations and dashboards to report these insights effectively.

High-level bundle description: High-Level Bundle Description: This

As part of the Certified Insider Threat Professional program, this bundle includes the Insider Threat Core Curriculum. This curriculum features insider threat-specific courses from the Center for Development of Security Excellence (CDSE) and the Federal Virtual Training Environment (FedVTE (now CISA Learning)), among other valuable resources. This comprehensive training ensures that participants are well-prepared to tackle insider threat challenges and contribute effectively to their organizations.

Requirements for certification: To earn the certification and be awarded the applied micro degree, the student must complete all courses and pass each CompTIA (doesn't include Linux+) and HDI exam.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links:

- CompTIA Security+
- CompTIA Data+ custom Data Analyst bundle
- DataSys+
- Linux+ (course and labs only)
- HDI-SCA

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional – Infrastructure Operator™ (CITP-IO™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-41

Courses in bundle: CompTIA Secure Cloud Professional AND CompTIA Cloud Admin Professional (Security+ / Cloud+ / Network+), Linux+ (course and labs only), CCNA and HDI-SCA, NIST SP 800-53 Controls Mastery Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Cyber Defense Infrastructure Support Specialist (Work Role Code: 521)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005) and Infrastructure Support (Nice Work Role ID: PD-WRL-004)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. The Infrastructure Support specialty requires testing, implementing, deploying, maintaining, and administering infrastructure hardware and software, to include that pertaining to cybersecurity.

High-level bundle description: This bundle develops the expertise needed to support secure cloud and network infrastructure for insider threat detection and response. This bundle includes the CompTIA Secure Cloud Professional and CompTIA Cloud Admin Professional certifications (Security+ / Cloud+ / Network+), Linux+ (with labs), CCNA, and HDI-SCA. Participants will gain skills in cloud security, network administration, and infrastructure management. The CCNA builds foundational networking capabilities, while HDI-SCA develops essential communication and problem-solving skills for support operations, and the NIST Master Controls course to align projects with RMF and governance frameworks. This bundle prepares professionals to deploy, maintain, and secure infrastructure systems, enabling seamless integration of tools to monitor and mitigate insider risks effectively. As part of the Certified Insider Threat Professional program, this bundle includes the Certified Insider Threat Professional Core curriculum.

Requirements for certification: To earn the ITI certification and be awarded the applied micro degree, the student must complete all courses and pass the CompTIA and HDI exams.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CompTIA Secure Cloud Professional (Security+ / Cloud+)
- CompTIA Network+ Bundle
- CCNA
- CompTIA Linux+
- HDI-SCA

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional - Program Manager™ (CCITP-PM™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-42

Courses in bundle: CompTIA Security+, Project+, PMP, NIST SP 800-53 Controls Mastery Bundle and HDI-SCL.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: IT Project Manager (Work Role Code: 802)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005) and Secure Project Management (Nice Work Role ID: OG-WRL-011)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and

counterintelligence activities and investigations. Project Management specialty involves directly managing information technology projects to provide a unique service or product. This role ensures that cybersecurity is built into projects to protect the organization's critical infrastructure and assets, reduce risk, and meet organizational goals. Responsibilities include overseeing and managing technology projects, tracking and communicating project status, and demonstrating project value to the organization.

High-level bundle description: This bundle equips program managers to oversee secure IT projects with a focus on insider threat mitigation and regulatory compliance. It includes CompTIA Security+ for foundational cybersecurity knowledge, CompTIA Project+ with labs and a certification voucher for practical project management experience, PMP for advanced project leadership skills, HDI-SCL for developing service center leadership and communication abilities, and the NIST Master Controls course to align projects with RMF and governance frameworks. This bundle ensures participants can effectively manage IT initiatives, integrating security measures to protect critical infrastructure and reduce insider risks. As part of the Certified Insider Threat Professional program, this bundle includes the Certified Insider Threat Professional Core curriculum.

Requirements for certification: To earn the ITI certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA and HDI.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- Project+ and PMP Bundle
- Security+ Bundle
- NIST SP 800-53 Controls Mastery Bundle
- HDI-SCL

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional -Hub Chief™ (CITP-HC™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-43

Courses in bundle: CompTIA CySA+, CISSP and CISM bundle, CTI PMI-RMP, NIST SP 800-53 Controls Mastery Bundle and HDI-SCL.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Program Manager (Work Role Code: 801)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005) and Program Management (Nice Work Role ID: OG-WRL-010)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. The Program Management specialty is responsible for leading, coordinating, and ensuring the overall success of a defined program. This role involves communicating about the program, integrating various components, and ensuring alignment with agency or organizational priorities. The Program Manager is accountable for the program's success, ensuring it meets critical agency priorities through effective leadership and coordination.

High-level bundle description: This bundle equips professionals to lead insider threat programs by integrating cybersecurity expertise, project management skills, and leadership development. It includes CompTIA CySA+, CompTIA Project+, and HDI-SCL, with exam vouchers for all three. Project+ adds practical project management experience through hands-on labs and introduces Agile methodologies to enhance program oversight. The bundle also features the PMI-RMP (training only), NIST SP 800-53 Controls Mastery, and CISSP/CISM Bundle for advanced knowledge in risk management, security governance, and compliance. This well-rounded program ensures participants can effectively lead complex projects, mitigate risks, and align security initiatives with organizational priorities. As part of the Certified Insider Threat Professional program, this bundle includes the Certified Insider Threat Professional Core curriculum.

Requirements for certification: To earn the certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for each certification.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links (or descriptions)

- CompTIA CySA+
- CISSP and CISM bundle
- CTI PMI-RMP
- NIST SP 800-53 Controls Mastery Bundle
- HDI-SCL

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional - Senior Official™ (CITP-SO™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-44

Courses in bundle: PECB CCISO, CompTIA Project+ with PMP, CompTIA Security+, CTI CISM and CISSP (course and labs only), CISSP-ISSMP (FedVTE (now CISA Learning)), and NIST SP 800-53 Controls Mastery Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: IT Investment/Portfolio Manager (Work Role Code: 804)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005), Technology Portfolio Management (Nice Work Role ID: OG-WRL-015)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. The Technology Portfolio Manager is responsible for managing a portfolio of IT capabilities and technology investments that align with the overall needs of mission and business enterprise priorities. This role involves overseeing and governing the portfolio to ensure strategic alignment with organizational goals, optimizing resource allocation, and maximizing the value of technology investments to support mission-critical operations.

High-level bundle description: This bundle equips senior officials to lead and govern insider threat programs by combining advanced cybersecurity, project management, and risk management expertise. It includes the Insider Threat Core Curriculum along with PECB CCISO, CompTIA Security+, and CompTIA Project+, with exam vouchers for all three. Participants gain critical leadership and governance skills through additional training in CISM and CISSP (course and labs), CISSP-ISSMP (FedVTE (now CISA Learning)), PMI-RMP (training only), and NIST SP 800-53 Controls Mastery. This bundle ensures that senior leaders can align technology investments with mission priorities, oversee insider threat operations, and optimize resources to protect against internal risks effectively. As part of the Certified Insider Threat Professional program, this bundle includes the Certified Insider Threat Professional Core curriculum.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the certification exams for the Security+, Project+ and CISO.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

Security+

Project+ and PMP Bundle

CISSP and CISM

CCISO

FedVTE (now CISA Learning) Online Self-Paced CISSP-ISSMP

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional - Incident Responder™ (CITP-IR™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-45

Courses in bundle: EC-Council CEH (Certified Ethical Hacker), CHFI (Computer Hacking Forensic Investigator), ECIH (Incident Handler), CTIA (Certified Threat Intelligence Analyst), and CompTIA Linux+ (labs only).

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Cyber Defense Incident Responder (Work Role Code: 531)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005), and Incident Response (Nice Work Role ID: PD-WRL-003)

Combined Work Role Description: This role is responsible for identifying and assessing the capabilities and activities of insider threats, utilizing cybersecurity tools and analytical methods. The analyst's findings support law enforcement, counterintelligence activities, and organizational security operations. Additionally, this role is involved in investigating, analyzing, and responding to cybersecurity incidents to mitigate their impact on networks and systems. The role requires expertise in both proactive and reactive cybersecurity measures. It involves identifying potential insider threats, monitoring suspicious activities, and responding to incidents through containment and remediation efforts. The position ensures that the organization can effectively detect and address internal and external security risks.

High-level bundle description: This bundle equips insider threat professionals to investigate and respond to malicious internal activities. CEH and CTIA build knowledge of adversarial tools, techniques, and methods, while CHFI and ECIH provide expertise in forensic investigations and incident response. With Linux+ (labs only), participants gain familiarity with essential tools used during investigations. This bundle ensures professionals are prepared to thoroughly investigate insider activities, contain risks, and protect critical systems and operations. As part of the Certified Insider Threat Professional program, this bundle includes the Certified Insider Threat Professional Core curriculum.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for EC-Council CEH, CHFI, ECIH, and CTIA certifications.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

SOC and Incident Handling Bundle (ECOH, CTIA, and CSA)

EC-Council CEH and CHFI (course and labs only)

CTI Custom CompTIA Linux+

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional - Cyber Lead (CITP-CL) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-46

Courses in bundle: CompTIA Cloud+, CASP+ and PenTest+ and EC-Council CEH (courses and labs only), and CHFI (courses and labs only).

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Cyber Defense Forensics Analyst (Work Role Code: 212) and Cyber Defense Infrastructure Support Specialist (Work Role Code: 521)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005), and Digital Forensics (Nice Work Role ID: PD-WRL-002) and Infrastructure Support (Nice Work Role ID: PD-WRL-004)

Combined Work Role Description: As a Cyber Lead supporting Insider Threat Operations, this role is responsible for identifying, investigating, and assessing insider threats using cybersecurity tools, digital forensics, and infrastructure analysis methods. The role involves monitoring and analyzing insider activities, producing findings that support law enforcement, counterintelligence, and internal security operations. In addition to insider threat analysis, this role focuses on conducting digital forensic investigations to gather evidence from cyber incidents and mitigate vulnerabilities within systems and networks. As part of the infrastructure support responsibilities, this role also includes testing, implementing, deploying, and maintaining infrastructure hardware and software that supports cybersecurity operations. The analyst ensures that the infrastructure is secure, reliable, and capable of supporting effective threat detection and incident response.

High-level bundle description: This bundle equips professionals to manage insider threat operations by combining expertise in cybersecurity infrastructure, penetration testing, and forensics. It includes CompTIA Cloud+, CASP+, and PenTest+, along with EC-Council CEH and CHFI (courses and labs only). Participants develop the skills

needed to implement secure infrastructure, investigate insider activities, and conduct forensic investigations. Upon completion, participants earn the CompTIA Security Analytics Expert and Security Infrastructure Expert stackable certifications, having previously completed the CITP-CA™ or CITP-IGA™ prerequisite.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Cloud+, CASP+ and PenTest+ certifications, and complete all other courses.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans). ***In addition, prerequisite for this certification and micro degree is completion of the CITP-CA***.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Cloud+

CompTIA CASP+

CompTIA PenTest+

CTI Custom EC-Council CEH (course and labs only)

CTI Custom CHFI Bundle (course and labs only)

See each course link for how to access the material and exam information.

Certified Insider Threat Professional -ICS-SCADA Analyst™ (CITP-ICS™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-47

Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), and ICS/SCADA Security Bundle (EC-Council ICS/SCADA Cybersecurity and PECB SCADA Security Manager), EC-Council Industrial Control Systems (ICS) Cybersecurity Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Control Systems Security Specialist (Work Role Code: 462)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. Control Systems Security Specialist role is responsible for device, equipment, and system-level cybersecurity configuration and day-to-day security operations of control systems, including security monitoring and maintenance along with stakeholder coordination to ensure the system and its interconnections are secure in support of mission operations.

High-level bundle description: This bundle equips professionals to manage insider threats in industrial control systems (ICS) and SCADA environments. It includes the CompTIA Security Analytics Professional Stack (Security+ / CySA+) and the ICS/SCADA Security Bundle, featuring EC-Council ICS/SCADA Cybersecurity and PECB SCADA Security Manager. Participants develop expertise in security monitoring, configuration, and maintenance of control systems, along with analytical tools to investigate insider threats. This bundle ensures professionals can secure operational technologies, manage vulnerabilities, and support mission-critical operations through effective threat detection and mitigation. As part of the Certified Insider Threat Professional program, this bundle includes the Certified Insider Threat Professional Core curriculum.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for each certification.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

ICS/SCADA Security Bundle (EC-Council ICS/SCADA Cybersecurity and PECB SCADA Security Manager)

EC-Council Industrial Control Systems (ICS) Cybersecurity Bundle

See each course link for how to access the material and exam information.

Certified Insider Threat Professional - Data Scientist™ (CITP-DS™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-88

Courses in bundle: CompTIA CySA+ and DataX, CTI Python with Labs, ITI Custom EC-Council Data Science bundle, HDI-SCA.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Data Scientist (Work Role Code: 423)

NICE Work Role: Insider Threat Analysis (Nice Work Role ID: PD-WRL-005)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. The Data Scientist specialty role Uncovers and explains actionable insights from data by combining scientific method, math and statistics, specialized programming, advanced analytics, AI, and storytelling.

High-level bundle description: This bundle equips professionals to use data science and analytics to detect and assess insider threats. It includes CompTIA CySA+, DataX, CTI Python with Labs, the ITI Custom EC-Council Data Science Bundle, and HDI-SCA. Participants develop expertise in programming, machine learning, and advanced analytics, gaining the ability to extract actionable insights from complex data sets. This bundle ensures professionals can apply cybersecurity tools and data science techniques to monitor and investigate insider activities, supporting decision-making and mission-critical operations. As part of the Certified Insider Threat Professional program, this bundle includes the Certified Insider Threat Professional Core curriculum.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CySA+, DataX and HDI certifications.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA CySA+

CompTIA DataX

EC-Council Data Science Bundle

HDI-SCA

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Professional – User Activity Monitoring™ (CITP-UAM™) Applied Micro degree Bundle

ITI SKU: NICE-DCWF-89

Courses in bundle: CompTIA CySA+, Microsoft Certified: Information Protection and Compliance Administrator Associate, Linux+ (courses and labs only) CEH and CHFI (course and labs only), Teramind Insider Detection Course, Mastering Microsoft Sentinel.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Warning Analyst (Work Role Code: 141)

NICE Work Role: Threat Analysis (Nice Work Role ID: PD-WRL-006) and Insider Threat Analysis (Nice Work Role ID: PD-WRL-005)

Combined Work Role Description: Responsible for identifying and assessing the capabilities and activities of insider threats through using cybersecurity and other analytical tools; produces findings to help initialize and support law enforcement and counterintelligence activities and investigations. The Threat/Warning Analyst specialty role Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessment.

High-level bundle description: This bundle equips professionals to monitor, investigate, and respond to insider threats using advanced tools for tracking user activity and forensic analysis. It includes CompTIA CySA+ for threat detection and Microsoft Certified: Information Protection and Compliance Administrator Associate for

leveraging Microsoft Purview Insider Risk Management to manage insider risks and enforce DLP policies. Linux+ supports investigative tools, while CEH and CHFI develop expertise in forensics. Teramind Insider Detection, a CNSSD 504-compliant UAM tool, and Mastering Microsoft Sentinel provide seamless data integration and analysis for insider threat operations. As part of the Certified Insider Threat Professional program, this bundle includes the Certified Insider Threat Professional Core curriculum.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses, Including Linux+, CEH and CHFI, and pass the exams for the CompTIA CySA+, and Microsoft Certified: Information Protection and Compliance Administrator Associate certifications.

Recommended CITP prerequisites: This program is for US Government employees and their contractors only (this includes federal, state, local, tribal, and territorial government employees, their contractors, and US military veterans).

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CySA+

CHFI with Labs

CEH with Labs

Linux+ with Labs

Microsoft Certified: Information Protection and Compliance Administrator Associate

Master Microsoft Sentinel

Teramind Insider Threat Detection Course

See each of the other course links for how to access the material and exam information.

Vulnerability Assessor Certified™ (VAC™) Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-48

Courses in bundle: CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CEH (Course and labs only), CISA (course only) and EC-Council Gateway to Pen Testing Starter Pack bundle, Official EC-Council Web Application Hacking and Security.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Vulnerability Assessment Analyst (Work Role Code: 541)

NICE Work Role: Vulnerability Analysis (Nice Work Role ID: PD-WRL-007)

Combined Work Role Description: A Vulnerability Assessment Analyst performs assessments of systems and networks within the NE or enclave to identify deviations from acceptable configurations, enclave policy, or local policy. The role includes measuring the effectiveness of defense-in-depth architecture against known vulnerabilities.

High-level bundle description: This bundle equips professionals with the tools and expertise needed for comprehensive vulnerability assessments and penetration testing. It includes the CompTIA Network Vulnerability Assessment Professional Stack (Security+ / PenTest+ with exams), CEH (course and labs), CISA (course only), the EC-Council Gateway to Pen Testing Starter Pack (featuring 50+ labs), and Web Application Hacking and Security (course, labs, and certification exam). Through hands-on labs and advanced certifications, participants develop skills to identify, assess, and mitigate vulnerabilities across systems, networks, and web applications, preparing them for real-world security roles

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, PenTest+ and EC-Council Web Application Hacking and Security certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)
- CTI CEH (Course and Labs only)
- CTI CISA (Course only)
- EC-Council Gateway to Pen Testing Starter Pack Bundle
- EC-Council Web Application Hacking and Security

See each of the other course links for how to access the material and exam information.

Certified Intrusion Forensics Analyst™ (CIFA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-49

Courses in bundle: Certified Ethical Hacker (CEH), Certified Hacking Forensic Investigator (CHFI), Certified Incident Handler (ECIH), Mobile Forensics, Malware and Memory Forensics, Dark Web Investigations, CompTIA CySA+.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Forensics Analyst (Work Role Code: 211)

NICE Work Role: Cybercrime Investigation (Nice Work Role ID: IN-WRL-001)

Combined Work Role Description: The Cyber Intrusion Forensics Analyst conducts in-depth investigations of cyber intrusion incidents and digital crimes, utilizing forensic tools to analyze digital evidence, logs, and artifacts. The role combines digital forensic analysis with cybercrime investigation, balancing the goals of legal prosecution and intelligence gathering, while adhering to industry standards and legal requirements.

High-level bundle description: This training bundle equips professionals with essential skills in security operations, threat detection, intrusion response, and digital forensics. CEH provides an understanding of hacking methods to better investigate and mitigate attacks, while CHFI equips learners to investigate intrusions and analyze digital evidence. ECIH focuses on incident handling and response, helping students contain and manage cyber incidents. CySA+ builds expertise in threat detection and security analytics through proactive defense strategies. Mobile Forensics teaches participants to extract and analyze data from mobile devices, Malware and Memory Forensics enables the detection and mitigation of malicious software within system memory, and Dark Web Investigations develops skills to gather intelligence from hidden online networks. This comprehensive program provides a robust foundation in cybersecurity, proactive threat defense, intrusion detection, and digital evidence analysis, preparing learners for roles such as forensics analyst and cybercrime investigator.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA CySA+ and EC-Council CHFI and ECIH certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA CySA+

EC-Council Forensics and Incident Handling Bundle (OnDemand only, no live courses)

See each of the other course links for how to access the material and exam information.

Certified Cyber Crime Forensic Investigator™ (CCCFI™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-50

Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), CTI Custom EC-Council CEH and CHFI, and PECB Certified Forensics Examiner

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Cyber Crime Investigator (Work Role Code: 221)

NICE Work Role: Digital Evidence Analysis (Nice Work Role ID: IN-WRL-002)

Combined Work Role Description: The Cyber Crime Investigator is responsible for identifying, collecting, examining, and preserving digital evidence related to cybercrimes. This role applies controlled and documented analytical and investigative techniques to ensure the integrity and accuracy of evidence throughout the investigation process, supporting both legal proceedings and internal security operations.

High-level bundle description: This bundle is designed for professionals responsible for investigating cybercrimes and handling digital evidence. It includes CompTIA CySA+, Security+, EC-Council's Certified Ethical Hacker (CEH) and Certified Hacking Forensic Investigator (CHFI), along with PECB's ISO 27037-aligned Forensics Examiner certification. CEH equips learners with hacking techniques to support investigations, while CHFI focuses on intrusion forensics and evidence analysis. The PECB Forensics Examiner certification develops expertise in gathering, preserving, and presenting digital evidence following ISO standards, ensuring compliance with legal and investigative protocols. CySA+ enhances security analytics and threat detection, and Security+ builds foundational IT security knowledge to support secure operations during investigations. This comprehensive bundle prepares participants for roles in cybercrime investigation and forensic analysis.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+, CySA+ and PECB certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

CTI Custom EC-Council CEH

CTI Custom EC-Council CHFI

PECB Certified Forensics Examiner

See each of the other course links for how to access the material and exam information.

Certified All-Source Analyst™ (CASA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-51

Courses in bundle: CompTIA Security+, CySA+, EC-Council CTIA, and EC-Council Master Open-Source Intelligence Curriculum, OSINT for Ethical Hackers (Instagram/Facebook) Curriculum and Master Threat Intelligence Curriculum

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: All-Source Analyst (Work Role Code: 111)

NICE Work Role: All-Source Analysis (Nice Work Role ID: CI-WRL-001)

Combined Work Role Description: The All-Source Analyst role involves analyzing information from multiple sources to support operational planning and decision-making. This includes preparing the operational environment, addressing requests for intelligence, and formulating collection and production requirements. The role supports intelligence planning and operations through comprehensive analysis, ensuring insights are actionable and relevant to mission needs.

High-level bundle description: This bundle provides targeted training for professionals specializing in multi-source intelligence analysis. The bundle includes CompTIA Security+ and CySA+ to build foundational cybersecurity and analytical skills, along with

EC-Council CTIA for expertise in cyber threat intelligence. Advanced OSINT curricula, including the Master Open-Source Intelligence and OSINT for Ethical Hackers (Instagram/Facebook) modules, enhance open-source intelligence capabilities. The Master Threat Intelligence Curriculum provides in-depth training for developing actionable insights. With eligibility for Master Designation through the Mission Readiness Range Capstone, this bundle prepares analysts to effectively integrate data from multiple sources to support critical operational decisions.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA CySA+, Security+, and EC-Council CTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CompTIA Security Analytics Professional (Security+ / CySA+)
- EC-Council CTIA
- Master Open-Source Intelligence Curriculum
- Mastering Threat Intelligence
- OSINT for Ethical Hackers (Instagram/Facebook)

See each of the other course links for how to access the material and exam information.

Certified All-Source Collection Manager™ (CASCM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-52

Courses in bundle: ISCAC CISM and ISC2 CISSP Bundle, CompTIA CySA+, EC-Council CTIA, and EC-Council Master Open-Source Intelligence Curriculum, OSINT for Ethical Hackers (Instagram/Facebook) Curriculum and Master Threat Intelligence Curriculum, and HDI-SCL.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: All-Source Collection Manager (Work Role Code: 311)

NICE Work Role: All-Source Collection Management (Nice Work Role ID: CI-WRL-002)

Combined Work Role Description: The All-Source Collection Manager role is responsible for managing intelligence collection by identifying authorities and environments, integrating priority information requirements, and developing concepts to meet leadership's intent. The role involves assessing the capabilities of available collection assets, identifying new capabilities, constructing, and disseminating collection plans. It also includes monitoring the execution of collection tasks to ensure effective alignment with strategic objectives and the successful implementation of the intelligence collection plan, supporting intelligence operations within cyberspace.

High-level bundle description: This Bundle provides specialized training tailored to the skills required for effective intelligence collection management. CompTIA CySA+ and EC-Council CTIA focus on cyber threat detection, analysis, and response, while ISC2 CISSP and ISACA CISM develop expertise in security governance and risk management—key for aligning intelligence efforts with organizational priorities. The OSINT curricula enhance open-source intelligence gathering across platforms like Instagram and Facebook, essential for modern intelligence operations. The HDI-SCL component is adapted to strengthen leadership, communication, and coordination skills, ensuring smooth collaboration across support centers and intelligence teams, making it ideal for managing complex collection workflows and meeting operational goals.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CySA+, CTIA and HDI-SCL certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CompTIA CySA+
- EC-Council CTIA
- ISACA CISM and ISC2 CISSP
- Master Open-Source Intelligence Curriculum
- Mastering Threat Intelligence
- OSINT for Ethical Hackers (Instagram/Facebook) Curriculum
- HDI-SCL

See each of the other course links for how to access the material and exam information.

Certified All-Source Requirements Manager™ (CASRM™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-53

Courses in bundle: CompTIA Project+ and PMP Bundle, CompTIA CySA+, EC-Council CTIA and EC-Council Master Open-Source Intelligence Curriculum, OSINT for Ethical Hackers (Instagram/Facebook) Curriculum and Master Threat Intelligence Curriculum.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: All-Source Collection Requirements Manager (Work Role Code: 312)

NICE Work Role: All-Source Collection Requirements Management (Nice Work Role ID: CI-WRL-003)

Combined Work Role Description: The All-Source Collection Requirements Manager role focuses on evaluating intelligence collection operations and developing strategies to optimize collection efforts. This includes creating, processing, validating, and coordinating the submission of collection requirements using various sources and methods to enhance effectiveness. The role also involves assessing the performance of collection assets and operations to ensure alignment with mission objectives and continuous improvement in intelligence collection capabilities within cyberspace intelligence operations.

High-level bundle description: The Certified All-Source Requirements Manager™ (CASRM™) and Applied Micro Degree Bundle equips professionals with essential skills for managing and optimizing intelligence collection requirements. It features CompTIA Project+ and PMI PMP to build project management capabilities for coordinating complex collection efforts. CompTIA CySA+ strengthens cybersecurity analytics skills, while EC-Council CTIA focuses on identifying and responding to cyber threats. The bundle also offers advanced OSINT training, including modules on platforms like Instagram and Facebook, and master-level threat intelligence courses, providing the expertise needed to develop, validate, and refine collection strategies for effective intelligence operations.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CySA+, CTIA and Project+ certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CompTIA CySA+
- EC-Council CTIA
- Project+ and PMP Bundle
- Master Open-Source Intelligence Curriculum
- Mastering Threat Intelligence
- OSINT for Ethical Hackers (Instagram/Facebook) Curriculum

See each of the other course links for how to access the material and exam information.

Certified Cyber Intelligence Planner Professional™ (CCIPP™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-54

Courses in bundle: EC-Council CEH (Course and labs only), CompTIA CySA+ and CASP+, EC-Council CTIA and Master Open-Source Intelligence Curriculum and Master Threat Intelligence Curriculum.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Cyber Intelligence Planner (Work Role Code: 331)

NICE Work Role: Cyber Intelligence Planning (Nice Work Role ID: CI-WRL-004)

Combined Work Role Description: This bundle equips professionals with the skills needed to develop and execute effective cyber intelligence plans. The bundle features EC-Council CEH for foundational ethical hacking knowledge, CompTIA CySA+ for cyber threat detection and response, and CASP+ for advanced security operations. EC-Council CTIA, along with Master Open-Source and Threat Intelligence curricula, provides expertise in intelligence gathering, analysis, and targeting. This comprehensive training

prepares learners to collaborate with cyber operations teams, validate intelligence requirements, and align intelligence activities with mission objectives to support strategic and operational goals.

High-level bundle description: The Certified Cyber Intel Planner Professional™ (CCIPP™) and Applied Micro Degree Bundle is tailored for individuals in cyber intelligence planning, aligned with NICE CI-WRL-004 and 8140 DCWF Work Role 331. This bundle includes EC-Council CEH, CompTIA CySA+ and CASP+, and advanced curricula in Open-Source and Threat Intelligence. It equips learners to develop comprehensive intelligence plans, validate requirements, and support cyber operations, with skills in threat identification, analysis, and execution.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CySA+, CASP+ and CTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

- CompTIA CySA+
- EC-Council CTIA
- CEH Course and Labs Only
- CompTIA CASP+
- Master Open-Source Intelligence Curriculum
- Mastering Threat Intelligence

See each of the other course links for how to access the material and exam information.

Certified Cyberspace Operator™ (CCO™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-55

Courses in bundle: EC-Council CEH, CompTIA CySA+, EC-Council CTIA and CPENT and Master Open-Source Intelligence Curriculum and Master Threat Intelligence Curriculum.

MSRP: $4,299

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Cyberspace Operator (Work Role Code: 322)

NICE Work Role: Cyberspace Operations (Nice Work Role ID: CE-WRL-001)

Combined Work Role Description: The Cyber Operations Specialist conducts network navigation, tactical forensic analysis, and on-net operations to support offensive cyberspace missions. The role involves using various software tools to collect, process, and geolocate data, tracking targets to exploit or mitigate threats from criminal or foreign intelligence entities. It also includes gathering evidence and conducting surveillance and reconnaissance to protect against possible or real-time cyber threats.

High-level bundle description: This bundle provides comprehensive training in offensive and defensive cyber skills, combining certifications in ethical hacking (CEH), penetration testing (C|PENT), and threat intelligence (CTIA) with CompTIA CySA+ for cybersecurity analytics. It includes specialized training in Open-Source Intelligence (OSINT) and threat intelligence techniques, equipping professionals with the knowledge to conduct network exploitation, tactical forensics, threat detection, and incident response to effectively manage cyber threats.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for each certification.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

EC-Council CEH and CPENT bundle

CompTIA CySA+

EC-Council CTIA

Master Open-Source Intelligence Curriculum

Master Threat Intelligence Curriculum

See each of the other course links for how to access the material and exam information.

Certified Cyber Operations Planner™ (CCOP™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-56

Courses in bundle: CompTIA CySA+, EC-Council official CEH, CTIA and Master Open Source Intelligence, Mastering Threat Intelligence, OSINT for Ethical Hackers (Instagram/Facebook), and OPSEC Demystified: Strategies for Secure Operations

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Cyber Operations Planner (Work Role Code: 332)

NICE Work Role: Cyber Operations Planning (Nice Work Role ID: CE-WRL-002)

Combined Work Role Description: The Cyber Operations Planner develops comprehensive plans for cybersecurity operations, collaborating with planners, operators, and analysts to ensure effective execution. The role involves participating in targeting selection, validation, synchronization, and integrating cyber actions to achieve mission objectives and enhance organizational security posture.

High-level bundle description: This bundle equips professionals with the skills to develop and execute comprehensive cyber operations plans. It combines certifications in ethical hacking (CEH), threat intelligence (CTIA), and cybersecurity analytics (CySA+), alongside specialized training in Open-Source Intelligence (OSINT), operational security (OPSEC), and threat intelligence. This bundle prepares planners to effectively integrate intelligence, validate targets, and implement security measures, ensuring successful and secure execution of cyber operations.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for CompTIA CySA+, EC-Council official CEH, and CTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CySA+

CEH

CTIA

OPSEC Demystified: Strategies for Secure Operations

Master Open-Source Intelligence Curriculum

Master Threat Intelligence Curriculum

OSINT for Ethical Hackers (Instagram/Facebook) Curriculum

See each of the other course links for how to access the material and exam information.

Certified Exploitation and Penetration Analyst™ (CEPA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-57

Courses in bundle: CompTIA PenTest+, EC-Council CEH and CPENT and Web Application Hacking and Security and EC-Council Gateway to Pen Testing Starter Pack bundle.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Exploitation Analyst (Work Role Code: 121)

NICE Work Role: Exploitation Analysis (Nice Work Role ID: CE-WRL-003)

Combined Work Role Description: Collaborates to identify access and intelligence collection gaps that can be satisfied through cyber collection and/or preparation activities, leveraging all authorized resources and analytic techniques to penetrate targeted networks as part of Cyberspace Effects (CE) operations.

High-level bundle description: This bundle equips professionals with the skills needed for advanced penetration testing and exploitation analysis. The EC-Council Gateway to Pen Testing Starter Pack provides foundational tools and methodologies, building a strong baseline for more advanced topics. CompTIA PenTest+ focuses on essential testing techniques, while EC-Council CEH and CPENT deliver expertise in ethical hacking and network penetration. Web Application Hacking and Security enhances proficiency in identifying web-based vulnerabilities. With eligibility for Master Designation through the Mission Readiness Range Capstone, this bundle prepares learners to identify and exploit weaknesses, supporting cyber operations and intelligence missions.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the PenTest+, EC-Council CEH and either CPENT or Web Application Hacking and Security certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

EC-Council CEH and CPENT with PenTest+

EC-Council Web Application Hacking and Security

EC-Council Gateway to Pen Testing Starter Pack bundle

See each of the other course links for how to access the material and exam information.

Certified Mission Assurance Specialist™ (CMAS™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-58

Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), CompTIA Project+ and PMP Bundle and EC-Council Risk Management Approach and Practices – RM and PMI Risk Management Professional (PMI-RMP) Bundle.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Mission Assessment Specialist (Work Role Code: 112)

NICE Work Role: Mission Assessment (Nice Work Role ID: CE-WRL-004)

Combined Work Role Description: Develops assessment plans and performance measures, conducts strategic and operational effectiveness assessments for cyber events, determines whether systems performed as expected, and provides input to the determination of operational effectiveness as part of Cyberspace Effects (CE) operations.

High-level bundle description: The Certified Mission Assurance Specialist™ (CMAS™) and Applied Micro Degree Bundle is designed to equip professionals with key competencies in cybersecurity and project management. This comprehensive bundle includes the CompTIA Security Analytics Professional, merging Security+ and CySA+ for advanced security threat identification. It also features the CompTIA Project+ and PMP Bundle, focusing on IT project management skills, alongside the EC-Council and PMI Risk Management bundle, which combines risk management techniques and practices. The training aligns with the 8140 DCWF Work Role as a Mission Assessment Specialist and the NICE Work Role for Mission Assessment, preparing learners to develop assessment plans, conduct effectiveness assessments, and ensure operational effectiveness in Cyberspace Effects operations.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, CySA+, Project+ and EC-Council RM certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

CompTIA Project+ and PMP Bundle

EC-Council Risk Management Approach and Practices – RM and PMI-RMP Bundle

See each of the other course links for how to access the material and exam information.

Certified Joint Targeting Analyst™ (CJTA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-59

Courses in bundle: CompTIA Network Security Professional (Security+ / PenTest+ / CySA+), EC-Council Courses Master Open-Source Intelligence, Mastering Threat Intelligence; OSINT for Ethical Hackers (Instagram); OSINT for Ethical Hackers and (Facebook); OPSEC Demystified: Strategies for Secure Operations; and Cyber Warfare and Nation-State Threats

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Joint Targeting Analyst (Work Role Code: 131)

NICE Work Role: Partner Integration Planning (Nice Work Role ID: CE-WRL-005)

Combined Work Role Description: The Joint Targeting Analyst role encompasses a broad spectrum of responsibilities, focusing on target development at the system, component, and entity levels. Analysts are tasked with building and maintaining Electronic Target Folders (ETFs), incorporating inputs from Joint Intelligence Preparation of the Operational Environment (JIPOE), Target Systems Analysis, Geospatial Intelligence (GMI), and other Intelligence Community (IC) sources. Senior analysts lead collaborative targeting working groups across Geographic Combatant Commands (GCCs) and IC members, presenting and vetting candidate targets for inclusion on target lists. They also assess the impact of both lethal and non-lethal

military force, author Battle Damage Assessment reports, and coordinate federated support as needed. Additionally, this role involves Partner Integration Planning, driving cooperation across organizational or national borders among cyber operations partners, providing guidance, and facilitating the development of best practices to support integrated cyber actions.

High-level bundle description: This specialized bundle is tailored for Joint Targeting Analysts, blending advanced cybersecurity knowledge with specialized intelligence gathering skills. It includes the CompTIA Network Security Professional (Security+, PenTest+, CySA+) for foundational security expertise. EC-Council's courses, like Master Open-Source Intelligence, Mastering Threat Intelligence, and OSINT for Ethical Hackers (Instagram and Facebook), enhance tactical intelligence capabilities. OPSEC Demystified strengthens security operations, and Cyber Warfare - Defense Against Nation-State Threats provides strategies for managing sophisticated cyber threats, equipping analysts with the necessary tools for comprehensive cyber operations and strategic assessments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Network Security Professional (Security+ / PenTest+ / CySA+)

Master Open-Source Intelligence

Mastering Threat Intelligence

OSINT for Ethical Hackers (Instagram/ Facebook)

OPSEC Demystified: Strategies for Secure Operations

Cyber Warfare and Nation-State Threats

See each of the other course links for how to access the material and exam information.

Certified Target Developer™ (CTD™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-60

Courses in bundle: EC-Council CEH, CND and CTIA, EC-Council Courses Master Open-Source Intelligence, Mastering Threat Intelligence; OSINT for Ethical Hackers

(Instagram); OSINT for Ethical Hackers and (Facebook); OPSEC Demystified: Strategies for Secure Operations; and Cyber Warfare and Nation-State Threats

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Target Developer (Work Role Code: 131)

NICE Work Role: Target Analysis (Nice Work Role ID: CE-WRL-006)

Combined Work Role Description: The Target Developer performs comprehensive target system analysis and is responsible for developing, maintaining, and updating electronic target folders (ETFs) based on inputs from environment preparation, as well as internal and external intelligence sources. This role involves coordinating with partner target activities, intelligence organizations, and relevant working groups to ensure accurate target vetting and validation. Additionally, the Target Developer assesses and reports on damage resulting from military force application and facilitates federal support coordination as needed.

High-level bundle description: The Certified Target Developer™ (CTD™) and Applied Micro Degree Bundle equips professionals with comprehensive skills in offensive and defensive cybersecurity, threat intelligence, and open-source intelligence (OSINT). This bundle includes foundational courses from EC-Council, such as Certified Ethical Hacker (CEH) for penetration testing, Certified Network Defender (CND) for network security, and Certified Threat Intelligence Analyst (CTIA) for advanced threat detection. Complementing these certifications are targeted OSINT courses—covering tools and techniques for social media intelligence (Instagram and Facebook), OPSEC principles, and nation-state defense strategies—alongside specialized modules like Master Open-Source Intelligence and Mastering Threat Intelligence. Designed to prepare individuals for real-world operational roles, this bundle provides the knowledge and tools necessary to build and maintain electronic target profiles, coordinate intelligence efforts, and defend against advanced cyber threats.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CEH, CTIA and CND certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CEH Course

CND course

CTIA Course

Master Open-Source Intelligence

Mastering Threat Intelligence

OSINT for Ethical Hackers (Instagram/ Facebook)

OPSEC Demystified: Strategies for Secure Operations

Cyber Warfare and Nation-State Threats

See each of the other course links for how to access the material and exam information.

Certified Target Digital Network Analyst™ (CTDNA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-61

Courses in bundle: CompTIA Cloud Admin Professional (Network+ / Cloud+), CySA+, PenTest+, EC-Council Courses Master Open-Source Intelligence, Mastering Threat Intelligence; OSINT for Ethical Hackers (Instagram); OSINT for Ethical Hackers and (Facebook); OPSEC Demystified: Strategies for Secure Operations; and Cyber Warfare - Defense Against Nation-State Threats

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Target Digital Network Analyst (Work Role Code: 132)

NICE Work Role: Target Network Analysis (Nice Work Role ID: CE-WRL-007)

Combined Work Role Description: The TDNA performs advanced analysis of both collection and open-source data to maintain target continuity and develop profiles of targets and their activities. This role requires expertise in cyberspace networks, technologies, and applications to uncover how targets communicate, move, and operate within the digital domain. TDNAs apply analytical techniques to evaluate content within target communications and leverage data from diverse network forms for target development. Flexible and technology-savvy, TDNAs can adapt quickly across multiple

targets, developing techniques to extract actionable intelligence for cyberspace operations.

High-level bundle description: This course equips professionals with the advanced skills needed to analyze and profile targets within cyberspace. Combining key CompTIA certifications—Network+, Cloud+, CySA+, and PenTest+—this bundle ensures expertise in cloud administration, network security, vulnerability management, and threat detection. Complementing these are specialized EC-Council courses that focus on open-source intelligence (OSINT), threat intelligence, and operational security (OPSEC). Participants will also gain insights into cyber warfare strategies against nation-state threats, with practical OSINT modules tailored for Instagram and Facebook intelligence gathering. This well-rounded training develops proficiency in analyzing digital networks, tracking targets, and securing operations in complex threat environments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Cloud Admin Professional (Network+ / Cloud+)

CySA+

PenTest+

Master Open Source Intelligence

Mastering Threat Intelligence

OSINT for Ethical Hackers (Instagram/ Facebook)

OPSEC Demystified: Strategies for Secure Operations

Cyber Warfare and Nation-State Threats

See each of the other course links for how to access the material and exam information.

Certified AI Adoption Specialist™ (CAIAS™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-62

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), AI Fundamentals (CTI), Python Programming Course (CTI), introduction to Programming Using Python (lab) (CTI), Microsoft Azure AI Fundamentals, EC-Council AI-Driven

Network Security, Generative AI for Cybersecurity, and Practical Artificial Intelligence for Professionals

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: AI Adoption Specialist (Work Role Code: 753)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Facilitates AI adoption by supporting the users of AI-enabled solutions.

High-level bundle description: This bundle provides comprehensive training for professionals driving the adoption of AI-enabled solutions. The bundle includes CompTIA Secure Cloud Professional (Security+ / Cloud+) to ensure cloud and cybersecurity readiness, along with AI Fundamentals and Python programming courses to build essential technical skills. Hands-on labs in Python further reinforce programming capabilities. Microsoft Azure AI Fundamentals introduces learners to AI services and cloud integration, while EC-Council's AI-Driven Network Security and Generative AI for Cybersecurity explores AI applications in cyber defense. Practical Artificial Intelligence for Professionals equips participants with actionable strategies to implement and support AI solutions effectively across organizations.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA and Microsoft Azure AI Fundamentals certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

AI Fundamentals (CTI)

Python Programming and introduction to Programming Using Python (lab)

Microsoft Azure AI Fundamentals

EC-Council AI-Driven Network Security

EC-Council Generative AI for Cybersecurity

EC-Council Practical Artificial Intelligence for Professionals

See each of the other course links for how to access the material and exam information.

Certified AI Innovation Leader™ (CAIL™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-63

Courses in bundle: CompTIA Security+, Project+ and PMP bundle, CISM and CISSP Bundle, AI Fundamentals (CTI), Microsoft Azure AI Fundamentals, EC-Council AI-Driven Network Security, Generative AI for Cybersecurity and Practical Artificial Intelligence for Professionals

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: AI Innovation Leader (Work Role Code: 902)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Builds the organization's AI vision and plan and leads policy and doctrine formation including how AI solutions can or will be used.

High-level bundle description: This bundle prepares professionals to drive AI initiatives with strategic, technical, and security expertise. This bundle includes CompTIA Security+ for foundational cybersecurity knowledge, essential for securing AI systems; Project+ and PMP for managing complex AI projects aligned with organizational goals; and CISM and CISSP to ensure AI solutions meet robust security and compliance standards. AI Fundamentals (CTI) and Microsoft Azure AI Fundamentals establish a foundation in AI and cloud-based AI deployment, while EC-Council AI-Driven Network Security and Generative AI for Cybersecurity address AI's role in advanced threat protection. Finally, Practical Artificial Intelligence for Professionals equips leaders to apply AI innovations effectively, rounding out the skills needed to lead transformative, secure AI programs.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for CompTIA and Microsoft Azure AI Fundamentals certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security+

AI Fundamentals (CTI)

CISM and CISSP Bundle

Project+ and PMP bundle

Microsoft Azure AI Fundamentals

EC-Council AI-Driven Network Security

EC-Council Generative AI for Cybersecurity

EC-Council Practical Artificial Intelligence for Professionals

See each of the other course links for how to access the material and exam information.

Certified AI Risk & Ethics Specialist™ (CARES™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-64

Courses in bundle: CompTIA Security+, AI Fundamentals (CTI), EC-Council Risk Management Approach and Practices – RM and PMI Risk Management Professional (PMI-RMP) Bundle, Microsoft Azure AI Fundamentals, EC-Council AI-Driven Network Security (CR), Generative AI for Cybersecurity and Practical Artificial Intelligence for Professionals.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: AI Risk & Ethics Specialist (Work Role Code: 902)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Educates those involved in the development of AI and conducts assessments on the technical and societal risks across the lifecycle of AI solutions from acquisition or design to deployment and use.

High-level bundle description: This bundle offers a specialized training pathway for professionals responsible for identifying, evaluating, and managing the ethical and technical risks associated with artificial intelligence. The Certified AI Risk & Ethics Specialist™ (CARES™) and Applied Micro Degree Bundle combines foundational and advanced courses in cybersecurity, AI, risk management, and governance. Learners will gain skills in AI-driven security strategies, risk assessment, and ethical decision-making, aligned with industry standards. Key training includes CompTIA Security+, AI

fundamentals, and focused modules from EC-Council, Microsoft Azure AI, and PMI, equipping professionals to assess AI solutions across their lifecycle from design to deployment.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+, EC-Council Risk Management Approach and Practices – RM and Microsoft Azure AI Fundamentals certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security+

EC-Council Risk Management Approach and Practices – RM and PMI PMI-RMP Bundle

AI Fundamentals (CTI)

Microsoft Azure AI Fundamentals

EC-Council AI-Driven Network Security

EC-Council Generative AI for Cybersecurity

EC-Council Practical Artificial Intelligence for Professionals

See each of the other course links for how to access the material and exam information.

Certified AI Test & Evaluation Specialist™ (CATES™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-65

Courses in bundle: CompTIA PenTest+, CISA, introduction to Programming Using Python (lab), Python Programming Course, Microsoft Certified Azure AI Engineer Associate and AWS Certified Machine Learning Specialist, CTI AWS Cloud Practitioner and CTI Azure fundamentals

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: AI Test & Evaluation Specialist (Work Role Code: 672)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Performs testing, evaluation, verification, and validation on AI solutions to ensure they are developed to be and remain robust, resilient, responsible, secure, and trustworthy; and communicates results and concerns to leadership.

High-level bundle description: This bundle provides comprehensive training for professionals tasked with evaluating and validating artificial intelligence systems to ensure their robustness, security, and ethical integrity. The Certified AI Test & Evaluation Specialist™ (CATES™) and Applied Micro Degree Bundle integrates courses in AI engineering, machine learning, cloud fundamentals, and cybersecurity, supporting the rigorous testing and evaluation of AI solutions. Core courses include CompTIA PenTest+, Microsoft Certified Azure AI Engineer Associate, AWS Certified Machine Learning Specialist, and Python programming essentials. This bundle equips learners to conduct thorough assessments of AI systems, communicate findings, and ensure that AI implementations meet industry standards for reliability and trustworthiness throughout their lifecycle.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA PenTest+, Microsoft Certified Azure AI Engineer Associate and AWS Certified Machine Learning Specialist certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA PenTest+

CTI Custom CISA

CTI Custom Introduction to Programming Using Python with lab bundle

CTI Custom AWS Cloud Practitioner

CTI Custom Azure fundamentals

Microsoft Certified Azure AI Engineer Associate

AWS Certified Machine Learning Specialist

See each of the other course links for how to access the material and exam information.

Certified AI/ML Specialist™ (CAIMLS™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-66

Courses in bundle: CompTIA Security+, Python Programming Course, Introduction to Programming Using Python (lab), Microsoft Azure AI Fundamentals, AWS Cloud Practitioner, AWS Certified Machine Learning Specialist, AZ-900 Azure Fundamentals Certification Course

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: AI/ML Specialist (Work Role Code: 623)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Designs, develops, and modifies AI applications, tools, and/or other solutions to enable successful accomplishment of mission objectives.

High-level bundle description: This bundle is designed for professionals focused on developing, enhancing, and deploying artificial intelligence and machine learning solutions to support mission-critical objectives. The Certified AI/ML Specialist™ (CAIMLS™) and Applied Micro Degree Bundle combines essential and advanced training in cybersecurity, programming, cloud platforms, and machine learning. Core courses include CompTIA Security+, AWS Certified Machine Learning Specialist, Microsoft Azure AI Fundamentals, and foundational Python programming. This comprehensive curriculum equips learners with the skills needed to design, build, and refine AI applications, ensuring they meet both technical requirements and organizational goals.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+, Microsoft Azure AI Fundamentals and AWS Certified Machine Learning Specialist certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CTI Custom Introduction to Programming Using Python with lab bundle

CTI Custom AWS Cloud Practitioner

CTI Custom Azure fundamentals

Microsoft Azure AI Fundamentals

AWS Certified Machine Learning Specialist

CompTIA Security+

See each of the other course links for how to access the material and exam information.

Certified Control Systems Security Specialist™ (CCSSS™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-67

Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), PECB SCADA Security Manager, ICS/SCADA Cybersecurity (EC-Council), EC-Council AI Mastery: Securing ICS/SCADA and Industrial Control Systems (ICS) Cybersecurity Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Control Systems Security Specialist (Work Role Code: 462)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Responsible for device, equipment, and system-level cybersecurity configuration and day-to-day security operations of control systems, including security monitoring and maintenance along with stakeholder coordination to ensure the system and its interconnections are secure in support of mission operations.

High-level bundle description: This bundle offers comprehensive training in securing ICS and SCADA environments. It includes courses like CompTIA Security Analytics Professional (Security+ / CySA+), PECB SCADA Security Manager, ICS/SCADA Cybersecurity, and EC-Council's Industrial Control Systems Cybersecurity Bundle. This bundle emphasizes best practices from IEC 62443 and NIST 800-82 Rev 3, equipping professionals with advanced skills in cybersecurity analytics, SCADA management, and AI-driven security strategies to safeguard critical infrastructure against modern threats.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, CySA+, PECB SCADA Security Manager, and EC-Council ICS/SCADA Cybersecurity certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

EC-Council's Industrial Control Systems Cybersecurity Bundle

ICS/SCADA Security Bundle (EC-Council ICS/SCADA Cybersecurity and PECB SCADA Security Manager)

See each of the other course links for how to access the material and exam information.

Certified Digital Network Exploitation Analyst™ (CDNEA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-68

Courses in bundle: CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CCNA, Network+, EC-Council Wireshark for Hacking and Network Forensics Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Digital Network Exploitation Analyst (Work Role Code: 122)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: The DNEA analyzes intercepted intelligence information for metadata and content. They use this data to reconstruct and document target networks to judge the intelligence value and maintain target continuity. DNEAs understand and analyze target implementation of communication technologies and digital network systems. They discover methods and suggest strategies to exploit specific target networks, computer systems, or specific hardware and/or software.

High-level bundle description: This bundle equips professionals with the skills required to analyze and exploit digital network systems, reconstruct target networks, and extract valuable intelligence insights. The Certified Digital Network Exploitation Analyst™ (CDNEA™) and Applied Micro Degree Bundle combines training in network security, forensics, and vulnerability assessment. Key courses include CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), Cisco CCNA, Network+, and EC-Council's Wireshark for Hacking and Network Forensics. This comprehensive curriculum prepares learners to understand and analyze target communication technologies, identify network vulnerabilities, and recommend strategic exploitation methods to support intelligence and operational objectives.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)

CCNA Bundle

Network+ Bundle

EC-Council Wireshark for Hacking and Network Forensics Bundle

See each of the other course links for how to access the material and exam information.

Certified Data Architect™ (CDA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-69

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), AZ-104 Azure Administrator, Data Engineering on Microsoft Azure (Microsoft Certified: Azure Data Engineer Associate) (***Live Online***), EC-Council Becoming a Data Engineer Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Data Architect (Work Role Code: 653)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Designs a system's data models, data flow, interfaces, and infrastructure to meet the information requirements of a business or mission.

High-level bundle description: This This bundle provides comprehensive training for professionals in cloud architecture, data engineering, and IT operations. It includes CompTIA Secure Cloud Professional (Security+ / Cloud+) to build cloud security and infrastructure skills, AZ-104 Azure Administrator for managing Azure resources, and Microsoft Certified: Azure Data Engineer Associate for mastering data processing and analytics pipelines. The addition of the EC-Council Becoming a Data Engineer Bundle

further enhances the learning experience by equipping participants with advanced data engineering techniques across various platforms and cloud environments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, Cloud+ and Microsoft Certified: Azure Data Engineer Associate certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

AZ-104 Azure Administrator

Microsoft Certified: Azure Data Engineer Associate

EC-Council Becoming a Data Engineer Bundle

See each of the other course links for how to access the material and exam information.

Certified Data Officer™ (CDO™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-70

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), PECB Certified Data Protection Officer, EC-Council COBIT 2019 Foundation Training Plus Exam Prep, Implementing Information Security in Your Enterprise, Implementing Global Data Protection Policy, and NIST SP 800-53 Controls Mastery Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Data Officer (Work Role Code: 903)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Holds responsibility for developing, promoting, and overseeing implementation of data as an asset and the establishment and enforcement of data-related strategies, policies, standards, processes, and governance.

High-level bundle description: This bundle provides a comprehensive approach to data governance, security, and compliance. It includes CompTIA Secure Cloud Professional (Security+ / Cloud+) for cybersecurity expertise, PECB Certified Data Protection Officer for mastering regulatory compliance and data privacy frameworks, and COBIT 2019

Foundation Training to establish IT governance and business alignment. The bundle also features Implementing Information Security in Your Enterprise for hands-on experience with ISO/IEC 27001 and ISO 15489 standards, ensuring effective security strategies and data governance. Adding Implementing Global Data Protection Policy strengthens the program by equipping professionals to navigate international data privacy frameworks and ensure compliance across jurisdictions. Furthermore, the inclusion of NIST SP 800-53 Controls Mastery Bundle ensures alignment with federal cybersecurity controls and frameworks, enhancing the ability to manage risks effectively and meet U.S. government standards. Together, these courses empower data officers to manage data as a strategic asset, align policies with operational goals, and mitigate security risks.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, Cloud+, and PECB Certified Data Protection Officer certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

PECB Certified Data Protection Officer

EC-Council COBIT 2019 Foundation Training Plus Exam Prep

EC-Council Implementing Information Security in Your Enterprise

NIST SP 800-53 Controls Mastery Bundle

See each of the other course links for how to access the material and exam information.

Certified Data Operations Specialist™ (CDOS™) (Azure) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-71

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), Azure Fundamentals (AZ-900) Azure Administrator (AZ-104), Microsoft Certified: Azure Data Engineer Associate (Live course), EC-Council's Implementing DevOps in Microsoft Azure and DevSecOps – Implementing Security in DevOps Processes.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Data Operations Specialist (Work Role Code: 624)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Builds, manages, and operationalizes data pipelines.

High-level bundle description: This bundle equips professionals with the essential skills to design, manage, and secure data pipelines in cloud environments with a focus on automation, security, and compliance. Participants start with AZ-900: Azure Fundamentals and CompTIA Cloud+ to build foundational cloud infrastructure knowledge. Security+ ensures mastery of essential security principles. Learners will progress through Azure Administrator to manage Azure environments effectively and then dive into DevOps principles in Azure and DevSecOps processes to embed security in automation workflows. The program culminates with Microsoft Azure Data Engineer Associate, equipping participants with advanced skills to design and manage scalable data pipelines in cloud environments. ***Contact us to schedule your Microsoft Azure Data Engineer Associate live online training***.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA and Microsoft Certified: Azure Data Engineer Associate certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

Azure Fundamentals (AZ-900)

Azure Administrator (AZ-104)

Microsoft Certified: Azure Data Engineer Associate

EC-Council Implementing DevOps in Microsoft Azure

EC-Council DevSecOps – Implementing Security in DevOps Processes

See each of the other course links for how to access the material and exam information.

Applied Data Scientist Certified Professional (ADSCP) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-72

Courses in bundle: CompTIA Security+, Data Analyst Career Path, DataX, Microsoft Certified: Azure Data Scientist Associate (live online), Introduction to Python Programming (with Labs) bundle, EC-Council: Machine Learning with Python

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Data Scientist (Work Role Code: 423)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Uncovers and explains actionable insights from data by combining scientific methods, math and statistics, specialized programming, advanced analytics, AI, and storytelling.

High-level bundle description: This bundle provides a complete learning path for professionals aiming to master data science and analytics. It begins with CompTIA Security+, focusing on data security and governance fundamentals. Participants develop essential analytics and visualization skills through the Data Analyst Career Path and apply them in advanced scenarios with DataX's hands-on machine learning and data science simulations. The bundle also includes Microsoft Azure Data Scientist Associate, equipping learners to build and deploy AI models in cloud environments. In addition, the Python Programming Course and Lab provide practical scripting skills for automating processes and working with data. Finally, EC-Council's Machine Learning with Python further enhances participants' ability to implement machine learning frameworks such as TensorFlow and Scikit-learn, preparing them for real-world applications. ***Contact us to schedule the Microsoft Azure Data Scientist Associate live online course.***

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+ and DataX, and Microsoft Certified: Azure Data Scientist Associate certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security+

Data Analyst Career Path

CompTIA DataX

Microsoft Certified: Azure Data Scientist Associate

Introduction to Python Programming (with Labs) bundle

EC-Council: Machine Learning with Python

See each of the other course links for how to access the material and exam information.

Certified Data Steward Analyst™ (CDSA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-73

Courses in bundle: CompTIA Security+, CompTIA Data+, and CompTIA DataSys+ Bundle, and EC-Council NIST SP 800-53 Controls Mastery Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Data Steward (Work Role Code: 424)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Develops and maintains plans, policies, and processes for data management, data governance, security, quality, accessibility, use, and disposal.

High-level bundle description: This bundle equips professionals with the skills needed to manage, govern, and secure data effectively within government frameworks. Participants develop expertise in data security, governance, infrastructure management, and compliance through CompTIA Security+, CompTIA Data+, and CompTIA DataSys+ with MSSQL and Oracle Database. Additionally, the EC-Council NIST SP 800-53 Controls Mastery Bundle ensures alignment with federal compliance standards, covering risk management, auditing, and continuous monitoring practices. This comprehensive bundle prepares data stewards to manage the entire data lifecycle, ensuring data quality, accessibility, and security across its use and disposal.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security+

CompTIA Data+

CompTIA DataSys+ bundle

EC-Council NIST SP 800-53 Controls Mastery Bundle

See each of the other course links for how to access the material and exam information.

DevSecOps Specialist Certified™ (DevSC™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-74

Courses in bundle: CTI DevOps Fundamentals, Introduction to Python, Introduction to Programming Using Python (lab), Certified Kubernetes Administrator (CKA), Certified Kubernetes Application Developer (CKAD), Kubernetes - Containerizing Applications in the Cloud, Security+, SAFe® 6.0 DevOps (Live Online), EC-Council Certified DevSecOps Engineer (ECDE).

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: DevSecOps Specialist (Work Role Code: 627)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Selects/Deploys/Maintains the set of Continuous Integration/Continuous Deployment (CI/CD) tools and processes used by the development team and/or maintains the deployed software product and ensures observability and security across the lifecycle.

High-level bundle description: This bundle provides comprehensive training in DevOps, containerization, automation, and security integration. Participants gain hands-on expertise with tools like Kubernetes, Python, and CI/CD practices to manage software delivery pipelines and secure cloud-native environments. Courses include DevOps Fundamentals, CKA, CKAD, and Kubernetes Containerization, with additional certifications in CompTIA Security+, SAFe® 6.0 DevOps, and EC-Council Certified DevSecOps Engineer (ECDE). This bundle prepares professionals to maintain software observability, automation, and security throughout the product lifecycle.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the

Security+, SAFe® 6.0 DevOps, EC-Council Certified DevSecOps Engineer (ECDE) certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security+

Introduction to Agile, Scrum and DevOps

Kubernetes Series

SAFe® 6.0 DevOps (Live Online)

EC-Council Certified DevSecOps Engineer (ECDE)

See each of the other course links for how to access the material and exam information.

Certified Secure Host Configuration Analyst™ (CSHCA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-75

Courses in bundle: CompTIA Systems Support Specialist (A+ / Linux+), Security+, Server+ and Microsoft Bundle, Linux+, EC-Council NIST SP 800-53 Controls Mastery Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Host Analyst (Work Role Code: 463)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: A Host Analyst (HA) will have knowledge of various system configurations encountered. A Host Analyst will have knowledge of system services and the security and configuration of them, as well as knowledge of file systems, permissions, and operation system configurations. The Host Analyst conducts analysis using built-in tools and capabilities.

High-level bundle description: The Host Analyst Training Bundle develops practical skills for securing and managing both Windows and Linux systems. It includes courses aligned with Security+, A+, Server+ and Microsoft Server, Linux+, and NIST SP 800-53 Controls. Learners will focus on system hardening, permissions management, service

configuration, and troubleshooting using built-in tools like PowerShell and Bash. This training ensures participants can lock down hosts, apply NIST-compliant security controls, and maintain operational integrity across diverse environments

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Systems Support Specialist (A+ / Linux+)

CompTIA Security+

CompTIA Server+ and Microsoft Bundle

CompTIA Linux+

EC-Council NIST SP 800-53 Controls Mastery

See each of the other course links for how to access the material and exam information.

Certified Network Monitoring Analyst™ (CNMA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-76

Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), Network+, CCNA, EC-Council Cisco Certified CyberOps Associate

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Network Analyst (Work Role Code: 443)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: The Network Analyst will understand network traffic signatures and discover anomalies through network traffic and packet capture (PCAP) analysis. The Network Analyst will identify, assess, and mitigate intrusions into networks that are vital to cyberspace operations security. Network Analysts also use

GUI or command-line based tools and assist in developing network mapping and signatures. Network Analysts will develop advanced network detection rules and alerts, queries and dashboards to gain a holistic view of the network.

High-level bundle description: The CNMA™ bundle equips learners with critical skills to monitor, secure, and analyze networks using industry-standard tools and frameworks. It combines courses from CompTIA Security Analytics Professional (Security+ / CySA+), Network+, CCNA, and Cisco Certified CyberOps Associate (200-201) Parts 1 & 2, providing hands-on experience in PCAP analysis, intrusion detection, and network troubleshooting. Learners will develop expertise in creating detection rules, alerts, and dashboards to detect anomalies and safeguard network environments through both CLI and GUI-based tools, ensuring robust network security.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

CompTIA Network+ Bundle

CCNA bundle

EC-Council Cisco Certified CyberOps Associate Bundle

See each of the other course links for how to access the material and exam information.

Certified Network Technician™ (CNT™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-77

Courses in bundle: CompTIA Cloud Admin Professional (Network+ / Cloud+), CCNA, Security+, CCNP Enterprise Bundle

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Network Technician (Work Role Code: 442)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: The Network Technician provides enterprise and tactical infrastructure knowledge, experience, and integration to the Cyber Protection Team (CPT). The Network Technician supports CPT elements by understanding network technologies, defining mission scope, and identifying terrain.

High-level bundle description: The CNT™ bundle provides learners with the skills needed to manage and troubleshoot both enterprise and cloud-based networks. It includes training in CompTIA Network+ and Cloud+, CCNA, Security+, and advanced topics from CCNP Enterprise Core (ENCOR 350-401) and ENARSI (300-410). The program focuses on network installation, configuration, and troubleshooting, with practical coverage of routing, switching, virtualization, and security. Learners gain the expertise required to support complex infrastructure environments and integrate networks across enterprise and tactical deployments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Cloud Admin Professional (Network+ / Cloud+)

CompTIA Security+

Network Engineer Bundle

See each of the other course links for how to access the material and exam information.

Certified User Interface Designer™ (CUID™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-78

Courses in bundle: Security+, CISSP (with labs) and CISM Bundle, CTI Web Designer Career Path, EC-Council CASE .Java and Web Application Hacking and Security

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Product Designer User Interface (UI) (Work Role Code: 625)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Manages the user interface design portion of the design process of a product.

High-level bundle description: This bundle offers a comprehensive blend of cybersecurity, UI/UX design, and secure application development training. It includes key certifications such as Security+, CISSP with labs and CISM, CTI Web Designer Career Path, and EC-Council CASE Java & Web Application Hacking and Security. Designed for professionals managing the UI design process, the program equips learners with the skills to create secure, user-friendly interfaces while addressing vulnerabilities in web and software applications. Completing all courses and passing certification exams ensures mastery across both design and cybersecurity disciplines.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+ and EC-Council CASE - Java and Web Application Hacking and Security certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security+

CTI Web Design Curriculum

CISSP and CISM

EC-Council CASE - Java

EC-Council Web Application Hacking and Security

See each of the other course links for how to access the material and exam information.

Certified Product Manager Professional™ (CPMP™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-79

Courses in bundle: CompTIA Security+, Introduction to Agile, Scrum and DevOps, SAFe® 6.0 DevOps (Live Online), EC-Council CASE - JAVA, Certified Scrum Product Owner (CSPO) Certification (Live Online).

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Product Manager (Work Role Code: 806)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Manages the development of products including the resource management, product strategy (physical or digital), functional requirements, and releases. Coordinate work done by functions (like software engineers, data scientists, and product designers).

High-level bundle description: This bundle provides the skills necessary to manage product development, strategy, and resource coordination. It includes CompTIA Security+ for cybersecurity fundamentals and Introduction to Agile, Scrum, and DevOps to enhance product delivery efficiency. SAFe® 6.0 DevOps and Certified Scrum Product Owner (CSPO) certifications offer deeper expertise in agile frameworks, ensuring participants are equipped to lead cross-functional teams. With EC-Council CASE Java, students will also gain essential knowledge in secure software development. This program aligns with Agile principles included in both Project+ and PMP standards, preparing learners to manage product lifecycles effectively over 12 months.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+, SAFe® 6.0 DevOps, EC-Council CASE - JAVA, and Certified Scrum Product Owner (CSPO) certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security+

SAFe® 6.0 DevOps

EC-Council CASE - JAVA

Certified Scrum Product Owner (CSPO)

See each of the other course links for how to access the material and exam information.

Certified User Experience Service Designer™ (CUXSD™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-80

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CTI Web Designer Curriculum, EC-Council CASE -.NET and Web Application Hacking and Security

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Service Designer User Experience (UX) (Work Role Code: 626)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Manages the user experience of a product focused on human factors by making products intuitive and maximizing usability, accessibility, and simplicity.

High-level bundle description: This bundle offers a comprehensive blend of user experience design, cloud security, and secure application development. It includes courses on CompTIA Secure Cloud Professional (Security+ / Cloud+), CTI Web Designer Curriculum, and EC-Council CASE .NET and Web Application Hacking and Security. Designed for professionals managing UX design, the program emphasizes usability, accessibility, and intuitive design, while equipping learners with essential cybersecurity skills. The combination ensures participants can create seamless user experiences without compromising security.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA Security+ and Cloud+ and EC-Council CASE – .NET and Web Application Hacking and Security certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CTI Web Designer Curriculum

CISSP and CISM bundle

EC-Council CASE .Java

EC-Council Web Application Hacking and Security

See each of the other course links for how to access the material and exam information.

Certified Software Test & Evaluation Specialist™ (CSTES™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-81

Courses in bundle: CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CTI Fundamentals of the Software Development Lifecycle (SDLC) and Software Testing Lab, EC-Council CASE .NET and Web Application Hacking and Security

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Software Test & Evaluation Specialist (Work Role Code: 673)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Plans, prepares, and performs testing, evaluation, verification, and validation of software to evaluate results against specifications, requirements, and operational need.

High-level bundle description: This bundle equips professionals with the skills to manage software testing, security validation, and performance evaluation. It includes CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+) for security testing, EC-Council CASE .NET for secure software development, and Web Application Hacking and Security to identify web vulnerabilities. The bundle also offers Software Testing Fundamentals (98-379)—while no longer officially available, it remains relevant for foundational testing skills. This program prepares participants to meet modern challenges in functional testing, security validation, and software evaluation.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for CompTIA Security+, PenTest+, and EC-Council CASE .NET certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)

CTI Fundamentals of the SDLC and Software Testing Lab

EC-Council CASE .NET

EC-Council Web Application Hacking and Security

See each of the other course links for how to access the material and exam information.

Certified Software & Cloud Architect™ (CSCA™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-82

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), ISC2 CCSP, Introduction to Agile, Scrum and DevOps, Introduction to Python and Introduction to Programming Using Python (lab) bundle, Certified Kubernetes Series

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Software/Cloud Architect (Work Role Code: 628)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Manages and identifies program high-level technical specifications, which may include application design, cloud computing strategy and adoption, and integration of software applications into a functioning system to meet requirements.

High-level bundle description: This bundle equips professionals with the skills needed to design, integrate, and secure complex cloud-based and software solutions. It includes CompTIA Secure Cloud Professional (Security+ / Cloud+) for cloud infrastructure and security fundamentals, ISC2 CCSP for advanced cloud security management, and the Kubernetes Series for container orchestration and microservices. Python programming courses provide essential knowledge in automation and software integration, while Introduction to Agile, Scrum, and DevOps ensures participants understand modern development practices. This bundle prepares participants to manage high-level technical specifications across cloud platforms, development lifecycles, and application design.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, Cloud+ and ISC2 CCSP certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

ISC2 Certified Cloud Security Professional (CCSP)

Introduction to Agile, Scrum and DevOps

Introduction to Python and Introduction to Programming Using Python (lab) bundle

Certified Kubernetes Series

See each of the other course links for how to access the material and exam information.

Certified Information Systems Developer™ (CISD™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-83

Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CASP+, PenTest+, Microsoft MD-102: Endpoint Administration (CompTIA) Course and labs only

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Systems Developer (Work Role Code: 632)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: Designs, develops, tests, and evaluates information systems throughout the systems development lifecycle.

High-level bundle description: This bundle provides comprehensive training in developing, managing, and securing information systems. It includes CompTIA Secure Cloud Professional (Security+ / Cloud+), offering expertise in cloud infrastructure and cybersecurity fundamentals, and CASP+ for advanced enterprise security. PenTest+ focuses on hands-on vulnerability testing, ensuring participants can evaluate system weaknesses effectively. Microsoft MD-102: Endpoint Administration provides practical skills for managing and securing endpoints. This bundle prepares participants to create reliable and secure information systems by integrating cloud technologies, security frameworks, and endpoint management practices.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ / Cloud+)

CASP+

PenTest+

See each of the other course links for how to access the material and exam information.

Microsoft MD-102: Endpoint Administration (CompTIA) Course description: The TestOut Client Pro for Microsoft MD-102 course prepares students to configure, manage, and support modern desktops and devices in enterprise environments. Using interactive video lessons, quizzes, lab simulations, and practice exams on the TestOut LabSim platform, learners gain hands-on experience with Windows installation, identity and application management, network connectivity, and compliance policies. This comprehensive training aligns with the Microsoft MD-102 certification, equipping students with practical skills in client systems administration and real-world troubleshooting for enterprise-level Windows environments.

Topics Covered

- Chapter 1: Course Introduction
- Chapter 2: Windows Installation
- Chapter 3: Post Installation Tasks
- Chapter 4: Deploy Windows
- Chapter 5: Manage Identity
- Chapter 6: Group Policy
- Chapter 7: Network Connectivity
- Chapter 8: File and Storage Management
- Chapter 9: System Recovery and Protection
- Chapter 10: Monitor and Manage Windows
- Chapter 11: Compliance Policies and Configuration Profiles
- Chapter 12: Manage, Maintain, and Protect Devices
- Chapter 13: Application Management
- Appendix A: TestOut Client Pro - Practice Exams
- Appendix B: Microsoft MD-102 – Practice Exams

License Information:

- One Client Pro license – this is single user license and may not be shared
- Once activated, Client Pro is valid for 12 months
- Access keys must be redeemed within 12 months of purchase

How to Access Client Pro: An access key and instructions will be sent via email after your purchase is complete.

Certified Target Analyst Reporter™ (CTAR™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-84

Courses in bundle: CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), Project+ and PMP bundle, EC-Council Courses Master Open Source Intelligence, Mastering Threat Intelligence; OSINT for Ethical Hackers (Instagram); OSINT for Ethical Hackers and (Facebook); OPSEC Demystified: Strategies for Secure Operations; and Cyber Warfare - Defense Against Nation-State Threats

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Target Analyst Reporter (Work Role Code: 133)

NICE Work Role: Not Applicable (currently does not exist)

Combined Work Role Description: The Target Analyst Reporter (TAR) provides synthesized products to customers by researching, analyzing, and reporting intelligence via appropriate reporting vehicles in response to customer requirements and IAW missions of SIGINT, cybersecurity, and cyberspace operations. They prioritize, assess, evaluate, and report information obtained from SIGINT collection, cyber surveillance, and reconnaissance operations sources. The TAR enhances reporting with collateral information as required, maintains awareness of internal and external customer requirements, and collaborates with other collectors and analysts to refine collection and reporting requirements. The TAR shares target-related information and provides feedback to customers as appropriate. The TAR develops working aids and provides database updates on target activity to enhance and build target knowledge and improve collection. The TAR performs quality control and product-release functions.

High-level bundle description: The Certified Target Analyst Reporter (CTAR) Bundle prepares professionals for success in cyber intelligence by combining skills in threat

detection, OSINT, and secure project management. It includes the CompTIA Network Vulnerability Assessment Professional (Security+ and PenTest+), Project+ and PMP to develop cybersecurity and operational management capabilities. EC-Council's specialized courses—Master Open-Source Intelligence, Mastering Threat Intelligence, OSINT for Ethical Hackers (Facebook and Instagram)—provide targeted training in open-source investigations. The bundle is rounded out with OPSEC Demystified: Strategies for Secure Operations and Cyber Warfare – Defense Against Nation-State Threats, equipping participants to analyze, secure, and report intelligence effectively in complex threat environments.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+)

Project+ and PMP bundle

EC-Council Master Open Source Intelligence

EC-Council Mastering Threat Intelligence

EC-Council OSINT for Ethical Hackers (Instagram and Facebook)

EC-Council OPSEC Demystified: Strategies for Secure Operations

EC-Council Cyber Warfare - Defense Against Nation-State Threats

See each of the other course links for how to access the material and exam information.

Certified Site Reliability Engineer™ (CSRE™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-85

Courses in bundle: CompTIA Security+, Cloud+, Network+, Linux+, Server+ with Microsoft Bundle, Kubernetes series.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Software/Cloud Architect (Work Role Code: 628), Network Operations Specialist (Work Role Code: 441), and System Administrator (Work Role Code: 451),

NICE Work Role: Network Operations (Nice Work Role ID: IO-WRL-004), Systems Administration (Nice Work Role ID: IO-WRL-005),

Combined Work Role Description: Plans, implements, and operates network services and systems, including hardware and virtual environments. Installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts. Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedures. This includes hardware and software installation, configuration, and updates; user account management; backup and recovery management; and security control implementation. Manages and identifies program high-level technical specifications, which may include application design, cloud computing strategy and adoption, and integration of software applications into a functioning system to meet requirements.

High-level bundle description: The Certified Site Reliability Engineer (CSRE) and Applied Micro Degree Bundle equips learners with essential skills and industry-recognized certifications to manage and optimize IT infrastructure. This bundle includes CompTIA Secure Cloud Professional courses, covering Security+ and Cloud+ for cybersecurity and cloud administration, and CompTIA Cloud Admin Professional courses, such as Network+ for networking fundamentals. It also features the CompTIA Server+ and Microsoft Bundle, providing expertise in server operations and hybrid environments. Additional training includes Linux+ for systems administration and Kubernetes (CKA and CKAD) for deploying and managing containerized applications in cloud-native environments. With a focus on security, cloud computing, networking, server management, and scalable IT solutions, this bundle prepares students to excel in SRE roles, ensuring the reliability, performance, and scalability of modern IT systems.

Requirements for certification: To earn the ITI CSRE™ and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Security+, Cloud+, Server+, and Linux+, certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Secure Cloud Professional (Security+ and Cloud+)

CompTIA Network+

CompTIA Linux+

CompTIA Server+ with Microsoft Bundle

Kubernetes Series Bundle

See each of the other course links for how to access the material and exam information.

Certified Malware Reverse Engineer™ (CMRE™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-87

Courses in bundle: CompTIA Security Analytics Professional, CompTIA Network Vulnerability Assessment Professional, and CompTIA Network Security Professional (Through Security+ / PenTest+ / CySA+), CHFI (course and labs only) and ITI Official EC-Council Hacking, Malware Analysis and Reverse Engineer Curriculum.

MSRP: $4,499

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

Master Designation Eligible with Mission Readiness Range Capstone: Yes

8140 DCWF Work Role: Forensics Analyst (Work Role Code: 211) and Cyber Crime Investigator (Work Role Code: 221)

NICE Work Role: Cybercrime Investigation (Nice Work Role ID: IN-WRL-001) and Digital Evidence Analysis (Nice Work Role ID: IN-WRL-002)

Combined Work Role Description: Performs deep-dive investigations into computer-based crimes and cyber intrusion incidents by collecting, analyzing, and preserving digital evidence. Utilizes documented forensic techniques and investigative tools to identify, gather, and examine physical and digital media, including logs, ensuring the integrity of evidence. Applies advanced tactics, techniques, and procedures to balance the goals of prosecution with intelligence gathering throughout the investigative process.

High-level bundle description: This bundle offers in-depth training in cybersecurity through a blend of industry-leading certifications and advanced technical courses. It includes CompTIA Security Analytics Professional, Network Vulnerability Assessment Professional, and Network Security Professional (through Security+ / PenTest+ / CySA+), along with the CHFI course and labs. The bundle also features a specialized curriculum in malware analysis and reverse engineering, covering topics such as x64dbg debugging, reverse engineering .NET and Java applications, binary analysis on Linux, malicious document analysis, mobile app penetration testing and more. Designed

for professionals seeking mastery in intrusion analysis, malware detection, and cybercrime investigation, this bundle provides practical expertise not only in identifying and analyzing malicious artifacts but also in transforming that knowledge into effective defensive countermeasures.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the CompTIA certifications.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Security Analytics Professional (Security+ / CySA+)

CompTIA PenTest+

CTI CHFI (Course and Labs only)

EC-Council Hacking, Malware Analysis and Reverse Engineer Curriculum

See each of the other course links for how to access the material and exam information.

Chief Information Officer Certified™ (CIOC™) and Applied Micro Degree Bundle

ITI SKU: NICE-DCWF-90

Courses in bundle: CISSP and CISM Bundle, Program and Project Management (Project+ and PMP Training), Cloud+, PECB Certified Digital Transformation Officer (CDTO), PECB Certified IT Governance Manager (ISO 38500), NIST Mastery Modules (EC-Council).

MSRP: $4,599

Sales Price: $3,999

Bundle Access Period: 12 months from purchase.

8140 DCWF Work Role: Executive Cyber Leader (Work Role Code: 901) and Program Manager (Work Role Code: 801)

NICE Work Role: Executive Cybersecurity Leadership (Nice Work Role ID: OG-WRL-007) and Program Management (Nice Work Role ID: OG-WRL-010)

Combined Work Role Description: Leads, coordinates, and communicates effectively to ensure the overall success of the IT programs, integrating all aspects to meet regulatory

compliance and critical agency priorities. Accountable for program outcomes, this role demands proactive leadership and coordination to align efforts with broader organizational objectives. Responsible for developing and maintaining cybersecurity and cyberspace plans, strategies, and policies to support and align with organizational missions, initiatives, and regulatory compliance.

High-level bundle description: The Chief Information Officer Certified (CIOC) and Applied Micro Degree Bundle equips students with the essential skills required for IT leadership and governance roles. It provides project management training through Project+ certification and PMP coursework, covering both traditional and Agile methodologies. The bundle also offers cybersecurity governance expertise through CISSP and CISM coursework, practical knowledge in cloud operations through Cloud+, and leadership development in digital transformation through the PECB Certified Digital Transformation Officer program. Additionally, students gain expertise in IT governance with the ISO 38500 framework and receive training on NIST compliance frameworks through EC-Council. This comprehensive blend of strategic, operational, and technical knowledge prepares future CIOs to lead IT initiatives, manage projects effectively, and align technology with business and regulatory goals.

Requirements for certification: To earn the ITI Certification and be awarded the applied micro degree, the student must complete all courses and pass the exams for the Cloud+, Project+, PECB Certified Digital Transformation Officer and PECB Certified IT Governance Manager certification.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled Course Links

CompTIA Cloud +

CompTIA Project+ and PMP bundle

CISSP and CISM Bundle

PECB Certified Digital Transformation Officer

PECB Certified IT Governance Manager

EC-Council NIST Mastery

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Cyber (Defense)™ (DCOE-CD™) and Applied Master Micro Degree

ITI SKU: Exp-1

ITI Certifications and micro degrees in bundle: Certified Cyber Defense Analyst™ (CCDA™), Certified Cyber Forensics Analyst™ (CCFA™), Certified Cyber Defense Incident Responder™ (CCDIR™)

Partner Certifications and/or Courses in bundle: EC-Council ECIH, CSA, CTIA, and CEH and CHFI (course and lab only), CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), Security Analytics Professional (Security+ / CySA+), and Secure Cloud Professional (Security+ / Cloud+) and PECB Forensic Examiner. When purchasing this bundle as the Expert bundle under ITI SKU: Exp-1, the CASP+ course and exam is included, resulting in the candidate earning the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations upon completion. Exams are provided for all courses that have exams except CEH and CHFI.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC401 - GIAC Security Essentials (GSEC); SEC450 - GIAC Security Operations Certified (GSOC); SEC504 - GIAC Certified Incident Handler (GCIH); FOR578 - GIAC Cyber Threat Intelligence (GCTI)); SEC503 - GIAC Certified Intrusion Analyst (GCIA); and SEC511 - GIAC Continuous Monitoring Certification (GMON).

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Primary DCWF Workforce Element: Cybersecurity

Primary NICE Workforce Category: Protect and Defend

Combined DCWF/NICE Work Role Description: The Defensive Cyber Operations Expert - Cyber (Defense)™ (DCOE-CD™) encompasses a multidimensional expertise critical to modern cybersecurity challenges. Graduates of this program are prepared to excel in

roles requiring advanced threat detection, forensic investigation, and incident response. This comprehensive role integrates the skills to anticipate and neutralize cybersecurity threats, coordinate effective response strategies, and lead teams in maintaining mission-critical system integrity and resilience.

High-level bundle description: The Defensive Cyber Operations Expert – Cyber (Defense)™ (DCOE-CD™) and Applied Master Micro Degree Bundle provides an immersive and rigorous learning experience designed to prepare students for the complexities of today's cyber defense landscape. This all-encompassing program combines advanced certifications, applied micro degrees, and extensive hands-on training in areas such as cyber defense, incident response, forensic analysis, and secure cloud architecture. Graduates will develop not only the technical skills but also the operational understanding necessary to protect and defend critical systems against evolving threats. With the added distinction of earning two master designations through mission-focused evaluations, this bundle equips learners to excel in high-stakes environments.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Cyber Defense Analyst™ (CCDA™)

Certified Cyber Forensics Analyst™ (CCFA™)

Certified Cyber Defense Incident Responder™ (CCDIR™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Cyber (Infrastructure)™ (DCOE-CI™) and Applied Master Micro Degree

ITI SKU: Exp-2

ITI Certifications in bundle: Certified Cyber Defense Analyst™ (CCDA™), Certified Information Systems Security Developer™ (CISSD™), Certified Security Architect™ (CSA™)

Partner Certifications and/or Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CompTIA Security Analytics Expert and Secure Infrastructure Expert (Security+ / CySA+ / PenTest+ / CASP+), Server+ and Microsoft Bundle, CISM and CISSP bundle, CCSP, EC-Council ECIH, CSA, CTIA and CEH (course and labs only), and Microsoft MD-102: Endpoint Administration (CompTIA) (Course and labs only). Exams are provided for all courses that have exams except CISM, CISSP, CCSP and Microsoft.

MSRP: $17,499

Sales Price: $14,999

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC401 - GIAC Security Essentials (GSEC); SEC450 - GIAC Security Operations Certified (GSOC); SEC501 - GIAC Certified Enterprise Defender (GCED); SEC511 - GIAC Continuous Monitoring Certification (GMON); SEC505 - Certified Windows Security Administrator (GCWN) and SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Cyber (Infrastructure)™ (DCOE-CI™) encompasses expertise across cloud, on-premise, and hybrid environments. Professionals in this role are adept at securing and optimizing complex infrastructures, including cloud-based systems, hybrid architectures, and traditional on-premises networks. By combining advanced security analysis, architectural design, and endpoint administration, graduates are equipped to protect critical assets, ensure seamless operational integration, and respond effectively to evolving cyber threats.

High-level bundle description: The Defensive Cyber Operations Expert – Cyber (Infrastructure)™ (DCOE-CI™) and Applied Master Micro Degree Bundle offers a comprehensive training pathway for individuals seeking to master the security and operational demands of modern infrastructure. Covering cloud-native, on-premises, and hybrid technologies, this bundle includes certifications in advanced threat detection,

secure architecture, endpoint management, and governance frameworks. With hands-on labs and applied learning, participants will gain the technical depth and practical expertise to secure and manage dynamic environments. Graduates will also earn two master designations, proving their readiness to protect mission-critical infrastructure in any deployment scenario.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Cyber Defense Analyst™ (CCDA™)

Certified Information Systems Security Developer™ (CISSD™)

Certified Security Architect™ (CSA™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Cyber (Management)™ (DCOE-CM™) and Applied Master Micro Degree

ITI SKU: Exp-2

ITI Certifications in bundle: Certified Cyber Workforce Developer™ (CCWD™), Certified Cyber Authorizing Official™ (CCAO™), Systems Certified Security Manager™ (SCSM™)

Partner Certifications and/or Courses in bundle: CompTIA Project+ (with exam) and PMP Bundle, CISM and CISSP bundle, HDI-SCL (with exam), CCSP, CompTIA Secure Cloud Professional (Security+ / Cloud+), FedVTE (now CISA Learning) ISC CAP and CISSP-ISSMP, CompTIA Security Analytics Professional (Security+ / CySA+), CompTIA CASP+. Exams are provided for all courses that have exams except PMP, CISM, CISSP, CCSP, CAP and CISSP-ISSMP.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure

practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: LDR512 - GIAC Security Leadership (GSLC); LDR514 - GIAC Strategic Planning, Policy, and Leadership (GSTRT); SEC566 - GIAC Critical Controls Certification (GCCC); LDR551 - GIAC Security Operations Manager (GSOM); LDR414 - GIAC Information Security Professional (GISP); and LDR333 - SANS Security Awareness Professional (SSAP).

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Cyber (Management™) (DCOE-CM™) prepares professionals for leadership roles in cybersecurity program development, governance, and strategic decision-making. Combining workforce development, authorizing official responsibilities, and security management expertise, graduates are equipped to design and oversee cybersecurity frameworks, align organizational goals with compliance requirements, and effectively manage cross-functional teams to ensure operational excellence in mission-critical environments.

High-level bundle description: The Defensive Cyber Operations Expert – Cyber (Management™) (DCOE-CM™) and Applied Master Micro Degree Bundle is tailored for individuals aspiring to lead cybersecurity initiatives at the organizational level. This program includes advanced certifications and applied learning in project management, governance frameworks, workforce development, and secure cloud operations. Through immersive courses and practical assessments, participants gain the skills to oversee security programs, develop policies, and manage large-scale projects. With the added distinction of earning two master designations, graduates demonstrate their capability to drive mission-focused strategies and ensure resilience across diverse cyber ecosystems.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Cyber Workforce Developer™ (CCWD™)

Certified Cyber Authorizing Official™ (CCAO™)

Systems Certified Security Manager™ (SCSM™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Cyber (Assessments)™ (DCOE-CA™) and Applied Master Micro Degree

ITI SKU: Exp-4

ITI Certifications in bundle: Certified Cyber Defense Analyst™ (CCDA™), Certified Security Control Assessor™ (CSCA™), Certified Secure Software Assessor™ (CSSA™)

Partner Certifications and/or Courses in bundle: EC-Council ECIH, CSA, CTIA, and CEH (Course and Labs only), CompTIA CySA+ and CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CISA, Fundamentals of Cyber Risk Management (FedVTE (now CISA Learning)), Software Testing Fundamentals, FedVTE (now CISA Learning) CISSP-ISSEP and Static Code Analysis and Supply Chain Assurance using Sonatype Nexus. When purchasing this bundle as the Expert bundle under ITI SKU: Exp-4, the ISC CCSP (course only) and CASP+ course and exam is included, resulting in the candidate earning the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations upon completion. Exams are provided for all courses except CEH, CISA, Fundamentals of Cyber Risk Management (FedVTE (now CISA Learning)), Software Testing Fundamentals, FedVTE (now CISA Learning) CISSP-ISSEP and Static Code Analysis and Supply Chain Assurance using Sonatype Nexus.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: AUD507 - GIAC Systems and Network Auditor (GSNA); SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA); SEC560 - GIAC Penetration

Tester (GPEN); SEC488 - GIAC Cloud Security Essentials (GCLD); SEC510 - GIAC Public Cloud Security (GPCS); and SEC511 - GIAC Continuous Monitoring Certification (GMON)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Cyber (Assessments™) (DCOE-CA™) operates as a key member of the Blue Team, specializing in validating and strengthening cybersecurity defenses through detailed assessments and audits. This role focuses on defensive operations, conducting vulnerability analyses, auditing security controls, and evaluating software and system integrity to ensure compliance with established frameworks and regulations. By proactively identifying risks and validating security measures, professionals in this role ensure mission-critical systems are prepared to withstand adversarial threats while maintaining operational resilience.

High-level bundle description: This Bundle prepares participants to excel in cybersecurity evaluation and validation. Through a blend of certifications, applied learning, and hands-on assessments, this program equips learners to perform vulnerability analysis, audit security controls, assess software security, and validate compliance with cybersecurity frameworks. Graduates of this program demonstrate mastery by completing two master designations, showcasing their ability to secure and assess mission-critical systems with a focus on operational resilience and compliance.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Cyber Defense Analyst™ (CCDA™)

Certified Security Control Assessor™ (CSCA™)

Certified Secure Software Assessor™ (CSSA™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Cyber (Red Team)™ (DCOE-CR™) and Applied Master Micro Degree

ITI SKU: Exp-5

ITI Certifications in bundle: Certified Cyber Defense Analyst™ (CCDA™), Vulnerability Assessor Certified™ (VAC™), Certified Exploitation and Penetration Analyst™ (CEPA™)

Partner Certifications and/or Courses in bundle: EC-Council ECIH, CSA, CTIA, CompTIA CySA+, and CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CISA (course only), Official EC-Council CEH, CPENT and Web Application Hacking and Security, EC-Council Gateway to Pen Testing Starter Pack bundle. When purchasing this bundle as the Expert bundle under ITI SKU: Exp-4, the ISC CCSP (course only) and CASP+ course and exam is included, resulting in the candidate earning the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations upon completion. Exams are provided for all courses that have exams except CISA.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include; SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA); SEC560 - GIAC Penetration Tester (GPEN); SEC542 - GIAC Web Application Penetration Tester (GWAPT); SEC588 - Certification: GIAC Cloud Penetration Tester (GCPN); SEC504 - GIAC Certified Incident Handler (GCIH); and FOR578 - GIAC Cyber Threat Intelligence (GCTI)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Cyber (Red Team)™ (DCOE-CR™) focuses on identifying vulnerabilities and testing system defenses through ethical hacking and penetration testing methodologies. This role is critical for understanding adversarial techniques, tactics, and procedures (TTPs) to strengthen organizational cybersecurity. Professionals are adept at vulnerability assessments,

exploit analysis, and penetration testing, simulating real-world cyber threats to enhance overall security posture. This expertise ensures that organizations remain resilient against evolving cyber risk.

High-level bundle description: This bundle is tailored for cybersecurity professionals specializing in offensive security and red team operations. It combines ITI proprietary certifications with partner-recognized training to deliver advanced skills in ethical hacking, vulnerability assessment, and penetration testing. Participants gain hands-on experience and practical knowledge, preparing them to emulate adversarial behaviors and identify potential security gaps effectively. Graduates of this bundle demonstrate mastery in offensive cybersecurity techniques and tools, achieving recognition as experts capable of securing complex environments through simulated attack scenarios.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Cyber Defense Analyst™ (CCDA™)

Vulnerability Assessor Certified™ (VAC™)

Certified Exploitation and Penetration Analyst™ (CEPA™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Investigations (Analytics)™ (DCOE-IA™) and Applied Master Micro Degree

ITI SKU: Exp-6

ITI Certifications in bundle: Certified Cyber Defense Analyst™ (CCDA™), Certified Intrusion Forensics Analyst™ (CIFA™), Certified Malware Reverse Engineer™ (CMRE™)

Partner Certifications and/or Courses in bundle: EC-Council ECIH, CSA, CTIA, Certified Ethical Hacker (CEH), Certified Hacking Forensic Investigator (CHFI), Mobile Forensics, Malware and Memory Forensics, Dark Web Investigations, CompTIA Security Analytics Professional, CompTIA Network Vulnerability Assessment Professional, and CompTIA Network Security Professional (Through Security+ / PenTest+ / CySA+), and ITI Official EC-Council Hacking, Malware Analysis and Reverse Engineer Curriculum. When

purchasing this bundle as the Expert bundle under ITI SKU: Exp-6, the CASP+ course and exam is included, resulting in the candidate earning the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations upon completion. Exams are provided for all courses that have exams.

MSRP: $17,499

Sales Price: $14,999

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC450 - GIAC Security Operations Certified (GSOC); SEC504 - GIAC Certified Incident Handler (GCIH); FOR578 - GIAC Cyber Threat Intelligence (GCTI); SEC503 - GIAC Certified Intrusion Analyst (GCIA); FOR610 - GIAC Reverse Engineering Malware (GREM); and FOR508 - GIAC Certified Forensic Analyst (GCFA)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Investigations (Analytics)™ is a critical role within defensive cybersecurity, specializing in analyzing and investigating advanced threats. This role includes intrusion forensics, malware analysis, reverse engineering, and dark web investigations. Professionals in this field leverage cutting-edge tools and techniques to detect, understand, and mitigate sophisticated cyber threats, providing actionable intelligence to enhance organizational security and resilience.

High-level bundle description: This Bundle equips participants with advanced analytical and investigative skills critical to modern cybersecurity operations. Focusing on areas such as intrusion forensics, malware analysis, and reverse engineering, this bundle combines hands-on labs and expert-level training to prepare learners for identifying and mitigating complex cyber threats. Graduates demonstrate their mastery through practical assessments and two master designations, showcasing their ability to deliver actionable intelligence and strengthen organizational defenses against evolving adversaries.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Cyber Defense Analyst™ (CCDA™)

Certified Intrusion Forensics Analyst™ (CIFA™)

Certified Malware Reverse Engineer™ (CMRE™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Intelligence (Cyberspace)™ (DCOE-IC™) and Applied Master Micro Degree

ITI SKU: Exp-7

ITI Certifications in bundle: Certified All-Source Requirements Manager™ (CASRM™), Certified All-Source Analyst™ (CASA™), Certified Cyber Intelligence Planner Professional™ (CCIPP™)

Partner Certifications and/or Courses in bundle: CompTIA Project+ and PMP Bundle, CompTIA Security+. CASP+, and CySA+, EC-Council CTIA and EC-Council Master Open-Source Intelligence Curriculum, OSINT for Ethical Hackers (Instagram/Facebook) Curriculum and Master Threat Intelligence Curriculum. EC-Council CEH (Course and labs only). When purchasing this bundle as the Expert bundle under ITI SKU: Exp-7, the PenTest+ course and exam is included, resulting in the candidate earning the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations upon completion. Exams are provided for all courses except CEH, PMP, EC-Council Master Open-Source Intelligence Curriculum, OSINT for Ethical Hackers (Instagram/Facebook) Curriculum and Master Threat Intelligence Curriculum.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure

practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC450 - GIAC Security Operations Certified (GSOC); SEC40 - GIAC Security Essentials (GSEC); FOR578 - GIAC Cyber Threat Intelligence (GCTI); SEC504 - GIAC Certified Incident Handler (GCIH); LDR525 - GIAC Certified Project Manager (GCPM); and SEC497 - GIAC Open Source Intelligence (GOSI)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Intelligence (Cyberspace)™ (DCOE-IC™) role focuses on safeguarding critical infrastructure and sensitive data from adversaries. This work role integrates comprehensive all-source intelligence analysis with defensive cyber operations to preempt, identify, and mitigate cybersecurity threats in real time. Key responsibilities include strategic planning for cyber defense, conducting threat analysis, leveraging open-source intelligence (OSINT), and utilizing advanced penetration testing to evaluate vulnerabilities. Professionals in this role are equipped to support mission-critical cybersecurity objectives across government and private sectors.

High-level bundle description: This bundle provides an all-encompassing learning experience tailored for cybersecurity professionals specializing in intelligence-driven cyber operations. Participants gain expertise in multiple domains, including all-source intelligence management, advanced OSINT techniques, threat intelligence, and penetration testing. The program incorporates ITI proprietary certifications alongside prestigious partner certifications to prepare learners for strategic and tactical cybersecurity challenges. By completing this bundle, candidates achieve two master designations, underscoring their applied knowledge and technical proficiency. It offers a cost-effective alternative to industry expert certifications such as the SANS GIAC Security Expert (GSE), delivering robust hands-on components and requiring advanced certifications for practical application in operational environments.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified All-Source Requirements Manager™ (CASRM™)

Certified All-Source Analyst™ (CASA™)

Certified Cyber Intelligence Planner Professional™ (CCIPP™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Cyber Enabler (Leaders)™ (DCOE-CL™) and Applied Master Micro Degree

ITI SKU: Exp-8

ITI Certifications in bundle: Certified Cyber Policy and Strategy Planner™ (CCPSP™), Certified Executive Cyber Leader™ (CECL™), Chief Information Officer Certified™ (CIOC™)

Partner Certifications and/or Courses in bundle: Security+ (with exam), EC-Council CCISO (with exam), CTI CISSP and CISM bundle (courses and labs only), Cloud+ (course and exam), HDI Support Center Lead (HDI-SCL) (with exam), CISSP-ISSMP (FedVTE (now CISA Learning) Course only) and PECB CISO, Program and Project Management (Project+ and PMP Training), PECB Certified Digital Transformation Officer (CDTO), PECB Certified IT Governance Manager (ISO 38500), NIST Mastery Modules (EC-Council). When purchasing this bundle as the Expert bundle under ITI SKU: Exp-8, the Project+ course and exam is included. Exams are provided for all courses that have exams except CISSP, CISM, and CISSP-ISSMP.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC401- GIAC Security Essentials (GSEC); LDR525 - GIAC Certified Project Manager (GCPM); and LDR512 - GIAC Security Leadership (GSLC); LDR514 - GIAC Strategic Planning, Policy, and Leadership (GSTRT); SEC566 - GIAC

Critical Controls Certification (GCCC); and LDR414 - GIAC Information Security Professional (GISP).

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Cyber Enabler (Leaders)™ (DCOE-CL™) is a pivotal role in aligning cybersecurity initiatives with organizational goals. Professionals in this role lead policy development, strategy planning, and high-level decision-making to enhance cyber resilience across critical infrastructure. This work role emphasizes strategic leadership in cybersecurity operations, including governance, executive leadership, and digital transformation to address emerging threats and opportunities in cyberspace. Cyber Enablers ensure operational compliance and guide teams toward mission-focused cybersecurity solutions.

High-level bundle description: This bundle is designed for cybersecurity leaders and executives aiming to influence organizational and national cyber strategies. The program equips participants with expertise in crafting and implementing cybersecurity policies, managing complex IT projects, and driving organizational change through digital transformation. The curriculum combines ITI proprietary certifications with renowned partner courses to deliver a well-rounded educational experience. Participants who complete this bundle demonstrate mastery in strategic leadership, policy development, and program management, earning recognition as cyber leaders. This cost-effective alternative to comparable programs like the SANS GSE offers robust practical components and hands-on learning experiences to meet operational demands

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Cyber Policy and Strategy Planner™ (CCPSP™)

Certified Executive Cyber Leader™ (CECL™)

Chief Information Officer Certified™ (CIOC™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Cyber Enabler (Legal/LE)™ (DCOE-CLE™) and Applied Master Micro Degree

ITI SKU: Exp-9

ITI Certifications in bundle: Certified Cyber Legal Advisor™ (CCLA™), Certified Intrusion Forensics Analyst™ (CIFA™), Certified Cyber Crime Forensic Investigator™ (CCCFI™)

Partner Certifications and/or Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CISM and CISSP bundle, CCSP, CISA, PECB Forensics Examiner, CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CompTIA Security Analytics Professional (Security+ / CySA+), CTI Custom EC-Council CEH and CHFI. When purchasing this bundle as the Expert bundle under ITI SKU: Exp-8, the CASP+ course and exam is included, resulting in the candidate earning the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations upon completion. Exams are provided for all courses that have exams except CCSP, CISSP, CISM, CISA, CEH and CHFI.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC401- GIAC Security Essentials (GSEC); AUD507 - GIAC Systems and Network Auditor (GSNA); SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA); and LDR414 - GIAC Information Security Professional (GISP); LEG523: - GIAC Law of Data Security & Investigations (GLEG); and FOR508 - GIAC Certified Forensic Analyst (GCFA)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Cyber Enabler (Legal/LE)™ (DCOE-CLE™) bridges the gap between technical cybersecurity operations and legal, law enforcement, and compliance responsibilities. This role requires expertise in cybercrime investigations, forensic analysis, and cyber legal advising to support the prosecution of cybercrimes and ensure compliance with regulatory frameworks. Professionals are skilled at conducting forensic examinations, developing legal strategies for cyber incidents, and advising on policies to mitigate risks. They play a critical role in addressing emerging legal challenges in the digital domain.

High-level bundle description: This bundle is specifically tailored for cybersecurity professionals operating in legal, law enforcement, and regulatory environments. Participants develop advanced skills in cyber forensics, legal advisory, and compliance management, preparing them to navigate complex cybersecurity incidents and legal disputes. Combining ITI proprietary certifications with leading industry-recognized credentials, this bundle equips learners with the tools necessary to address the intersection of technology and law effectively. Graduates of this program are well-prepared to conduct investigations, provide expert legal counsel, and drive initiatives ensuring adherence to global cybersecurity standards.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Cyber Legal Advisor™ (CCLA™)

Certified Intrusion Forensics Analyst™ (CIFA™)

Certified Cyber Crime Forensic Investigator™ (CCCFI™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Cyber Enabler (Programs)™ (DCOE-PM™) and Applied Master Micro Degree

ITI SKU: Exp-10

ITI Certifications in bundle: Certified Program Manager™ (CPM™), Certified IT Project Manager™ (CITPM™), Certified IT Program Auditor™ (CITPA™)

Partner Certifications and/or Courses in bundle: CISM and CISSP bundle, Project+ and PMP bundle, HDI-SCL, CompTIA Secure Cloud Professional (Security+ / Cloud+), CSM, CISA, CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), PECB ISO/IEC 20000 Auditor. When purchasing this bundle as the Expert bundle under ITI SKU: Exp-10, the EC-Council Risk Management Approach and Practices – RM course and exam are included, as well as the CTI PMI Risk Management Professional (PMI-RMP) course. Exams are provided for all courses that have exams except CISSP, CISM, PMP, PMI-RMP and CISA.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: LDR512 - GIAC Security Leadership (GSLC); LDR514 - GIAC Strategic Planning, Policy, and Leadership (GSTRT); SEC566 - GIAC Critical Controls Certification (GCCC); LDR525 - GIAC Certified Project Manager (GCPM); LDR414 - GIAC Information Security Professional (GISP); and LDR333 - SANS Security Awareness Professional (SSAP).

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Cyber Enabler (Programs)™ (DCOE-PM™) specializes in managing and auditing complex cybersecurity programs and projects. This role is essential for ensuring that cybersecurity initiatives are effectively planned, executed, and evaluated. Professionals in this role combine technical knowledge with project and program management expertise to align cybersecurity objectives with organizational strategies. They oversee risk management, compliance, and resource optimization to support mission-critical operations in government and enterprise environments.

High-level bundle description: This bundle is specifically tailored for program managers and cybersecurity professionals focused on leading and auditing IT programs. Participants develop advanced skills in project management, IT auditing, and program leadership, ensuring alignment with organizational goals and compliance with international standards. The curriculum integrates ITI proprietary certifications and prestigious partner courses, offering a comprehensive learning experience that prepares participants to lead and audit large-scale cybersecurity programs effectively. By completing this bundle, candidates gain mastery in program management, auditing, and cybersecurity leadership, earning recognition as experts in managing mission-critical IT initiatives.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Program Manager™ (CPM™)

Certified IT Project Manager™ (CITPM™)

Certified IT Program Auditor™ (CITPA™)

See each of the other course links for how to access the material and exam information.

Defensive Cyber Operations Expert – Cyber Enabler (Training)™ (DCOE-TR™) and Applied Master Micro Degree

ITI SKU: Exp-11

ITI Certifications in bundle: Certified Cyber Curriculum Developer™ (CCCD™), Certified Cyber Instructor™ (CCI™), Certified Secure System Administrator™ (CSSA™)

Partner Certifications and/or Courses in bundle: CompTIA Secure Cloud Professional (Security+ / Cloud+), CompTIA Network Vulnerability Assessment Professional and CompTIA Secure Infrastructure Expert and CompTIA Security Analytics Expert (official Security+ / CySA+ / PenTest+ / CASP+) with labs and exam vouchers, CompTIA Linux Network Professional (Network+ / Linux+), and CompTIA Server+ and Microsoft Bundle. Exams are provided for all courses that have exams except Microsoft.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC401 - GIAC Security Essentials (GSEC); SEC450 - GIAC Security Operations Certified (GSOC); SEC501 - GIAC Certified Enterprise Defender (GCED); SEC511 - GIAC Continuous Monitoring Certification (GMON); and SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA); and SEC488 - GIAC Cloud Security Essentials (GCLD)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Defensive Cyber Operations Expert – Cyber Enabler (Training)™ (DCOE-TR™) plays a critical role in developing, delivering, and managing cybersecurity training programs. Professionals in this role design effective curricula, deliver technical training, and support organizational readiness through tailored instruction. They are responsible for ensuring that cybersecurity personnel are equipped with the skills and knowledge required to secure and operate complex systems. This role combines technical expertise with pedagogical skills, enabling the creation and implementation of cutting-edge training programs that support mission-critical operations.

High-level bundle description: This bundle is tailored for cybersecurity training professionals focused on developing and delivering technical education and training. Participants gain expertise in curriculum development, secure systems administration, and technical instruction. By combining ITI proprietary certifications with industry-recognized credentials, this program provides a comprehensive path to mastery in cybersecurity training and operational readiness. Graduates of this bundle demonstrate advanced capabilities in training design, delivery, and support, earning recognition as leaders in cybersecurity education and training program.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each

certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Cyber Curriculum Developer™ (CCCD™)

Certified Cyber Instructor™ (CCI™)

Certified Secure System Administrator™ (CSSA™)

See each of the other course links for how to access the material and exam information.

Offensive Cyber Operations Expert (OCOE) - Cyber Effects (CE)™ (OCOE-CE™) and Applied Master Micro Degree

ITI SKU: Exp-12

ITI Certifications in bundle: Certified Exploitation and Penetration Analyst™ (CEPA™), Certified Joint Targeting Analyst™ (CJTA™), Certified Mission Assurance Specialist™ (CMAS™)

Partner Certifications and/or Courses in bundle: EC-Council CEH and CPENT and Web Application Hacking and Security and EC-Council Gateway to Pen Testing Starter Pack bundle, CompTIA Network Security Professional (Security+ / PenTest+ / CySA+), EC-Council Courses Master Open-Source Intelligence, Mastering Threat Intelligence; OSINT for Ethical Hackers (Instagram); OSINT for Ethical Hackers and (Facebook); OPSEC Demystified: Strategies for Secure Operations; and Cyber Warfare and Nation-State Threats, CompTIA Project+ and PMP Bundle and EC-Council Risk Management Approach and Practices – RM and PMI Risk Management Professional (PMI-RMP) Bundle. When purchasing this bundle as the Expert bundle under ITI SKU: Exp-12, the CASP+ course and exam is included, resulting in the candidate earning the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations upon completion. Exams are provided for all courses that have exams except PMP and PMI-RMP.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that

include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA); SEC560 - GIAC Penetration Tester (GPEN); SEC542 - GIAC Web Application Penetration Tester (GWAPT); SEC588 - Certification: GIAC Cloud Penetration Tester (GCPN); SEC504 - GIAC Certified Incident Handler (GCIH); and FOR578 - GIAC Cyber Threat Intelligence (GCTI)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Offensive Cyber Operations Expert – Cyber Effects (CE)™ (OCOE-CE™) specializes in planning and executing offensive cyber operations to achieve tactical and strategic effects in cyberspace. This role focuses on exploiting vulnerabilities, conducting penetration testing, and leveraging cyber capabilities to neutralize threats and support joint targeting initiatives. Professionals in this role also ensure mission assurance by integrating operational security measures with actionable intelligence, playing a critical part in advancing national security and organizational objectives in cyberspace.

High-level bundle description: This bundle is tailored for professionals focused on offensive cyber strategies, equipping them with advanced skills in penetration testing, vulnerability exploitation, and mission-oriented targeting analysis. Combining ITI proprietary certifications with globally recognized partner programs, it provides a comprehensive learning experience that balances technical expertise with strategic planning. Participants gain hands-on training in ethical hacking, open-source intelligence, and threat assessment, preparing them to deliver measurable impacts in high-stakes cyber environments and enhance mission-critical operations.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added, and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Exploitation and Penetration Analyst™ (CEPA™)

Certified Joint Targeting Analyst™ (CJTA™)

Certified Mission Assurance Specialist™ (CMAS™)

See each of the other course links for how to access the material and exam information.

Technical Support Operations Expert – IT (Cyberspace)™ (TSOE-IT™) and Applied Master Micro Degree

ITI SKU: Exp-13

ITI Certifications in bundle: Certified Network Operations Specialist™ (CNOS™), Certified Secure System Administrator™ (CSSA™), Certified Enterprise Security Architect™ (CESA™)

Partner Certifications and/or Courses in bundle: CompTIA Cloud Admin Professional (Network+ / Cloud+), CASP+, Linux+, Windows Server 2019 - Administration Concepts, CCNA, CompTIA Server+ and Microsoft Bundle (Microsoft MTA 98-365, AZ-104 Azure Administrator and Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure), CTI CISSP and CISM bundle, CISSP-ISSEP (FedVTE (now CISA Learning)) and EC-Council Mastering Microsoft Sentinel and EC-Council Cisco Certified CyberOps Associate (200-201). When purchasing this bundle as the Expert bundle under ITI SKU: Exp-13, the PenTest+ course and exam is included, resulting in the candidate earning the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations upon completion. Exams are provided for all courses that have exams except Microsoft (all), CISSP, CISM, CISSP-ISSEP, and Cisco.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC401 - GIAC Security Essentials (GSEC); SEC450 - GIAC Security Operations Certified (GSOC); SEC501 - GIAC Certified Enterprise Defender (GCED); SEC511 - GIAC Continuous Monitoring Certification (GMON); SEC505 - Certified

Windows Security Administrator (GCWN); and SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Technical Support Operations Expert – IT (Cyberspace)™ (TSOE-IT™) is a key role focused on maintaining and securing enterprise IT systems to ensure operational stability and resilience. This role encompasses network operations, secure system administration, and enterprise architecture, providing comprehensive support for IT infrastructure in mission-critical environments. Professionals are skilled in troubleshooting, system configuration, and implementing security best practices across diverse platforms, ensuring the seamless operation of complex IT ecosystems while addressing emerging cyber threats.

High-level bundle description: This bundle is designed for IT professionals specializing in technical support operations, equipping them with the skills needed to manage and secure enterprise IT environments effectively. It combines ITI proprietary certifications with industry-leading partner programs to deliver a robust curriculum focused on network administration, secure system management, and enterprise security architecture. Through hands-on labs and real-world scenarios, participants gain the practical expertise required to optimize IT operations and protect against evolving cyber risks, positioning them as essential contributors to organizational success.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Network Operations Specialist™ (CNOS™)

Certified Secure System Administrator™ (CSSA™)

Certified Enterprise Security Architect™ (CESA™)

See each of the other course links for how to access the material and exam information.

Technical Support Operations Expert – Software Engineering™ (TSOE-SE™) and Applied Master Micro Degree

ITI SKU: Exp-14

ITI Certifications in bundle: Certified Secure Software Development Professional™ (CSSDP™), Certified Product Support Manager™ (CPSM™), Certified Software Test & Evaluation Specialist™ (CSTES™)

Partner Certifications and/or Courses in bundle: DevOps Fundamentals, Agile Scrum Master – Master the Principles, Introduction to Python, Introduction to Programming Using Python (lab), Certified Kubernetes Administrator (CKA), Certified Kubernetes Application Developer (CKAD), Kubernetes - Containerizing Applications in the Cloud, CompTIA Secure Cloud Professional (Security+ / Cloud+), HDI-SCL, CompTIA Project+ and PMP Bundle, Certified Scrum Product Owner (CSPO) Certification (course and exam), CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CTI Fundamentals of the Software Development Lifecycle (SDLC) and Software Testing Lab, EC-Council CASE .NET and Web Application Hacking and Security. When purchasing this bundle as the Expert bundle under ITI SKU: Exp-14, the EC-Council Certified DevSecOps Engineer course and exam is included. Exams are provided for all courses that have exams except Kubernetes.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA); SEC560 - GIAC Penetration Tester (GPEN); SEC542 - GIAC Web Application Penetration Tester (GWAPT); SEC588 - Certification: GIAC Cloud Penetration Tester (GCPN); SEC573 - GIAC Python Coder (GPYC); and SEC540 - GIAC Cloud Security Automation (GCSA)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Technical Support Operations Expert – Software Engineering™ (TSOE-SE™) focuses on developing, testing, and maintaining secure software systems while ensuring robust operational support throughout the software lifecycle. This role combines expertise in secure software development, product support, and test and evaluation practices to optimize software reliability, security, and functionality. Professionals in this role are critical to building resilient software solutions and providing technical leadership in software engineering operations.

High-level bundle description: This bundle is designed for professionals specializing in software engineering and technical operations, equipping them with the skills to develop, test, and secure software in complex environments. Combining ITI proprietary certifications with leading industry-recognized training, it offers a comprehensive curriculum in DevSecOps, secure software development, and software lifecycle management. Through practical labs and real-world application, participants gain expertise in securing and managing software systems, positioning them as leaders in technical operations and software engineering.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Secure Software Development Professional™ (CSSDP™)

Certified Product Support Manager™ (CPSM™)

Certified Software Test & Evaluation Specialist™ (CSTES™)

See each of the other course links for how to access the material and exam information.

Technical Support Operations Expert – Data/AI™ (TSOE-DA™) and Applied Master Micro Degree

ITI SKU: Exp-15

ITI Certifications in bundle: Certified Data Analyst Professional™ (CDAP™), Applied Data Scientist Certified Professional™ (ADSCP™), Certified AI Test & Evaluation Specialist™ (CATES™)

Partner Certifications and/or Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+), CompTIA Data+ and DataX, CTI Data Analyst Career Path, Microsoft Certified: Azure Data Scientist Associate (live online), CTI Introduction to Python Programming (Course and Labs) bundle, EC-Council: Machine Learning with Python, CompTIA PenTest+, CISA, Microsoft Certified Azure AI Engineer Associate (live online) and AWS Certified Machine Learning Specialist (live online), CTI AWS Cloud Practitioner and CTI Azure fundamentals. Exams are provided for all courses that have exams except AWS Cloud Practitioner and Azure fundamentals.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA); SEC595 - GIAC Machine Learning Engineer (GMLE); SEC542 - GIAC Web Application Penetration Tester (GWAPT); SEC588 - Certification: GIAC Cloud Penetration Tester (GCPN); SEC573 - GIAC Python Coder (GPYC); and SEC540 - GIAC Cloud Security Automation (GCSA)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand, unless otherwise noted as live online.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Technical Support Operations Expert – Data/AI™ (TSOE-DA™) specializes in applying data science, machine learning (ML), and artificial intelligence (AI) to enhance operational effectiveness and decision-making. This role involves managing data systems, developing and deploying ML models, and testing AI systems for reliability and security. Professionals in this position leverage data-driven insights and predictive analytics to optimize workflows and implement innovative AI and ML solutions for mission-critical environments.

High-level bundle description: This bundle is designed for professionals in data science and analytics, machine learning, and artificial intelligence, providing comprehensive training in data analytics, AI engineering, and secure data workflows. Combining ITI proprietary certifications with industry-recognized programs, it equips participants with practical expertise in ML model development, AI integration, and cloud-based data

solutions. Through hands-on labs and live-online instruction, participants gain the skills to lead data science initiatives, implement AI-driven solutions that incorporate machine learning, and address complex challenges in operational environments.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Data Analyst Professional™ (CDAP™)

Applied Data Scientist Certified Professional™ (ADSCP™)

Certified AI Test & Evaluation Specialist™ (CATES™)

See each of the other course links for how to access the material and exam information.

Critical Infrastructure Certified Expert™ (CICE™) and Applied Master Micro Degree

ITI SKU: Exp-16

ITI Certifications in bundle: Certified Control Systems Security Specialist™ (CCSSS™), Certified Infrastructure Support Specialist™ (CISS™), Certified System Testing and Evaluation Specialist™ (CSTES™)

Partner Certifications and/or Courses in bundle: CompTIA Security Analytics Professional (Security+ / CySA+) and Secure Cloud Professional (Security+ / Cloud+), PECB SCADA Security Manager, ICS/SCADA Cybersecurity (EC-Council), EC-Council AI Mastery: Securing ICS/SCADA and Industrial Control Systems (ICS) Cybersecurity Bundle, Certified Network Defender – EC-Council CND and CEH Blended Bundle, CISSP-ISSEP (FedVTE (now CISA Learning)), CTI Linux+ (course and lab only) and CompTIA CASP+, CompTIA Network Vulnerability Assessment Professional (Security+ / PenTest+), CCSP, CISA, CTI Software Testing Fundamentals. This bundle also meets the requirements for the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations. When purchasing this bundle as the Expert bundle under ITI SKU: Exp-16, the EC-Council Applied Secure Smart City, Cybersecurity for Telecommunications, Cybersecurity for FinTech, and Industrial Cybersecurity:

Healthcare courses are included. Exams are provided for all courses that have exams except CCSP, CISA, CISSP-ISSEP and Linux+.

MSRP: $17,499

Sales Price: $14,999

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA); : SEC401 - GIAC Security Essentials (GSEC); SEC450 - GIAC Security Operations Certified (GSOC); SEC501 - GIAC Certified Enterprise Defender (GCED); ICS410 - Global Industrial Cyber Security Professional (GICSP); and ICS515 - GIAC Response and Industrial Defense (GRID)

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand, unless otherwise noted as live online.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Critical Infrastructure Certified Expert™ (CICE™) is responsible for protecting and supporting critical infrastructure systems, including Industrial Control Systems (ICS), SCADA systems, and other essential infrastructure components. This role involves expertise in control systems security, infrastructure support, and rigorous system testing and evaluation to ensure operational continuity and resilience against cyber threats. Professionals in this position apply advanced cybersecurity principles and frameworks to secure critical infrastructure environments and manage emerging risks in diverse sectors, such as healthcare, telecommunications, and smart cities.

High-level bundle description: This bundle is designed for professionals specializing in securing and supporting critical infrastructure systems. Combining ITI proprietary certifications with industry-leading partner programs, it provides a robust curriculum in ICS/SCADA and other critical infrastructure security, infrastructure support, and system evaluation. Participants gain hands-on experience in securing industrial environments, testing system vulnerabilities, and implementing advanced cybersecurity strategies. The training prepares candidates to lead efforts in safeguarding critical infrastructure against evolving threats, ensuring operational safety and national security.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Control Systems Security Specialist™ (CCSSS™)

Certified Infrastructure Support Specialist™ (CISS™)

Certified System Testing and Evaluation Specialist™ (CSTES™)

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Expert – Cyber™ (CITE-C™) and Applied Master Micro Degree

ITI SKU: Exp-17

ITI Certifications in bundle: Certified Insider Threat Professional - Cyber Analytics (CITP-CA), Certified Insider Threat Professional - User Activity Monitoring (CITP-UAM™), Certified Insider Threat Professional - Cyber Lead (CITP-CL)

Partner Certifications and/or Courses in bundle: CompTIA Security Analytics Professional Certification (Security+ / CySA+), Linux+ (course and labs only), EC-Council CSA, CompTIA Cloud+, CASP+ and PenTest+ and EC-Council CEH (courses and labs only), and CHFI (courses and labs only), Microsoft Certified: Information Protection and Compliance Administrator Associate, Teramind Insider Detection Course, Mastering Microsoft Sentinel. This bundle also meets the requirements for the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations. Exams are provided for all courses that have exams except CEH, CHFI and Linux+.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the

completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC450 - GIAC Security Operations Certified (GSOC); SEC504 - GIAC Certified Incident Handler (GCIH SEC401 - GIAC Security Essentials (GSEC); SEC503 - GIAC Certified Intrusion Analyst (GCIA); SEC501 - GIAC Certified Enterprise Defender (GCED); and FOR508 - GIAC Certified Forensic Analyst (GCFA).

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand, unless otherwise noted as live online.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Certified Insider Threat Expert – Cyber™ (CITE-C™) focuses on identifying, mitigating, and managing risks associated with insider threats in cybersecurity environments. This role combines expertise in user activity monitoring, cyber analytics, and leadership to safeguard organizational assets against internal vulnerabilities. Professionals in this position implement advanced detection strategies, oversee compliance with information protection policies, and lead proactive insider threat management programs to protect critical infrastructure and sensitive data.

High-level bundle description: This bundle is designed for professionals specializing in insider threat detection and management, offering a comprehensive curriculum in cyber analytics, user monitoring, and advanced cybersecurity practices. Combining ITI proprietary certifications with globally recognized partner programs, participants gain hands-on experience in using cutting-edge tools and strategies to identify and mitigate insider risks. This training equips professionals with the skills to develop robust insider threat programs, ensure compliance, and enhance organizational resilience against internal cyber risks associated with insider threats.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Insider Threat Professional - Cyber Analytics (CITP-CA)

Certified Insider Threat Professional - User Activity Monitoring (CITP-UAM™)

Certified Insider Threat Professional - Cyber Lead (CITP-CL)

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Expert – Infrastructure™ (CITE-I™) and Applied Master Micro Degree

ITI SKU: Exp-17

ITI Certifications in bundle: Certified Insider Threat Professional – Infrastructure Operator™ (CITP-IO™), Certified Insider Threat Professional – User Activity Monitoring™ (CITP-UAM™), Certified Insider Threat Professional – Infrastructure Engineer™ (CITP-IE™)

Partner Certifications and/or Courses in bundle: CompTIA Linux Network Professional and CompTIA Network Infrastructure Professional (Network+ / Server+ / Linux+), CompTIA CASP+ and Microsoft Bundle, NIST SP 800-53 Controls Mastery Bundle, CompTIA Secure Cloud Professional AND CompTIA Cloud Admin Professional (Security+ / Cloud+ / Network+), CCNA and HDI-SCA, CompTIA CySA+, Microsoft Certified: Information Protection and Compliance Administrator Associate, Linux+ (courses and labs only) CEH and CHFI (course and labs only), Teramind Insider Detection Course, Mastering Microsoft Sentinel. When purchasing this bundle as the Expert bundle under ITI SKU: Exp-17, the PenTest+ course and exam is included, resulting in the candidate earning the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations upon completion. Exams are provided for all courses that have exams except CEH, CHFI and CCNA.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC450 - GIAC Security Operations Certified (GSOC); SEC504 - GIAC Certified Incident Handler (GCIH), SEC401 - GIAC Security Essentials (GSEC); SEC503 - GIAC Certified Intrusion Analyst (GCIA); SEC501 - GIAC Certified Enterprise Defender (GCED); and SEC555 - GIAC Certified Detection Analyst (GCDA).

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand, unless otherwise noted as live online.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Certified Insider Threat Expert – Cyber™ (CITE-C™) focuses on identifying, mitigating, and managing risks associated with insider threats in cybersecurity environments. This role combines expertise in user activity monitoring, cyber analytics, and leadership to safeguard organizational assets against internal vulnerabilities. Professionals in this position implement advanced detection strategies, oversee compliance with information protection policies, and lead proactive insider threat management programs to protect critical infrastructure and sensitive data.

High-level bundle description: This bundle is designed for professionals specializing in insider threat detection and management, offering a comprehensive curriculum in cyber analytics, user monitoring, and advanced cybersecurity practices. Combining ITI proprietary certifications with globally recognized partner programs, participants gain hands-on experience in using cutting-edge tools and strategies to identify and mitigate insider risks. This training equips professionals with the skills to develop robust insider threat programs, ensure compliance, and enhance organizational resilience against internal cyber risks associated with insider threats.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Insider Threat Professional - Cyber Analytics (CITP-CA)

Certified Insider Threat Professional - User Activity Monitoring (CITP-UAM™)

Certified Insider Threat Professional - Cyber Lead (CITP-CL)

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Expert – Data™ (CITE-D™) and Applied Master Micro Degree

ITI SKU: Exp-18

ITI Certifications in bundle: Certified Insider Threat Professional - Data Analytics™ (CITP-DA™), Certified Insider Threat Professional - Cyber Analytics (CITP-CA™) and Certified Insider Threat Professional - Data Scientist™ (CITP-DS™)

Partner Certifications and/or Courses in bundle: CompTIA Security+, Data+ and DataSys+, Linux+ (course and labs only), ITI's custom Data Analyst bundle, and HDI-SCA, CompTIA CySA+ and DataX, CTI Python with Labs, ITI Custom EC-Council Data Science bundle, CompTIA Cloud+, CASP+ and PenTest+ and EC-Council CEH (courses and labs only), and CHFI (courses and labs only). This bundle also meets the requirements for the CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations. Exams are provided for all courses that have exams except CEH and CHFI.

MSRP: $17,499

Sales Price: **$14,999**

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: SEC460 - GIAC Enterprise Vulnerability Assessor (GEVA); SEC595 - GIAC Machine Learning Engineer (GMLE); SEC588 - Certification: GIAC Cloud Penetration Tester (GCPN); SEC573 - GIAC Python Coder (GPYC); SEC401 - GIAC Security Essentials (GSEC); and SEC501 - GIAC Certified Enterprise Defender (GCED).

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand, unless otherwise noted as live online.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Certified Insider Threat Expert – Data™ (CITE-D™) focuses on detecting, analyzing, and mitigating insider threats through advanced data analytics and data science methodologies. This role requires expertise in managing large datasets, applying statistical and machine learning techniques, and leveraging cyber analytics to identify patterns of risky behavior. Professionals in this position play

a critical role in safeguarding organizational data assets by developing and implementing robust data-driven insider threat programs.

High-level bundle description: This bundle is designed for professionals specializing in insider threat detection and data-driven cybersecurity solutions. Combining ITI proprietary certifications with globally recognized partner courses, it offers a comprehensive curriculum in data analytics, data science, and cyber analytics. Participants gain hands-on experience with Python programming, data systems, and advanced statistical models, equipping them with the tools needed to identify and mitigate insider threats effectively. This program prepares professionals to lead data-centric insider threat initiatives and protect critical organizational assets.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Insider Threat Professional - Data Analytics™ (CITP-DA™)

Certified Insider Threat Professional - Data Scientist™ (CITP-DS™)

Certified Insider Threat Professional - Cyber Lead (CITP-CL)

See each of the other course links for how to access the material and exam information.

Certified Insider Threat Expert – Operations™ (CITE-O™) and Applied Master Micro Degree

ITI SKU: Exp-18

ITI Certifications in bundle: Certified Insider Threat Professional – Program Manager™ (CITP-PM™), Certified Insider Threat Professional – Cyber Lead (CITP-CL) and Certified Insider Threat Professional – Hub Chief™ (CITP-HC™)

Partner Certifications and/or Courses in bundle: CompTIA Cloud+, CASP+ and PenTest+ and EC-Council CEH (courses and labs only), and CHFI (courses and labs only), CompTIA Security+, Project+, PMP, NIST SP 800-53 Controls Mastery Bundle and HDI-SCL, CompTIA CySA+, CISSP and CISM bundle, CTI PMI-RMP, NIST SP 800-53 Controls Mastery Bundle and HDI-SCL. This bundle also meets the requirements for the

CompTIA Security Analytics Expert and CompTIA Secure Infrastructure Expert designations. In addition, students must take the Teramind Insider Detection Course. Exams are provided for all courses that have exams except CEH, CHFI, CISSP, CISM, PMP and PMI-RMP.

MSRP: $17,499

Sales Price: $14,999

Compare to SANS/GIAC GSE: Our Expert Series offers a significantly lower cost at comparable value to SANS GIAC Security Expert (GSE), featuring ITI certifications that include robust hands-on components, and requiring two master designations to ensure practical application to mission-critical operations. Award of the GSE requires the completion of any six Practitioner certifications and any four Applied Knowledge certifications at a cost of approximately $60,670 (Practitioner Certifications: $58,674 and Applied Knowledge Certifications (exam-only): $1,996). Comparable courses and certifications may include: LDR512 - GIAC Security Leadership (GSLC); LDR514 - GIAC Strategic Planning, Policy, and Leadership (GSTRT); SEC566 - GIAC Critical Controls Certification (GCCC); LDR551 - GIAC Security Operations Manager (GSOM); LDR414 - GIAC Information Security Professional (GISP); and SEC501 - GIAC Certified Enterprise Defender (GCED).

Bundle Access Period and Delivery: Access is for 36 months from purchase (one ITI certification bundle at a time over consecutive 12-month periods) and all courses are Online OnDemand, unless otherwise noted as live online.

Master Designation Requirement: Two (included in price)

Combined Work Role Description: The Certified Insider Threat Expert – Operations™ (CITE-O™) focuses on managing and executing insider threat operations to safeguard organizational assets and mitigate risks. This role integrates operational management, program leadership, and centralized oversight to detect, deter, and respond to insider threats. Professionals in this role are skilled in coordinating cross-functional teams, implementing security policies, and utilizing advanced tools and methodologies to ensure the successful operation of insider threat programs across complex environments.

High-level bundle description: This bundle is tailored for professionals responsible for the operational aspects of insider threat management. It combines ITI proprietary certifications with globally recognized training to provide expertise in program management, operational leadership, and insider threat detection. Participants gain hands-on experience with tools, frameworks, and policies that enable them to identify and neutralize insider risks effectively. This comprehensive program equips professionals with the skills to lead insider threat initiatives, coordinate operational responses, and protect critical organizational resources in dynamic environments.

Requirements for certification: To earn the ITI Practitioner, Master, and Exert Certifications and be awarded the applied micro degrees and applied master micro degree, the student must complete all courses and pass the exams for each certification described within that ITI Certification and applied micro degree bundle and any new courses and certifications that have been added and pass two Master Designations within the Mission Readiness Range.

Recommended prerequisites, certification validity and renewals: Visit our dedicated webpage for more information and vendor links.

Bundled ITI Certification Course and Applied Micro Degree Links:

Certified Insider Threat Professional – Program Manager™ (CITP-PM™)

Certified Insider Threat Professional – Hub Chief™ (CITP-HC™)

Certified Insider Threat Professional - Cyber Lead (CITP-CL)

See each of the other course links for how to access the material and exam information.

Additional Training

CompTIA Secure Cloud Professional (Security+ / Cloud+) and CompTIA Cloud Admin Professional (Network+ / Cloud+) Dual Bundle

ITI SKU: CompTIA-34
Bundle Program Name: CompTIA Secure Cloud Professional (Security+ / Cloud+) and CompTIA Cloud Admin Professional (Network+ / Cloud+)
MSRP: $2999
Sales Price: $2799
Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Secure Cloud Professional (Security+ / Cloud+) and CompTIA Cloud Admin Professional (Network+ / Cloud+) provides comprehensive training for individuals seeking to excel in network and cloud security and administration. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Security+, Network+ and Cloud+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam vouchers and an exam pass guarantee: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Security+ and Cloud+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Security+ SY0-701: Develop critical security skills with our CompTIA Security+ course, designed to provide the knowledge needed to secure and protect networks and systems.

Course Highlights:

- Duration: 30+ hours
- Content: 110+ On-demand Videos
- Exam Prep: 300 Prep Questions
- Certificate of Completion for CompTIA Security+ SY0-701

Topics Areas Included:

- Fundamental Security Concepts
- Threat Types Comparison
- Cryptographic Solutions
- Identity and Access Management
- Securing Enterprise and Cloud Network Architectures
- Resiliency and Site Security
- Vulnerability Management
- Network Security Capabilities
- Endpoint Security Capabilities
- Application Security Capabilities
- Incident Response and Monitoring
- Indicators of Malicious Activity
- Security Governance Concepts
- Risk Management Processes
- Data Protection and Compliance Concepts

Modules:

- Module 1: General Security Concepts
- Module 2: Threats, Vulnerabilities, and Mitigations
- Module 3: Security Architecture
- Module 4: Security Operations
- Module 5: Security Program Management and Oversight

Labs included (17 hours):

19. Security Concept Fundamentals
20. Cryptographic Solutions
21. Threat Vectors and Attack Surfaces
22. Identifying Security Vulnerabilities
23. Analyze Malicious Activity
24. Mitigation Techniques
25. Security Architecture Models
26. Securing Enterprise Infrastructures
27. Data Protection Strategies
28. Resilience in Security Architecture
29. Securing Computing Resources
30. Asset Management Techniques
31. Vulnerability Management
32. Monitoring Computing Resources
33. Enhancing Enterprise Security
34. Implement Identity & Access Management
35. Implementation of Automation & Orchestration for Security Operations
36. Investigative Data Sources

CompTIA Cloud+ CV0-003: Master cloud infrastructure and services with our CompTIA Cloud+ course, covering essential cloud computing skills.

Course Highlights:

- Duration: 8+ hours
- Content: 130+ On-demand Videos
- Exam Prep: 45+ Prep Questions
- Certificate of Completion for CompTIA Cloud+ CV0-003

Topics Areas Included:

- Cloud Architecture and Design
- Cloud Security
- Cloud Deployment
- Operations and Support
- Troubleshooting

Modules:

- Module 1: CompTIA Cloud+ CV0-003 Course Overview
- Module 2: General Cloud Knowledge
- Module 3: Cloud Security
- Module 4: Cloud Deployment
- Module 5: Operations and Support
- Module 6: Troubleshooting
- Module 7: Course Closeout

Labs included (28 hours):

34. Cloud Deployment Models
35. Different Cloud Service Models
36. Cloud Resource Capacity Planning
37. High Availability and Scalability in the Cloud
38. Analyzing Business Requirements for a Cloud Solution
39. Configuring and Managing Cloud Identities
40. Cloud Networking Concepts
41. Securing Cloud Infrastructure Resources

42. Data Security and Compliance in the Cloud
43. Cloud Security Assessments and Tools
44. Incident Response Procedures
45. Cloud Solution Integration
46. Provisioning Cloud Resources
47. Provisioning Public Cloud Storage Solutions
48. Provisioning Private Cloud Storage Solutions
49. Deploying Cloud Networking Solutions
50. Virtualization Concepts and Platforms
51. Cloud Migration Techniques
52. Configuring Logging for Cloud Resources
53. Implementing Cloud Resource Monitoring Solutions
54. Implementing Cloud Resource Monitoring and Alert Solutions
55. Cloud Dashboards and Reporting
56. Cloud Patches, Upgrading and Lifecycle Management
57. Optimizing Cloud Solutions
58. Implementing Cloud Resource Automation Solutions
59. Implementing Cloud Backup and Restore Solutions
60. Cloud Disaster Recovery Concepts
61. Cloud Troubleshooting Methodologies
62. Security Troubleshooting Techniques
63. Troubleshooting Cloud Deployments
64. Cloud Networking Troubleshooting Concepts
65. Troubleshooting Cloud Resource Utilization
66. Automation and Orchestration Troubleshooting Methodologies

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Security+ (SY0-701) CertMaster Learn and Labs: CertMaster Learn is a self-paced, comprehensive online learning experience that helps you gain the knowledge

and practical skills necessary to be successful on your CompTIA certification exam, and in your IT career. A Learning Plan helps you stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for you to practice and apply your skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on inputs.

When purchased with CertMaster Learn in a bundle, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Comparing Security Roles and Security Controls
- Explaining Threat Actors and Threat Intelligence
- Performing Security Assessments
- Identifying Social Engineering and Malware
- Summarizing Basic Cryptographic Concepts
- Implementing Public Key Infrastructure
- Implementing Authentication Controls
- Implementing Identity and Account Management Controls
- Implementing Secure Network Designs
- Implementing Network Security Appliances

- Implementing Secure Network Protocols
- Implementing Host Security Solutions
- Implementing Secure Mobile Solutions
- Summarizing Secure Application Concepts
- Implementing Secure Cloud Solutions
- Explaining Data Privacy and Protection Concepts
- Performing Incident Response
- Explaining Digital Forensics
- Summarizing Risk Management Concepts
- Implementing Cybersecurity Resilience
- Explaining Physical Security

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Scanning and Identifying Network Nodes
- Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
- Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- APPLIED LAB: Performing Network Reconnaissance and Vulnerability Scanning
- Assisted Lab: Managing the Lifecycle of a Certificate
- Assisted Lab: Managing Certificates with OpenSSL
- Assisted Lab: Auditing Passwords with a Password Cracking Utility
- Assisted Lab: Managing Centralized Authentication
- Assisted Lab: Managing Access Controls in Windows Server
- Assisted Lab: Configuring a System for Auditing Policies
- Assisted Lab: Managing Access Controls in Linux
- APPLIED LAB: Configuring Identity and Access Management Controls
- Assisted Lab: Implementing a Secure Network Design

- Assisted Lab: Configuring a Firewall
- Assisted Lab: Configuring an Intrusion Detection System
- Assisted Lab: Implementing Secure Network Addressing Services
- Assisted Lab: Implementing a Virtual Private Network
- Assisted Lab: Implementing a Secure SSH Server
- Assisted Lab: Implementing Endpoint Protection
- APPLIED LAB: Securing the Network Infrastructure
- Assisted Lab: Identifying Application Attack Indicators
- Assisted Lab: Identifying a Browser Attack
- Assisted Lab: Implementing PowerShell Security
- Assisted Lab: Identifying Malicious Code
- APPLIED LAB: Identifying Application Attacks
- Assisted Lab: Managing Data Sources for Incident Response
- Assisted Lab: Configuring Mitigation Controls
- Assisted Lab: Acquiring Digital Forensics Evidence
- Assisted Lab: Backing Up and Restoring Data in Windows and Linux
- APPLIED LAB: Managing Incident Response, Mitigation and Recovery

CompTIA Cloud+ (CV0-003) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow. Easy-to-use course management tools provide a comprehensive suite of

instructor resources alongside a reporting dashboard, making course preparation and progress tracking simple and efficient.

Topics Covered:

- Understanding Cloud Concepts
- Planning and Designing a Cloud Environment
- Administering Cloud Resources
- Managing Cloud Storage
- Managing Networks in the Cloud
- Securing and Troubleshooting Networks in the Cloud
- Managing Cloud Migrations and Troubleshooting Cloud Deployments
- Managing Cloud Automation and Orchestration
- Understanding Cloud Security Concepts
- Managing Cloud Security
- Managing Cloud Performance
- Managing Maintenance in the Cloud
- Implementing High Availability and Disaster Recovery in the Cloud

Labs Available:

- Assisted Lab: Explore the Lab Environment
- Assisted Lab: Plan and Design a Cloud Environment
- Assisted Lab: Deploy and Manage Cloud Resources
- Assisted Lab: Manage Compute Resources
- Assisted Lab: Manage Networks in the Cloud
- Assisted Lab: Secure Cloud Components
- APPLIED LAB: Deploy Cloud Resources
- Assisted Lab: Manage Cloud Automation
- Assisted Lab: Manage Baseline Configurations
- Assisted Lab: Deploy Patches
- Assisted Lab: Configure Monitoring

- Assisted Lab: Manage Backup and Restore Processes
- APPLIED LAB: Manage Cloud Resources

CTI Custom Online Self-Paced ILT Description:

CompTIA Network+ N10-008: Master networking with our comprehensive CompTIA Network+ course, designed to provide the skills needed to manage and troubleshoot various network systems effectively.

Course Highlights:

- Duration: 25 hours
- Content: 110 On-demand Videos
- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Network+ N10-008

Topics Areas Included:

- Networking Fundamentals
- Network Implementations
- Network Operations
- Network Security
- Network Troubleshooting

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching

- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

Engage in over 33+ hours of labs that reinforce the material learned and prepare you for real-world networking scenarios:

- Introduction to the OSI Model
- Networking Topologies and Characteristics
- Internet Protocol Addressing Solutions
- Cable and Connector Types
- Cable Management Solutions
- Virtual Network Concepts
- Network Security Concept Fundamentals
- General Network Attacks
- Network Services and Protocols
- Network Command Line Tools
- Network Analysis Software
- Configuring and Maintaining DNS Servers
- DHCP Server Installation and Configuration
- Remote Access and Management
- Load Balancing and NIC Teaming
- NTP Server Management
- High Availability and Disaster Recovery Concepts
- Configuring Switching Features
- Routing Concepts and Protocols

- Troubleshooting Common Networking Issues
- Cloud Concepts
- Network Architecture
- Networking Device Monitoring
- Network Troubleshooting Techniques
- Networking Hardening Techniques and Best Practices
- Physical Networking Tools
- Defining Networking Devices
- Troubleshooting Cable Connectivity
- Wireless Configuration Techniques and Standards
- Troubleshooting and Securing Wireless Networks
- Physical Network Security Concepts
- Organizational Documentation and Procedures
- Organizational Networking Diagrams and Agreements

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Network+ (N10-008) CertMaster Learn and Labs: CertMaster Learn for CompTIA Network+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Comparing OSI Model Network Functions
- Lesson 2: Deploying Ethernet Cabling
- Lesson 3: Deploying Ethernet Switching
- Lesson 4: Troubleshooting Ethernet Networks
- Lesson 5: Explaining IPv4 Addressing
- Lesson 6: Supporting IPv4 and IPv6 Networks
- Lesson 7: Configuring and Troubleshooting Routers
- Lesson 8: Explaining Network Topologies and Types
- Lesson 9: Explaining Transport Layer Protocols
- Lesson 10: Explaining Network Services
- Lesson 11: Explaining Network Applications
- Lesson 12: Ensuring Network Availability
- Lesson 13: Explaining Common Security Concepts
- Lesson 14: Supporting and Troubleshooting Secure Networks
- Lesson 15: Deploying and Troubleshooting Wireless Networks
- Lesson 16: Comparing WAN Links and Remote Access Methods
- Lesson 17: Explaining Organizational and Physical Security Concepts
- Lesson 18: Explaining Disaster Recovery and High Availability Concepts
- Lesson 19: Applying Network Hardening Techniques
- Lesson 20: Summarizing Cloud and Datacenter Architecture

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Capture Network Traffic
- Assisted Lab: Configure Interface Settings
- Assisted Lab: Configure IPv4 Static Addressing

- Assisted Lab: Analyze ARP Traffic
- Assisted Lab: Use Tools to Test IP Configuration
- Assisted Lab: Configure IPv6 Static Addressing
- Assisted Lab: Configure Static Routing
- Assisted Lab: Configure Dynamic Routing
- APPLIED Lab: Troubleshoot IP Networks
- Assisted Lab: Use Network Scanners
- Assisted Lab: Analyze a DHCP Server Configuration
- Assisted Lab: Analyze a DNS Server Configuration
- Assisted Lab: Analyze Application Security Configurations
- Assisted Lab: Configure Secure Access Channels
- Assisted Lab: Configure SNMP and Syslog Collection
- Assisted Lab: Analyze Network Performance
- APPLIED Lab: Verify Service and Application Configuration
- Assisted Lab: Configure a NAT Firewall
- Assisted Lab: Configure Remote Access
- APPLIED Lab: Troubleshoot Service and Security Issues
- Assisted Lab: Develop Network Documentation
- Assisted Lab: Backup and Restore Network Device Configurations
- Assisted Lab: Analyze an On-Path Attack
- Assisted Lab: Configure Port Security

Product and License Information:

- One license provides access to CertMaster Learn for Security+, Network+ and Cloud+ with CertMaster Labs integrated throughout the courses and ITI courses and labs.
- Access keys must be redeemed within 12 months of purchase.
- Once redeemed, licenses will be valid for 12 months

How to Access CertMaster Learn with integrated CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Security+ and Cloud+): This bundle includes an exam voucher and an exam pass guarantee for Security+, Network+ and Cloud+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CompTIA Linux Network Professional and CompTIA Network Infrastructure Professional (Network+ / Server+ / Linux+), CompTIA CASP+ and Microsoft Bundle

ITI SKU: CompTIA-35

MSRP: $3,999

Sales Price: $3,499

Bundle Access Period: 12 months from purchase.

High-level description: The CompTIA Linux Network Professional (Network+ / Linux+) Bundle provides comprehensive training for individuals seeking to excel in networking and Linux system administration. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Network+ and Linux+, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee for Network+ and Linux+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for Network+ and Linux+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA Network+ N10-008: Master networking with our comprehensive CompTIA Network+ course, designed to provide the skills needed to manage and troubleshoot various network systems effectively.

Course Highlights:

- Duration: 25 hours
- Content: 110 On-demand Videos

- Exam Prep: 500 Prep Questions
- Certificate of Completion for CompTIA Network+ N10-008

Topics Areas Included:

- Networking Fundamentals
- Network Implementations
- Network Operations
- Network Security
- Network Troubleshooting

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

CompTIA Linux+ XK0-004: Gain expertise in Linux system administration with our CompTIA Linux+ course.

Course Highlights:

- Duration: 30+ hours
- Content: 120+ On-demand Videos
- Exam Prep: 400+ Prep Questions
- Certificate of Completion for CompTIA Linux+ XK0-004

Topics Areas Included:

- Introduction to Linux
- Administering Users and Groups
- Configuring Permissions
- Implementing File Management
- Managing Software and Storage
- Configuring Network Settings
- Securing Linux Systems
- Scripting and Automation

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching
- Module 10 - Wireless Technologies
- Module 11 Network Performance

- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

Labs Included:

CompTIA Network+ (33 hours)

1. Introduction to the OSI Model
2. Networking Topologies and Characteristics
3. Internet Protocol Addressing Solutions
4. Cable and Connector Types
5. Cable Management Solutions
6. Virtual Network Concepts
7. Network Security Concept Fundamentals
8. General Network Attacks
9. Network Services and Protocols
10. Network Command Line Tools
11. Network Analysis Software
12. Configuring and Maintaining DNS Servers
13. DHCP Server Installation and Configuration
14. Remote Access and Management
15. Load Balancing and NIC Teaming
16. NTP Server Management
17. High Availability and Disaster Recovery Concepts
18. Configuring Switching Features
19. Routing Concepts and Protocols
20. Troubleshooting Common Networking Issues
21. Cloud Concepts

22. Network Architecture
23. Networking Device Monitoring
24. Network Troubleshooting Techniques
25. Networking Hardening Techniques and Best Practices
26. Physical Networking Tools
27. Defining Networking Devices
28. Troubleshooting Cable Connectivity
29. Wireless Configuration Techniques and Standards
30. Troubleshooting and Securing Wireless Networks
31. Physical Network Security Concepts
32. Organizational Documentation and Procedures
33. Organizational Networking Diagrams and Agreements

CompTIA Linux+ (63 hours)

1. Design Hard Disk Layout
2. Create Partitions and Filesystems
3. Using Various Disk Management Tools
4. Working with Kernel, Boot Modules, and Files
5. Working with Relative and Absolute Paths
6. Work with the Flow Control Constructs
7. Control Mounting and Unmounting of Filesystems
8. View the Hard Drive Details
9. Check and Repair Filesystems
10. Using RPM and YUM Package Management
11. Using Debian Package Management
12. Using Repositories
13. Managing User and Group Accounts and Related System Files
14. Run User Level Queries

15. Managing Disk Quotas
16. Working with Bash Profiles and Bash Scripts
17. Setup Host Security
18. Perform Basic File Editing Operations Using vi
19. Search Text Files using Regular Expressions
20. Using Shell Input and Output Redirections
21. Install and Configure a Web Server
22. Performing Basic File Management
23. Amending Hard and Symbolic Links
24. Find System Files and Place Files in the Correct Location
25. Use Systemctl and update-rc.d Utility to Manage Services
26. Configuring Host Names
27. Change Runlevels and Shutdown or Reboot System
28. Maintain System Time
29. Configure Client Side DNS
30. Configure System Logging
31. Mail Transfer Agent (MTA) Basics
32. Automate System Administration Tasks by Scheduling Jobs
33. Create, Monitor and Kill Processes
34. Manage Printers and Printing
35. Accessibility
36. Manage File Permissions and Ownership
37. Perform Security Administration Tasks
38. Working with Access Control List
39. Configure SELinux
40. Maintain the Integrity of Filesystems
41. Work with Pluggable Authentication Modules (PAM)

42. Secure Communication using SSH
43. Securing Data with Encryption
44. Work with TTY
45. Set up SFTP to Chroot Jail only for Specific Group
46. Secure a Linux Terminal and Implement Logging Services
47. Boot the System
48. Configure UFW and DenyHosts
49. Compress Data Using Various Tools and Utilities
50. Process Text Streams using Filters
51. Basic Network Troubleshooting
52. Use Streams Pipes and Redirects
53. Perform CPU Monitoring and Configuration
54. Perform Memory Monitoring and Configuration
55. Perform Process Monitoring
56. Modify Process Execution Priorities
57. Manage File and Directory Permissions
58. Access the Linux System
59. Configure Inheritance and Group Memberships
60. Patch the System
61. Working with the Environment Variables
62. Shells, Scripting and Data Management
63. Customize or Write Simple Scripts
64. Configure Permissions on Files and Directories
65. Work with PKI

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA Network+ (N10-008) CertMaster Learn and Labs: CertMaster Learn for CompTIA Network+ provides a comprehensive eLearning experience that helps learners

gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Comparing OSI Model Network Functions
- Lesson 2: Deploying Ethernet Cabling
- Lesson 3: Deploying Ethernet Switching
- Lesson 4: Troubleshooting Ethernet Networks
- Lesson 5: Explaining IPv4 Addressing
- Lesson 6: Supporting IPv4 and IPv6 Networks
- Lesson 7: Configuring and Troubleshooting Routers
- Lesson 8: Explaining Network Topologies and Types
- Lesson 9: Explaining Transport Layer Protocols
- Lesson 10: Explaining Network Services
- Lesson 11: Explaining Network Applications
- Lesson 12: Ensuring Network Availability
- Lesson 13: Explaining Common Security Concepts
- Lesson 14: Supporting and Troubleshooting Secure Networks
- Lesson 15: Deploying and Troubleshooting Wireless Networks
- Lesson 16: Comparing WAN Links and Remote Access Methods

- Lesson 17: Explaining Organizational and Physical Security Concepts
- Lesson 18: Explaining Disaster Recovery and High Availability Concepts
- Lesson 19: Applying Network Hardening Techniques
- Lesson 20: Summarizing Cloud and Datacenter Architecture

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Configure a SOHO Router
- Assisted Lab: Capture Network Traffic
- Assisted Lab: Configure Interface Settings
- Assisted Lab: Configure IPv4 Static Addressing
- Assisted Lab: Analyze ARP Traffic
- Assisted Lab: Use Tools to Test IP Configuration
- Assisted Lab: Configure IPv6 Static Addressing
- Assisted Lab: Configure Static Routing
- Assisted Lab: Configure Dynamic Routing
- APPLIED Lab: Troubleshoot IP Networks
- Assisted Lab: Use Network Scanners
- Assisted Lab: Analyze a DHCP Server Configuration
- Assisted Lab: Analyze a DNS Server Configuration
- Assisted Lab: Analyze Application Security Configurations
- Assisted Lab: Configure Secure Access Channels
- Assisted Lab: Configure SNMP and Syslog Collection
- Assisted Lab: Analyze Network Performance
- APPLIED Lab: Verify Service and Application Configuration
- Assisted Lab: Configure a NAT Firewall
- Assisted Lab: Configure Remote Access
- APPLIED Lab: Troubleshoot Service and Security Issues
- Assisted Lab: Develop Network Documentation

- Assisted Lab: Backup and Restore Network Device Configurations
- Assisted Lab: Analyze an On-Path Attack
- Assisted Lab: Configure Port Security

CompTIA Linux+ (XK0-005) CertMaster Learn and Labs: CertMaster Learn for CompTIA Linux+ provides a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Lesson 1: Introducing Linux
- Lesson 2: Administering Users and Groups
- Lesson 3: Configuring Permissions
- Lesson 4: Implementing File Management
- Lesson 5: Authoring Text Files
- Lesson 6: Managing Software
- Lesson 7: Administering Storage
- Lesson 8: Managing Devices, Processes, Memory, and the Kernel
- Lesson 9: Managing Services
- Lesson 10: Configuring Network Settings
- Lesson 11: Configuring Network Security

- Lesson 12: Managing Linux Security
- Lesson 13: Implementing Simple Scripts
- Lesson 14: Using Infrastructure as Code
- Lesson 15: Managing Containers in Linux
- Lesson 16: Installing Linux

Integrated Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Basic Linux Interaction
- Assisted Lab: Manage User Accounts
- Assisted Lab: Manage Group Accounts
- Assisted Lab: Configure and troubleshoot privilege escalation
- Assisted Lab: Configure Standard Permissions
- Assisted Lab: Configure Special Permissions
- Assisted Lab: Configure ACLs
- Assisted Lab: Troubleshoot permissions
- APPLIED LAB: Identity and Access Control
- Assisted Lab: Manage File Links
- Assisted Lab: Use File Management Commands
- Assisted Lab: Search for Files
- Assisted Lab: Edit Text Files
- Assisted Lab: Backup, Restore, and Compress Files
- Assisted Lab: Manage RPM Packages
- Assisted Lab: Manage DEB Packages
- Assisted Lab: Compile a Program
- Assisted Lab: Download Files From a Web Server
- APPLIED LAB: File and software management
- Assisted Lab: Deploy Storage and LVM

- Assisted Lab: Manage Processes
- Assisted Lab: Manage Services
- Assisted Lab: Deploy Services
- Assisted Lab: Configure Network Settings
- Assisted Lab: Configure Remote Administration
- Assisted Lab: Troubleshoot Network Configurations
- APPLIED LAB: System Management
- Assisted Lab: Configure a Firewall
- Assisted Lab: Intercept Network Traffic
- Assisted Lab: Harden a Linux System
- Assisted Lab: Verify file integrity by using hashes.
- Assisted Lab: Configure SELinux
- APPLIED LAB: Security
- Assisted Lab: Manage Scripts
- Assisted Lab: Configure a System with Ansible
- Assisted Lab: Manage Version Control with Git
- Assisted Lab: Deploy Docker Containers
- Assisted Lab: Manage GRUB2
- Assisted Lab: Deploy a Linux System
- APPLIED LAB: Scripting, Orchestration, Installation

Product and License Information:

- One license provides access to CertMaster Learn for Network+ and Linux+ with CertMaster Labs integrated throughout the courses
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses are valid for 12 months

How to Access Courses and Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Network+ and Linux+): This bundle includes an exam voucher and an exam pass guarantee for Network+ and Linux+: if you don't pass the exams on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

High-level description: The CompTIA Server+ and Microsoft Bundle are designed to provide comprehensive training for individuals looking to gain expertise in server management and hybrid cloud environments. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA Server+ and Microsoft technologies, combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. Although the Microsoft MTA 98-365 is no longer offered, the training, in addition to the AZ-104 Azure Administrator training, prepares you for both the Server+ and Microsoft Hybrid Core exams. The bundle also includes an exam voucher and an exam pass guarantee for Server+.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT, followed by the integrated CompTIA Server+ CertMaster Learn and Labs and TestOut training for Microsoft Hybrid Core.

CTI Custom Online Self-Paced ILT Descriptions:

Microsoft MTA 98-365 course and labs: This training provides valuable knowledge and skills necessary for server management, which is useful for preparing for the Server+ certification. This course offers comprehensive content delivered through engaging video lessons, quizzes, and hands-on labs. Once purchased, you have 12 months' access to the course.

Course Highlights:

- Duration: 5+ Training Hours
- Content: 35+ On-demand Videos, covering essential server management topics
- Preparation Questions: 74

Modules:

- Module 1 Introducing Windows Server 2016
- Module 2 Managing Windows Server 2016
- Module 3 Managing Storage
- Module 4 Monitoring and Troubleshooting Servers
- Module 5 Essential Services

- Module 6 Understanding File and Print Services
- Module 7 Windows Network Services and Applications
- Mod 8 Key Takeaways
- Mod 9 Terms to Know
- Mod 10 Hands on Labs

Labs included (30 hours)

- Install and Configure Nano Server
- Install and Configure Server Core
- Configure Network Installation of Windows
- Manage Windows Services
- Working with Mail Servers
- Configure Remote Assistance and Remote Server Admin Tools
- Manage Remote Access with VPN
- Configure Application Virtualization
- Manage Active Directory Infrastructure - Part 1
- Manage Active Directory Infrastructure - Part 2
- Manage Active Directory Infrastructure - Part 3
- Manage Virtual Hard Disks with Hyper-V
- Enable Nested Virtualization
- Manage Shared Storage using iSCSI
- Manage Updates with Windows Server Update Services
- Configure Group Policy Settings
- Configure Disk Types
- Configure Distributed File System
- Manage Disk Redundancy
- Manage File System Security
- Manage Windows Event Logs
- Configure Audit Policies
- Administer OUs and Containers
- Administer User and Group Accounts

- Implement Group Nesting
- Backup and Restore Active Directory
- Install and Configure a Database Server
- Install and Configure a Failover Cluster
- Configure User Profiles
- Implement Folder Redirection
- Implement Performance Monitor
- Install and Configure Web Services
- Working with Collaboration Software
- Install and Configure Threat Management Software
- Manage Remote Desktop Services

CompTIA Server+ labs: The Server+ Practice Lab's primary focus is the practical application of the CompTIA exam objectives, providing a 19-hour hands-on practical lab experience. Once purchased, you have 12 months' access to the labs.

Labs included (19 hours):

- Server Operating Systems Installation Methods
- Server Network Infrastructure Configuration
- Installing and Configuring Server Roles and Features
- Server Identity and Access Management
- Deploying and Managing Server Storage
- Implementing a Backup and Restore Solution
- Automation of Server Administration using Scripts
- Server Virtualization Concepts
- Configuring Server High Availability
- Server and Application Hardening Techniques
- Server Hardware Components
- Securing a Physical Server Infrastructure
- Server Hardware Maintenance
- Server Licensing Concepts
- Data Security Concepts
- Troubleshooting Server Storage Related Issues

- Server Operating Systems Troubleshooting Techniques
- Troubleshooting Network Connectivity Issues

AZ-104 Microsoft Azure Administrator Certification: Prepare for the Microsoft AZ-104 Azure Administrator certification with this comprehensive course. This course covers advanced Azure administration, including managing Azure identities and governance, implementing and managing storage, and configuring and managing virtual networks.

Course Highlights:

- Duration: 35+ Training Hours
- Content: 85+ On-demand Videos, covering Azure administration topics
- Preparation Questions: 200

Modules:

- Module 1 – Overview: Azure Essentials for Success
- Module 2 – Tools: Navigating the Azure Ecosystem
- Module 3 – Identities and Governance: Secure and Efficient Identity Management
- Module 4 – Master Data Storage and Security
- Module 5 – Compute Resources: Unlock the Power of Azure Compute
- Module 6 – Virtual Networks: Connect and Secure Your Resources
- Module 7 – Monitoring and Backup: Ensure Stability and Recovery

Labs included (8 hours):

- Azure Management Concepts Lab (3 Hours):
  - Azure Service Level Agreements (SLAs)
  - Management Tools
  - Monitoring Tools
  - The Azure Marketplace
- Azure Storage Management Lab (2 Hours):
  - Azure Storage Services
  - Working with Blobs
  - Azure SQL Databases
  - Azure Cosmos Databases
- Azure Security Concepts Lab (3 Hours):
  - Using Azure Key Vault

- Security Tools
- Network Security

Sever+ CertMaster Learn with Labs:

Server+ CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with your studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow. Easy-to-use course management tools provide a comprehensive suite of instructor resources alongside a reporting dashboard, making course preparation and progress tracking simple and efficient.

Topics Covered:

- Lesson 1: Understanding Server Administration Concepts
- Lesson 2: Understanding Virtualization and Cloud Computing
- Lesson 3: Understanding Physical and Network Security Concepts
- Lesson 4: Managing Physical Assets
- Lesson 5: Managing Server Hardware
- Lesson 6: Configuring Storage Management
- Lesson 7: Installing and Configuring an Operating System
- Lesson 8: Troubleshooting OS, Application, and Network Configurations
- Lesson 9: Managing Post-Installation Administrative Tasks
- Lesson 10: Managing Data Security
- Lesson 11: Managing Service and Data Availability
- Lesson 12: Decommissioning Servers

Integrated Labs:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Reporting Windows Server Specifications
- Assisted Lab: Reporting Linux Server Specifications
- Assisted Lab: Deploying a Hyper-V VM
- Assisted Lab: Deploying a Docker Container

- Assisted Lab: Auditing Network Services
- Assisted Lab: Securing Network Traffic with IPSec
- Assisted Lab: Managing System Inventories
- Assisted Lab: Monitoring Performance in Windows
- Assisted Lab: Monitoring Performance in Linux
- APPLIED LAB: Deploying and Monitoring Servers
- Assisted Lab: Managing Event Logs in Windows
- Assisted Lab: Managing Event Logs in Linux
- Assisted Lab: Configuring RAID Storage in Windows
- Assisted Lab: Provisioning iSCSI Storage
- Assisted Lab: Deploying a Linux Application Server
- Assisted Lab: Configuring Volumes in Linux
- Assisted Lab: Managing Network Configurations
- Assisted Lab: Developing Network Documentation
- Assisted Lab: Developing Administrative Bash Scripts
- Assisted Lab: Developing Administrative PowerShell Scripts
- APPLIED LAB: Managing Storage and Networks
- Assisted Lab: Troubleshooting a Network Issue
- Assisted Lab: Auditing Accounts and Permissions in Windows
- Assisted Lab: Configuring Server Roles
- Assisted Lab: Configuring Administrative Interfaces
- Assisted Lab: Managing Virtual Memory
- Assisted Lab: Configuring Group Policy Objects
- Assisted Lab: Analyzing Configuration Baselines
- APPLIED LAB A: Troubleshooting Servers Scenario #1
- APPLIED LAB B: Troubleshooting Servers Scenario #2
- APPLIED LAB C: Troubleshooting Servers Scenario #3
- Assisted Lab: Configuring EFS and BitLocker
- Assisted Lab: Troubleshooting a Security Issue
- Assisted Lab: Configuring Backup Solutions on Windows Server
- Assisted Lab: Configuring Backup Solutions on Linux
- Assisted Lab: Configuring a File Server Cluster
- Assisted Lab: Decommissioning a Domain Controller
- APPLIED LAB A: Troubleshooting Server Security Scenario #1
- APPLIED LAB B: Troubleshooting Server Security Scenario #2

TestOut Hybrid Server Pro: Core

Hybrid Server Pro: Core is a high-quality, easy-to-use curriculum where you will gain the knowledge and skills you need to configure and manage both on-premise and cloud based servers. Hosted on the online TestOut learning platform, LabSim, it provides a

comprehensive experience for gaining knowledge and practical skills through interactive learning modules like video lessons and lab simulations.

LabSim is ideal for learning server technology in a self-paced engaging way. Instructional lessons are combined with instructor-led videos, demonstrations, quizzes, practice exams, and performance-based lab simulations to provide hours of content to prepare you for the ***Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure*** certification exam.

- Engaging video lessons and text lessons teach you key on-premise and cloud concepts and skills
- Section quizzes help you gauge how well you're retaining what you've learned
- Performance-based labs simulations let you apply what you've learned in real-world scenarios and provide detailed feedback reports and scores
- Exam practice for Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure certification exam includes Readiness Reports, Domain Exams, and full-length exams that emulate the real certification exam

Topics and Integrated Labs Covered

- Chapter 1: Course Introduction
- Chapter 2: On-Premises Windows Server
- Chapter 3: Cloud and Azure
- Chapter 4: Manage IP Addressing
- Chapter 5: Implement DNS
- Chapter 6: Active Directory
- Chapter 7: Active Directory Objects
- Chapter 8: Group Policy
- Chapter 9: Manage Servers and Workloads in a Hybrid Environment
- Chapter 10: Manage Storage Devices
- Chapter 11: Manage File Services
- Chapter 12: Virtualization and Containers
- Chapter 13: On-Premises and Hybrid Network Connectivity
- Appendix A: TestOut Hybrid Server Pro: Core - Practice Exams
- Appendix B: Microsoft AZ-800: Administering Windows Server Hybrid Core Infrastructure - Practice Exams

License Information

- One license provides access to CertMaster Learn for Server+ (SK0-005) with CertMaster Labs integrated throughout the course, TestOut, as well as ITI custom courses and labs.

- Once activated, the license is valid for 12 months

How to Access Courses and Labs

An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher and Exam Pass Guarantee (Server+ only): This bundle includes an exam voucher and an exam pass guarantee for Server+: if you don't pass the Server+ exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

High-level description: The CompTIA CASP+ Bundle provides comprehensive training for individuals seeking to excel in advanced security practices and enterprise security. This blended bundle includes custom self-paced online instructor-led training (ILT) courses for CompTIA CASP+ (CAS-004), combined with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. The bundle also includes an exam voucher and an exam pass guarantee: if you don't pass the exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT for CASP+, followed by the integrated CompTIA CertMaster Learn and Labs.

CTI Custom Online Self-Paced ILT Description:

CompTIA CASP+: Gain expertise in advanced security practices with our CompTIA CASP+ course, covering essential concepts and practices for enterprise security.

Course Highlights:

- Duration: 28+ hours
- Content: 85+ On-demand Videos
- Exam Prep: 250 Prep Questions
- Certificate of Completion for CompTIA CASP+

Topics Areas Included:

- Risk Management: Understanding and applying risk management frameworks and methodologies.
- Enterprise Security Architecture: Designing and implementing secure network architectures.

- Security Operations: Conducting security assessments and implementing advanced security measures.
- Technical Integration: Integrating security controls and technologies in enterprise environments.
- Incident Response: Developing and implementing effective incident response strategies.
- Cryptography: Applying cryptographic techniques to secure communications and data.
- Threat Intelligence: Gathering and analyzing threat intelligence to protect against advanced threats.

Modules:

- Module 1: Enterprise Security Architecture
- Module 2: Enterprise Security Operations
- Module 3: Technical Integration of Enterprise Security
- Module 4: Research, Development, and Collaboration
- Module 5: Risk Management
- Module 6: Security Operations and Monitoring
- Module 7: Incident Response
- Module 8: Security Controls for Hosts
- Module 9: Network Security
- Module 10: Cloud and Virtualization Security
- Module 11: Identity and Access Management
- Module 12: Application Security

Labs included (30 hours):

- With Remote Connectivity
- Perform digital forensics
- Security and Risk Management Support Materials
- Configuring SCCM Configuration Items and Baselines
- Integrate Network and Security Components
- Install and Configure Network Load Balancing
- Perform Firewall Rule-based Management
- Implement SSL VPN using ASA Device Manager
- Configure Verify and Troubleshoot Port Security

- Scanning and Remediating Vulnerabilities with OpenVAS
- Configure and Verify IPv4 and IPv6 Access Lists for Traffic Filtering
- Analyze network traffic with Wireshark
- Configuring Endpoint Security
- Configuring Advanced Authentication and Authorization
- Encryption and Hashing
- Performing security assessment using various tools
- Using various tools for security assessments
- Perform Security Assessment Using MBSA
- Compliance Patching
- Mapping Networks
- Install and Configure ManageEngine OpManager
- Implementing DNSSEC
- Implementing AD Federation Services
- Performing Offline Attacks
- Configure Verify and Troubleshoot GRE Tunnel Connectivity
- Implement OpenPGP
- PKI Concepts
- Perform Banner Grabbing
- Using Password Cracking Tools
- Upgrading and Securing SSH Connection
- Configure Two Factor Authentication
- Using Encryption and Steganography

CompTIA CertMaster Learn and Labs Descriptions:

CompTIA CASP+ (CAS-004) CertMaster Learn and Labs: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams, and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

CertMaster Learn Features:

- Lessons cover all exam objectives with integrated videos
- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario
- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Performing Risk Management Activities
- Summarizing Governance & Compliance Strategies
- Implementing Business Continuity & Disaster Recovery
- Identifying Infrastructure Services
- Performing Software Integration
- Explain Virtualization, Cloud, and Emerging Technology
- Exploring Secure Configurations and System Hardening
- Understanding Security Considerations of Cloud and Specialized Platforms
- Implementing Cryptography
- Implementing Public Key Infrastructure (PKI)
- Understanding Threat and Vulnerability Management
- Developing Incident Response Capabilities

Labs Available:

- Assisted Lab: Exploring the Lab Environment
- Assisted Lab: Using Automation to Identify Sensitive Data
- Assisted Lab: Understanding DR Capabilities in the Cloud
- Assisted Lab: Implementing a Web Application Firewall
- Assisted Lab: Understanding the Role of SPF Records and DNSSEC

- Assisted Lab: Using Security Incident and Event Management Features
- Assisted Lab: Performing Static Code Analysis
- Assisted Lab: Exploiting Web Applications – Stored XSS, SQL Injection
- APPLIED LAB: Analyzing Web Application Vulnerabilities
- Assisted Lab: Implementing a VNet in Azure
- Assisted Lab: Deploying a Virtual Private Cloud in Amazon Web Services
- Assisted Lab: Implementing and Updating Containers on Windows Server 2019
- APPLIED LAB: Performing Container Update Tasks
- Assisted Lab: Understanding DNS over HTTPS (DoH)
- Assisted Lab: Deploying a Hardened Server Image in the Cloud
- Assisted Lab: Implementing an Application Blocklist Policy
- Assisted Lab: Configuring Monitoring in the Cloud
- Assisted Lab: Implementing Data Protection using Symmetric Encryption
- Assisted Lab: Exploring Cryptography and Cryptanalysis using Visual Tools
- Assisted Lab: Implementing HTTP Server Certificates
- APPLIED LAB: Troubleshooting HTTP Server Certificates
- Assisted Lab: Exploring MITRE ATT&CK Navigator
- Assisted Lab: Exploring and Interpreting Intrusion Detection System Alerts
- APPLIED LAB: Analyzing Intrusion Detection System Logs
- Assisted Lab: Exploiting the Server Message Block Protocol
- Assisted Lab: Analyzing SMB Vulnerabilities
- Assisted Lab: Analyzing Firmware using Binary Analysis and Hardware Emulation
- Assisted Lab: Analyzing and Attack Wireless Network Protections

Product Information:

- One license provides access to CertMaster Learn for CASP+ (CAS-004) with CertMaster Labs integrated throughout the course.
- Access keys must be redeemed within 12 months of purchase.

- Once redeemed, Learn for CASP+ (CAS-004) with CertMaster Labs integrated will be valid for 12 months.

Exam Voucher and Exam Pass Guarantee (CASP+): This bundle includes an exam voucher and an exam pass guarantee for CASP+: if you don't pass the exam on the first try, we will provide another 12 months of access to our custom online self-paced ILT along with additional exam vouchers. To qualify for the exam pass guarantee, you must show proof of completing all training materials, including course content, labs, and practice prep questions, before taking your exam.

CCNA Bundle (Cisco CCNA 200-301)

ITI SKU: Cisco-2
MSRP: $1199
Sales Price: $999
Bundle Access Period: 12 months from purchase.

High-level description: The Cisco CCNA 200-301 certification is a globally recognized credential that validates the fundamental skills necessary to perform essential networking functions. Our Cisco CCNA 200-301 Bundle combines custom self-paced online instructor-led training (ILT) courses with engaging video lessons, text lessons, section quizzes, performance-based lab simulations, and comprehensive exam practice. This approach ensures a thorough understanding by offering theoretical knowledge and practical skills, leading to better retention and mastery of networking concepts.

Recommended Study Sequence: We recommend you start with ITI's Custom Online Self-Paced ILT followed by the CertMaster Network+ with integrated labs and then the TestOut CCNA integrated training and hands-on labs, then the CCNP courses.

CTI Custom Online Self-Paced CCNA ILT with Labs Description: Master networking with our Cisco CCNA 200-301 Online Self-Paced ILT Course, designed for aspiring network specialists, administrators, and IT professionals. This course offers 45+ hours of content delivered over 150 short, easily digestible videos, covering 28 topics and providing more than 295 prep practice questions. Once purchased, you have 12 months' access to the course.

Topics Areas Included:

- Network Fundamentals
- Network Access
- IP Connectivity
- IP Services

- Security Fundamentals

Modules Included:

Module 1: Exploring the Functions of Networking

Module 2: Introducing the Host-To-Host Communications Model

Module 3: Introducing LANs

Module 4: Exploring the TCP/IP Link Layer

Module 5: Subnetting

Module 6: Explaining the TCP/IP Transport Layer and Application Layer

Module 7: Exploring the Functions of Routing

Module 8: Exploring the Packet Delivery Process

Module 9: Troubleshooting a Simple Network

Module 10: Introducing Basic IPv6

Module 11: Configuring Static Routing

Module 12: Implementing VLANs and Trunks

Module 13: Routing Between VLANs

Module 14: Introducing OSPF

Module 15: Building Redundant Switched Topologies

Module 16: Improving Redundant Switched Topologies with EtherChannel

Module 17: Exploring Layer 3 Redundancy

Module 18: Introducing WAN Technologies

Module 19: Explaining Basics of ACL

Module 20: Enabling Internet Connectivity

Module 21: Introducing QoS

Module 22: Introducing Architectures and Virtualization

Module 23: Introducing System Monitoring

Module 24: Managing Cisco Devices

Module 25: Examining the Security Threat Landscape

Module 26: Implementing Threat Defense Technologies

Module 27: Exam Preparation

Module 28: Practice Demos

Labs included (21 hours):

1. Networking Concepts - Part One
2. Networking Concepts - Part Two
3. IP Addressing and Virtualization Concepts
4. Switching Fundamentals - Part One
5. Switching Fundamentals - Part Two
6. Configuring VLANs - Part One
7. Configuring VLANs - Part Two
8. Static and Dynamic Routing Principles
9. Configure OSPFv2
10. FHRP Configuration and Verification
11. Static NAT Configuration
12. NTP Configuration
13. DHCP Concepts, Configuration and Verification
14. Network Traffic Management using SNMP
15. Configuring Syslog for Switching and Routing
16. Remote Management Techniques
17. Using File Transfer Protocols on Routers
18. Network Management Tools
19. Applying Security Protocols
20. QoS for Routing Configuration using PHB
21. Security Mitigation Techniques
22. Wireless Architecture and Application

TestOut CCNA Routing and Switching Pro Description: Unlock your potential with our comprehensive Routing and Switching Pro course. Designed for junior network administrators and seasoned professionals, this course includes:

- Self-paced instructor-led and demonstration video lessons
- Visual text lessons
- Quizzes
- Lab simulations
- Certification practice exams It prepares you for the modern demands in networking, IP services, security, automation, and programmability, and prepares you for the Cisco CCNA 200-301 certification exam.

Topics Covered (Integrated lessons and labs):

- Introduction to Routing and Switching Pro
- Networking Concepts
- Cisco Devices
- IP Addressing
- Switching
- IPv4 Routing
- IPv4 Routing Protocols
- IPv6 Routing
- Wireless Networks
- WAN Implementation
- Advanced Switching
- Access Control Lists
- Network Management
- Network Security
- Cryptography

License Information:

- One TestOut Routing & Switching Pro license valid for 12 months once activated. 12 months access to ITI course and labs.
- Access keys must be redeemed within 12 months of purchase.
- Instructions for accessing the course will be emailed after purchase.

ICS/SCADA Security Bundle

ITI SKU: EC-Council-27

MSRP: $2499

Sales Price: $2299

Bundle Access Period: 12 months from purchase.

Courses Included: EC-Council ICS/SCADA Cybersecurity and PECB SCADA Security Manager

High-level description: The bundled online self-paced courses on ICS/SCADA from EC-Council and PECB are designed to prepare IT professionals for securing industrial control systems and supervisory control and data acquisition systems against cyber

threats. The EC-Council's course provides hands-on training, where learners will understand the foundational security concepts and defense mechanisms by adopting a hacker's mindset to anticipate and thwart potential attacks. It covers the essentials of network defense, risk management, vulnerability management, and intrusion detection systems in the context of ICS/SCADA. Simultaneously, the PECB course, focused on becoming a SCADA Security Manager, teaches participants about implementing best practices for security and compliance in industrial environments. This program is structured around comprehensive risk assessment and mitigation strategies, emphasizing the importance of creating and maintaining a secure infrastructure that complies with international standards. Together, these courses offer a comprehensive overview of the necessary measures and methodologies for protecting critical infrastructure, making them ideal for professionals tasked with the management and security of industrial systems.

EC-Council ICS/SCADA Cybersecurity Description: This course is specially designed for IT professionals who are involved in managing or directing their organization's IT infrastructure and who are responsible for establishing and maintaining information security policies, practices and procedures. The focus in the course is on the Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Systems.

Course Outline (3 days)

- Module 1: Introduction to ICS/SCADA Network Defense
    - IT Security Model
    - ICS/SCADA Security Model
- Module 2: TCP/IP 101
    - Introduction and Overview
    - Introducing TCP/IP Networks
    - Internet RFCs and STDs
    - TCP/IP Protocol Architecture
    - Protocol Layering Concepts
    - TCP/IP Layering
    - Components of TCP/IP Networks
    - ICS/SCADA Protocols
- Module 3: Introduction to Hacking
    - Review of the Hacking Process

  - Hacking Methodology
  - Intelligence Gathering
  - Footprinting
  - Scanning
  - Enumeration
  - Identify Vulnerabilities
  - Exploitation
  - Covering Tracks
- Module 4: Vulnerability Management
  - Challenges of Vulnerability Assessment
  - System Vulnerabilities
  - Desktop Vulnerabilities
  - ICS/SCADA Vulnerabilities
  - Interpreting Advisory Notices
  - CVE
  - ICS/SCADA Vulnerability Sites
  - Life Cycle of a Vulnerability and Exploit
  - Challenges of Zero-Day Vulnerability
  - Exploitation of a Vulnerability
  - Vulnerability Scanners
  - ICS/SCADA Vulnerability Uniqueness
  - Challenges of Vulnerability Management Within ICS/SCADA
- Module 5: Standards and Regulations for Cybersecurity
  - ISO 27001
  - ICS/SCADA
  - NERC CIP
  - CFATS

  - ISA99
  - IEC 62443
  - NIST SP 800-82
- Module 6: Securing the ICS network
  - Physical Security
  - Establishing Policy – ISO Roadmap
  - Securing the Protocols Unique to the ICS
  - Performing a Vulnerability Assessment
  - Selecting and Applying Controls to Mitigate Risk
  - Monitoring
  - Mitigating the Risk of Legacy Machines
- Module 7: Bridging the Air Gap
  - Do You Really Want to Do This?
  - Advantages and Disadvantages
  - Guard
  - Data Diode
  - Next Generation Firewalls
- Module 8: Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention
  - Systems (IPS)
  - What IDS Can and Cannot Do
  - Types IDS
  - Network
  - Host
  - Network Node
  - Advantages of IDS
  - Limitations of IDS
  - Stealthing the IDS

- Detecting Intrusions

EC-Council Brochure: https://www.eccouncil.org/wp-content/uploads/2024/03/ICS-SCADA-Brochure-1.pdf

PECB SCADA Security Manager Description: SCADA Security Manager training enables you to develop the necessary expertise to plan, design, and implement an effective program to protect SCADA systems. In addition, you will be able to understand common Industrial Control System (ICS) threats, vulnerabilities, risks related to the Industrial Control Systems (ICS) and techniques used to manage these risks. This training focuses on several aspects of security management and skills related to SCADA/ICS security.

Course Outline:

- Day 1 Introduction to SCADA and ICS
  - Course objectives and structure
  - Fundamental principles and concepts of SCADA and SCADA Security
  - Industrial Control Systems (ICS) characteristics, threats and vulnerabilities
- Day 2 Designing a Security Program and Network Security Architecture
  - SCADA Security program
  - Risk assessment
  - Network security architecture for SCADA systems
- Day 3 Implementing ICS Security Controls, Incident Management and Business Continuity
  - Implementation of security controls for SCADA systems
  - Incident management
  - Linkage to business continuity
  - Monitoring, measurement analysis and evaluation
- Day 4 Security testing of SCADA systems
  - Testing principles
  - Legal and ethical issues
  - Penetration testing approaches
  - Security testing of ICS

  - Management of a penetration test
  - Documentation of the test, quality review and report
  - Maintaining a testing program
  - Competence and evaluation of SCADA Security Managers
  - Closing the training
- Day 5 Certification Exam

PECB Brochure: https://pecb.com/pdf/brochures/4/iso-lead-scada-security-manager_4p.pdf

Exam Information:
The EC-Council course includes an exam voucher and retake for the EC-Council exam. The exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers. The PECB course comes with the exam, and instructions on taking the exam will be provided to the student after purchase.

License Information:
One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access:
Instructions for accessing the course will be emailed after purchase.

CTI CISSP and CISM bundle

ITI SKU: CISSP-CISM-1
MSRP: Not for individual sale
Sales Price: Not for individual sale
Bundle Access Period: 12 months from purchase.

High-level description: This bundled online self-paced courses provide an integrated learning path for professionals aiming to enhance both technical and managerial cybersecurity skills. This bundle combines the advanced security architecture and risk management expertise of the **CISSP** with the strategic oversight and governance focus of the **CISM**. Through a blend of in-depth video instruction and hands-on labs, participants will gain practical skills in securing complex information systems, managing security frameworks, and responding to incidents. Designed for those seeking leadership roles in information security, this bundle offers a comprehensive approach to mastering the critical domains of cybersecurity.

CTI CISSP Description: The Certified Information Systems Security Professional (CISSP) course is designed to provide comprehensive training in the field of

cybersecurity. This course covers key concepts such as Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security. Each module delves deep into the principles and practices necessary for securing and managing information systems effectively. This course includes 19+ hours of ILT broken up into over 45 videos and 8 topics and provides over 250 exam preparation questions, as well as 25 hours of labs.

Topics Covered (19+ hours):

- Module 1: Security and Risk Management
- Module 2: Asset Security
- Module 3: Security Architecture and Engineering
- Module 4: Communication and Network Security
- Module 5: Identity and Access Management (IAM)
- Module 6: Security Assessment and Testing
- Module 7: Security Operations
- Module 8: Software Development Security

Labs Included (25 hours):

- Introduction to CISSP
- Security and Risk Management
- Encryption and Hashing
- SCCM Configuration Items and Baselines
- Implement OpenPGP
- Two factor Authentication with SSH
- Implement SSL VPN using ASA Device Manager
- Configure and Verify IPv4 and IPv6 Access Lists for Traffic Filtering
- Configuring IPtables
- Windows Command Line Tools
- Administering and Deploying Endpoint Protection
- Bitlocker on Portable Media
- Managing Remote Desktop
- Manage Role-based Security
- Configuring MBSA Scanner
- Compliance Patching
- Passive Topology Discovery
- Scanning and Remediating Vulnerabilities with OpenVAS
- Installing Kali
- Implement Backup and Recovery
- Installation and Verification of Snort

- Configuring and Securing IIS
- Upgrading and Securing SSH Connection
- DVWA - Manual SQL Injection and Password Cracking

CTI CISM Course Description: This intensive training course is tailored for professionals looking to excel in information security management. It covers essential topics such as information security governance, risk management, program development, and incident management, equipping participants with the skills to develop and enforce robust security frameworks and best practices within their organizations. Participants will engage in practical applications and in-depth studies of security architecture, risk assessment, and incident response, all aimed at preparing them for the CISM certification exam and advancing their careers in information security management. This course includes over 17 hours of ILT covered over 45+ videos and 6 topic areas and provides 100 exam preparation questions.

Course Outline (17 hours):

- Module 1: Introduction
  - Instructor Introduction
  - Course Introduction
  - Exam Overview
- Module 2: Information Security Governance
  - Module Overview
  - InfoSec Strategic Context Part 1
  - InfoSec Strategic Context Part 2
  - GRC Strategy and Assurance
  - Roles and Responsibilities
  - GMA Tasks Knowledge and Metrics
  - IS Strategy Overview
  - Strategy Implemenation
  - Strategy Development Support
  - Architecture and Controls
  - Considerations and Action Plan
  - InfoSec Prog Objectives and Wrap-Up
- Module 3: Information Security Risk Management
  - Module Overview
  - Risk Identification Task and Knowledge
  - Risk Management Strategy
  - Additional Considerations
  - Risk Analysis and Treatment Tasks & Knowledge
  - Leveraging Frameworks
  - Assessment Tools and Analysis
  - Risk Scenario Development
  - Additional Risk Factors

    - Asset Classification and Risk Management
    - Risk Monitoring and Communication
    - Information Risk Management Summary
- Module 4: InfoSec Prog Development and Management
    - Module Overview
    - Alignment and Resource Management - Task and Knowledge
    - Key Relationships
    - Standards Awareness and Training - Tasks and Knowledge
    - Awareness and Training
    - Building Security into Process and Practices - Tasks and Knowledge
    - Additional Technology Infrastructure Concerns
    - Security monitoring and reporting Overview Tasks and Knowledge
    - Metrics and Monitoring
    - Summary
- Module 5: Information Security Incident Management
    - Module Overview
    - Planning and Integration Overview Task and Knowledge
    - Incident Response Concepts and Process
    - Forensics and Recovery
    - Readiness and Assessment - Overview Tasks and Knowledge
    - Identification and Response Overview Tasks and Knowledge
    - Incident Processes
- Module 6: Exam Prep
    - Case Study - Security On a Shoestring Budget
    - Case Study - APT In Action
    - Summary
- Exam Prep

Exam Information:
This bundle does not come with exam vouchers.

License Information:
One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access:
Instructions for accessing the course will be emailed after purchase.

CTI Certified Information Systems Auditor (CISA)

ITI SKU: CISA-1
MSRP: Not for individual sale
Sales Price: Not for individual sale
Bundle Access Period: 12 months from purchase.

This Certified Information Systems Auditor (CISA) course offers professionals a deep dive into the practices and standards for auditing and securing IT environments. Covering topics like Audit Processes, Governance and Compliance, System Infrastructure, and Business Continuity, participants will develop the skills to manage and assess risk in IT systems and ensure adherence to regulatory frameworks. With 12+ hours of instructor-led content and hands-on labs, this course thoroughly prepares learners for the CISA certification exam.

Course Outline (12+ Hours):

- **Module 1**: The Audit Process
    - Introduction, Auditing Standards, Cobit Model, Audit Management, CSA Control Self-Assessment.
- **Module 2**: Audit Governance and Compliance
    - IT Governance, Outsourcing & Governance, Organizational Compliance, IT Performance.
- **Module 3**: System Infrastructure, Project Management, and Testing
    - Project Management Tools, Testing Process, Agile Development, Data Conversion.
- **Module 4**: Media Disposal, Reviews, and System Maintenance
    - Media Disposal, Post Implementation Reviews, System Maintenance.
- **Module 5**: IT Service Level Management
    - Operations Management, SQL, Incident Management, Patch Management, Monitoring Performance.
- **Module 6**: Auditor Technical Overview
    - Security Design, Cryptography, VPNs, Firewalls, Network Security Devices, OSI Networking.
- **Module 7**: Business Continuity and Disaster Recovery
    - Fault Tolerance, Disaster Recovery Regulations.

Exam Information:

This bundle does not include exam vouchers.

License Information:

Access to each course is valid for 12 months.

How to Access:

Instructions will be emailed after purchase.

HDI Support Center Manager (HDI-SCM)

ITI SKU: HDI-1

MSRP: Not for individual sale

Sales Price: Not for individual sale

Bundle Access Period: 12 months from purchase.

ITI Partner Delivered HDI-SCM online self-paced course description: The HDI Support Center Manager course equips participants with the knowledge and leadership skills to manage support centers effectively. It covers topics such as IT service management, strategic planning, financial management, performance optimization, and workforce development. The course includes 11 modules focusing on service level agreements, cost management, service technology, and leadership. Designed for professionals looking to excel in support center leadership, this course prepares participants for the HDI Support Center Manager certification exam. This is a live online course so contact us to schedule it.

Course Outline (3 days):

- **Module 1: Support Center Overview**
    - Explore the core functions, strategies, and challenges of managing a modern support center, including role responsibilities and key metrics for success.
- **Module 2: Leadership and Management**
    - Focus on developing strong leadership abilities, including team motivation, decision-making, and setting strategic goals for support teams.
- **Module 3: Strategic Planning**
    - Learn to create long-term plans for service excellence, aligned with business objectives, while managing resources and performance.
- **Module 4: Technology and Support Delivery**
    - Examine the role of technology in support centers, including service delivery tools, automation, and enhancing customer experience with IT solutions.

- **Module 5: Service Level Management**
    - Understand how to define, measure, and enforce Service Level Agreements (SLAs), along with strategies to improve service quality and meet targets.
- **Module 6: Financial Management**
    - Gain insights into budgeting, cost control, and financial planning in support center operations to ensure optimal resource use and cost-efficiency.
- **Module 7: Metrics and Reporting**
    - Focus on key performance indicators (KPIs) and how to gather, analyze, and report data to measure success and identify areas for improvement.
- **Module 8: Quality Assurance**
    - Learn methods for maintaining high service standards, including quality monitoring, customer feedback mechanisms, and process improvements.
- **Module 9: Workforce Management**
    - Explore techniques for workforce planning, staff scheduling, and managing the balance between demand and capacity in the support center.
- **Module 10: Team Development and Coaching**
    - Build skills in coaching, mentoring, and training to foster continuous improvement and professional growth within your team.
- **Module 11: Customer Satisfaction and Loyalty**
    - Learn strategies for enhancing customer relationships, building loyalty, and using feedback to drive service improvements and long-term success.

Exam Information:

- This course comes with the exam. The HDI Support Center Manager certification exam consists of 65 multiple-choice questions, requiring a passing score of 80%. The exam must be completed within six weeks of finishing the course.

License Information:

- Includes 12 months of access to the course content.

How to Access:

- Instructions will be provided via email following purchase.

HDI Support Center Lead (HDI-SCL)

ITI SKU: HDI-2
MSRP: Not for individual sale
Sales Price: Not for individual sale
Bundle Access Period: 12 months from purchase.

ITI Partner Delivered HDI-SCL online self-paced course description: HDI Support Center Team Lead training ensures that participants learn how to deliver exceptional customer support, promote process improvement, coach for success, and take charge of the day-to-day operational activities of a team. This course is designed for support professionals who need to develop fundamental management and leadership skills. Online, self-paced training allows student to train at their own speed, permitting them to concentrate on areas of specific need. Students can train from any computer with Internet access, and the course takes about 10-12 hours to complete.

Course Outline:

- **Unit 1: Support Center Overview**
  - Evolution of Service & Support
  - Successful Service & Support
- **Unit 2: Role of the Support Center Team Lead**
  - Role of the Team Lead
  - Effective Leadership
  - Emotional Intelligence
  - Managing Relationships
- **Unit 3: Business Planning and Strategy**
  - Strategic Perspective
  - Building a Strategy
  - Service Level Management
  - SOPs
  - Alignment
- **Unit 4: Support Center Processes**
  - Best Practices for Support
  - Service Operations
  - Additional Processes
  - Knowledge Management
- **Unit 5: Service Delivery Methods & Technology**
  - Systems Thinking Approach
  - Support Tools & Tech
  - Service Delivery Methods
  - Social Media
- **Unit 6: Workforce Management and Training**

    - Workforce Management
    - Sourcing and Recruitment
    - Training
- **Unit 7: Communication and Coaching**
    - Communication Skills
    - Cross-Cultural Communication
    - Managing Conflict
    - Coaching
- **Unit 8: Teamwork**
    - Motivation, Rewards, Recognition
    - Performance Management
    - Retention
- **Unit 9: Metrics and Quality Assurance**
    - Metrics
    - Quality Assurance
    - Using Surveys
    - Performance Reporting
    - Promoting the Support Center

Product Information:

- Once registered for an online course, you have 12 weeks to access the course. A 28-day extension is available for an online course for a fee of $50. Exam retakes are available for a $99 fee

HDI Support Center Analyst (HDI-SCA)

ITI SKU: HDI-3

MSRP: Not for individual sale

Sales Price: Not for individual sale

Bundle Access Period: 12 months from purchase.

ITI Partner Delivered HDI-SCA online self-paced course description: HDI Support Center Analyst (HDISCA) 2-day training course focuses on support center strategies for effective customer service, emphasizing problem-solving and trouble-shooting skills, contact handling procedures, incident management, critical thinking, communication skills, and an introduction to service management process. Given the critical role that Insider Threat analysts play in incident detection, analysis, and response services, this course offers a robust foundation for anyone working on a team that provides these services. Whether you're detecting or managing incidents or offering other support, the skills learned in this course will be invaluable across various service delivery scenarios.

What You Will Learn

- The process of incident management, from detection and recording to closure.
- Critical thinking skills to resolve incidents quickly and consistently.
- The value of service management processes and the role they play in providing quality support.
- An awareness of the core help desk processes and best practices.
- Valuable active listening skills and effective communication strategies.
- Proven techniques for improving customer interactions.
- Effective support center strategies for managing difficult customers.

Course Outline

Unit 1: Role of the Support Center Analyst

- Support Industry Evolution
- The Role of the Analyst
- The Value of the Analyst
- The Future of Service and Support

Unit 2: Structural Framework of Service and Support

- Understanding the Business
- Structural Components Overview
- Strategy
- Services
- Service Level Management
- Standard Operating Procedures
- Business Alignment

Unit 3: Service Management Processes

- Best Practices for Service and Support
- Incident Management
- Request Fulfillment
- Access Management
- Security Management
- Knowledge Management

Unit 4: Tools, Technology, and Service Delivery

- Systems Thinking Approach

- ITIL Support Tools and Technology
- Support Delivery Methods
- Social Media

Unit 5: Understanding Metrics

- Systems Thinking - Applied to Metrics
- Metrics
- Dashboards
- Quality Assurance

Unit 6: Communication Essentials

- Communication Essentials
- Active Listening
- Voice Components
- Effective Word Choices
- Written Communication
- Effective Cross-Cultural Communication

Unit 7: Troubleshooting & Incident Management

- Troubleshooting and Problem-Solving
- The Incident Management Process

Unit 8: Customer Management Skills

- Challenging Customer Behaviors
- Emotional Intelligence
- Expressing Empathy
- Managing Customer Behaviors

Unit 9: Personal & Professional Development

- SWOT Assessment
- Personal Development Skills Overview
- Time Management
- Stress Management
- Managing Your Career

Product Information:

- For the HDI-SCA: Once registered for an online course, you have 12 weeks to access the course. A 28-day extension is available for an online course for a fee of $50. Exam retakes are available for a $99 fee. Details for accessing the course and taking the exam will be emailed upon purchase.

EC-Council CCISO (Online Self-Paced)

ITI SKU: EC-Council-11
MSRP: $2,499
Sales Price: $2,499
Bundle Access Period: 12 months from purchase.

EC-Council CCISO Description: The CCISO course is designed for current and aspiring information security executives. This program includes 40 hours of content, combining theoretical knowledge with practical skills required to establish and maintain an information security program.

EC-Council CCISO Description: The CCISO course is designed for current and aspiring information security executives. This program includes 40 hours of content, combining theoretical knowledge with practical skills required to establish and maintain an information security program.

Topics Covered:

Domain 1: Governance and Risk Management

1. Define, Implement, Manage, and Maintain an Information Security Governance Program

1.1. Form of Business Organization

1.2. Industry

1.3. Organizational Maturity

2. Information Security Drivers

3. Establishing an information security management structure

3.1. Organizational Structure

3.2. Where does the CISO fit within the organizational structure

3.3. The Executive CISO

3.4. Nonexecutive CISO

4. Laws/Regulations/Standards as drivers of Organizational Policy/Standards/Procedures

5. Managing an enterprise information security compliance program

5.1. Security Policy

5.1.1. Necessity of a Security Policy

5.1.2. Security Policy Challenges

5.2. Policy Content

5.2.1. Types of Policies

5.2.2. Policy Implementation

5.3. Reporting Structure

5.4. Standards and best practices

5.5. Leadership and Ethics

5.6. EC-Council Code of Ethics

6. Introduction to Risk Management

3.1. Organizational Structure

3.2. Where does the CISO fit within the organizational structure

3.3. The Executive CISO

3.4. Nonexecutive CISO

Exam Information: The course comes with CCISO exam (does not come with a retake) and can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course and taking the exams will be emailed after purchase.

Link to EC-Council Brochure: https://www.eccouncil.org/wp-content/uploads/2023/07/CCISO-brochure-V.11-1.pdf

CTI Kubernetes Training Series Bundle

ITI SKU: MISC-1

MSRP: Not for individual sale, include in bundles

Sales Price: Not for individual sale, include in bundles

Bundle Access Period: 12 months from purchase.

Courses in bundle: Certified Kubernetes Administrator (CKA), Certified Kubernetes Application Developer (CKAD, Kubernetes – Containerizing Applications in the Cloud

EC-Council CCISO Description: The Kubernetes Training Series offered through CTI provides a comprehensive, hands-on approach to mastering Kubernetes, an essential platform for container orchestration. This series covers key concepts over 25 topics and 12+ hours, from deploying and managing containerized applications to advanced Kubernetes administration and development. It includes courses on Kubernetes fundamentals, Certified Kubernetes Administrator (CKA), and Certified Kubernetes Application Developer (CKAD). Participants will gain expertise in setting up Kubernetes clusters, managing pods and services, containerizing applications, and ensuring high availability in cloud environments, making this an essential training for DevOps professionals, cloud architects, and IT developers.

Topics Covered:

Certified Kubernetes Administrator (CKA) Course Content

- Module 1: Course Overview
- Module 2: Kubernetes and Container Fundamentals
- Module 3: Kubernetes Installation
- Module 4: Working with Kubernetes Clusters and Nodes
- Module 5: API Access and Commands
- Module 6: Running Pods and Deployments
- Module 7: Configuring Storage
- Module 8: Kubernetes Networking
- Module 9: Managing Security
- Module 10: Managing Kubernetes In the Enterprise
- Module 11: Kubernetes Monitoring and Troubleshooting
- Module 12: CKA Practice Exams
- Module 13: Course Closeout

Certified Kubernetes Application Developer (CKAD) Course Content

- Module 1: Course Overview
- Module 2: Kubernetes and Container Fundamentals
- Module 3: Configuration
- Module 4: Multi Container Pods
- Module 5: Observability
- Module 6: Pod Design
- Module 7: Services and Networking
- Module 8: State Persistence

- Module 9: CKA Practice Exams
- Module 10: Course Closeout

Kubernetes - Containerizing Applications in the Cloud Course Content

- Module 1: Course Overview
- Module 2: Basics of Kubernetes
- Module 3: Kubernetes Design and Architecture
- Module 4: Deployments
- Module 5: Course Closeout

Exam Information: To register for a Kubernetes certification exam like the CKA or CKAD, visit the Linux Foundation's Certification Portal, purchase the exam, and schedule it through their platform. The exam is taken online, and you'll receive instructions after registration.

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course and taking the exams will be emailed after purchase.

CTI Introduction to Agile, Scrum and DevOps

ITI SKU: MISC-2

Courses in bundle: Introduction to Agile and Scrum, and DevOps Fundamentals
MSRP: Not for individual sale, include in bundles
Sales Price: Not for individual sale, include in bundles
Bundle Access Period: 12 months from purchase.

High level Description: This Agile and DevOps Fundamentals course offers a comprehensive introduction to two critical methodologies in modern software development. Learners will explore Agile principles, focusing on Scrum for managing iterative and adaptive projects, fostering collaboration, and increasing team productivity. Simultaneously, they will dive into DevOps, learning how to automate processes, implement continuous integration/continuous delivery (CI/CD), and streamline collaboration between development and operations teams. Together, Agile and DevOps provide a framework to improve development cycles, enhance software quality, and enable faster, more reliable deployments. This course is ideal for professionals seeking to enhance project management skills while adopting efficient software delivery practices.

Agile and Scrum Course Description: The Introduction to Agile and Scrum course provides a comprehensive overview of Agile methodologies, with a focus on the Scrum framework, which is widely used for managing software development projects. This

course, delivered over 7 topics and 3+ hours, is designed for professionals seeking to understand the core principles of Agile, how Scrum supports iterative progress, and the roles and ceremonies essential for effective project management. By the end of this course, learners will be able to apply Agile best practices to enhance team collaboration, improve project outcomes, and adapt to evolving requirements efficiently.

Course Outline:

- Module 1 : Agile Principles and Mindset
  - Agile Introduction Scrum
  - Agile Core Principles Scrum
  - Lean Product Development Scrum
  - Agile Leadership Tasks Scrum
  - Agile Communications Scrum
- Module 2 : Value Driven Delivery
  - Value Driven Delivery Scrum
  - Value Driven Delivery Scrum Part2
- Module 3 : Stakeholder Engagement
  - Stakeholder Engagement Scrum
  - Facilitation Tools Scrum
- Module 4 : Team Performance
  - Team Performance Scrum
  - Digital Tools for Distibuted Teams Scrum
- Module 5 : Adaptive Planning
  - Adaptive Planning Scrum
  - Adaptive Planning Scrum Part2
- Module 6 : Problem Detection and Resolution
  - Problem Detection and Resolution Scrum
- Module 7 : Continuous Improvement
  - Continuous Improvement Scrum

Develops Fundamentals Course Description: The DevOps Fundamentals course is designed to provide learners with a solid foundation in DevOps practices, focusing on the principles that drive modern software development and deployment. This course, delivered over 3 hours and 6 topics, covers key concepts such as continuous integration/continuous delivery (CI/CD), automation, and collaboration between development and operations teams. It highlights how DevOps reduces development cycles, increases deployment frequency, and delivers high-quality software efficiently.

Course Outline:

- Module 1: Course Overview
  - Course Overview

    - Course Pre Reqs
- Module 2: The Basics
    - The Basics
    - What is DevOps
    - DevOps Building Blocks
    - DevOps Best Practices
    - Why Containers
    - What is a Pipeline
    - Continuous Integration and Continous Delivery
    - Continuous Deployment
    - Pipelines - Whiteboard
- Module 3: Development
    - Development Basics
    - CICD Strategy
    - Source Control Management
    - Demo - Build Management
- Module 4: Infrastructure
    - Release and Deployments
    - Release Management
    - Demo - Release Management
    - Reliability Engineering
    - DevOps Tools
    - Infrastructure as Code
    - Automation
    - Demo - (IaaC) CloudFormation
    - Demo - Jenkins
    - Demo - GitHub

- Module 5: Key Performance Indicators (KPIs)
    - Key Performance Indicators (KPI)
    - KPI Metrics
    - KPI Tools
    - Monitoring Applications
    - Demo - AWS CloudWatch
- Module 6: Course Closeout
    - Module 6 Introduction
    - Course Closeout
    - Course Review
    - Summary Review
    - Additional Resources
    - Blockchain Roles
    - DevOps Job Outlook
    - Course Closeout

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

CTI Introduction to Python Programming with Labs Bundle

ITI SKU: MISC-3

MSRP: Not for individual sale, include in bundles

Sales Price: Not for individual sale, include in bundles

Bundle Access Period: 12 months from purchase.

Courses in bundle: CTI Python Programming and Introduction to Python Labs

High level Description: This **Python Programming Course** offers a comprehensive introduction to Python, one of the most widely-used programming languages today. This course, with over 9 hours of instruction and 6 hours of labs, covers the fundamentals of Python, making it accessible to beginners while also providing valuable insights for those with prior programming experience. Students will learn about Python's syntax, data types, control structures, functions, and modules, as well as how

to work with libraries and frameworks for more advanced programming. The course is ideal for aspiring developers and IT professionals who want to learn Python for web development, data analysis, automation, and more. Through practical exercises and real-world applications, learners will gain hands-on experience in writing Python code, enabling them to build their own projects and improve problem-solving skills in a development environment. This course is designed to be accessible for all learners and helps build a strong foundation in Python programming.

Course Outline:

- Module 1: Getting Started with Python
- Module 2: Working with Primitive Data Types
- Module 3: Working with Multiple Assignments Statements
- Module 4: Convert Types in Python
- Module 5: Creating Lists
- Module 6: Modifying Lists
- Module 7: Sorting and Reversing Lists
- Module 8: Slicing Lists
- Module 9: Working With Operators
- Module 10: Determining Operator Precedence
- Module 11: Working with IF Statements
- Module 12: Working With For Loops
- Module 13: Working With While Loops
- Module 14: Nesting for Loops
- Module 15: Reading Files
- Module 16: More on Files
- Module 17: Merging Emails
- Module 18: Reading Console Inputs and Formatting Outputs
- Module 19: Reading Command Line Argument
- Module 20: Defining Functions
- Module 21: Using Default Argument
- Module 22: Using Keyword and Positional Arguments
- Module 23: Handling Exceptions
- Module 24: Using Math and Random Modules
- Module 25: Displaying Daytime Working Directory and File Metadata

Included Labs:

- Working with Primitive Data Types
- Working with Multiple Assignment Statements
- Converting Types in Python
- Creating Lists

- Modifying Lists
- Sorting and Reversing Lists
- Slicing Lists
- Working with Operators
- Determining Operator Precedence
- Working with If Statements
- Using Compound Conditional Expressions
- Working with For Loops
- Working with While Loops
- Nesting For Loops
- Reading Files
- Copying Files
- Merging Mails
- Reading Console Inputs and Formatting Outputs
- Reading Command Line Arguments
- Defining Functions
- Using Default Arguments
- Using Keyword and Positional Arguments
- Handling Exceptions
- Using Math and Random Modules
- Displaying Datetime, Working Directory and File Metadata

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

FedVTE (now CISA Learning) CISSP-ISSEP

ITI SKU: MISC-4

MSRP: Free through FedVTE (now CISA Learning)

Sales Price: Free through FedVTE (now CISA Learning)

Bundle Access Period: 12 months from purchase.

Courses in bundle: CISSP-ISSEP

Course Description: The CISSP-ISSEP (Information Systems Security Engineering Professional) course offered through FedVTE (now CISA Learning) is a self-paced study program designed to help professionals prepare for the ISSEP certification exam. This specialized certification focuses on integrating security engineering principles into business processes and systems. The course covers the five domain areas critical to the ISSEP exam, equipping learners with the knowledge and skills to incorporate

security measures into information systems, demonstrate subject matter expertise in security engineering, and apply these principles to enhance business functions.

Learning Objectives:

- Incorporate security practices into business processes and information systems.
- Demonstrate expertise in security engineering across various domains.
- Apply engineering principles to enhance security within business environments.

This course is ideal for security professionals aiming to enhance their expertise in system security engineering and to prepare for the CISSP-ISSEP certification.

Course Outline:

- ISSEP Course Introduction
- ISSE Responsibilities and Principles
- ISSE and IATF
- Security Design Principles
- Elements of Defense in Depth
- RMF Characteristics
- Maintaining Operational Resilience
- Risk Management Overview
- Assessing Risk Part 1 of 2
- Assessing Risk Part 2 of 2
- Determining Risks
- Categorizing Information Systems
- Stakeholder Roles and Responsibilities
- Requirements Analysis
- Using Common and Tailored Controls
- Assessing Security Controls
- Implementing Security Controls
- Authorizing Information Systems
- Systems Verification and Validation
- Monitor, Manage, and Decommissioning
- Defense Acquisition System Overview
- Acquisitions Process
- System Development Process Models
- Project Processes
- Project Management
- ISSEP Practice Exam

How to access: To sign up for FedVTE (now CISA Learning), you can:

1. Go to https://fedvte.usalearning.gov/register.php
2. Enter the email address you use for official government business
3. Click Submit

If you are a veteran or federal contractor, you can use your personal or professional email address.

CTI Certified Cloud Security Professional (CCSP)

ITI SKU: MISC-5

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

Courses in bundle: CTI CCSP

Course Description: The Certified Cloud Security Professional (CCSP) course offered through CTI is designed to equip IT professionals with the expertise required to secure cloud environments. This comprehensive course, providing over 15 hours of instruction, covers key cloud security concepts, including cloud architecture, governance, risk management, and compliance. Learners will gain in-depth knowledge of securing cloud data, managing identity and access, and ensuring compliance with regulatory frameworks. The course prepares individuals to pass the CCSP certification exam, validating their ability to protect cloud-based assets and maintain secure cloud infrastructure. Ideal for cloud architects, security engineers, and IT professionals, this course helps advance careers in cloud security.

Course Outline:

- Cloud Concepts, Architecture and Design
  - Course Intro
  - Cloud Concepts, Architecture and Design - Part 1
  - Cloud Concepts, Architecture and Design - Part 2
  - Cloud Concepts, Architecture and Design - Part 3
  - Cloud Concepts, Architecture and Design - Part 4
  - Cloud Concepts, Architecture and Design - Part 5
  - Cloud Concepts, Architecture and Design - Part 6
  - Cloud Concepts, Architecture and Design - Part 7
  - Cloud Concepts, Architecture and Design - Part 8
  - Cloud Concepts, Architecture and Design - Part 9
- Legal, Risk and Compliance
  - Legal, Risk and Compliance Part 1
  - Legal, Risk and Compliance Part 2

    - Legal, Risk and Compliance Part 3
    - Legal, Risk and Compliance Part 4
    - Legal, Risk and Compliance Part 5
    - Legal, Risk and Compliance Part 6
    - Legal, Risk and Compliance Part 7
- Cloud Data Security
    - Cloud Data Security - Part 1
    - Cloud Data Security - Part 2
    - Cloud Data Security - Part 3
    - Cloud Data Security - Part 4
    - Cloud Data Security - Part 5
    - Cloud Data Security - Part 6
    - Cloud Data Security - Part 7
- Cloud Platform and Infrastructure Security
    - Cloud Platform and Infrastructure Security - Part 1
    - Cloud Platform and Infrastructure Security - Part 2
    - Cloud Platform and Infrastructure Security - Part 3
    - Cloud Platform and Infrastructure Security - Part 4
    - Cloud Platform and Infrastructure Security - Part 5
    - Cloud Platform and Infrastructure Security - Part 6
    - Cloud Platform and Infrastructure Security - Part 7
    - Cloud Platform and Infrastructure Security - Part 8
- Cloud Application Security
    - Cloud Application Security - Part 1
    - Cloud Application Security - Part 2
    - Cloud Application Security - Part 3
    - Cloud Application Security - Part 4
    - Cloud Application Security - Part 5
    - Cloud Application Security - Part 6
    - Cloud Application Security - Part 7
    - Cloud Application Security - Part 8
    - Cloud Application Security - Part 9
- Cloud Security Operations
    - Cloud Security Operations - Part 1
    - Cloud Security Operations - Part 2
    - Cloud Security Operations - Part 3
    - Cloud Security Operations - Part 4
    - Cloud Security Operations - Part 5
    - Cloud Security Operations - Part 6
    - Cloud Security Operations - Part 7

- Cloud Security Operations - Part 8
- Cloud Security Operations - Part 9
- Cloud Security Operations - Part 10
- Cloud Security Operations - Part 11

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Exam Information: Register Through Pearson VUE.

FedVTE (now CISA Learning) Static Code Analysis and Supply Chain Assurance

ITI SKU: MISC-6

MSRP: Free through FedVTE (now CISA Learning)

Sales Price: Free through FedVTE (now CISA Learning)

Bundle Access Period: 12 months from purchase.

Courses in bundle: FedVTE (now CISA Learning) Static Code Analysis with HPE Fortify, Static Code Analysis with Synopsis Coverity, and Supply Chain Assurance using Sonatype Nexus

Course Description: This comprehensive course bundle offers IT professionals advanced skills in secure software development and supply chain management by combining Static Code Analysis using HPE Fortify and Synopsis Coverity with Supply Chain Assurance using Sonatype Nexus. Learners will gain expertise in identifying and mitigating vulnerabilities in source code through static analysis with Fortify and Coverity, while mastering the security of open-source components and third-party dependencies with Sonatype Nexus. Together, these tools provide a complete approach to automating vulnerability detection, securing software supply chains, and ensuring compliance throughout the software development lifecycle.

Static Code Analysis with HPE Fortify: This 2-hour course focuses on integrating static code analysis tools into the software development process from a developer's/cybersecurity professional's perspective. The course demonstrates how Fortify is used to identify and remove Common Weakness Enumeration (CWE) from applications in which the source code is available.

Learning Objectives:

- Understand how static code analysis tools work.
- Utilize integrated development environment (IDE) plugins in order to find CWE in source code during the development phase.

- Apply visualization tools available to developers and security professionals.
- Participate in accreditation reporting.

Course Outline

- AppSec with HPE Product Overview and Workflow
- HPE Fortify Static Code Analyzer Suite Overview
- HPE Static Code Analyzer Command Line Demo
- Audit Workbench Demo
- Fortify SCA Process Flow
- Audit Workbench Demo Continued
- STIG Reporting with Audit Workbench
- IDE Plugin
- Questions and Answers
- Fortify Priority
- Software Security Center

Static Code Analysis course utilizing Synopsis Coverity: This 1-and-a-half-hour course focuses on integrating static code analysis tools into the software development process. This course explains how developers can use tools such as Coverity to identify and remove Common Weakness Enumeration (CWE) from applications in which the source code is available, prior to deployment.

Learning Objectives:

- Understand how static code analysis tools work.
- The use of integrated development environment (IDE) plugins in order to find CWE in source code during the development phase.
- Visualization tools available to developers and security.

Course Outline:

- Overview of Synopsis Software Integrity Platform
- Demonstration
- Questions and Answers
- Closing.

Supply Chain Assurance using Sonatype Nexus: This 2-and-a-half-hour course focuses on integrating static code analysis tools into the software development process from both a developer's and a security professional's perspective. This course demonstrates how tools such as Sonatype can be used to evaluate the software supply chain in order to identify and remove

components with known Common Vulnerabilities and Exposures (CVE) from applications in which the source code is available.

Learning Objectives:

- Understand why software supply chain is important.
- Utilize integrated development environment (IDE) plugins in order to identify and avoid the use of libraries, applications, tools, etc. with known CVE used by an application.
- Apply tools to enforce organizational security policies and governance.

Course Outline:

Course Modules/Units

- Professionalizing Election Admin Intro
- Being an IT Manager
- Election Systems
- Technology and the Election Office
- Procuring IT
- Testing and Audits
- Election Security
- Principles of Information Security
- Physical Security
- Cybersecurity and Elections
- Human Security
- Risk Management and Elections
- Incident Response Scenarios and Exercises
- Phishing and Elections
- DDOS Attacks and Elections
- Website Defacing
- Election Infrastructure Security
- DHS Cyber Security Tools and Services
- EAC Resources

How to access: To sign up for FedVTE (now CISA Learning), you can:

4. Go to https://fedvte.usalearning.gov/register.php
5. Enter the email address you use for official government business
6. Click Submit

If you are a veteran or federal contractor, you can use your personal or professional email address.

CTI Custom CEH with Labs

ITI SKU: MISC-7

Courses in bundle: CEH
MSRP: Not for individual Sale, for bundles only
Sales Price: Not for individual Sale, for bundles only
Bundle Access Period: 12 months from purchase.

CTI Custom CEH Course Description: Our course offers CEH training to provide you the tools to research, discover and scan targets, analyze vulnerabilities and test attack methods and tools. The focus of this CEH online training course is to solve the challenge of breaking into a target network, collect evidence of success, and escape unnoticed.

Topics Covered:

- Introduction to the key concepts of ethical hacking and information security.
- Conducting footprinting and reconnaissance using advanced tools and techniques.
- Scanning networks and identifying vulnerabilities.
- Performing system hacking and exploiting operating systems.
- Understanding malware threats and implementing countermeasures.
- Utilizing social engineering techniques and tools.
- Executing Denial-of-Service (DoS) and session hijacking attacks.
- Evading IDS, firewalls, and honeypots.
- Hacking web servers and applications.
- Performing SQL injection and securing databases.
- Hacking wireless networks and mobile platforms.
- Exploring IoT and OT hacking methodologies.
- Securing cloud environments and implementing cryptographic techniques.

Labs included (15 hours):

- Footprinting and Reconnaissance Techniques
- Network Reconnaissance Techniques

- Enumeration Reconnaissance Techniques
- Vulnerability Analysis Tools & Techniques
- System Hacking Methodologies
- Malware Threat Concepts
- Network Sniffing Techniques
- Social Engineering Exploits
- Denial of Service Attacks
- Session Hijacking Concepts
- Compromising Web Servers
- Web Application Hacking
- SQL Injection Methodologies
- Introduction to Cloud Computing
- Cryptography Techniques

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Exam Information: This course does not come with the exam. Exam vouchers can be purchased directly from EC-Council and exams can be scheduled through EC-Council.

CTI Custom CHFI with Labs

ITI SKU: MISC-8

Courses in bundle: CHFI
MSRP: Not for individual Sale, for bundles only
Sales Price: Not for individual Sale, for bundles only
Bundle Access Period: 12 months from purchase.

CTI Custom CHFI Course Description: Our CHFI course will cover the security discipline of computer forensics from a vendor-neutral perspective and work towards preparing students to become Forensic Investigators in Computer Hacking.

Topics Covered (18+ hours):

- Comprehensive understanding of computer forensics and the forensic investigation process.
- Techniques for searching and seizing digital evidence.
- Methods for analyzing and handling digital evidence.
- First responder procedures for incident management.
- Setup and operation of a forensic lab.
- Gain in-depth knowledge of hard disks, file systems, and Windows forensics.

- Data acquisition and duplication techniques.
- Recovering deleted files and partitions.
- Utilizing Access Data FTK and EnCase for forensic investigations.
- Understanding and applying steganography and password cracking techniques.
- Log correlation, network forensics, and analyzing wireless and web attacks.
- Investigating email crimes and conducting mobile investigations.
- Preparing investigative reports and serving as an expert witness.

Labs included (12+ hours):

- Understanding the Digital Forensics Profession and Investigations
- Data Acquisition
- Processing Crime and Incident Scenes
- Working with Windows and CLI Systems
- Current Digital Forensics Tools
- Linux and Macintosh File Systems
- Recovering Graphics Files
- Digital Forensics Analysis and Validation
- Virtual Machine Forensics, Live Acquisitions, and Network Forensics
- E-mail and Social Media Investigations
- Mobile Device Forensics
- Cloud Forensics
- Report Writing for High-Tech Investigations
- Expert Testimony in Digital Investigations
- Ethics for the Expert Witness
- Techniques

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Exam Information: This course does not come with the exam. Exam vouchers can be purchased directly from EC-Council and exams can be scheduled through EC-Council.

Official EC-Council Certified Incident Handle (ECIH) with Labs

ITI SKU: MISC-9

MSRP: $1,399

Sales Price: $1,399

Bundle Access Period: 12 months from purchase.

Courses in bundle: EC-Council ECIH (Online Ondemand)

Official EC-Council ECIH Description: Prepare for effective incident handling with our ECIH course, which provides 24 hours of content focusing on incident management. This course covers the essentials of incident handling, from identifying security incidents to responding and recovering from them.

Topics Covered:

- Introduction to Incident Handling and Response
- Incident Handling and Response Process
- Forensic Readiness and First Response
- Incident Handling Tools and Techniques
- Incident Handling Policies and Laws
- Risk Assessment
- Handling Different Types of Incidents
- Incident Recovery Techniques

What you will learn:

- Key issues plaguing the information security world
- Various types of cyber security threats, attack vectors, threat actors, and their motives, goals, and objectives of cyber security attacks
- Various attack and defense frameworks (Cyber Kill Chain Methodology, MITRE ATT&CK Framework, etc.)
- Fundamentals of information security concepts (Vulnerability assessment, risk management, cyber threat intelligence, threat modeling, and threat hunting)
- Fundamentals of incident management (information security incidents, signs and costs of an incident, incident handling and response, and incident response automation and orchestration)
- Different incident handling and response best practices, standards, cyber security frameworks, laws, acts, and regulations
- Various steps involved in planning incident handling and response program (Planning, recording and assignment, triage, notification, containment, evidence gathering and forensic analysis, eradication, recovery, and post-incident activities)

- Importance of first response and first response procedure (Evidence collection, documentation, preservation, packaging, and transportation)
- How to handle and respond to different types of cyber security incidents in a systematic way (malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, insider threat-related incidents, and endpoint security incidents)

Exam Information: Each course includes an exam voucher. The EC-Council exams can be taken online through the EC-Council's remote proctoring service or at authorized testing centers and CompTIA exams can be taken online through Pearson OnVUE.

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Official EC-Council Certified Threat Intelligence Analyst (CTIA) with Labs

ITI SKU: MISC-10

Courses in bundle: EC-Council CTIA (Online OnDemand)

MSRP: $1,399

Sales Price: $1,399

Bundle Access Period: 12 months from purchase.

Official EC-Council CTIA Description: This course covers the fundamentals of threat intelligence, including its types, lifecycle, strategy, and frameworks. It explores various cybersecurity threats and attack frameworks such as APTs, Cyber Kill Chain, MITRE ATT&CK, and Diamond Model. Participants will learn the steps involved in planning a threat intelligence program, data collection methods, and processing techniques. The course also delves into threat data analysis, threat modeling, creating and sharing intelligence reports, threat hunting, and using Python scripting for automation and intelligence sharing in SOC operations and incident response.

Topics Covered:

- Introduction to Threat Intelligence
- Cyber Threats and Attack Frameworks
- Requirements, Planning, Direction, and Review
- Data Collection and Processing
- Data Analysis
- Intelligence Reporting and Dissemination

- Threat Hunting and Detection
- Threat Intelligence in SOC Operations, Incident Response, & Risk Management

What You'll Learn

- Fundamentals of threat intelligence (Threat intelligence types, lifecycle, strategy, capabilities, maturity model, frameworks, platforms, etc.)
- Various cyber security threats and attack frameworks (Advanced Persistent Threats, Cyber Kill Chain Methodology, MITRE ATT&CK Framework, Diamond Model of Intrusion Analysis, etc.)
- Various steps involved in planning a threat intelligence program (Requirements, Planning, Direction, and Review)
- Different types of threat intelligence feeds, sources, data collection methods
- Threat intelligence data collection and acquisition through Open-Source Intelligence (OSINT), Human Intelligence (HUMINT), Cyber Counterintelligence (CCI), Indicators of Compromise (IoCs), malware analysis, and Python scripting
- Threat intelligence data processing and exploitation
- Threat data analysis techniques (Statistical Data Analysis, Analysis of Competing Hypotheses (ACH), Structured Analysis of Competing Hypotheses (SACH), etc.)
- Complete threat analysis process, which includes threat modeling, fine-tuning, evaluation, and runbook and knowledge base creation
- How to create and share threat intelligence reports
- Threat intelligence sharing and collaboration using Python scripting
- Different platforms, acts, and regulations for sharing intelligence
- How to perform threat intelligence in a cloud environment
- Fundamentals of threat hunting (Threat hunting types, process, loop, methodology, etc.)
- Threat-hunting automation using Python scripting
- Threat intelligence in SOC operations, incident response, and risk management

Exam Information: The course includes an exam voucher. The CTIA exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the CTIA course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Official EC-Council Certified Chief Information Security Officer (CCISO)

ITI SKU: MISC-11

MSRP: $2,499

Sales Price: $2,499

Bundle Access Period: 12 months from purchase.

Courses in bundle: EC-Council CCISO (OnDemand)

EC-Council CCISO Description: The CCISO course is designed for current and aspiring information security executives. This program includes 40 hours of content, combining theoretical knowledge with practical skills required to establish and maintain an information security program.

Topics Covered:

Domain 1: Governance and Risk Management

1. Define, Implement, Manage, and Maintain an Information Security Governance Program
2. Information Security Drivers
3. Establishing an information security management structure
4. Laws/Regulations/Standards as drivers of Organizational Policy/Standards/Procedures
5. Managing an enterprise information security compliance program
6. Introduction to Risk Management

Domain 2: Information Security Controls, Compliance, and Audit Management

1. Information Security Controls
2. Compliance Management
3. Guidelines, Good and Best Practices
4. Audit Management
5. Summary

Domain 3: Security Program Management & Operations

1. Program Management
2. Operations Management

3. Summary

Domain 4: Information Security Core Competencies

1. Access Control
2. Physical Security
3. Network Security
4. Certified Chief
5. Endpoint Protection
6. Application Security
7. Encryption Technologies
8. Virtualization Security
9. Cloud Computing Security
10. Transformative Technologies
11. Summary

Domain 5: Strategic Planning, Finance, Procurement and Vendor Management

1. Strategic Planning
2. Designing, Developing, and Maintaining an Enterprise Information Security Program
3. Understanding the Enterprise Architecture (EA)
4. Finance
5. Procurement
6. Vendor Management
7. Summary

Exam Information:
The course includes an exam voucher and retake for the EC-Council exam. The exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information:
One license provides access to the course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access:
Instructions for accessing the course will be emailed after purchase.

FedVTE (now CISA Learning) CISSP-ISSMP

ITI SKU: MISC-12

MSRP: Free through FedVTE (now CISA Learning)

Sales Price: Free through FedVTE (now CISA Learning)

Bundle Access Period: 12 months from purchase.

Courses in bundle: FedVTE (now CISA Learning) CISSP-ISSMP (Online OnDemand)

Course Description: This course is designed for IT professionals seeking to enhance their expertise in the management and oversight of information security programs. The CISSP-ISSMP certification is an advanced concentration under the Certified Information Systems Security Professional (CISSP) and focuses on establishing, presenting, and governing information security management programs. Through this self-paced online course, participants will gain an in-depth understanding of topics such as risk management, business continuity, security governance, legal and regulatory compliance, and incident response planning. The course prepares learners for the CISSP-ISSMP certification exam, ensuring they are equipped to lead and manage security teams and initiatives within an organization.

Course Outline:

- ISSMP Course Introduction
- Security's Role - Culture, Vision and Mission
- Security's Role – Management, Support and Commitment
- Security's Role – Board of Dir, Steering Committee
- Security Role – IT, HR and Legal
- Security's Role – Strategic Alignment
- IS Governance Defined
- IS Governance Goals Part 1 of 2
- IS Governance Goals Part 2 of 2
- Importance of IS Governance
- Information Security Strategies
- Data Classification and Privacy
- Threats to Data Privacy
- Data Classification and Privacy Implementations
- Security Policy Framework and Lifecycle
- Security Requirements in Contracts and Agreements
- Security Awareness and Training Programs
- Managing the Security Organization
- Security Metrics
- Security Metrics Indicators

- Integrating Project Management with SDLC
- System Development Life Cycle (SDLC)
- Systems Engineering (CMM)
- Vulnerability Management and Security Controls
- Service Oriented Architecture Controls
- Oversee System Security Testing
- Managing Change Control
- Risk Management
- Risk Management – Threats and Vulnerabilities
- Risk Management – Risk Assessments
- Calculating Risks
- Mitigating Risks
- Cyber Threat Intelligence
- Detection of Attack Sources
- Discovery Challenges and Escalation
- DEMO: Escalating Event to Incident
- Common Attack Vectors
- Root Cause and Investigation
- Incident Management Concepts
- Incident Management Process
- Incident Management Classification
- Financial Impact of Incidents
- Investigation and Forensic Evidence
- Investigations, IH and Response
- DEMO: Ditigal Forensics Investigation
- Security Compliance Frameworks
- Auditing Introduction and Preparation
- Evidence Reporting and Auditors
- Exception Management
- Continuity and Disaster Recovery Planning
- Understanding the Business
- Insurance
- Critical Processes Recovery Objectives
- Recovery Obligation Considerations
- BCM Site and IT Strategies
- Personnel and Recommended Strategies
- Design and Testing BCP and COOP
- Implementing Continuity and Recovery Plans
- Intellectual Property and Licensing
- (ISC)2 Code of Ethics

- DEMO: Verification and Quality Control
- Audit Planning Process
- ISSMP Self Study Practice Exam

How to access: To sign up for FedVTE (now CISA Learning), you can:

1. Go to https://fedvte.usalearning.gov/register.php
2. Enter the email address you use for official government business
3. Click Submit

If you are a veteran or federal contractor, you can use your personal or professional email address.

CTI Azure Administrator with labs

ITI SKU: MISC-13

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

Courses in bundle: Microsoft AZ-104 Azure Administrator certification (Online OnDemand)

CTI Custom AZ-104 Microsoft Azure Administrator Certification: Prepare for the Microsoft AZ-104 Azure Administrator certification with this comprehensive course. This course covers advanced Azure administration, including managing Azure identities and governance, implementing and managing storage, and configuring and managing virtual networks.

Course Highlights:

- Duration: 35+ Training Hours
- Content: 85+ On-demand Videos, covering Azure administration topics
- Preparation Questions: 200

Modules:

- Module 1 – Overview: Azure Essentials for Success
- Module 2 – Tools: Navigating the Azure Ecosystem
- Module 3 – Identities and Governance: Secure and Efficient Identity Management
- Module 4 – Master Data Storage and Security
- Module 5 – Compute Resources: Unlock the Power of Azure Compute

- Module 6 – Virtual Networks: Connect and Secure Your Resources
- Module 7 – Monitoring and Backup: Ensure Stability and Recovery

Labs included (8 hours):

- Azure Management Concepts Lab (3 Hours):
  - Azure Service Level Agreements (SLAs)
  - Management Tools
  - Monitoring Tools
  - The Azure Marketplace
- Azure Storage Management Lab (2 Hours):
  - Azure Storage Services
  - Working with Blobs
  - Azure SQL Databases
  - Azure Cosmos Databases
- Azure Security Concepts Lab (3 Hours):
  - Using Azure Key Vault
  - Security Tools
  - Network Security

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Exam Information: This course does not come with the exam. Exam vouchers can be purchased directly from Microsoft.

CTI Linux+ with labs

ITI SKU: MISC-14

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

Courses in bundle: CTI CompTIA Linux+ (Online OnDemand)

CTI Custom Online Self-Paced ILT Description: Gain expertise in Linux system administration with our CompTIA Linux+ course. This course will provide you with the

knowledge and skills required to configure, manage, operate, and troubleshoot a Linux environment by using security best practices, scripting, and automation computing models.

Course Highlights:

- Duration: 30+ hours
- Content: 120+ On-demand Videos
- Exam Prep: 400+ Prep Questions
- Certificate of Completion for CompTIA Linux+

Topics Areas Included:

- Introduction to Linux
- Administering Users and Groups
- Configuring Permissions
- Implementing File Management
- Managing Software and Storage
- Configuring Network Settings
- Securing Linux Systems
- Scripting and Automation

Modules:

- Module 0 - Course introduction
- Module 1 - Networking Fundamentals
- Module 2 - Cables and Connectors
- Module 3 - Internet Protocol (IP)
- Module 4 - Layer 7 Protocols
- Module 5 - Network Services
- Module 6 - Networking Devices
- Module 7 - Networked Devices
- Module 8 - Routing and Bandwidth Management
- Module 9 - Ethernet Switching

- Module 10 - Wireless Technologies
- Module 11 Network Performance
- Module 12 High Availability and Disaster Recovery
- Module 13 Organizational Documents
- Module 14 Network Security
- Module 15 Network Troubleshooting

CompTIA Linux+ labs included (63 hours):

1. Design Hard Disk Layout
2. Create Partitions and Filesystems
3. Using Various Disk Management Tools
4. Working with Kernel, Boot Modules, and Files
5. Working with Relative and Absolute Paths
6. Work with the Flow Control Constructs
7. Control Mounting and Unmounting of Filesystems
8. View the Hard Drive Details
9. Check and Repair Filesystems
10. Using RPM and YUM Package Management
11. Using Debian Package Management
12. Using Repositories
13. Managing User and Group Accounts and Related System Files
14. Run User Level Queries
15. Managing Disk Quotas
16. Working with Bash Profiles and Bash Scripts
17. Setup Host Security
18. Perform Basic File Editing Operations Using vi
19. Search Text Files using Regular Expressions
20. Using Shell Input and Output Redirections

21. Install and Configure a Web Server
22. Performing Basic File Management
23. Amending Hard and Symbolic Links
24. Find System Files and Place Files in the Correct Location
25. Use Systemctl and update-rc.d Utility to Manage Services
26. Configuring Host Names
27. Change Runlevels and Shutdown or Reboot System
28. Maintain System Time
29. Configure Client Side DNS
30. Configure System Logging
31. Mail Transfer Agent (MTA) Basics
32. Automate System Administration Tasks by Scheduling Jobs
33. Create, Monitor and Kill Processes
34. Manage Printers and Printing
35. Accessibility
36. Manage File Permissions and Ownership
37. Perform Security Administration Tasks
38. Working with Access Control List
39. Configure SELinux
40. Maintain the Integrity of Filesystems
41. Work with Pluggable Authentication Modules (PAM)
42. Secure Communication using SSH
43. Securing Data with Encryption
44. Work with TTY
45. Set up SFTP to Chroot Jail only for Specific Group
46. Secure a Linux Terminal and Implement Logging Services
47. Boot the System

48. Configure UFW and DenyHosts
49. Compress Data Using Various Tools and Utilities
50. Process Text Streams using Filters
51. Basic Network Troubleshooting
52. Use Streams Pipes and Redirects
53. Perform CPU Monitoring and Configuration
54. Perform Memory Monitoring and Configuration
55. Perform Process Monitoring
56. Modify Process Execution Priorities
57. Manage File and Directory Permissions
58. Access the Linux System
59. Configure Inheritance and Group Memberships
60. Patch the System
61. Working with the Environment Variables
62. Shells, Scripting and Data Management
63. Customize or Write Simple Scripts
64. Configure Permissions on Files and Directories
65. Work with PKI

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase

CTI Custom CEH and CHFI with labs and EC-Council Official CEH and CHFI Bundle

ITI SKU: MISC-15

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

Courses in bundle: CTI Custom CEH and CHFI with labs and EC-Council Official CEH and CHFI (OnDemand)

CTI Custom CEH Course Description: Our course offers CEH training to provide you the tools to research, discover and scan targets, analyze vulnerabilities and test attack methods and tools. The focus of this CEH online training course is to solve the challenge of breaking into a target network, collect evidence of success, and escape unnoticed.

Topics Covered:

- Introduction to the key concepts of ethical hacking and information security.
- Conducting footprinting and reconnaissance using advanced tools and techniques.
- Scanning networks and identifying vulnerabilities.
- Performing system hacking and exploiting operating systems.
- Understanding malware threats and implementing countermeasures.
- Utilizing social engineering techniques and tools.
- Executing Denial-of-Service (DoS) and session hijacking attacks.
- Evading IDS, firewalls, and honeypots.
- Hacking web servers and applications.
- Performing SQL injection and securing databases.
- Hacking wireless networks and mobile platforms.
- Exploring IoT and OT hacking methodologies.
- Securing cloud environments and implementing cryptographic techniques.

Labs included (15 hours):

- Footprinting and Reconnaissance Techniques
- Network Reconnaissance Techniques
- Enumeration Reconnaissance Techniques
- Vulnerability Analysis Tools & Techniques
- System Hacking Methodologies
- Malware Threat Concepts
- Network Sniffing Techniques
- Social Engineering Exploits
- Denial of Service Attacks
- Session Hijacking Concepts
- Compromising Web Servers
- Web Application Hacking

- SQL Injection Methodologies
- Introduction to Cloud Computing
- Cryptography Techniques

CTI Custom CHFI Course Description: Our CHFI course will cover the security discipline of computer forensics from a vendor-neutral perspective and work towards preparing students to become Forensic Investigators in Computer Hacking.

Topics Covered (18+ hours):

- Comprehensive understanding of computer forensics and the forensic investigation process.
- Techniques for searching and seizing digital evidence.
- Methods for analyzing and handling digital evidence.
- First responder procedures for incident management.
- Setup and operation of a forensic lab.
- Gain in-depth knowledge of hard disks, file systems, and Windows forensics.
- Data acquisition and duplication techniques.
- Recovering deleted files and partitions.
- Utilizing Access Data FTK and EnCase for forensic investigations.
- Understanding and applying steganography and password cracking techniques.
- Log correlation, network forensics, and analyzing wireless and web attacks.
- Investigating email crimes and conducting mobile investigations.
- Preparing investigative reports and serving as an expert witness.

Labs included (12+ hours):

- Understanding the Digital Forensics Profession and Investigations
- Data Acquisition
- Processing Crime and Incident Scenes
- Working with Windows and CLI Systems
- Current Digital Forensics Tools
- Linux and Macintosh File Systems
- Recovering Graphics Files
- Digital Forensics Analysis and Validation
- Virtual Machine Forensics, Live Acquisitions, and Network Forensics
- E-mail and Social Media Investigations

- Mobile Device Forensics
- Cloud Forensics
- Report Writing for High-Tech Investigations
- Expert Testimony in Digital Investigations
- Ethics for the Expert Witness

Official EC-Council CEH Course (Online OnDemand) Description: Master ethical hacking with our CEH Master course, tailored for security professionals aiming to protect their organizations from cyber threats. This course includes 40 hours of content, delivered through engaging videos, quizzes, and hands-on labs. Participants will learn to think like hackers and use the same tools and techniques to identify and mitigate vulnerabilities.

Topics Covered (labs integrated):

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial of Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking

- Cloud Computing
- Cryptography

Official EC-Council CHFI Course (Online OnDemand) Description: Enhance your investigative skills with the CHFI course, which provides 30 hours of content focusing on digital forensics. This course covers the essentials of computer forensics, including the investigation process, tools, and techniques for analyzing digital evidence.

Topics Covered (labs integrated):

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-Forensics Techniques
- Operating System Forensics
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigative Reports

Exam and exam pass guarantee information: All courses include an exam voucher and the CEH comes with a retake. Exams can be taken online through the EC-Council's remote proctoring service or at authorized testing centers. If you don't pass the CEH or CHFI exam, upon request you will be provided an additional 12 months of access to ITI's custom CEH and CHFI training.

License Information: One license provides access to both official EC-Council CEH and CHFI, ITI's CEH and CHFI courses and labs for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Link to brochure: https://www.eccouncil.org/wp-content/uploads/2022/09/CEH-brochure.pdf and https://www.eccouncil.org/wp-content/uploads/2023/03/CHFI-brochure.pdf

CTI CHFI with labs and EC-Council Official CHFI Bundle

ITI SKU: MISC-16

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

Courses in bundle: CTI Custom CEH and CHFI with labs and EC-Council Official CEH and CHFI (OnDemand)

CTI Custom CHFI Course Description: Our CHFI course will cover the security discipline of computer forensics from a vendor-neutral perspective and work towards preparing students to become Forensic Investigators in Computer Hacking.

Topics Covered (18+ hours):

- Comprehensive understanding of computer forensics and the forensic investigation process.
- Techniques for searching and seizing digital evidence.
- Methods for analyzing and handling digital evidence.
- First responder procedures for incident management.
- Setup and operation of a forensic lab.
- Gain in-depth knowledge of hard disks, file systems, and Windows forensics.
- Data acquisition and duplication techniques.
- Recovering deleted files and partitions.
- Utilizing Access Data FTK and EnCase for forensic investigations.
- Understanding and applying steganography and password cracking techniques.
- Log correlation, network forensics, and analyzing wireless and web attacks.
- Investigating email crimes and conducting mobile investigations.
- Preparing investigative reports and serving as an expert witness.

Labs included (12+ hours):

- Understanding the Digital Forensics Profession and Investigations
- Data Acquisition
- Processing Crime and Incident Scenes
- Working with Windows and CLI Systems
- Current Digital Forensics Tools

- Linux and Macintosh File Systems
- Recovering Graphics Files
- Digital Forensics Analysis and Validation
- Virtual Machine Forensics, Live Acquisitions, and Network Forensics
- E-mail and Social Media Investigations
- Mobile Device Forensics
- Cloud Forensics
- Report Writing for High-Tech Investigations
- Expert Testimony in Digital Investigations
- Ethics for the Expert Witness

Official EC-Council CHFI Course (Online OnDemand) Description: Enhance your investigative skills with the CHFI course, which provides 30 hours of content focusing on digital forensics. This course covers the essentials of computer forensics, including the investigation process, tools, and techniques for analyzing digital evidence.

Topics Covered (labs integrated):

- Computer Forensics in Today's World
- Computer Forensics Investigation Process
- Understanding Hard Disks and File Systems
- Data Acquisition and Duplication
- Defeating Anti-Forensics Techniques
- Operating System Forensics
- Network Forensics
- Investigating Web Attacks
- Database Forensics
- Cloud Forensics
- Malware Forensics
- Investigative Reports

Exam and exam pass guarantee information: All courses include an exam voucher. Exams can be taken online through the EC-Council's remote proctoring service or at authorized testing centers. If you don't pass the exam, upon request you will be provided an additional 12 months of access to CTI's custom CHFI training.

License Information: One license provides access to official EC-Council CHFI, CTI's CHFI course and labs for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Link to brochure: https://www.eccouncil.org/wp-content/uploads/2023/03/CHFI-brochure.pdf

EC-Council Master Open-Source Intelligence Curriculum Bundle

ITI SKU: MISC-17

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

Courses in bundle: EC-Council Master Open-Source Intelligence Curriculum (Online OnDemand)

EC-Council Course Description: Master Open Source Intelligence provides a deep dive into the techniques and tools used to gather actionable intelligence from publicly available data. The course covers methods for identifying, analyzing, and leveraging OSINT sources across social media, websites, and other digital platforms. Participants learn how to extract critical insights, conduct investigations, and apply OSINT practices to enhance security operations and decision-making. This training equips professionals to stay ahead of evolving threats by turning open data into valuable intelligence..

Topics Covered (14+ hours):

Course 1 Open Source Intelligence

- 9 Chapters , 5 Labs - Duration: 4 hrs
- Learn and understand what Open Source Intelligence is and how you can use it to your advantage and protection in a virtual Linux environment.
- Content:
  - Chapter 1: OSINT Introduction
  - Chapter 2: Environment Preparation
  - Chapter 3: Notes and Password Managers
  - Chapter 4: Search Engines
  - Chapter 5: Social Media Intelligence
  - Chapter 6: Email Addresses, Usernames, and Images
  - Chapter 7: OSINT and IT Systems
  - Chapter 8: Data Breaches and Leaks
  - Chapter 9: Final Thoughts

Course 2 Advanced Open Source Intelligence and Privacy

- 6 Chapters , 3 Labs - Duration: 5 hrs 16 mins
- Expand your Open Source Intelligence skillset and toolbelt to be more efficient and better at conducting your OSINT investigations. This is an advanced approach to Open Source Intelligence with Privacy in mind.
- Content:
    - Chapter 1: OSINT 101
    - Chapter 2: Configuring the OSINT Virtual Environment
    - Chapter 3: Advanced Search Engine Usage
    - Chapter 4: Advanced Linux OSINT Tools
    - Chapter 5: OSINT Summarization and Reporting
    - Chapter 6: Conclusion

Course 3 OSINT for Hackers and Penetration Testers

- 18 Chapters - Duration: 5 hrs
- Uncover hidden information, track people and analyze networks
- Content:
    - Chapter 1: Introduction
    - Chapter 2: Setting up Our Virtual Machine
    - Chapter 3: Miscellaneous
    - Chapter 4: Taking Notes
    - Chapter 5: OSINT Basics
    - Chapter 6: Hiding Our Identity
    - Chapter 7: Google
    - Chapter 8: Physical OSINT
    - Chapter 9: Web OSINT
    - Chapter 10: Phone OSINT
    - Chapter 11: People OSINT
    - Chapter 12: Social Media OSINT
    - Chapter 13: Business OSINT
    - Chapter 14: Network OSINT
    - Chapter 15: Password Cracking with John
    - Chapter 16: Firefox
    - Chapter 17: Chrome
    - Chapter 18: Finishing Up

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Master Threat Intelligence Bundle

ITI SKU: MISC-18

Courses in bundle: EC-Council Master Threat Intelligence Bundle (Online OnDemand)

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

EC-Council Course Description: This Mastering Threat Intelligence course provides comprehensive training on understanding, gathering, and applying threat intelligence effectively. It covers both foundational concepts and practical applications, ensuring learners can analyze cyber threats and improve organizational defenses. This course offers hands-on exposure to tools and methodologies, preparing participants for real-world intelligence operations and reporting..

Topics Covered (5+ hours):

- **Course 1 - Microsoft Cybersecurity Pro Track: Threat Detection**
  - 5 Chapters - Duration: 5 hrs 45 mins
  - Security Administrators, Security Analysts, System Administrator, any IT enthusiast who wants to get started in cyber security and be comfortable with the Microsoft Security services
  - Content
    - Chapter 1: Introduction
    - Chapter 2: Introduction to Threat Detection as Part of the Defense In-Depth Strategy
    - Chapter 3: Detecting Threats in On-Premises Environments
    - Chapter 4: Detecting Threats in Hybrid Cloud Environments
    - Chapter 5: Analyzing Threat Detection Solutions in Action
- **Course 2 - Applied Threat Hunting**
  - 8 Chapters - Duration: 4 hrs
  - Investigating, detecting, and defending your systems against modern threats.
  - Content
    - Chapter 1: Introduction to Threat Hunting
    - Chapter 2: Hunting TTPs
    - Chapter 3: Hunting Logs and Events
    - Chapter 4: Hunting Network Traffic
    - Chapter 5: Hunting with a SIEM
    - Chapter 6: Hunting with Other Tools
    - Chapter 7: Hunting Use Cases
    - Chapter 8: Course Conclusion
- **Course 3 - Practical Cyber Threat Intelligence**

- 8 Chapters , 1 Labs - Duration: 4 hrs 1 mins
- Learn the Fundamentals of Cyber Threat Identification, Analysis, and Mitigation.
- Content
  - Chapter 1: The What and Why of Cyber Threat Intelligence
  - Chapter 2: Better Than the Rest: Brand Differentiation Through Security
  - Chapter 3: The Threat Intelligence Lifecycle
  - Chapter 4: Cyber Threat Intelligence Frameworks
  - Chapter 5: Cyber Threat Detection Toolkit
  - Chapter 6: Machine Learning & Cloud Security
  - Chapter 7: Threat Actors & Cyberwarfare
  - Chapter 8: CVSS & Vulnerability Assessment

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Certified Ethical Hacker (CEH) Master with Certified Penetration Tester (CPENT) Blended Bundle

SKU: Misc-19

MSRP: $3,499

Sales Price: $3,499

High-level description: The Certified Ethical Hacker (CEH) Master with Certified Penetration Testing Professional (CPENT) blended bundle is designed to provide IT professionals with comprehensive training in ethical hacking and advanced penetration testing. This training program focuses on both defensive and offensive cybersecurity skills.

Course Delivery:

- **Official EC-Council CEH:** Self-paced Online ILT
- **Official EC-Council CPENT:** Self-paced Online ILT
- **ITI Custom CEH:** Self-paced Online ILT

Duration:

- **Official EC-Council CEH Master (live):** 5 days
- **Official EC-Council CEH Master (self-paced):** 5 days
- **Official EC-Council CPENT:** 5 days
- **ITI Custom CEH:** ~7+ days (70+ hours)

Recommended Study Sequence: Begin with the Official CEH Master training then the ITI CEH training to understand the core concepts of ethical hacking. Follow this with the CPENT course to develop advanced penetration testing skills and then ITI's PenTest+ course and labs.

CTI Custom CEH Course Description: Our course offers CEH training to provide you the tools to research, discover and scan targets, analyze vulnerabilities and test attack methods and tools. The focus of this CEH online training course is to solve the challenge of breaking into a target network, collect evidence of success, and escape unnoticed.

Topics Covered:

- Introduction to the key concepts of ethical hacking and information security.
- Conducting footprinting and reconnaissance using advanced tools and techniques.
- Scanning networks and identifying vulnerabilities.
- Performing system hacking and exploiting operating systems.
- Understanding malware threats and implementing countermeasures.
- Utilizing social engineering techniques and tools.
- Executing Denial-of-Service (DoS) and session hijacking attacks.
- Evading IDS, firewalls, and honeypots.
- Hacking web servers and applications.
- Performing SQL injection and securing databases.
- Hacking wireless networks and mobile platforms.
- Exploring IoT and OT hacking methodologies.
- Securing cloud environments and implementing cryptographic techniques.

Labs included (15 hours):

- Footprinting and Reconnaissance Techniques
- Network Reconnaissance Techniques
- Enumeration Reconnaissance Techniques
- Vulnerability Analysis Tools & Techniques
- System Hacking Methodologies
- Malware Threat Concepts
- Network Sniffing Techniques

- Social Engineering Exploits
- Denial of Service Attacks
- Session Hijacking Concepts
- Compromising Web Servers
- Web Application Hacking
- SQL Injection Methodologies
- Introduction to Cloud Computing
- Cryptography Techniques

Official EC-Council CEH Course Description: Master ethical hacking with our CEH course, designed for security professionals aiming to protect their organizations from cyber threats. This course includes 40 hours of content, delivered through engaging videos, quizzes, and hands-on labs.

Topics Covered:

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial of Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking

- Cloud Computing
- Cryptography

Official EC-Council CPENT Course Description: Advance your penetration testing skills with the CPENT course, which provides 40 hours of content focused on real-world penetration testing scenarios. This course covers advanced topics such as IoT hacking, binary exploitation, and writing exploits.

Topics Covered:

- Advanced Windows Attacks
- Attacking IoT Systems
- Writing Exploits: Advanced Binary Exploitation
- Bypassing a Filtered Network
- Pentesting Operational Technology (OT)
- Accessing Hidden Networks with Pivoting
- Double Pivoting
- Privilege Escalation
- Evading Defense Mechanisms
- Reporting and Documentation

Exam Information: All courses include an exam voucher. Exams can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to all course's for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Link to brochure: https://www.eccouncil.org/wp-content/uploads/2022/09/CEH-brochure.pdf and https://www.eccouncil.org/wp-content/uploads/2023/02/CPENT-brochure.pdf

EC-Council Certified Ethical Hacker (CEH) Blended Bundle

SKU: Misc-20

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

High-level description: The Certified Ethical Hacker (CEH) Master blended bundle is designed to provide IT professionals with comprehensive training in ethical hacking and advanced penetration testing. This training program focuses on both defensive and offensive cybersecurity skills.

Course Delivery:

- **Official EC-Council CEH:** Self-paced Online ILT
- **ITI Custom CEH:** Self-paced Online ILT

Duration:

- **Official EC-Council CEH:** 5 days
- **ITI Custom CEH:** ~7+ days (70+ hours)

CTI Custom CEH Course Description: Our course offers CEH training to provide you the tools to research, discover and scan targets, analyze vulnerabilities and test attack methods and tools. The focus of this CEH online training course is to solve the challenge of breaking into a target network, collect evidence of success, and escape unnoticed.

Topics Covered:

- Introduction to the key concepts of ethical hacking and information security.
- Conducting footprinting and reconnaissance using advanced tools and techniques.
- Scanning networks and identifying vulnerabilities.
- Performing system hacking and exploiting operating systems.
- Understanding malware threats and implementing countermeasures.
- Utilizing social engineering techniques and tools.
- Executing Denial-of-Service (DoS) and session hijacking attacks.
- Evading IDS, firewalls, and honeypots.
- Hacking web servers and applications.
- Performing SQL injection and securing databases.
- Hacking wireless networks and mobile platforms.
- Exploring IoT and OT hacking methodologies.
- Securing cloud environments and implementing cryptographic techniques.

Labs included (15 hours):

- Footprinting and Reconnaissance Techniques
- Network Reconnaissance Techniques
- Enumeration Reconnaissance Techniques
- Vulnerability Analysis Tools & Techniques
- System Hacking Methodologies
- Malware Threat Concepts
- Network Sniffing Techniques
- Social Engineering Exploits
- Denial of Service Attacks
- Session Hijacking Concepts
- Compromising Web Servers
- Web Application Hacking
- SQL Injection Methodologies
- Introduction to Cloud Computing
- Cryptography Techniques

Official EC-Council CEH Course Description: Master ethical hacking with our CEH course, tailored for security professionals aiming to protect their organizations from cyber threats. This course includes 40 hours of content, delivered through engaging videos, quizzes, and hands-on labs. Participants will learn to think like hackers and use the same tools and techniques to identify and mitigate vulnerabilities.

Topics Covered (labs integrated):

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial of Service
- Session Hijacking

- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

Exam and exam pass guarantee information: All courses include an exam voucher. Exams can be taken online through the EC-Council's remote proctoring service or at authorized testing centers. If you don't pass the CEH exam, upon request you will be provided an additional 12 months of access to ITI's custom CEH training.

License Information: One license provides access to both official EC-Council CEH and ITI's CEH courses and labs for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Link to brochure: https://www.eccouncil.org/wp-content/uploads/2022/09/CEH-brochure.pdf and https://www.eccouncil.org/wp-content/uploads/2023/03/CHFI-brochure.pdf

EC-Council OSINT for Ethical Hackers (Instagram/Facebook)

ITI SKU: MISC-21

Courses in bundle: OSINT for Ethical Hackers (Instagram) and OSINT for Ethical Hackers (Facebook) Curriculum (Online OnDemand)

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

EC-Council Course Description: This course on Open Source Intelligence (OSINT) for Ethical Hackers, focusing on Instagram and Facebook, provides an in-depth exploration of OSINT techniques tailored to these popular social platforms. Participants will learn to uncover hidden information, create undetectable online identities, and leverage advanced search capabilities to gather deep intelligence. These courses are designed

for ethical hackers looking to enhance their capabilities in extracting valuable data from extensive social media networks.

Topics Covered (13+ hours):

Course 1: OSINT for Ethical Hackers (Instagram)

1. Introduction to Instagram OSINT:
    - Overview of Open Source Intelligence concepts.
    - Specific challenges and opportunities with Instagram.
2. Setting Up for Instagram Reconnaissance:
    - Tools and software setup for Instagram intelligence gathering.
    - Privacy settings and their impact on OSINT efforts.
3. Data Collection Techniques on Instagram:
    - Techniques for extracting information from profiles, posts, and connections.
    - Utilizing Instagram's API for data collection.
4. Analyzing Instagram Data:
    - Methods to analyze images and metadata.
    - Understanding geotagging and its implications for location tracking.
5. Operational Security for Instagram OSINT:
    - Best practices for maintaining anonymity and security while conducting research.
    - Legal considerations to keep in mind during investigations.

Course 2: OSINT for Ethical Hackers (Facebook)

1. Introduction to Facebook OSINT:
    - Discussing the breadth of data available on Facebook for OSINT.
    - Ethical and legal considerations specific to Facebook.
2. Tools and Techniques for Facebook Data Gathering:
    - Overview of tools for scraping Facebook data.
    - Advanced search techniques to find detailed user information.
3. Practical Exercises in Facebook OSINT:
    - Hands-on examples of crafting queries to extract useful data.
    - Case studies demonstrating the application of gathered data.

4. Analysis and Utilization of Facebook Information:
    - Techniques for analyzing Facebook activity logs and friend networks.
    - Leveraging Facebook data for cybersecurity and ethical hacking scenarios.
5. OPSEC and Legal Aspects of Facebook OSINT:
    - Strategies to mitigate personal exposure while gathering data.
    - Understanding the legal framework governing data collection on Facebook.

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council OPSEC Demystified: Strategies for Secure Operations

ITI SKU: MISC-22

Courses in bundle: EC-Council OPSEC Demystified: Strategies for Secure Operations

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

EC-Council Course Description: This course explores the fundamentals of Operations Security (OPSEC) and its role in protecting sensitive information from adversaries. The course covers methodologies for identifying potential vulnerabilities, analyzing threats, and implementing best practices to secure operations in both physical and digital environments. Learners will gain practical insights into risk mitigation strategies and learn how to design security policies that prevent critical data leakage during mission planning and execution.

Topics Covered (5+ hours):

- Chapter 1: Introduction to OPSEC, and OPSEC Cycle
- 3 Videos
    - OPSEC Concepts and Definitions
    - OPSEC Cycle
    - Chapter 1 Quiz
    - Preview
- Chapter 2: Information Classification and Identification
- 2 Videos
    - Information Concepts
    - How to Identify Your Main Assets and Priorities?
    - Chapter 2 Quiz

    - Preview
- Chapter 3: Threats and Attack Vectors
- 7 Videos
    - Threat Landscape
    - Actors and Adversaries
    - Types of Threats
    - Threat Intelligence
    - Attack Vectors
    - Attack Surface
    - Threat Modelling
    - Chapter 3 Quiz
    - Preview
- Chapter 4: OPSEC Assessment
- 3 Videos
    - Risk Concepts and Risk Assessment
    - Risk Assessment Tools
    - OPSEC Assessment
    - Chapter 4 Quiz
    - Preview
- Chapter 5: Controls and Countermeasures
- 4 Videos
    - Concepts
    - Incident Response Fundamentals
    - Reports and Recommended Content and Structure
    - Cyber Deception
    - Chapter 5 Quiz
    - Preview
- Chapter 6: OPSEC for Offensive Security – Red Teams
- 4 Videos
    - Don't Overexpose
    - Pen testing Lab Setup with OPSEC Measures
    - Incorporate OPSEC in Your Pen testing Exercises
    - Creating Your Reports
    - Chapter 6 Quiz
    - Preview
- Chapter 7: OPSEC Validation
- 4 Videos
    - OPSEC Checklist
    - Key Considerations
    - OPSEC Roles
    - OPSEC Career Path

- Chapter 7 Quiz

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Cyber Warfare: Defense Against Nation-State Threat

ITI SKU: MISC-23

Courses in bundle: Cyber Warfare: Defense Against Nation-State Threat

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

EC-Council Course Description: This course focuses on strategies to defend against sophisticated cyber-attacks originating from nation-states. The course covers tactics used by state-sponsored actors, the geopolitical landscape of cyber warfare, and methods for identifying and mitigating high-level threats. Participants will gain insights into both offensive and defensive cyber strategies, preparing them to counteract advanced persistent threats (APTs) and strengthen national or organizational cyber defenses against hostile actors.

Topics Covered (5+ hours):

- **Chapter 1: Cybersecurity Fundamentals**
  - Fundamental Security Concepts and Terminology (CIA+)
  - Cryptography – The Basics
  - Common Types of Threats and Attacks
  - Threat Actors and Threat Intelligence
  - Security Management - Standards and Frameworks
  - Chapter 1 Quiz
  - Preview
- **Chapter 2: Introduction to Cyber Warfare**
  - Types of Adversaries
  - Cyber Weapons and Types of Threats
  - Chapter 2 Quiz
  - Preview
- **Chapter 3: Critical Infrastructure**
  - Introduction to Operational Technology Cybersecurity
  - DCS, ICS, and SCADA
  - OSINT and Critical Infrastructure
  - Chapter 3 Quiz
  - Preview
- **Chapter 4: Examples of Cyber Attacks**

  - Examples of Cyber Attacks (Part 1)
  - Examples of Cyber Attacks (Part 2)
  - Chapter 4 Quiz
  - Preview
- **Chapter 5: Cyber Warfare Defense**
  - Cyber Awareness
  - Detection of malware and Spear Phishing
  - Open-source Threat Hunting
  - Analyzing Threats
  - Chapter 5 Quiz
  - Preview
- **Chapter 6: Conclusion**
  - Final Thoughts Quiz

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Certified Network Defender

SKU: MISC-24

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Certified Network Defender (Online OnDemand)

High-level description: The Certified Network Defender (CND) 5 day course is designed to teach IT professionals the skills needed to protect, detect, and respond to network security threats. This course covers network security controls, protocols, perimeter appliances, secure VPN implementation, IDS/IPS, network traffic signature analysis, and vulnerability scanning. This course covers the essentials of network defense, from designing secure network architectures to implementing and managing security controls.

Topics Covered:

- Network Security Fundamentals
- Network Security Threats, Vulnerabilities, and Attacks
- Network Security Controls
- Network Security Policy Design and Implementation
- Physical Security
- Host Security

- Secure Firewall Configuration and Management
- Secure IDS Configuration and Management
- Secure VPN Configuration and Management
- Wireless Network Defense
- Network Traffic Monitoring and Analysis
- Network Incident Response and Management

Exam Information: The course includes an exam voucher for the CND exam. The CND exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the CND course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Link to brochure: CND Brochure

EC-Council Industrial Control Systems (ICS) Cybersecurity Bundle

SKU: MISC-25

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Industrial Control Systems (ICS) Cybersecurity Bundle (Online OnDemand)

High-level description: The Industrial Control Systems (ICS) Cybersecurity Bundle combines two comprehensive courses—Comprehensive Guide to Industrial Cybersecurity with IEC 62443 and ICS/OT Cybersecurity – NIST 800-82 Rev 3—to equip professionals with the skills needed to secure critical infrastructure. This bundle covers both the IEC 62443 and NIST 800-82 frameworks, focusing on best practices for managing risks, ensuring system resilience, and applying defense-in-depth strategies in industrial control systems (ICS) and operational technology (OT) environments. Learners will gain practical expertise to protect complex industrial networks from evolving cyber threats.

Topics Covered:

- **Course 1 Comprehensive Guide to Industrial Cybersecurity with IEC 6244 (5 hours)**
    - **Chapter 1: Foundational Requirements from 62443-4-2**

        - FR 1 - Identification and Authentication Control
        - Detailed Use Case Study for FR1
        - FR 2 - Use Control
        - Detailed Use Case Study for FR2
        - FR 3 - System Integrity
        - Detailed Use Case Study for FR3
        - FR 4 - Data Confidentiality
        - Detailed Use Case Study for FR4
        - FR 5 - Restricted Data Flow
        - Detailed Use Case Study for FR5
        - FR 6 - Timely Response to Events
        - Detailed Use Case Study for FR6
        - FR 7 - Resource Availability
        - Detailed Use Case Study for FR7
        - Chapter 1 Quiz
        - Preview
    - **Chapter 2: Authentication & Authorization Technologies - 62443-3-1**
        - Role-based Access Control
        - Password Authentication
        - Challenge/Response Authentication
        - Physical Token Authentication
        - Smart Card Authentication
        - Biometric Authentication
        - Location-based Authentication
        - Password Distribution & Management
        - Device to Device Authentication
        - Chapter 2 Quiz
        - Preview
    - **Chapter 3: Network Protection Technologies from 62443-3-1**
        - Network Firewalls
        - Host-based Firewalls
        - Virtual Local Area Networks (VLAN)
        - Chapter 3 Quiz
        - Preview
    - **Chapter 4: Encryption Technologies and Data Validation from 62443-3-1**
        - Virtual Private Networks (VPN)
        - Symmetric Key Encryption
        - Public Key Encryption
        - Chapter 4 Quiz
- **Course 2 ICS/OT Cybersecurity – NIST 800-82 Rev 3 (5 hours)**
    - **Chapter 1: OT Overview**

- OT Based System and their Interdependencies
- SCADA Systems
- Distributed Control Systems
- Programmable Logic Controller Based Topologies
- Building Automation Systems
- Physical Access Control Systems
- Safety Systems
- Industrial Internet of Things
- $7 Million Cybersecurity Scholarship by EC-Council
- Chapter 1 Quiz
- Preview

- **Chapter 2: OT Cybersecurity Program Development**
  - OT Cybersecurity Program Development
  - Establish Charter for OT Cybersecurity Program
  - Benefits of OT Cybersecurity Program
  - OT Cybersecurity Program Content
  - Cybersecurity Program Implementation Team
  - OT Cybersecurity Strategy
  - Chapter 2 Quiz
  - Preview
- **Chapter 3: Risk Management for OT Systems**
  - Managing OT Security Risk
  - Framing OT Risk
  - Assessing Risk
  - Responding to Risk
  - Monitoring Risk
  - Applying Risk Management Framework
  - Chapter 3 Quiz
  - Preview
- **Chapter 4: Risk Management Framework Steps**
  - Prepare
  - P-1: Risk Management Roles
  - P-2: Risk Management Strategy
  - P-3: Risk Assessment – Organization
  - P-4: Organizationally Tailored Control Baselines and Cybersecurity Framework
  - P-5: Common Control Identification
  - P-6: Impact-Level Prioritization
  - P-7: Continuous Monitoring Strategy – Organization
  - P-8: Mission Or Business Focus
  - P-9: System Stakeholders

- P-10: Asset Identification
- Task P-11: Authorization Boundary
- P-12: Information Types
- P-13: Information Life Cycle
- P-14: Risk Assessment – System
- P-15: Requirements Definition
- P-16: Enterprise Architecture
- P-17: Requirements Allocation
- P-18: System Registration
- Categorize
- Task C-1: System Description
- Task C-2: Security Categorization
- Task C-3: Security Categorization Review and Approval
- Select
- Task S-1: Control Selection
- Task S-2: Control Tailoring
- Task S-3: Control Allocation
- Task S-4: Documentation Of Planned Control Implementations
- Task S-5: Continuous Monitoring Strategy – System
- Implement
- Task I-1: Control Implementation
- TASK I-2: Update Control Implementation Information
- Assess
- Task A-1: Assessor Selection
- Task A-2: Assessment Plan
- Task A-3: Control Assessments
- Task A-4: Assessment Reports
- Task A-5: Remediation Actions
- Task A-6: Plan Of Action and Milestones
- Authorize
- Task R-1: Authorization Package
- Task R-2: Risk Analysis and Determination
- Task R-3: Risk Response
- Task R-4: Authorization Decision
- Task R-5: Authorization Reporting
- Monitor
- Task M-1: Checking System and Environment Changes
- Task M-2: Ongoing Assessments
- Task M-3: Ongoing Risk Response
- Task M-4: Authorization Package Updates
- Task M-5: Security and Privacy Reporting

- Task M-6: Ongoing Authorization
- Chapter 4 Quiz
- Preview

- **Chapter 5: OT Cybersecurity Architecture**
  - Defense in Depth Architecture
  - Layer - 1 Security Management
  - Layer - 2 Physical Security
  - Layer - 3 Network Security
  - Network Architecture
  - Centralized Logging
  - Network Monitoring
  - Zero Trust Architecture
  - Layer - 4 Hardware Security
  - Layer - 5 Software Security
  - Additional Considerations
  - Distributed Control System (DCS)-Based OT Systems
  - DCS/PLC-Based OT with IIoT
  - SCADA-Based OT Environments
  - Chapter 5 Quiz
  - Preview
- **Chapter 6: OT Security Capabilities and Tools**
  - Segmentation - Firewall
  - Segmentation - Unidirectional Gateways
  - Segmentation - VLAN
  - Segmentation - Software Defined Networking
  - Network Monitoring/SIEM-BAD/DLP
  - Network Monitoring/SIEM-Deception & Digital Twin
  - Data Security - Immutable Storage/Hashing
  - Data Security - Digital Signatures/Remote Access
  - Chapter 6 Quiz
  - Preview
  - Instructor

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

EC-Council Wireshark for Hacking and Network Forensics Bundle

SKU: MISC-26

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Wireshark for Hacking and Network Forensics Bundle (Online OnDemand)

High-level description: The Wireshark for Hacking and Network Forensics Bundle offers comprehensive training in network traffic analysis and forensic investigation. Combining "Wireshark for Ethical Hackers" and "Getting Started with Network Forensics," this bundle equips learners with the skills to capture, analyze, and interpret network data for both security monitoring and forensic purposes. Participants will learn to identify vulnerabilities, track malicious activities, and reconstruct cyber events from captured traffic. This dual-focus bundle is ideal for professionals aiming to develop expertise in network exploitation and digital forensics, providing practical tools and methodologies essential for roles like Digital Network Exploitation Analysts.

Topics Covered:

Instructor

Course 1: Wireshark for Ethical Hackers

Chapter 1: Introduction and Analysis

- Enabling Monitor Mode
- Port and IP Filtering
- Identifying Open, Closed, and Filtered Ports with Wireshark
- Understanding Nmap Scans with Wireshark
- ICMP Protocol Analysis with Wireshark
- Quiz
- Preview

Chapter 2: Capturing and Analyzing

- Analyzing HTTP Packets and Detecting HTTP Errors
- Check Out Sneaky Non-Standard Port Use
- Investigating Lost Packets with Wireshark
- Capturing Wireless Traffic on a Selected Network
- Decrypting Wi-Fi Traffic
- Sniffing Activity Over USB Interfaces
- Using Wireshark to Detect TCP Delays

- Quiz
- Preview

Chapter 3: Stealing Credentials and Files

- How Credentials Can Be Stolen on HTTP
- Extract Images from PCAP Files Using Wireshark
- Saving PDF and ZIP Files from Wireshark
- Capturing Telnet and SMTP Passwords
- Identifying Hosts and Users with Wireshark
- Quiz
- Preview

Chapter 4: Detecting and Analyzing Attacks

- Capturing Traffic of a Particular Host
- Analyzing SSL Stripping Attacks
- Detecting Christmas Tree Attacks
- Decrypting SSL and TLS Traffic Using Wireshark
- Converting PCAP to XML
- Detecting ICMP Flooding (Smurf Attack)
- Detecting MAC Flooding and ARP Cache Poisoning
- Examining Tor Traffic
- Detecting Brute Force and Denial-of-Service Attacks
- Identifying Bot-Infected Hosts
- Quiz

Course 2: Getting Started with Network Forensics

Chapter 1: A Hands-on Approach to the OSI Model

- Demystifying the OSI Model with Wireshark
- Analyzing IP and ICMP with Tcpdump
- Analyzing ARP and DNS with Wireshark

- Reviewing TCP Sequence with Tcpdump and Tshark
- Examining UDP with Wireshark
- Analyzing HTTP with Wireshark
- Chapter 1 Quiz
- Preview

Chapter 2: Detecting Network Attacks with Wireshark

- Detecting Reconnaissance Attacks (Ping Sweeping)
- Detecting Nmap Scans
- Identifying Man-in-the-Middle Attacks
- Detecting Brute-Force Attacks
- Chapter 2 Quiz
- Preview

Chapter 3: Detecting Network Attacks with ELK

- Installing Docker and ELK Stack (sebp/elk)
- Ingesting FTP Logs Using Logstash
- Detecting FTP Server Attacks with Kibana
- Uploading and Analyzing evtx Logs Using ELK
- Conclusion
- Chapter 3 Quiz

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

EC-Council Becoming a Data Engineer Bundle

SKU: MISC-27

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Becoming a Data Engineer Bundle (Online OnDemand)

High-level description: This bundle offers comprehensive training in data engineering, focusing on building data pipelines, managing cloud infrastructure, and developing analytics solutions. It covers essential tools, including cloud services and big data frameworks, equipping learners with practical skills for modern data management and engineering roles. This path is ideal for professionals seeking expertise in designing scalable, data-driven solutions across various cloud environments.

Topics Covered:

- **Practical Visit to Data Mining**
  - Introduction to Data Mining
  - Essentials of Data Mining
  - Analyzing Mining Techniques and Algorithms
  - Clustering Techniques
  - Tree Classification
  - Handling Outliers
  - Project Pipeline Overview
  - Advanced Clustering Techniques
- **Data Analysis with Python Masterclass – Part 1**
  - Introduction to the Course
  - Setting up the Environment
  - Introduction to NumPy
  - Introduction to Pandas
  - Data Wrangling and Visualization
- **Data Analysis with Python Masterclass – Part 2**
  - Case Study 1: Data Understanding and Insights
  - Case Study 2: Analysis to Aid a Business Objective
  - Next Steps
- **Data Wrangling with Pandas – Part 1**
  - Introduction to Python and Setup
  - NumPy and Visualization Basics

    - Introduction to Pandas
- **Data Wrangling with Pandas – Part 2**
    - Data Processing with Pandas
    - Visualization with Matplotlib
    - Working with Real-Life Data
    - Visualization with Seaborn
- **Data Analysis with R Masterclass**
    - Introduction to the Course
    - Data Visualization and Reporting
    - Case Study 1
    - Case Study 2
    - Next Steps
- **Hands-on SQL for Data Science**
    - Welcome and Introduction
    - Database Concepts
    - SQL Basics
    - Advanced SQL Techniques
    - Data Analysis
    - Conclusion
- **Databases with Python**
    - Introduction to the Course
    - MySQL with Python
    - SQLite with Python
    - MongoDB with Python
- **Hands-on Azure Data Factory and Security**
    - Azure Data Factory in Data Pipelines
    - Implementing and Configuring Data Factory

- Data Flow and Transformation
- Monitoring and Security Practices

- **Amazon Redshift Demystified**
  - Introduction to Redshift and Cluster Management
  - Redshift Architecture Overview
  - Data Warehouse Design Considerations
  - Loading Data into Redshift
  - Securing Redshift Data
  - Backup and Recovery
  - Performance Tuning
  - Key Takeaways
- **Machine Learning with Python**
  - Introduction to Machine Learning
  - Data Pre-processing
  - Classification Techniques
  - Regression Models
  - Fine-Tuning Models
  - Deploying Machine Learning Models
  - Introduction to Deep Learning

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Microsoft Certified: Azure Data Engineer Associate

SKU: MISC-28

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: Microsoft Certified: Azure Data Engineer Associate (Online **Live**)

High-level description: This ITI partner-delivered live online course prepares participants for the Microsoft Certified: Azure Data Engineer Associate certification. It focuses on building secure, scalable data pipelines and optimizing analytics solutions using Azure tools like Data Factory, Synapse Analytics, and Databricks. Participants gain hands-on experience through real-world scenarios, equipping them with the skills needed to design, implement, and manage data solutions effectively on Azure. ***Contact us to schedule this course***.

Topics Covered:

1. **Data Engineering Introduction**
    - Overview of Azure
    - Fundamental Azure Concepts
    - Introduction to Azure Portal
2. **Design and Implement Data Storage**
    - Design an Azure Data Lake solution
    - Design for Efficient Querying and Data Pruning
    - Design a Distribution and Data Archiving Strategy
    - Implement Physical and Logical Data Structures
    - Implement the Serving Layer
3. **Design and Develop Data Processing**
    - Ingest and Transform Data
    - Develop Batch Processing Solutions
    - Create Stream Processing Solutions
    - Manage Data Batches and Pipelines
4. **Design and Implement Data Security**
    - Design Security Policies and Standards
    - Implement Data Masking and Security
5. **Monitor and Optimize Data Storage and Processing**
    - Configure Data Monitoring Services
    - Optimize and Troubleshoot Data Storage and Processing

License Information: One license provides access to the courses.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Exam Information: To purchase an exam voucher for the Microsoft Certified: Azure Data Engineer Associate (DP-203) exam, visit the Microsoft Certification Exam Registration page via Microsoft Learn or Pearson VUE, select your exam, and follow the prompts to pay for the voucher. Once purchased, you can schedule your exam either online or at an authorized testing center.

EC-Council COBIT 2019 Foundation Training Plus Exam Prep

SKU: MISC-29

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council COBIT 2019 Foundation Training Plus Exam Prep (Online OnDemand)

High-level description: This course provides a comprehensive introduction to the COBIT 2019 framework, focusing on the governance and management of enterprise IT. It covers key concepts, governance system principles, components, and the COBIT Core Model, along with practical tools to apply these frameworks effectively. Designed for professionals responsible for governance, data management, and IT strategy, this course equips learners with essential skills to align business goals with IT processes, making it a great fit for Data Officers and IT managers.

Topics Covered:

Course Content

- **Chapter 1: Key Concepts and Terminology of COBIT 2019**
    - Enterprise Governance of IT
    - COBIT 2019 Governance Framework
    - Governance and Management
    - Chapter 1 Quiz
    - Preview
- **Chapter 2: Governance Framework and System Principles**
    - Governance Framework Principles
    - Governance System Principles (1-3)

- Governance System Principles (4-6)
- Chapter 2 Quiz
- Preview

- **Chapter 3: Governance System and Components**
  - Introduction to Components of the Governance System
  - Components of the Governance System (2 & 3)
  - Components of the Governance System (4 & 5)
  - Components of the Governance System (6 & 7)
  - Chapter 3 Quiz
  - Preview
- **Chapter 4: COBIT Core and Goals Cascade**
  - COBIT Core Model
  - COBIT Core Model – The Five Domains
  - Goals Cascade
  - Chapter 4 Quiz
  - Preview
- **Chapter 5: Focus Areas and Design Factors**
  - Introduction to Focus Areas and Design Factors
  - Design Factors – Part 1
  - Design Factors – Part 2
  - Chapter 5 Quiz

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

EC-Council Implementing Information Security in Your Enterprise

SKU: MISC-30

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Implementing Information Security in Your Enterprise (Online OnDemand)

High-level description: Implementing Information Security in Your Enterprise offers a practical guide to building and managing secure information systems, aligning with globally recognized standards and frameworks. The course covers ISO/IEC 27001, focusing on developing an Information Security Management System (ISMS), implementing controls, and achieving compliance. It also explores ISO 15489 for document and records management, emphasizing the importance of data governance. Participants learn about GDPR and other global data protection standards, gaining insights into privacy laws and compliance requirements. Additionally, the course addresses cybersecurity regulations, hybrid cloud security practices, and blockchain technologies, equipping organizations to conduct risk assessments and align operations with best practices across multiple domains.

Topics Covered:

Chapter 1: Introduction to Information Security

- Course welcome and introduction
- High-level overview of the course
- Key aspects of information security
- Overview of EC-Council's $7 million cybersecurity scholarship
- **Quiz**

Chapter 2: Implementing ISO 27001 – Information Security Standards

- Overview of ISO 27001
- Implementing controls and risk mitigation plans
- Achieving compliance with ISO 27001
- **Quiz**

Chapter 3: Establishing Information Security Roles, Responsibilities, and Governance

- Best practices in information security governance
- Key roles and responsibilities within an ISMS
- Reporting and governance structures
- **Quiz**

Chapter 4: Best Practice Document and Records Management (ISO 15489)

- Overview of document and records management
- Implementation of ISO 15489 standards
- Importance of data governance
- **Quiz**

Chapter 5: Data Protection, Privacy, and GDPR

- Introduction to data protection and privacy
- Overview of GDPR regulations
- Global standards in data protection

Chapter 6: Compliance and Regulations in Cybersecurity

- Overview of cybersecurity compliance and regulations
- Key standards and best practices
- Implementing compliance measures

Chapter 7: Hybrid Cloud Computing and Security

- Mobility and hybrid cloud security overview
- Blockchain and information security best practices
- Conducting risk assessments
- **Quiz**

Chapter 8: Conclusion

- Key takeaways and course wrap-up

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

PECB Certified Data Protection Officer

SKU: MISC-31

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: PECB Certified Data Protection Officer (Online OnDemand)

High-level description: The PECB Certified Data Protection Officer course equips participants with the expertise needed to implement, manage, and align organizational data privacy practices with the General Data Protection Regulation (GDPR). Over five days, attendees develop a thorough understanding of privacy frameworks, governance principles, and compliance strategies. Key topics include privacy impact assessments (DPIAs), handling data breaches, managing international data transfers, and applying security measures like encryption and pseudonymization. The course also covers risk management principles and offers practical exercises to prepare participants for the CDPO certification exam. This training is ideal for professionals responsible for data protection, governance, and regulatory compliance within organizations.

Topics Covered:

Day 1: Privacy Foundations

- Introduction to personal data protection
- Overview of the General Data Protection Regulation (GDPR)
- Fundamental GDPR concepts and definitions
- European institutions involved in personal data protection (e.g., EDPS, EDPB)
- Key responsibilities of Data Protection Officers (DPOs)

Day 2: International Framework

- Internet governance and personal data protection in international contexts
- UN resolutions and cross-border data protection agreements
- Safe transfer of personal data outside the EU
- Binding Corporate Rules (BCRs) and Privacy Shield framework
- GDPR security measures (pseudonymization, cryptography)

Day 3: Privacy and Security

- Impact of technology (big data, IoT, quantum computing) on personal data
- Systematic and automated profiling under the GDPR
- Handling personal data breaches and incident response
- Developing continuity plans for accountability

Day 4: Data Protection Impact Assessment (DPIA)

- Introduction to DPIA and its purpose

- When, why, and how to conduct DPIAs
- Steps for carrying out DPIAs in practice
- Mapping personal data life cycles to GDPR principles

Day 5: Certification Exam

- 3-hour exam consisting of 150 multiple-choice questions
- Practice tests and review exercises included
- Certification awarded upon passing and meeting experience requirements

License and exam Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase. For the virtual, self-paced version of the PECB Certified Data Protection Officer (CDPO) course, students will have access to the exam as part of the course package. Detailed instructions on how to schedule and take the exam remotely will be provided within the course platform.

How to Access: Instructions for accessing the courses will be emailed after purchase.

EC-Council NIST SP 800-53 Controls Mastery Bundle

SKU: MISC-32

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council NIST SP 800-53 Controls Mastery Bundle (Online OnDemand)

High-level description: The NIST SP 800-53 Controls Mastery Bundle offers a comprehensive exploration of both the conceptual framework and practical application of NIST SP 800-53 standards. It combines Fundamentals and Control Families, which provides a deep understanding of the control structures, with Control Baselines and Implementation, focusing on the operational steps needed to apply these controls effectively. This dual approach ensures participants gain both the knowledge to align security and governance policies with NIST standards and the practical skills to implement control baselines for compliance. This bundle is ideal for professionals managing risk, security, and compliance in alignment with US federal frameworks.

Topics Covered:

Course 1 - The Ultimate Guide to NIST SP 800-53 - Fundamentals and Control Families

- **Chapter 1: Introduction to NIST SP 800-53**

- Overview of NIST SP 800-53 and its importance in information security
- Understanding the purpose, structure, and control families
- Mapping NIST SP 800-53 to other relevant standards and frameworks
- Chapter 1 Quiz

- **Chapter 2: Key Control Families**
  - Exploring the major control families and their objectives
  - Essential controls within each family relevant to different roles
  - Case studies and examples of control implementation
  - Chapter 2 Quiz
- **Chapter 3: Risk Management and Assessment**
  - Understanding the risk management framework within NIST SP 800-53
  - Overview of risk assessment methodologies and tools
  - Risk mitigation strategies and control selection based on risk levels
  - Chapter 3 Quiz

Course 2 - The Ultimate Guide to NIST SP 800-53 Control Baselines and Implementation

- **Chapter 1: Implementing Security Controls**
  - Technical aspects of security control implementation
  - Practical guidelines for implementing selected controls
  - Common challenges and best practices for control implementation
  - Chapter 1 Quiz
- **Chapter 2: Compliance and Auditing**
  - Regulatory landscape and compliance requirements
  - Conducting security assessments and audits based on NIST SP 800-53
  - Interpretation of control objectives and assessment findings
  - Chapter 2 Quiz
- **Chapter 3: Security Controls for Contractors and Service Providers**

  - Understanding the specific requirements for contractors and service providers
  - Contractual obligations and security control implementation
  - Best practices for managing security in outsourcing and vendor relationships
  - Chapter 3 Quiz
- **Chapter 4: Continuous Monitoring and Incident Response**
  - Importance of continuous monitoring in maintaining security
  - Overview of incident response planning and procedures
  - Incident handling and reporting essentials
  - Chapter 4 Quiz

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

CTI Custom Azure Fundamentals Course

ITI SKU: MISC-33

Courses in bundle: CTI Azure fundamentals

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Bundle Access Period: 12 months from purchase.

AZ-104 Microsoft Azure Administrator Certification: The AZ-900: Azure Fundamentals course provides a comprehensive introduction to Microsoft Azure, focusing on core cloud concepts and Azure services. It covers topics such as Azure's architecture, governance, and pricing models, helping learners understand essential concepts like compute, networking, storage, and databases. Participants also gain insights into Azure security, compliance, and identity management, along with best practices for deploying resources and managing costs. Designed for beginners and non-technical professionals, this course builds foundational knowledge required to pursue more advanced Azure certifications and supports roles involving cloud adoption strategies.

Course Highlights:

- Duration: 8+ Training Hours
- Content: 45+ On-demand Videos, covering Azure topics

- Preparation Questions: 100

Modules/Outline:

Module 1: Introduction

- Instructor Introduction
- Course Overview
- Expectations

Module 2: Cloud Fundamentals

- What is the Cloud
- Basic Terms
- Types of Cloud Computing
- Cloud Service Models

Module 3: Azure's Architecture

- Regions and Availability
- Resource Groups and Management
- Azure Marketplace
- Demo: Azure Console Exploration

Module 4: Compute

- Virtual Machines
- Containers
- Demo: Containers
- Functions
- Demo: Functions
- Windows Virtual Desktop and App Services

Module 5: Networking and CDN

- Virtual Networks
- Load Balancers
- Gateways
- Content Delivery Network (CDN)
- Network Security
- Demo: Connecting Two VMs

Module 6: Storage

- Storage
- Big Data and Analytics
- Databases
- Demo: SQL Database
- Database Migration

Module 7: Azure Solutions

- IoT
- Demo: IoT Hub
- AI
- Serverless Computing

Module 8: Administration

- Security
- Identity and Access Management
- Demo: Adding Users and Groups
- Governance
- Demo: Resource Locks
- Privacy and Compliance

Module 9: Pricing and Service Level Agreements

- Managing Costs
- Demo: Pricing Calculator
- Service Level Agreements and Service Lifecycles

Module 10: Exam Preparation

- Exam Layout
- Best Practices and Study Tips
- Overview and Conclusion

Module 11: Review Questions

- Part 1
- Part 2
- Part 3
- Part 4

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Exam Information: This course does not come with the exam. Exam vouchers can be purchased directly from Microsoft.

EC-Council Implementing DevOps in Microsoft Azure

SKU: MISC-34

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Implementing DevOps in Microsoft Azure (Online OnDemand)

High-level description: The Implementing DevOps in Microsoft Azure course provides hands-on training in leveraging Azure tools and services to implement DevOps practices effectively. Participants learn to automate infrastructure deployments, manage CI/CD pipelines, and enhance collaboration between development and operations teams using Azure DevOps. Key topics include source control, infrastructure as code, monitoring, and the use of services like Azure Pipelines, Repos, and Boards. This course is ideal for professionals seeking to streamline software delivery processes and integrate DevOps methodologies within Azure cloud environments.

Topics Covered (20 hours):

1. **DevOps Beginner to Advanced: Introduction to DevOps**
    - **Duration:** 10 hrs 47 mins
    - **Overview:** Start a DevOps career with topics like Linux, AWS, Jenkins, Ansible, Docker, Kubernetes, and N-Tier Projects.
    - **Content:**
        - Chapter 1: Introduction
        - Chapter 2: VM Setup
        - Chapter 3: Linux
        - Chapter 4: Vagrant and Linux Servers
        - Chapter 5: VProfile Project Setup (Manual and Automated)
        - Chapter 6: Bash Scripting
        - Chapter 7: Networking
2. **Continuous Integration and Continuous Deployment with Azure**

- **Duration:** 4 hrs
- **Overview:** Learn infrastructure development and CI/CD practices using Azure DevOps.
- **Content:**
  - Chapter 1: Introduction to Continuous Integration and Delivery
  - Chapter 2: Getting Started with Azure DevOps
  - Chapter 3: Continuous Integration with Azure Release Pipeline
  - Chapter 4: Managing Identity and Security
  - Chapter 5: Role-Based Access Control and Security

3. **Master Azure DevOps – Boards, App/Infra Deployment, Pipeline**
   - **Duration:** 4 hrs
   - **Overview:** Explore Azure DevOps services such as Boards, Repos, YAML-based CI/CD, and automated deployment pipelines.
   - **Content:**
     - Chapter 1: Introduction to Azure DevOps Organization & Boards
     - Chapter 2: Getting Started with Azure Repo – Migrate, Commit, Push, and Merge Code
     - Chapter 3: Continuous Integration and Delivery – Classic Way
     - Chapter 4: Configure & Deploy Infrastructure with Automated CI/CD Using YAML
4. **Infrastructure Testing with Azure DevOps**
   - **Duration:** 4 hrs
   - **Overview:** Learn how to test, automate, validate, and secure infrastructure using Azure DevOps.
   - **Content:**
     - Chapter 1: Test, Validate, and Secure Infrastructure as Code
     - Chapter 2: Infrastructure Testing with Chef InSpec for Production Environment
     - Chapter 3: Validate Infrastructure with Terratest

- Chapter 4: Automate and Monitor Applications/Resources on Cloud

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

EC-Council DevSecOps – Implementing Security in DevOps Processes

SKU: MISC-35

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council DevSecOps – Implementing Security in DevOps Processes (Online OnDemand)

High-level description: The DevSecOps: Implementing Security in DevOps Processes course focuses on integrating security practices into every stage of the DevOps lifecycle. Participants learn how to automate security checks, manage vulnerabilities, and implement secure coding practices within CI/CD pipelines. The course covers topics such as configuration management, continuous monitoring, and compliance validation to ensure security is embedded seamlessly into development and operations workflows. Designed for DevOps professionals and security teams, this course helps organizations reduce risks and enhance the resilience of their cloud and application environments..

Topics Covered (5+ hours):

Chapter 1: Introduction and Importance of DevSecOps

- High-level Overview of Course
- Key Aspects of DevSecOps
- Section Conclusion
- Chapter 1 Quiz
- Preview

Chapter 2: DevOps and CI/CD: Understanding the Difference

- Section Introduction
- Term Definition
- Scope and Purpose
- Process

- Implementation and Stages
- Benefits
- Challenges and Constraints
- Section Conclusion
- Chapter 2 Quiz
- Preview

Chapter 3: The Emergence of DevSecOps

- Section Introduction
- DevSecOps Concepts
- The Problem that DevSecOps Solves
- Benefits of DevSecOps
- Overview of DevSecOps Implementation
- Business Case Examples
- Section Conclusion
- Chapter 3 Quiz
- Preview

Chapter 4: Inserting Security into DevOps

- Section Introduction
- Using Infrastructure as Code
- Secure by Default
- Shift Security Left
- OWASP Proactive Controls
- Making Security Self-Service
- Honeymoon Effect
- Section Conclusion
- Chapter 4 Quiz
- Preview

Chapter 5: Practical Implementation

- Section Introduction
- Pen Testing
- Security in Unit and Integration Testing
- Dynamic Scanning (DAST)

- Fuzzing and Continuous Delivery
- Instituting Automated Attacks
- Bug Bounties
- Vulnerability Management
- Section Conclusion
- Chapter 5 Quiz
- Preview

Chapter 6: Securing Design

- Section Introduction
- Threat Modeling and Risk Assessment
- Defining Security Requirements
- Researching and Verifying Risk Mitigation
- Section Conclusion
- Chapter 6 Quiz
- Preview

Chapter 7: Securing Code and Software

- Section Introduction
- Importance of Writing Secure Code
- Manual Reviews
- Automated Reviews
- Compliance in Code Generation
- Ensuring Supplier or Vendor Code is Secure
- Section Conclusion
- Chapter 7 Quiz
- Preview

Chapter 8: Securing Infrastructure

- Section Introduction
- Conducting a Network Security Audit
- Training Staff
- Limiting Access
- Patches and Remediation
- Tools and Support

- Section Conclusion
- Chapter 8 Quiz
- Preview

Chapter 9: Production Processes

- Section Introduction
- Physically Securing Hardware and Network Devices
- Limiting Access and Safeguarding Passwords
- Training and Governance
- Section Conclusion
- Chapter 9 Quiz
- Preview

Chapter 10: Course Conclusion

- Overview of Major Concepts from Course
- Resources for More Information
- Thank You and Contact Information

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

EC-Council Machine Learning with Python

SKU: MISC-36

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Machine Learning with Python (Online OnDemand)

High-level description: The Machine Learning with Python course from EC-Council provides practical training on implementing machine learning algorithms using Python. Participants will explore key libraries such as Pandas and Scikit-learn, focusing on data manipulation, model building, and evaluation techniques. The course emphasizes hands-on problem-solving with real-world datasets, preparing learners to apply machine learning effectively in business and technical environments. This program is ideal for those looking to develop foundational skills in machine learning while leveraging the Python programming language.

Topics Covered (4+ hours):

Information **Chapter 1: Introduction to Machine Learning**

- Understanding Machine Learning
- Understanding the Machine Learning Process
- Types of Machine Learning
- Exploring Python for Machine Learning
- Development Environment Setup for ML
- Chapter 1 Quiz
- Preview

Chapter 2: Exploring Data Pre-processing

- Data Pre-processing Overview
- Understanding Data Pre-processing
- Steps for Data Pre-processing
- Demo: Pre-processing a Dataset Using Python, Pandas, NumPy, and Sklearn
- Chapter 2 Quiz
- Preview

Chapter 3: Exploring Classification in Machine Learning

- Module Overview
- Understanding Classification
- Types of Classification
- Implementing an ML Classifier for Diabetes Classification
- Evaluating Classification Models
- Summary
- Chapter 3 Quiz
- Preview

Chapter 4: Exploring Regression in Machine Learning

- Module Overview
- Why Use Regression?
- Types of Regression
- Demo: Building a Regression Model Using TensorFlow
- Understanding Regularization and Its Types
- Chapter 4 Quiz
- Preview

Chapter 5: Fine-tuning Models in Machine Learning

- Module Overview
- What Is Fine-tuning in Machine Learning?
- Understanding Hyperparameter Tuning
- Demo: Performing Hyperparameter Tuning
- Cross-validation Methods
- Chapter 5 Quiz
- Preview

Chapter 6: Deploying Machine Learning Models

- Module Overview
- Exporting Machine Learning Models
- Building a REST API to Serve an H5 ML Model
- Deploying ML Models with TensorFlow Serving
- Summary
- Chapter 6 Quiz
- Preview

Chapter 7: Introducing Deep Learning

- Module Overview
- What is Deep Learning?
- How Deep Learning Works
- Basic Concepts and Terms in Deep Learning
- Applications of Deep Learning
- Demo: Building a Deep Learning Model Using TensorFlow
- Summary
- Chapter 7 Quiz

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

CompTIA DataX Data Science Course

SKU: MISC-37

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: CompTIA DataX (Online OnDemand)

High-level description: The Official DataX course combines narrative instructional content, videos, performance-based questions (PBQs), and live labs to provide an immersive learning experience tailored for experienced data professionals. Designed to address knowledge gaps, the course offers a learning progression model, ensuring participants build skills through targeted instruction and hands-on practice. Technologies such as Jupyter Notebooks, SQL, R, and Python are integrated into labs, while videos are embedded within the content to provide relevant, real-time guidance. This structure ensures learners master advanced data science concepts through practice and customized feedback.

Topics Covered (40+ hours):

Topics Covered

1. **Introduction to Data Science and Problem Analysis**
    - Understand the data science process and apply CRISP-DM frameworks
    - Analyze business problems and align them with data science solutions
2. **Data Collection and Ingestion**
    - Work with structured, unstructured, and synthetic data
    - Implement batching, streaming, and pipelines
3. **Data Cleaning and Preparation**
    - Perform data wrangling and use imputation techniques for missing data
4. **Exploratory Data Analysis (EDA)**
    - Conduct univariate and multivariate analysis
    - Apply dimensionality reduction techniques like PCA
5. **Feature Engineering and Selection**
    - Identify key features and apply encoding and normalization techniques
6. **Statistical Modeling and Machine Learning**
    - Develop models using linear and logistic regression
    - Implement supervised learning techniques such as decision trees and random forests
7. **Deep Learning and Neural Networks**

- Build deep learning models with frameworks like TensorFlow
- Explore CNNs, RNNs, and transfer learning methods

8. **Specialized Applications**
    - Use NLP for text data and computer vision for image analysis
    - Apply graph analytics to extract insights from network data
9. **MLOps, CI/CD Pipelines, and Deployment**
    - Set up MLOps pipelines for continuous integration and delivery
    - Deploy models using tools like Docker and Kubernetes
10. **Monitoring and Model Drift**

- Monitor deployed models and detect concept and data drift

11. **Optimization and Hyperparameter Tuning**

- Apply grid search and random search for hyperparameter tuning
- Optimize models for performance and scalability

12. **Ethics, Bias, and Fairness**

- Identify and mitigate bias in data and models
- Ensure fairness, transparency, and accountability

13. **Communicating Insights and Business Impact**

- Present findings through data storytelling techniques
- Create visual reports and dashboards to communicate insights effectively

Technical Skills Covered in the DataX Certification and Training

1. **Mathematics and Statistics (17%)**
    - Apply appropriate statistical methods, probability, and synthetic modeling concepts.
    - Understand the importance of linear algebra, calculus, and temporal models.
2. **Modeling, Analysis, and Outcomes (24%)**
    - Use exploratory data analysis (EDA) techniques to address data issues.
    - Apply data enrichment, design model iterations, and analyze experimental results.

- Translate results and communicate insights through appropriate methods.

3. **Machine Learning (24%)**
    - Implement supervised, unsupervised, and tree-based ML methods.
    - Understand deep learning frameworks and explain ML concepts.
4. **Operations and Processes (22%)**
    - Manage data ingestion, storage, and wrangling tasks.
    - Implement MLOps principles, deploy models, and compare environments.
5. **Specialized Applications of Data Science (13%)**
    - Apply natural language processing (NLP), computer vision, and optimization techniques.
    - Understand the importance of specialized data science applications.

License Information: One license provides access to the courses for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Exam Voucher: This course comes with an exam voucher.

Microsoft Certified: Azure Data Scientist Associate

SKU: MISC-38

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: Microsoft Certified: Azure Data Scientist Associate (Online **Live**)

High-level description: This ITI partner-delivered live online course course, equips learners with the skills to develop and deploy end-to-end data science solutions using Azure. Participants explore tools like Azure Machine Learning, data pipelines, and advanced analytics services. The course covers essential concepts such as building and training models, managing data workflows, and operationalizing AI solutions in cloud environments. This program is ideal for data professionals looking to leverage Azure's capabilities to create scalable, production-ready solutions. ***Contact us to schedule this course***.

Topics Covered:

1. **Introduction**
    - Overview of Azure

- Fundamental Azure Concepts
- Introduction to the Azure Portal

2. **Manage Azure Resources for Machine Learning**
    - Create an Azure Machine Learning Workspace
    - Manage Data in the Azure Machine Learning Workspace
    - Configure Compute Resources for Experiments
    - Implement Security and Access Control in Azure
    - Set up an Azure Database Workspace
3. **Run Experiments and Train Models**
    - Build Models using Azure Machine Learning Designer
    - Execute Model Training Scripts
    - Generate Metrics from Experiments
    - Create Optimal Models with Automated Machine Learning
4. **Deploy and Operationalize Machine Learning Solutions**
    - Select Compute Resources for Model Deployment
    - Deploy Models as a Service
    - Manage Models in Azure Machine Learning
    - Create Pipelines for Batch Inferencing
    - Publish Designer Pipelines as Web Services
    - Implement Pipelines using the Azure Machine Learning SDK
    - Apply MLOps Practices
5. **Implement Responsible Machine Learning (ML)**
    - Use Model Explainers for Data Interpretation
    - Ensure Fairness in Model Predictions
    - Address Privacy Considerations for Data

License Information: One license provides access to the courses.

How to Access: Instructions for accessing the courses will be emailed after purchase.

Exam Information: To purchase an exam voucher for the Microsoft the exam, visit the Microsoft Certification Exam Registration page via Microsoft Learn or Pearson VUE, select your exam, and follow the prompts to pay for the voucher. Once purchased, you can schedule your exam either online or at an authorized testing center.

CTI Custom Data Analyst Career Path Bundle

SKU: MISC-39

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: CTI Custom Data Analyst Career Path Bundle (Online OnDemand)

High-level description: Embark on the Data Analyst Career Path with our comprehensive Online Self-Paced ILT bundle of mini-courses, designed for aspiring data analysts. This course covers a wide range of topics, including data collection, analysis, visualization, and advanced techniques using tools like Microsoft Power BI, Excel, and SQL Server.

Topics Areas Included:

- Data Collection and Management
- Data Analysis and Interpretation
- Database Management and Querying
- Data Visualization and Reporting
- Excel Proficiency
- Big Data Technologies
- Advanced Analysis Techniques

Once purchased, you have 12 months' access to the course.

Course Highlights:

- Duration: 56+ hours
- Content: 350+ On-demand Videos
- Exam Prep: 400+ Prep Questions

Topics Areas Included:

- Data Visualization
- Data Cleaning
- Data Analysis Techniques

- Data Interpretation

Courses Included:

- Course 1 Microsoft SQL Server – Introduction to Data Analysis
- Course 2 Microsoft SQL Server – Querying SQL Server
- Course 3 Introduction to Microsoft Power BI
- Course 4 Microsoft Excel for Data Analysis
- Course 5 Microsoft SQL Server – Big Data
- Course 6 Microsoft SQL Service Analysis Services (SSAS)

License Information: One license provides access to the courses.

How to Access: Instructions for accessing the courses will be emailed after purchase.

CompTIA Data+ Certification

SKU: MISC-40

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: CompTIA Data+ (Online OnDemand)

CompTIA Data+ CertMaster Learn and Labs Description: CertMaster Learn is a comprehensive eLearning experience that helps learners gain the knowledge and practical skills necessary to be successful on CompTIA certification exams and in their IT career. A Learning Plan helps learners stay on track with their studies, while robust analytics bring awareness of strengths and weaknesses.

CertMaster Labs make it easy for learners to practice and apply their skills in real workplace scenarios in preparation for the certification exam. All lab activities use real equipment and software, offer feedback and hints, and provide a score based on learner inputs, ultimately guiding learners to the most correct and efficient path through job tasks.

In the integrated experience, CertMaster Labs are integrated as Study Tasks within the CertMaster Learn Learning Plan, accessible through a single login and seamless workflow.

Lessons cover all exam objectives with integrated videos:

- Hundreds of practice questions test your knowledge
- Performance-based questions apply what you've learned in a scenario

- Assisted Labs guide you step-by-step through tasks
- Applied Labs present goal-oriented scenarios and require critical thinking and analysis
- Flashcards ensure you know the terminology and acronyms required for the exam
- The Learning Plan keeps you on track with your studies

Topics Covered:

- Identifying Basic Concepts of Data Schemas
- Understanding Different Data Systems
- Understanding Types and Characteristics of Data
- Comparing and Contrasting Different Data Structures, Formats, and Markup Languages
- Explaining Data Integration and Collection Methods
- Identifying Common Reasons for Cleansing and Profiling Data
- Executing Different Data Manipulation Techniques
- Explaining Common Techniques for Data Manipulation and Optimization
- Applying Descriptive Statistical Methods
- Describing Key Analysis Techniques
- Understanding the Use of Different Statistical Methods
- Using the Appropriate Type of Visualization
- Expressing Business Requirements in a Report Format
- Designing Components for Reports and Dashboards
- Distinguishing Different Report Types
- Summarizing the Importance of Data Governance
- Applying Quality Control to Data
- Explaining Master Data Management Concepts

Labs Available:

- Assisted Lab: Navigating and Understanding Database Design
- Assisted Lab: Understanding Data Types and Conversion
- Assisted Lab: Working with Different File Formats

- APPLIED LAB: Understanding Data Structure and Types and Using Basic Statements
- Assisted Lab: Using Public Data
- Assisted Lab: Profiling Data Sets
- Assisted Lab: Addressing Redundant and Duplicated Data
- Assisted Lab: Addressing Missing Values
- APPLIED LAB: Preparing Data for Use
- Assisted Lab: Recoding Data
- Assisted Lab: Working with Queries and Join Types
- APPLIED LAB: Building Queries and Transforming Data
- Assisted Lab: Using the Measures of Central Tendency
- Assisted Lab: Using the Measures of Variability
- APPLIED LAB: Analyzing Data
- Assisted Lab: Building Basic Visuals to Make Visual Impact
- Assisted Lab: Building Maps with Geographical Data
- Assisted Lab: Using Visuals to Tell a Story
- Assisted Lab: Filtering Data
- Assisted Lab: Designing Elements for Dashboards
- Assisted Lab: Building an Ad Hoc Report
- APPLIED LAB: Visualizing Data
- Assisted Lab: De-Identifying Records

Product and License Information:

- One license provides access to CertMaster Learn for Data+ (DA0-001) with CertMaster Labs integrated throughout the course
- Access keys must be redeemed within 12 months of purchase
- Once redeemed, Learn for Data+ (DA0-001) with CertMaster Labs integrated will be valid for 12 months

How to Access CertMaster Learn integrated with CertMaster Labs: An access key and instructions will be sent via email after your purchase is complete.

Exam Voucher: This bundle includes an exam voucher.

EC-Council Certified DevSecOps Engineer (ECDE)

SKU: MISC-41

MSRP: $1399

Sales Price: $1399

Courses Include: EC-Council Certified DevSecOps Engineer (Online OnDemand)

EC-Council Certified DevSecOps Engineer (ECDE) Course Description: Enhance your DevSecOps skills with our ECDE course, which provides 24 hours of content focusing on integrating security into DevOps processes. This course covers essential components of DevSecOps, including tools and practices for securing the development pipeline. This course is blended with both theoretical knowledge as well as the practical implementation of DevSecOps in your on-prem and cloud-native (AWS and Azure) environment. The course covers integration and automation of all the major and widely used tools, processes, and methodologies of DevSecOps that help organizations to build secure applications rapidly in a DevOps environment.

Topics Covered:

1. **Introduction to DevOps and DevSecOps**
    - Fundamentals of DevOps and CI/CD pipelines
    - Key principles of DevSecOps and shifting security left
    - Integrating security practices within the DevOps lifecycle
2. **Planning and Development Phase**
    - Threat modeling and continuous integration strategies
    - Pre-commit code evaluation and secret management tools
    - Implementing Static Application Security Testing (SAST) tools
    - Automating code repository scans for vulnerabilities
3. **Build and Test Stage**
    - Building CI/CD pipelines with security controls
    - Integrating SAST and DAST (Dynamic Application Security Testing) tools
    - Designing secure code review strategies and testing frameworks
4. **Release and Deployment Stage**
    - Runtime Application Self-Protection (RASP) concepts and tools

- Implementing Infrastructure as Code (IaC) practices
- Deployment strategies (e.g., Blue-Green and Canary releases)
- Vulnerability assessment and penetration testing (VAPT)

5. **Operate and Monitor Stage**
    - Monitoring and logging with native tools (e.g., Jenkins, ELK, Splunk)
    - Securing containers and deploying Docker environments
    - Best practices for container security and compliance as code
    - Continuous vulnerability scans with cloud services (e.g., AWS, Azure)

Exam Information: The course includes an exam voucher. The ECDE exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the ECDE course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

SAFe® 6.0 DevOps

SKU: MISC-42

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: SAFe® 6.0 DevOps (Online Live)

SAFe DevOps Course Description: The SAFe® 6.0 DevOps course, delivered through an ITI partner, equips participants with the skills needed to optimize value streams and implement DevOps practices within Agile frameworks. This two-day, instructor-led program focuses on mapping value streams, identifying bottlenecks, and building implementation plans for continuous delivery. Participants learn how to integrate technical and non-technical teams, ensure smooth collaboration, and master the end-to-end flow of software delivery using DevOps principles. The course concludes with the SAFe DevOps Practitioner certification exam, included as part of the program.

Topics Covered:

1. **Introduction to DevOps and DevSecOps**
    - Fundamentals of DevOps and CI/CD pipelines
    - Key principles of DevSecOps and shifting security left

- Integrating security practices within the DevOps lifecycle

2. **Planning and Development Phase**
   - Threat modeling and continuous integration strategies
   - Pre-commit code evaluation and secret management tools
   - Implementing Static Application Security Testing (SAST) tools
   - Automating code repository scans for vulnerabilities
3. **Build and Test Stage**
   - Building CI/CD pipelines with security controls
   - Integrating SAST and DAST (Dynamic Application Security Testing) tools
   - Designing secure code review strategies and testing frameworks
4. **Release and Deployment Stage**
   - Runtime Application Self-Protection (RASP) concepts and tools
   - Implementing Infrastructure as Code (IaC) practices
   - Deployment strategies (e.g., Blue-Green and Canary releases)
   - Vulnerability assessment and penetration testing (VAPT)
5. **Operate and Monitor Stage**
   - Monitoring and logging with native tools (e.g., Jenkins, ELK, Splunk)
   - Securing containers and deploying Docker environments
   - Best practices for container security and compliance as code
   - Continuous vulnerability scans with cloud services (e.g., AWS, Azure)

Exam Information: The course includes the exam at the conclusion of the course.

License Information: One license provides access to the course. ***Contact us to schedule.***

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Cisco Certified CyberOps Associate

SKU: MISC-43

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Cisco Certified CyberOps Associate (Online OnDemand)

Cisco Certified CyberOps Associate (200-201) - Part 1 and 2 Description: This course provides a comprehensive introduction to security operations, focusing on monitoring network traffic, analyzing alerts, and detecting intrusions. It covers key topics such as threat analysis, intrusion detection systems (IDS/IPS), log management, and traffic inspection with PCAP tools. Through practical labs and configurations using both GUI and command-line tools, participants will build the skills necessary to identify, assess, and respond to network threats effectively in real-world environments.

Cisco Certified CyberOps Associate (200-201) – Part 1 (4 hours)

Chapter 1: Security Concepts

- Introduction
- Describing the CIA Triad
- Comparing Security Deployments
- Exploring Security Terminologies
- Understanding Security Concepts
- Principles of Defense-in-Depth
- Comparing Various Access Control Models
- Components of CVSS 3.1
- Challenges of Data Visibility
- Identifying Potential Data Loss
- Using the 5-Tuple to Identify a Compromised Host
- Types of Threat Detection
- Chapter 1 Quiz
- Preview

Chapter 2: Security Monitoring

- Introduction
- Exploring Attack Surface and Vulnerabilities
- Identifying Data Through Various Security Technologies
- Impact of Data Visibility Through Networking Technologies

- Interpreting Data Types in Security Monitoring
- Exploring Network-based Attacks
- Discovering Web-based Attacks
- Social Engineering Attacks
- Endpoint-based Attacks
- Evasion and Obfuscation Techniques
- Understanding Cryptography
- Encryption Algorithms
- Public Key Infrastructure (PKI)
- Chapter 2 Quiz

Cisco Certified CyberOps Associate (200-201) – Part 2 (4 hours)

Chapter 1: Host-based Analysis

- Introduction
- Delving into Endpoint Security Technologies
- Identifying Components within Microsoft Windows
- Exploring Components in the Linux Operating System
- Understanding the Attribution in an Investigation
- Identifying Various Types of Evidence
- Understanding Tampered and Untampered Disk Image
- Exploring Operating System, Application, and Command Logs
- Delving in Malware Analysis
- $7 Million Cybersecurity Scholarship by EC-Council
- Chapter 1 Quiz
- Preview

Chapter 2: Network Intrusion Analysis

- Introduction
- Mapping Events to Security Technologies

- Comparing Antimalware and IPS Alert Types
- Exploring Firewall Operations
- Interpreting Traffic Analysis on a Network
- Transaction Data (NetFlow) in the Analysis of Network Traffic
- Extracting Files from a TCP Stream using Wireshark
- Understanding the Key Elements in an Intrusion from a PCAP File
- Identifying Fields in Protocol Headers Related to an Intrusion
- Interpreting Common Artifact Elements from an Event
- Understanding Basic Regular Expressions
- Chapter 2 Quiz
- Preview

Chapter 3: Security Policies and Procedures

- Introduction
- Security Management Concepts
- Elements of Incident Response using NIST.SP800-61
- NIST.SP800-61 Incident Response Handling Process
- Discovering Network and Server Profiling
- Types of Protected Data on a Network
- Understanding the Cyber Kill Chain
- Exploring the Diamond Model of Intrusion
- Understanding SOC Metrics
- Conclusion
- Chapter 3 Quiz

License Information: One license provides access to the course.

How to Access: Instructions for accessing the course will be emailed after purchase.

PECB Certified Digital Transformation Officer (CDTO)

SKU: MISC-44

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: PECB Certified Digital Transformation Officer (Online OnDemand)

PECB Digital Transformation description: This comprehensive training course equips participants with the knowledge and skills necessary to understand and implement digital transformation strategies within their organizations. Learners will gain a deep understanding of key digital technologies such as artificial intelligence, cloud computing, big data, machine learning, IoT, and blockchain. They will also learn how to adopt appropriate methodologies for strategy implementation, support the design and monitoring of digital transformation initiatives, and foster a digital culture. The course combines theoretical concepts with practical examples to facilitate a real-world understanding of digital transformation. Participants will engage in essay-type exercises and multiple-choice quizzes, including scenario-based questions, to prepare for practical application and certification exams. Interactive discussions and collaborative learning are encouraged to enhance the learning experience.

Course Outline

- **Day 1:** Introduction to Digital Transformation
  - Overview of digital ecosystems and business models
  - Key technologies: AI, machine learning, IoT, blockchain
- **Day 2:** Planning the Digital Transformation Strategy
  - Cloud computing and big data integration
  - Situational analysis and strategy development
- **Day 3:** Implementing and Managing Transformation Initiatives
  - Risk identification and mitigation
  - Executing digital transformation projects
- **Day 4:** Monitoring Progress and Managing Cultural Change
  - Measuring outcomes and tracking KPIs
  - Communicating strategies and fostering a digital culture
- **Day 5:** Certification Exam
  - PECB Digital Transformation Officer exam with a free retake option

Learning Objectives

- Understand and apply digital transformation methodologies
- Align technology initiatives with business objectives
- Manage risks and drive cultural change effectively
- Monitor, evaluate, and refine digital strategies

License Information: One license provides access to the course.

How to Access: Instructions for accessing the course will be emailed after purchase.

Exam: The course comes with the exam and instructions for taking the exam will be provided after purchase.

PECB Certified IT Governance Manager (ISO 38500)

SKU: MISC-45

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: PECB Certified IT Governance Manager (Online OnDemand)

PECB Certified IT Governance Manager: This course provides participants with the skills to evaluate, direct, and monitor IT governance frameworks in alignment with the ISO/IEC 38500 standard. It covers core principles of IT governance, stakeholder engagement, and performance management to ensure technology initiatives align with business goals. The training combines theory with real-world case studies, preparing professionals to lead governance initiatives effectively. Participants will learn how to apply best practices in IT governance, oversee technology investments, and ensure compliance with strategic objectives. Upon completion, learners will be equipped to manage governance frameworks that support business success.

Course Outline

- Day 1: Introduction to IT Governance and ISO/IEC 38500
    - Overview of ISO 38500 principles and framework.
    - Differences between IT governance and IT management.
    - Understanding the relationship between governance and business strategy.
- Day 2: Governance Principles, Responsibilities, and Risk Management
    - Core governance principles: accountability, transparency, and responsibility.

  - Identifying and engaging stakeholders in governance processes.
  - Overview of risk management practices within IT governance.
- Day 3: Evaluating and Directing IT Governance
  - Methods for evaluating governance performance.
  - Defining responsibilities for directing IT initiatives to meet business goals.
  - Techniques for aligning IT strategy with organizational objectives.
- Day 4: Monitoring, Reviewing, and Continual Improvement
  - Monitoring governance activities for compliance and effectiveness.
  - Tools for reviewing governance processes to identify areas of improvement.
  - Developing frameworks for continuous governance improvement.
- Day 5: Certification Exam
  - Participants take the PECB ISO/IEC 38500 IT Governance Manager exam.
  - Certification fees are included, with free exam retake options available.

Learning Objectives

- Master the ISO 38500 IT governance framework and principles.
- Learn how to engage stakeholders and define governance roles.
- Develop skills to monitor and improve IT governance within an organization.
- Align IT governance efforts with business strategies and regulatory compliance.

License Information: One license provides access to the course.

How to Access: Instructions for accessing the course will be emailed after purchase.

Exam: The course comes with the exam and instructions for taking the exam will be provided after purchase.

EC-Council Hacking, Malware Analysis and Reverse Engineer Curriculum

SKU: MISC-46

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Hacking, Malware Analysis and Reverse Engineer Curriculum (Online OnDemand)

Curriculum Description: This Curriculum provides comprehensive training in malware analysis, reverse engineering, hacking, and cyber defense. It covers binary analysis, memory hacking, software protection, mobile app testing, and analyzing malicious documents. Participants gain hands-on experience with tools like Ghidra, x64dbg, Frida, and Cheat Engine, while working on .NET, Java, and Ruby applications. The curriculum also integrates Linux security practices and strategies to counter nation-state cyberattacks, preparing learners with advanced skills in intrusion analysis, threat detection, and forensic investigations.

Curriculum Outline:

Malware Analysis Fundamentals

This course provides foundational skills for analyzing and understanding malware behavior. Participants learn both static and dynamic techniques to investigate malicious software and assess its impact on systems.

Course Chapters:

- Introduction to Malware Analysis
- Static Malware Analysis Techniques
- Dynamic Behavior Analysis
- Identifying Key Indicators of Compromise
- Memory Analysis for Malware Detection

Reverse Engineering - Part 1

This introductory course covers the basics of reverse engineering, focusing on binary analysis and software behavior. Participants learn to interpret code patterns, unpack files, and explore program logic.

Course Chapters:

- Introduction to Reverse Engineering Concepts
- Lab Setup for Reverse Engineering
- Binary Analysis Fundamentals
- Understanding Program Structures
- File Unpacking Techniques
- Basic Debugging Methods

Reverse Engineering - Part 2

This advanced course builds on Part 1, teaching more complex binary analysis and debugging techniques to reveal hidden software behaviors.

Course Chapters:

- Advanced Binary Code Analysis
- Handling Packed and Obfuscated Binaries
- Intermediate Debugging Techniques
- Software Patching Methods
- Reverse Engineering Multi-Stage Malware
- Modifying Program Logic

Malware Analysis of Malicious Documents

This course focuses on detecting and analyzing malware embedded within documents, such as PDFs and Microsoft Office files.

Course Chapters:

- Introduction to Document-Based Malware
- Static and Dynamic Analysis of Documents
- Extracting Malicious Payloads
- Analyzing Macros and Embedded Scripts
- Behavioral Analysis of Malicious Documents

Reverse Engineering 3: x64dbg Graphical Static Analysis

This course covers the use of x64dbg, a popular tool for binary analysis, to uncover hidden software behavior.

Course Chapters:

- Introduction to x64dbg Interface
- Static Binary Analysis Techniques
- Identifying Software Vulnerabilities
- Debugging with x64dbg
- Practical Exercises with x64dbg

Reverse Engineering, Memory Hacking, and Software Protection

This course explores memory manipulation and techniques to protect or bypass software defenses.

Course Chapters:

- Memory Structures and Hacking Basics
- Analyzing Software in Memory
- Implementing Software Protections
- Patching and Anti-Debugging Techniques
- Practical Memory Hacking Exercises

Reverse Engineering & Malware Analysis of .NET & Java

This course focuses on dissecting and analyzing .NET and Java applications for vulnerabilities and malicious code.

Course Chapters:

- Overview of .NET and Java Architectures
- Tools for .NET and Java Reverse Engineering
- Identifying Vulnerabilities in Managed Code
- Malware Analysis in .NET and Java Applications
- Practical Dissection of Malicious Code

Practical Linux for Security Professionals

This course provides security professionals with essential Linux skills for cybersecurity operations, covering administration, scripting, and tools.

Course Chapters:

- Linux Fundamentals for Security Tasks
- Command-Line Tools for Security Operations
- Network Monitoring and Management
- Security Scripting with Bash
- Practical Cybersecurity Exercises on Linux

Cyber Warfare - Defense Against Nation-State Threats

This course addresses tactics and techniques to detect and mitigate cyber threats posed by nation-state actors.

Course Chapters:

- Understanding Nation-State Cyber Threats
- Tools and Techniques for Cyber Defense
- Attribution and Threat Intelligence
- Incident Response to Nation-State Attacks
- Building Effective Defense Strategies

Learn Ethical Hacking and Reverse Engineering

This course blends ethical hacking techniques with reverse engineering to provide a comprehensive security toolkit.

Course Chapters:

- Introduction to Ethical Hacking and Reverse Engineering
- Identifying Software Vulnerabilities
- Exploiting and Mitigating Vulnerabilities
- Reverse Engineering for Offensive Security
- Practical Hacking Challenges

Reverse Engineering 2: Windows GUI Programs

This course focuses on the reverse engineering of Windows graphical applications, uncovering their internal logic and behavior.

Course Chapters:

- Basics of Windows GUI Programs
- Reverse Engineering Windows Executables
- Debugging GUI Applications
- Analyzing Event-Driven Programs
- Practical Reverse Engineering Exercises

Reverse Engineering 4: Software Protection

This course covers techniques to analyze and implement software protection mechanisms.

Course Chapters:

- Understanding Software Protection Concepts
- Analyzing Anti-Tamper Mechanisms
- Implementing Software Obfuscation
- Defeating Anti-Debugging Techniques
- Practical Software Protection Exercises

Reverse Engineering: Frida For Beginners

This course introduces Frida, a dynamic instrumentation toolkit, for advanced application analysis.

Course Chapters:

- Introduction to Frida and Dynamic Instrumentation
- Setting Up Frida for Application Analysis
- Injecting Scripts into Applications
- Analyzing and Modifying Application Behavior
- Practical Exercises with Frida

Mobile Penetration Testing (and Reverse Engineering) of Android Applications

This course covers penetration testing techniques for Android apps, with a focus on reverse engineering.

Course Chapters:

- Introduction to Android Application Architecture
- Setting Up an Android Testing Environment
- Reverse Engineering Android Apps
- Identifying and Exploiting Vulnerabilities
- Practical Penetration Testing Exercises

Reverse Engineering: Create Your Own GUI CrackMe using C++

This course teaches participants how to create and reverse engineer their own “CrackMe” programs using C++.

Course Chapters:

- Introduction to CrackMe Challenges

- Building GUI Programs in C++
- Implementing Software Protections
- Reverse Engineering Your CrackMe Program
- Practical Reverse Engineering Exercises

Reverse Engineering and Memory Hacking with Cheat Engine

This course explores how to use Cheat Engine for memory hacking and game modification.

Course Chapters:

- Introduction to Cheat Engine
- Memory Scanning Techniques
- Modifying Program Variables in Memory
- Reverse Engineering for Game Hacking
- Practical Cheat Engine Exercises

Reverse Engineering: Ghidra for Beginners

This course provides an introduction to Ghidra, a popular reverse engineering tool developed by the NSA.

Course Chapters:

- Introduction to Ghidra and Its Interface
- Setting Up Ghidra for Analysis
- Disassembling and Analyzing Binaries
- Identifying Vulnerabilities with Ghidra
- Practical Exercises in Ghidra

Ethical Hacking with Ruby for Beginners (and Reverse Engineering Ruby Applications)

This course covers ethical hacking techniques using Ruby, with a focus on reverse engineering Ruby applications.

Course Chapters:

- Introduction to Ruby for Hacking and Security
- Building and Analyzing Ruby Applications

- Identifying and Exploiting Vulnerabilities in Ruby Code
- Reverse Engineering Ruby Scripts
- Practical Hacking Exercises with Ruby

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

CTI Web Design Curriculum

SKU: MISC-47

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: CTI Web Design Curriculum (Online OnDemand)

PECB Certified IT Governance Manager: This Curriculum provides a complete learning journey for aspiring web designers. It covers the fundamentals of HTML, CSS, and JavaScript to build responsive websites, with additional modules focusing on UX/UI design, Adobe Photoshop, and Adobe XD for visual content creation. Participants gain hands-on experience with creating interactive elements, optimizing websites for mobile, and managing digital portfolios. This career path equips learners with both creative and technical skills to design functional, aesthetically pleasing websites that meet modern standards.

Curriculum Outline (34+ hours):

Course: 1 Web Fundamentals
Module 1 - HTML5-CSS3 Introduction
- Introduction to the Course

Module 2 - The Internet and World Wide Web
- The Internet and World Wide Web

Module 3 - HTML Fundamentals
- Web Development Tools
- HTML Skeletons
- Paragraph Elements
- Phrase Elements
- HTML Comments
- HTML Entities

Module 4 - CSS Fundamentals
- CSS Fundamentals

- Inline Styles
- Embedded Style Sheets
- External Style Sheets
- Selector Types
- Decendent Selectors
- CSS Colors
- ID Versus Class
- CSS Text Properties
- CSS Box Model

Module 5 - Images and Links

- Images and Links
- Image Elements
- Images with Hyperlinks
- Open Links in New Tab
- Telephone and Email Links
- Validate and Debug

Module 6 - Responsive Design

- Responsive Design
- Fixed Layouts
- Viewport Meta Element
- Usefull CSS Styles

Module 7 - Media Queries

- More About Responsive Design
- Global Changes
- Mobile Devices
- Manipulate Logo

Module 8 - Layouts

- Layouts
- Tablets Part 1
- Tablets Part 2
- Styling Part 1
- Styling Part 2
- Styling Part 3
- Styling Part 4
- Styling Part 5

- Styling Part 6

Module 9 - Tables

- Tables Part 1
- Tables Part 2

Module 10 - Multimedia

- Multimedia
- Multimedia Part 2
- Multimedia Part 3

Module 11 - Forms and JavaScript

- Forms and JavaScript
- jQuery
- Styling Tables

Module 12 - The Web Server

- The Web Server

Module 13 - Programming and JavaScript

- Data Types
- Global Methods
- Variables
- Conditional Statements
- Loops
- Operators

Module 14 - The Calculator

- Calculator Part 1
- Calculator Part 2
- Calculator Part 3
- Calculator Part 4
- Calculator Part 5
- Calculator Part 6
- Calculator Part 7

Course: 2 Javascript

Module 1: Introduction To Javascript

- Introduction
- Java Script From The Dawn Of The Web Part 1
- Java Script From The Dawn Of The Web Part 2
- Getting The Right Tools
- Creating Your First JavaScript Program Part 1

- Creating Your First JavaScript Program Part 2

Module 2: Core Concepts And Syntax

- The Structure And Content Part 1
- The Structure And Content Part 2
- Naming And Casing Best Practices
- Understanding Variables Part 1
- Understanding Variables Part 2
- Understanding Variables Part 3
- Working With Operators Part 1
- Working With Operators Part 2
- Working With Loops Part 1
- Working With Loops Part 2
- Creating Functions Part 1
- Creating Functions Part 2
- Understanding Types And Objects Part 1
- Understanding Types And Objects Part 2
- Understanding Types And Objects Part 3
- Understanding Types And Objects Part 4
- Understanding Types And Objects Part 5

Module 3: Getting A Handle On The DOM

- Introduction To The HTML Document Object Model
- Accessing DOM Elements
- Changing DOM Elements
- Creating DOM Elements
- Responding To Events Part 1
- Responding To Events Part 2

Module 4: Working With Libraries

- Introduction To Libraries
- Installing And Using jQuery Part 1
- Installing And Using jQuery Part 2
- Modifying Web Pages Using jQuery Part 1
- Modifying Web Pages Using jQuery Part 2
- Conclusion

Course: 3 Adobe Photoshop

Module 1: Getting Started

- Instructor Intro
- Course Intro
- Open Images
- Get Familiar with Work Space
- Zoom and Pan
- Undo and Save Pt 1
- Undo and Save Pt 2
- Resize and Resolution
- Crop and Straighten
- Expand the Canvas
- Basic Image Corrections

Module 2: Layers and More

- Layer Basics
- Resizing Layers
- Adding Text and Images
- Layer Styles
- Photo Merge and Panoramic Images
- Camera Raw
- Camera Raw Continued and Adjustment Layers
- Selection Basics

Module 3: Editing, Techniques and More

- Raw File XMP
- Masks
- Puppet Warp and Alpha Channel
- Typography
- Vector Drawing Techniques
- Advanced Compositing

Course: 4 – Adobe XD

Module 1 - Welcome to Adobe XD 2022

- Welcome to Adobe XD 2022
- What is Adobe XD 2022

Module 2 - Adobe XD 2022 Overview

- Adobe XD 2022 Overview

Module 3 - Designing in a Project with Adobe XD 2022

- Adobe XD 2022 Project Overview

- Designing Your First Screen in Adobe XD 2022

Module 4 - Assets, Reusable Styles, and Responsive Resize in Adobe XD 2022

- Assets and Reusable Styles in Adobe XD 2022
- Responsive Resize in Adobe XD 2022

Module 5 - Images and Visual Effects in Adobe XD 2022

- Imports, Images, and Masks in Adobe XD 2022
- Special Visual Effects in Adobe XD 2022

Module 6 - Making Interactive Buttons in Adobe XD 2022

- Plugins in Adobe XD 2022
- Stacks in Adobe XD 2022
- Components in Adobe XD 2022
- Repeat Grid in Adobe XD 2022

Module 7 - Grouped Imports and Scroll Groups in Adobe XD 2022

- Grouped imports in Adobe XD 2022
- Scroll Groups in Adobe XD 2022

Module 8 - Prototyping and Animations in Adobe XD 2022

- Prototyping with Adobe XD 2022
- Animations in Adobe XD 2022

Module 9 - Exporting and Sharing with Adobe XD 2022

- Exports in Adobe XD 2022
- Adobe XD 2022 Conclusion

Course: 5 – Adobe Stock

Module 1 - Adobe Stock

- Instructor Info
- Course Info
- Interface and Features
- Images
- Videos and Licensing
- Templaes and Premium
- Contributing Content
- Best Practices when Contributing

Course: 6 – Adobe Spark

Adobe Spark: Module 1

- Instructor Intro

- Course Intro
- Web Based vs Mobile Device
- How to Access Spark
- Branding in Spark

Adobe Spark: Module 2

- Using Spark Post
- Uploading Content from Post for Exporting
- Using Spark Video
- Exporting Finished Videos
- Using Spark Page
- Putting Spark Pages on the Web

Course: 7 – Adobe Behance

Get Creative With Adobe Behance

- Instructor Introduction
- Adobe Behance Course Introduction
- Adobe Behance - A Creative, Collaborative Application
- Using The Profile page
- Creating A Project
- Exploring The Jobs Section

Course: 8 – Adobe Portfilio

Module 1 - Adobe Portfolio Website Editor

- Instructor Introduction
- Getting Started With Adobe Portfolio
- Creating A Website To Showcase Your Work
- Importing And Syncing From Adobe Lightroom
- Customizing Your Landing Page

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Certified Application Security Engineer (CASE) - JAVA

SKU: MISC-48

MSRP: $1,399

Sales Price: $1,399

Courses Include: EC-Council Certified Application Security Engineer (CASE) (Online OnDemand)

EC-Council Certified Application Security Engineer (CASE) – Java Course Description: This 3-day course equips developers with essential skills in secure coding and software development. Focusing on Java applications, participants learn to identify and mitigate vulnerabilities, such as SQL injection and cross-site scripting (XSS), through hands-on labs. The course emphasizes secure coding practices, risk assessment, and application security frameworks to build resilient software and protect against cyber threats.

Topics Covered:

- **Understanding Application Security, Threats, and Attacks**: Explore common security threats, attack vectors, and the importance of secure software development.
- **Security Requirements Gathering**: Learn how to define and capture security needs early in the Software Development Lifecycle (SDLC).
- **Secure Application Design and Architecture**: Focus on building secure architectures by integrating security principles into the design phase.
- **Secure Coding Practices for Input Validation**: Implement methods to prevent injection attacks by sanitizing user inputs.
- **Secure Coding Practices for Authentication and Authorization**: Learn to enforce secure identity verification and access control mechanisms.
- **Secure Coding Practices for Cryptography**: Implement cryptographic methods to protect data in storage and transit.
- **Secure Coding Practices for Session Management**: Manage user sessions securely to prevent hijacking and misuse.
- **Secure Coding Practices for Error Handling**: Handle application errors effectively to avoid exposing sensitive information.
- **Static and Dynamic Application Security Testing (SAST & DAST)**: Use automated tools and manual testing to detect vulnerabilities in code and runtime.
- **Secure Deployment and Maintenance**: Ensure secure software deployment practices and continuous security monitoring post-release.

This course offers hands-on labs and covers both SAST and DAST to prepare learners for building, testing, and maintaining secure applications throughout the SDLC.

Exam Information: The course includes an exam voucher. The exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Certified Application Security Engineer (CASE) - .Net

SKU: MISC-49

MSRP: $1,399

Sales Price: $1,399

Courses Include: EC-Council Certified Application Security Engineer (CASE) (Online OnDemand)

EC-Council Certified Application Security Engineer (CASE) – Java Course Description: This 3-day course equips developers with essential skills in secure coding and software development. Focusing on Java applications, participants learn to identify and mitigate vulnerabilities, such as SQL injection and cross-site scripting (XSS), through hands-on labs. The course emphasizes secure coding practices, risk assessment, and application security frameworks to build resilient software and protect against cyber threats.

Topics Covered:

- **Understanding Application Security, Threats, and Attacks**: Explore common security threats, attack vectors, and the importance of secure software development.
- **Security Requirements Gathering**: Learn how to define and capture security needs early in the Software Development Lifecycle (SDLC).
- **Secure Application Design and Architecture**: Focus on building secure architectures by integrating security principles into the design phase.
- **Secure Coding Practices for Input Validation**: Implement methods to prevent injection attacks by sanitizing user inputs.
- **Secure Coding Practices for Authentication and Authorization**: Learn to enforce secure identity verification and access control mechanisms.
- **Secure Coding Practices for Cryptography**: Implement cryptographic methods to protect data in storage and transit.

- **Secure Coding Practices for Session Management**: Manage user sessions securely to prevent hijacking and misuse.
- **Secure Coding Practices for Error Handling**: Handle application errors effectively to avoid exposing sensitive information.
- **Static and Dynamic Application Security Testing (SAST & DAST)**: Use automated tools and manual testing to detect vulnerabilities in code and runtime.
- **Secure Deployment and Maintenance**: Ensure secure software deployment practices and continuous security monitoring post-release.

This course offers hands-on labs and covers both SAST and DAST to prepare learners for building, testing, and maintaining secure applications throughout the SDLC.

Exam Information: The course includes an exam voucher. The exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Certified Web Application Hacking and Security

SKU: MISC-50

MSRP: $1,399

Sales Price: $1,399

Courses Include: EC-Council Certified Application Security Engineer (CASE) (Online OnDemand)

EC-Council Certified Web Application Hacking and Security Course Description: This 3-day course provides hands-on training in identifying, exploiting, and mitigating vulnerabilities in web applications. Participants learn offensive and defensive techniques, including SQL injection, cross-site scripting (XSS), and other OWASP Top 10 vulnerabilities. The course emphasizes real-world scenarios, enabling learners to both conduct penetration tests and implement secure coding practices to protect against common attacks.

Topics Covered:

1. Advanced Web Application Penetration Testing
    a. Explore advanced techniques to assess and exploit web vulnerabilities.
2. SQL Injection (SQLi)
    a. Manipulate SQL queries to access or modify backend databases.

3. Cross-Site Scripting (XSS)
    a. Inject malicious scripts into web applications (Reflected, Stored, and DOM-based).
4. Cross-Site Request Forgery (CSRF)
    a. Exploit user sessions to perform unauthorized actions via GET or POST requests.
5. Server-Side Request Forgery (SSRF)
    a. Force a server to make unauthorized internal or external requests.
6. Security Misconfigurations
    a. Identify and exploit improperly configured security settings.
7. Directory Browsing and Bruteforcing
    a. Discover hidden directories and files through brute-force attacks.
8. CMS Vulnerability and Network Scanning
    a. Scan content management systems (CMS) and networks for vulnerabilities.
9. Authentication Bypass
    a. Exploit authentication weaknesses to gain unauthorized access.
10. Web Application Enumeration
    a. Gather information to identify potential vulnerabilities in web apps.
11. Dictionary Attack
    a. Use automated wordlists to crack passwords or gain access.
12. Insecure Direct Object Reference (IDOR)
    a. Access restricted data by manipulating input fields or parameters.
13. Broken Access Control
    a. Bypass access control mechanisms to gain unauthorized access.
14. Local and Remote File Inclusion (LFI/RFI)
    a. Include malicious files locally or remotely to compromise systems.
15. Arbitrary File Upload and Download
    a. Upload unauthorized files or download sensitive data.
16. Using Components with Known Vulnerabilities
    a. Exploit outdated libraries or frameworks with known flaws.
17. Command Injection and Remote Code Execution
    a. Inject commands or execute code to gain control over systems.
18. Privilege Escalation
    a. Exploit vulnerabilities to gain elevated access or permissions.
19. File Tampering and Log Poisoning
    a. Modify files or logs to hide malicious activities.
20. Weak SSL Ciphers and Cookie Modification
    a. Exploit weak encryption or manipulate cookies to hijack sessions.
21. Source Code and HTTP Header Analysis
    a. Analyze code and headers to uncover security flaws.

22. Session Fixation and Clickjacking
    a. Hijack active sessions or trick users into performing unintended actions.

Exam Information: The course includes an exam voucher. The exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Certified Scrum Product Owner

SKU: MISC-51

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: ITI Partner Delivered Certified Scrum Product Owner (Online LIVE)

ITI Partner Delivered Online Live Certified Scrum Product Owner (CSPO) course description: The Certified Scrum Product Owner (CSPO) certification course, accredited by the Scrum Alliance, provides a thorough understanding of Agile principles and the Scrum framework, focusing specifically on the Product Owner role. This course is ideal for professionals looking to enhance their skills in product management and Agile project delivery. ***Please contact us to schedule this course.***

Course Outline:

1. **Agile and Scrum Foundations:**
    - Introduction to Agile principles and the Scrum framework.
    - Understanding the values and practices that drive Agile methodologies.
2. **Roles and Responsibilities of a Product Owner:**
    - Defining the role of the Product Owner within a Scrum team.
    - Collaborating with stakeholders and development teams to maximize product value.
    - Establishing and communicating a clear product vision.
3. **Product Backlog Management:**
    - Techniques for creating, prioritizing, and maintaining the product backlog.
    - Writing effective user stories and acceptance criteria.
    - Backlog refinement processes to ensure readiness for sprints.

4. **Product Vision and Strategy:**
    - Developing a strategic product vision that aligns with business goals.
    - Techniques for communicating and maintaining vision.
    - Creating a product roadmap to guide development efforts.
5. **Release Planning and Tracking:**
    - Planning product releases and setting realistic expectations.
    - Tracking progress and adjusting plans to meet changing requirements.
    - Ensuring continuous delivery of valuable products.
6. **Customer and Stakeholder Engagement:**
    - Identifying and engaging key stakeholders.
    - Gathering and incorporating feedback to drive product improvements.
7. **Practical Application and Case Studies:**
    - Real-world scenarios and case studies to apply Scrum and Agile practices.
    - Group activities and discussions to reinforce learning.

Course Features:

- **Interactive Sessions:** Engaging lectures, group discussions, and hands-on exercises.
- **Practical Exercises:** Real-world scenarios to practice and apply Scrum principles.
- **Expert Instructors:** Learn from experienced Scrum trainers and practitioners.
- **Exam Preparation:** Comprehensive preparation for the CSPO certification exam.
- **Certification Exam:** Opportunity to take the CSPO exam at the end of the course.

Participants will gain practical skills to manage and optimize product development processes, ensuring alignment with customer needs and business objectives. Completing this course will prepare you for the CSPO certification exam, validating your expertise and enhancing your career in Agile project management.

Product Information:

- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

Exam Information: This course includes the exam at the end of the course.

CTI Software Development Lifecycle (SDLC) and Software Testing Lab Bundle

SKU: MISC-52

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: CTI Fundamentals of the Software Development Lifecycle (SDLC) and Software Testing Lab (Online OnDemand)

ITI Partner Delivered Online Live Certified Scrum Product Owner (CSPO) course description: This bundle combines the Software Testing Fundamentals (98-379) lab with the Fundamentals of the Software Development Lifecycle (SDLC) course to provide both practical and theoretical skills in software testing and development processes. The 98-379 lab offers hands-on experience with test automation, performance testing, bug tracking, and project management using Microsoft Visual Studio. The SDLC course adds a broader understanding of the development lifecycle, covering planning, design, development, testing, and deployment phases, ensuring participants can see the bigger picture of where testing fits within modern software projects. Together, this bundle equips students with the tools to effectively plan and manage testing activities throughout the software lifecycle. It's ideal for learners pursuing roles in software quality assurance, testing, and development, offering comprehensive knowledge and hands-on experience in both testing fundamentals and the SDLC framework.

Course Outline (2+ hours):

Module 1 – Introduction to SDLC

- Definition and Purpose of SDLC
- Overview of the SDLC Process

Module 2 – Phases of the SDLC

- Requirement Gathering and Analysis
- Planning Phase
- Design Phase
- Development Phase
- Testing Phase
- Deployment Phase
- Maintenance Phase

Module 3 – SDLC Methodologies

- Waterfall Methodology
- Agile Methodology
- Lean Methodology

- DevOps Methodology
- DevOps vs. Agile
- Which Methodology to Use

Module 4 – Role of QA in SDLC

- Importance of QA in the Software Development Process
- QA Methodologies and Tools

Module 5 – Best Practices for Effective SDLC Management

- Project Management and Communications
- Risk Management in the SDLC
- Continuous Improvement and Feedback Loops
- Course Closeout

Lab Outline (15 hours):

- Fundamentals of Software Programming
- Unit and Integration Testing
- Performance Testing and Testing Tools
- Creating Use Case Diagrams
- Implementing Test-Driven Development
- Exploratory Testing
- Logging Bugs and Defects
- Defining and Implementing Test Automation Strategies
- Managing Software Testing Projects and Test Scripts
- Detecting and Managing Software Defects

This hands-on lab offers essential training in software testing principles and methodologies using Microsoft Visual Studio. Through practical exercises, participants will gain skills in creating and automating software tests, managing testing projects, working with bugs, and applying testing frameworks like Test-Driven Development. The lab covers key areas such as unit testing, performance testing, exploratory testing, and test automation strategies, ensuring learners develop a comprehensive understanding of software verification and validation processes. While the 98-379 certification exam is

no longer officially available, the skills covered remain highly relevant for today's software testing and quality assurance roles.

Product Information:

- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

EC-Council Linux Crash Course for Beginners

SKU: MISC-53

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Linux Crash Course for Beginners (Online OnDemand)

Course description: This 1-day course provides a practical introduction to Linux, focusing on essential commands, file management, and system navigation. Designed for those new to Linux, it equips participants with the foundational skills needed for cybersecurity operations, insider threat scenarios, and mission readiness environments. Through hands-on learning, students will gain confidence working within Linux-based systems critical to modern security roles.

Course Outline (6+ hours):

Chapter 1: Introduction

- Syllabus Overview

Chapter 2: Basic Linux Administration

- What is Linux?
- VirtualBox Installation and Lab Setup
- Creating Virtual Machines and Installing Linux (CentOS Versions)
- Using Putty to Connect to Linux VMs
- File System and Structure Overview
- File and Directory Commands (create, navigate, manage)
- Permissions, Ownership, and Pipes (|)
- Getting Help with Commands (man, whatis, --help)

Chapter 3: Advanced Linux Administration

- File Maintenance (cp, rm, mv) and Display Commands (cat, less)

- Filters and Text Processing (e.g., cut, grep, awk)
- User Account Management (useradd, usermod) and Sudo Access
- System Utilities (date, uptime, processes)
- Shell Scripting Basics
- Network Files and Commands (ping, ifconfig, netstat, tcpdump)
- System Updates and Repository Management (rpm, yum)

Chapter 4: Additional Resources

- Troubleshooting Putty Connection
- Bonus Lecture

Product Information:

- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

EC-Council Data Science Bundle

SKU: MISC-54

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Data Science Bundle (Online OnDemand)

Course description: This Data Science Bundle provides participants with foundational and advanced skills in SQL, Python, R programming, and cloud-based analytics using AWS. The bundle ensures professionals can apply core data science techniques relevant to cybersecurity and insider threat analysis workflows. The courses cover data querying, statistical modeling, machine learning, and practical cloud-based analytics, equipping participants with hands-on skills for effective data-driven decision-making.

Bundle Outline and Topics Covered:

Python for Data Science and Machine Learning

- Duration: 12 hours
- Covers Python tools and libraries such as NumPy, Pandas, and Matplotlib.
- Introduction to machine learning models with Python.
- Exercises on data cleaning, processing, and visualization.

- Applications of supervised and unsupervised learning techniques.

Hands-On SQL for Data Science

- Duration: 4 hours
- Focuses on querying, filtering, and joining tables.
- Advanced SQL techniques: subqueries, window functions, and data aggregation.
- Data preparation for analytics workflows.
- Practical exercises to construct complex queries.

Applied R Programming Diploma

- Duration: 5 hours
- Introduction to R programming for data analysis and visualization.
- Creating statistical models and forecasts.
- Hands-on work with data visualizations using ggplot2.

Data Science with AWS

- Duration: 8 hours
- Overview of AWS cloud services for data science and storage (S3, Redshift).
- Introduction to AWS SageMaker for building machine learning models.
- Implementing real-time analytics using AWS tools.

Product Information:

- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

EC-Council Mastering Microsoft Sentinel

SKU: MISC-55

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Mastering Microsoft Sentinel (Online OnDemand)

Course description: This course provides hands-on training in using Microsoft Sentinel, a cloud-native SIEM and SOAR platform, to enhance threat detection, incident response, and automation capabilities. Participants will learn how to configure Sentinel, develop analytics rules, and automate workflows to streamline security operations. The course aligns with SOC

workflows and prepares learners for Microsoft's SC-200 Security Operations Analyst certification, equipping them to proactively manage modern cyber threats.

Content Overview for Mastering Microsoft Sentinel (5+ hours)

Chapter 1: Defender for Cloud

- Introduction to Defender for Cloud
- Respond to Alerts in Defender for Cloud
- Threat Mitigation with Defender for Cloud
- Section Summary
- Chapter 1 Quiz

Chapter 2: Microsoft Sentinel Introduction

- Section Introduction
- Introduction to Microsoft Sentinel
- Design and Configure Microsoft Sentinel Workspace
- Data Connectors in Sentinel
- Section Summary
- Chapter 2 Quiz

Chapter 3: Microsoft Sentinel Management

- Section Introduction
- Microsoft Sentinel Analytics Rules
- Data Classification and Normalization
- Hunting Capabilities in Microsoft Sentinel
- Section Summary
- Chapter 3 Quiz

Chapter 4: SOAR in Sentinel

- Section Introduction
- Configure SOAR in Sentinel
- Manage Microsoft Sentinel Incidents
- Sentinel Overview

- Section Summary
- Chapter 4 Quiz

Chapter 5: Course Conclusion

- Section Introduction
- Microsoft Security Operations Analyst Certification Prep Summary
- Microsoft Security Operations Analyst Certification Prep Content
- Section Summary
- Chapter 5 Quiz

Product Information:

- Access keys must be redeemed within 12 months of purchase
- Once redeemed, licenses will be valid for 12 months

Teramind Insider Threat Detection (UAM) Course

SKU: MISC-56

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: Teramind Insider Threat Detection Course (Online OnDemand)

Course description: The Teramind Insider Threat Detection Course equips participants with essential tools and techniques to identify and manage insider threats. It focuses on using behavioral rules, monitoring tools, and reports to detect and prevent risky activities. The course covers the configuration of custom monitoring settings, setting up rules and policies to track potentially concerning behaviors, and using OMNI dashboards and employee reports for quick investigations. Additionally, participants will learn to leverage business intelligence (BI) reports for proactive trend analysis. Upon completion, learners earn a Teramind Certificate.

Course Outline

- **Introduction to Rules and Policies for Insider Threat Detection**
    - Creating and customizing policies to monitor for risky activities.
    - Configuring rules to detect suspicious behaviors in real time.
- **Using OMNI and Employee Reports for Investigations**
    - Navigating the OMNI interface for quick access to insights.
    - Reviewing employee activity reports to identify anomalies.

- **Customizing Monitoring Settings and Access Controls**
    - Setting up and adjusting monitoring preferences to meet organizational needs.
    - Managing access controls to secure critical data.
- **Using BI Reports for Trend Analysis**
    - Leveraging business intelligence tools to detect behavioral patterns.
    - Generating reports for proactive risk management.
- **Course Completion and Certification**
    - Final knowledge check to assess understanding.
    - Issuance of Teramind Insider Threat Detection Certificate upon passing.

Product Information:

Information will be provided upon bundle purchase.

Administering Information Protection and Compliance (Purview Insider Risk Management) in Microsoft 365

SKU: MISC-57

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: Administering Information Protection and Compliance (Purview) in Microsoft (Online Live)

Course description: The This course equips IT professionals with the skills to manage data protection, governance, and compliance across Microsoft 365 environments, with a focus on insider risk management. Participants will explore Microsoft Purview (formerly known as Insider Risk Management) to detect, manage, and mitigate potential insider threats while maintaining compliance with regulatory standards. The course covers data loss prevention (DLP), sensitive information classification, retention policies, and compliance alerts to ensure critical data is protected. Learners will also gain hands-on experience in automating audits and compliance workflows, helping organizations maintain security while mitigating insider risks within Microsoft 365 applications. This course helps prepare learners for the Microsoft Information Protection Administrator (SC-400) certification exam.

This four-day course focuses on implementing data protection, compliance, and governance across Microsoft 365 environments. It prepares participants for the SC-400: Microsoft Information Protection Administrator exam, equipping them with the skills to safeguard sensitive data, manage insider risks, and maintain compliance with regulations. ***Please contact us to schedule this live course.***

Course Outline

1. **Introduction to Information Protection and Data Lifecycle Management**
    - Identify and protect data across the organization
    - Implement governance frameworks for data loss prevention
    - Manage data retention and archival policies
2. **Data Classification for Protection and Governance**
    - Use Microsoft Purview to classify data with sensitive information types
    - Leverage **trainable classifiers** for automated labeling
    - Monitor and report on data classification activities
3. **Create and Manage Sensitive Information Types**
    - Develop and use custom sensitive information types
    - Implement **document fingerprinting** and keyword dictionaries
    - Manage sensitive information to comply with privacy regulations
4. **Microsoft 365 Encryption**
    - Understand encryption at rest and in transit
    - Manage customer keys with Microsoft Purview
    - Deploy Purview Message Encryption for secure email
5. **Data Loss Prevention (DLP) Policies**
    - Implement DLP policies for **Power Platform and Defender for Cloud Apps**
    - Use optical character recognition (OCR) for identifying sensitive content
    - Manage DLP alerts and policy violations through Purview
6. **Managing Insider Risk with Microsoft Purview**
    - Develop and enforce insider risk policies
    - Monitor employee activities to detect anomalous behavior
    - Use **adaptive protection strategies** to respond to insider risks
7. **eDiscovery and Compliance Management**
    - Configure and manage **eDiscovery (Standard and Premium)**
    - Search for, retrieve, and secure data in Microsoft 365
    - Use the **Compliance Manager dashboard** to monitor regulatory compliance
8. **Audit and Communication Compliance**

- Set up **audit logs and alerts** for incident tracking
- Manage internal communications with compliance workflows
- Investigate and resolve compliance issues using Microsoft Priva

Product Information:

Information will be provided upon bundle purchase. Upon successful course completion, participants will receive an exam voucher for the Microsoft Information Protection Administrator (SC-400) certification exam.

EC-Council Certified SOC Analyst

SKU: MISC-58

MSRP: $1,399

Sales Price: $1,399

Courses Include: EC-Council Certified SOC Analyst (Online OnDemand)

CSA Description: Prepare for a career in a Security Operations Center (SOC) with our CSA course, which provides 24 hours of content focusing on SOC operations. This course covers the essentials of working in a SOC, from understanding SOC infrastructure to performing advanced incident detection and response. The lab-intensive CSA program emphasizes the holistic approach to deliver advanced knowledge of how to identify and validate intrusion attempts.

Course Outline / Topics Covered:

- **Introduction to SOC Operations**
  Understand the role of a SOC, its infrastructure, and core functions.
- **Cyber Threats, Indicators of Compromise (IoCs), and Attack Methodologies**
  Learn to recognize key cyber threats and attack patterns through IoCs and adversarial tactics.
- **Incident Detection with SIEM (Security Information and Event Management)**
  Develop skills to use SIEM tools for identifying, correlating, and managing security events.
- **Incident Response and Mitigation Strategies**
  Gain expertise in incident handling processes, from initial detection to containment and recovery.
- **Threat Intelligence, Modeling, and Threat Hunting Techniques**
  Leverage threat intelligence to predict and hunt for threats proactively.

- **Post-Incident Response and Reporting**
  Master best practices for post-incident analysis, reporting, and process improvement.

Exam Information: The course includes an exam voucher. The CSA exam can be taken online through the EC-Council's remote proctoring service or at authorized testing centers.

License Information: One license provides access to the CSA course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course will be emailed after purchase.

Link to brochure: https://www.eccouncil.org/wp-content/uploads/2023/01/CSA-Brochure.pdf

CTI PMI Risk Management Professional (PMI-RMP)

SKU: MISC-59

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: CTI PMI Risk Management Professional (PMI-RMP) (Online OnDemand)

PMI Risk Management Professional (PMI-RMP) Course Description: This course is tailored to provide comprehensive training in project risk management, aligning with the latest PMI-RMP exam guidelines. It covers essential concepts, tools, and techniques needed for effective risk management, including risk strategy, planning, stakeholder engagement, and specialized risk analyses. The course enhances your abilities in risk identification, assessment, and mitigation through practical examples and real-world scenarios, aiming for successful project outcomes. Additionally, it delves into the fundamentals of risk management, effective strategies for risk identification and assessment, techniques for risk mitigation, stakeholder engagement processes, and advanced methods for specialized analyses, equipping you with the skills to ensure project success and stakeholder satisfaction. This course is ideal for project managers looking to specialize in risk management or professionals seeking to bolster their risk management capabilities. This course is 8+ hours delivered over 28 videos within 10 topics, and includes 100 exam preparation questions.

Course Outline (8+ hours)

- Module 1: Risk Management Fundamentals
  - Instructor Intro
  - Course Intro

    - Risk Management Fundamentals Pt 1
    - Risk Management Fundamentals Pt 2
- Module 2: Test Requirements
    - Test Requirements
- Module 3: Test Domains
    - Test Domains Pt 1
    - Test Domains Pt 2
- Module 4: Risk Strategy and Planning
    - Risk Strategy and Planning Pt 1
    - Risk Strategy and Planning Pt 2
- Module 5: Stakeholder Engagement
    - Stakeholder Engagement Pt 1
    - Stakeholder Engagement Pt 2
    - Stakeholder Engagement Pt 3
    - Stakeholder Engagement Pt 4
- Module 6: Risk Process Facilitation
    - Risk Process Facilitation Pt1
    - Risk Process Facilitation Pt2
    - Risk Process Facilitation Pt3
- Module 7: Risk Monitoring and Reporting
    - Risk Monitoring and Reporting Pt 1
    - Risk Monitoring and Reporting Pt 2
    - Risk Monitoring and Reporting Pt 3
- Module 8: Specialized Risk Analyses
    - Specialized Risk Analyses Pt 1
    - Specialized Risk Analyses Pt 2
    - Specialized Risk Analyses Pt 3
- Module 9: RMP Recap
    - RMP Recap
- Module 10: RMP Review Questions

- RMP Review Questions Pt 1
- RMP Review Questions Pt 2
- RMP Review Questions Pt 3
- RMP Review Questions Pt 4
- RMP Review Questions Pt 5

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Gateway to Pen Testing Starter Pack Bundle

SKU: MISC-60

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Gateway to Pen Testing Starter Pack Bundle (Online OnDemand)

Course Bundle Description: The EC-Council Gateway to Pen Testing Starter Pack bundle provides participants with hands-on training in network vulnerability assessment, penetration testing, and exploitation techniques. This comprehensive program features over 50 lab exercises, offering practical experience with tools like Nmap, Burp Suite, Metasploit, QualysGuard, and Kali Linux. Participants will gain the skills needed to identify, exploit, and remediate vulnerabilities across networks, systems, and web applications, preparing them for roles in vulnerability management and offensive security operations.

Courses Included in the Gateway to Pen Testing Starter Pack

1. Ethical Hacking with Nmap

11 Chapters, 11 Labs – Duration: 3 hrs 59 mins
Nmap tips, tricks, and secrets every hacker should know.

- **Chapter 1:** Course Introduction and Lab Setup
- **Chapter 2:** Nmap Essentials
- **Chapter 3:** Nmap Scripting Engine Part 1: Basic Scripts
- **Chapter 4:** Nmap Scripting Engine Part 2: Enumeration

- **Chapter 5:** Nmap Scripting Engine Part 3: Web App Hacking
- **Chapter 6:** Integrating Nmap
- **Chapter 7:** Exploring Graphical Nmap Tools
- **Chapter 8:** NSE Advance Step
- **Chapter 9:** Analyzing
- **Chapter 10:** Vulnerability Audit
- **Chapter 11:** Taking It to The Next Level: Nmap Scripting

2. Getting Started with Vulnerability Analysis and Management

4 Chapters, 4 Labs – Duration: 5 hrs
Practical vulnerability and threat assessment, with insights on protecting companies.

- **Chapter 1:** Introduction
- **Chapter 2:** Network Vulnerabilities
- **Chapter 3:** Web Application Assessment
- **Chapter 4:** Host Security Assessments

3. Hands-on Vulnerability Management with QualysGuard

8 Chapters, 7 Labs – Duration: 3 hrs 21 mins
Manage vulnerabilities with Qualys Cloud Platform.

- **Chapter 1:** Introduction to Qualys Vulnerability Management
- **Chapter 2:** Qualys Vulnerability Knowledgebase
- **Chapter 3:** Qualys Asset Management
- **Chapter 4:** Qualys Vulnerability Assessment
- **Chapter 5:** User Management
- **Chapter 6:** Vulnerability Remediation
- **Chapter 7:** Patch Management

- **Chapter 8:** Summary

4. Windows Penetration Testing Essentials

7 Chapters, 6 Labs – Duration: 4 hrs 13 mins
A comprehensive guide to exploiting Windows OS vulnerabilities.

- **Chapter 1:** Setting Up Our Lab
- **Chapter 2:** Information Gathering & Service Enumeration
- **Chapter 3:** Exploitation
- **Chapter 4:** Privilege Escalation and Persistence
- **Chapter 5:** Password Attacks
- **Chapter 6:** Advanced Payload Encoding
- **Chapter 7:** Exploiting Metasploitable3

5. Malware Analysis Fundamentals

6 Chapters, 2 Labs – Duration: 4 hrs 22 mins
Explore how to find, analyze, and reverse engineer malware.

- **Chapter 1:** Introduction to the World of Malware
- **Chapter 2:** Malware Analysis Lab
- **Chapter 3:** Static Malware Analysis
- **Chapter 4:** Dynamic Malware Analysis
- **Chapter 5:** Malware Detection and AI
- **Chapter 6:** Wrap Up

6. Metasploit Like a Pro

8 Chapters – Duration: 12 hrs 48 mins
Learn to use Metasploit through practical, hands-on labs.

- **Chapter 1:** Getting Started with Metasploit
- **Chapter 2:** Getting Up and Running with Metasploit Basics

- **Chapter 3:** Working with Exploits, Payloads, and Shells
- **Chapter 4:** Process Migration with Meterpreter and Meterpreter Functions
- **Chapter 5:** Firewalls, Antivirus, and External Callbacks
- **Chapter 6:** Privilege Escalation and Persistence
- **Chapter 7:** Lateral Movement, Pivoting, and Common Practices
- **Chapter 8:** Final Thoughts and Wrapping Up

7. Mastering Database Reconnaissance and Exploitation

8 Chapters, 4 Labs – Duration: 4 hrs
Identify, enumerate, and exploit SQL and NoSQL databases.

- **Chapter 1:** Installation and Setup
- **Chapter 2:** Introduction to Databases
- **Chapter 3:** SQL vs. NoSQL Databases
- **Chapter 4:** Pentesting Test Cases for SQL and NoSQL
- **Chapter 5:** Exploiting Databases for Fun and Profit
- **Chapter 6:** Privilege Escalation and Chaining Attacks
- **Chapter 7:** Mitigation Techniques for Database Vulnerabilities
- **Chapter 8:** Course Conclusion and Final Comments

8. Getting Started with Kali Linux Penetration Testing

6 Chapters, 4 Labs – Duration: 5 hrs 19 mins
Learn how to use Kali Linux tools for vulnerability analysis.

- **Chapter 1:** Welcome and Introduction to Kali
- **Chapter 2:** Lab Setup for Pentesting
- **Chapter 3:** Information Gathering and Scanning
- **Chapter 4:** Vulnerability Analysis

- **Chapter 5:** Database Attacks
- **Chapter 6:** Password Attacks

9. Mastering Pentesting using Kali Linux

7 Chapters, 7 Labs – Duration: 4 hrs 34 mins
Learn how to use Kali Linux tools for professional pentesting.

- **Chapter 1:** Sniffing and Spoofing
- **Chapter 2:** Social Engineering Attacks
- **Chapter 3:** Wireless Attacks
- **Chapter 4:** Forensics Tools
- **Chapter 5:** Exploitation
- **Chapter 6:** Post Exploitation
- **Chapter 7:** Reporting Tools

10. Hands-on Password Attacks and Security

7 Chapters – Duration: 2 hrs 20 mins
Learn how attackers bypass passwords and how to prevent it.

- **Chapter 1:** Cracking Your First Password
- **Chapter 2:** Brute Force Attacks
- **Chapter 3:** Dictionary Attacks
- **Chapter 4:** Rainbow Table Attacks
- **Chapter 5:** Password Security Challenges
- **Chapter 6:** Remedies and Mitigations
- **Chapter 7:** Case Studies

11. Burp Suite: Web Application Penetration Testing

5 Chapters, 5 Labs – Duration: 2 hrs 46 mins
Simulate attacks using Burp Suite for web app security testing.

- **Chapter 1:** Setting Up Your Burp Suite Environment
- **Chapter 2:** Fast and Hybrid Spidering of Web Applications
- **Chapter 3:** Scanning Web Applications for Vulnerabilities
- **Chapter 4:** Exploiting Web Application Vulnerabilities
- **Chapter 5:** Deep-Dive Analysis of Reports

12. Securing Your Network from Attacks

9 Chapters – Duration: 5 hrs 53 mins
Identify, mitigate, and prevent network attacks.

- **Chapter 1:** Introduction to Network Threats
- **Chapter 2:** How Hackers Break into Networks
- **Chapter 3:** Securing Networks Through User Awareness
- **Chapter 4:** Securing Machines and Devices
- **Chapter 5:** Logs and Auditing
- **Chapter 6:** Phishing and Spear Phishing Attacks
- **Chapter 7:** Red Team vs. Blue Team Approach
- **Chapter 8:** Tracking Attackers (OSINT)
- **Chapter 9:** Recovering from an Attack

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

PECB Certified Forensics Examiner

SKU: MISC-61

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: PECB Certified Forensics Examiner (Online OnDemand)

Course Description: This course equips professionals with the skills to conduct thorough digital forensic investigations, following the standards outlined in ISO/IEC 27037. Participants learn how to identify, collect, analyze, and preserve digital evidence across a variety of systems, including Windows, macOS, Linux, and mobile devices. The course emphasizes maintaining the chain of custody to ensure the integrity of evidence for legal proceedings and internal investigations. Graduates will gain expertise in forensic tools, evidence reporting, and investigative best practices, making them well-prepared to lead complex forensic operations and support both legal compliance and cybersecurity initiatives.

Course Topics and Agenda

Day 1: Incident Response and Forensic Fundamentals

- Introduction to digital forensics and course objectives
- Overview of ISO/IEC 27037: Standards for digital evidence handling
- Roles and responsibilities of forensic investigators
- Setting up a forensic laboratory and tools
- Basics of incident response

Day 2: Preparing and Conducting Forensic Investigations

- Technical fundamentals of forensics operations
- File system forensic analysis (Windows, macOS, Linux)
- Operating system and file structure investigations
- Forensic data acquisition techniques
- Use of open-source and commercial forensic tools

Day 3: Digital Artifact Analysis and Management

- Identifying, collecting, and analyzing digital artifacts
- Managing digital evidence with forensic tools
- Using advanced search techniques (e.g., regex searches)
- Analysis of network traffic and logs
- Ensuring the integrity of collected data

Day 4: Case Reporting and Trial Preparation

- Preparing forensic reports for legal proceedings

- Maintaining the chain of custody for digital evidence
- Ethics in forensic investigations
- Presenting findings in court and legal testimony simulations
- Competency evaluation of forensic examiners

Day 5: Certification Exam and Review

- Final review of key topics and case studies
- Certification exam (3 hours)
- Guidelines for applying the ISO/IEC 27037 framework

License Information: One license provides access to the course.

How to Access: Instructions for accessing the course will be emailed after purchase.

Exam: The course comes with the exam and instructions for taking the exam will be provided after purchase.

Microsoft Azure AI Fundamentals, EC-Council AI-Driven Network Security (CR) and Generative AI for Cybersecurity, and Practical Artificial Intelligence for Professionals

Microsoft Azure AI Fundamentals

SKU: MISC-62

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: Microsoft Azure AI Fundamentals (Online **Live**)

Course Bundle Description: The Microsoft Azure AI Fundamentals Certification Training course introduces participants to essential AI concepts and how to implement them using Azure services. It covers AI workloads, machine learning principles, and cognitive services within Azure, focusing on real-world applications. This course is designed to build foundational knowledge for those preparing for the AI-900 certification, helping learners understand how AI integrates with cloud environments to create intelligent solutions. Participants will gain practical insights through hands-on activities, ensuring readiness to apply AI concepts effectively in professional settings. ***Please contact us to schedule this one day live online course.***

Course Outline (8 hours)

1. Microsoft Azure AI Fundamentals: Get started with artificial intelligence

- Common uses of artificial intelligence (AI)
- Different types of workloads associated with AI.
- Artificial Intelligence in Azure
- Responsible AI

2. Microsoft Azure AI Fundamentals: Explore visual tools for machine learning

- Fundamental machine learning concepts
- How to use the Azure Machine Learning service
- Ways to create and publish machine learning models
- Introduction to Machine Learning
- Azure Machine Learning

3. Microsoft Azure AI Fundamentals: Explore computer vision

- Computer vision techniques and services
- Computer Vision Concepts
- Computer Vision in Azure

4. Microsoft Azure AI Fundamentals: Explore natural language processing

- Azure services to build solutions that analyze text
- Recognize and synthesize speech
- Translate between languages
- Interpret commands

5. Microsoft Azure AI Fundamentals: Explore conversational AI

Topics:

- Basic principles for working with bots
- Conversational AI Concepts
- Conversational AI in Azure

License Information: One license provides access to the course on the dates scheduled.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council AI-Driven Network Security

SKU: MISC-63

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council ABC Bundle (Online OnDemand)

Course Bundle Description: The AI-Driven Network Security course from EC-Council focuses on applying artificial intelligence to enhance the security of network infrastructures. Participants learn how AI technologies can detect, predict, and respond to cyber threats in real-time by leveraging advanced algorithms and data analytics. The course provides hands-on experience with AI-based tools and strategies used across major cloud platforms such as AWS and Azure. It also covers the integration of AI for automating security operations, addressing emerging threats, and improving network resilience. This training is ideal for cybersecurity professionals looking to adopt AI-driven approaches for network defense and performance optimization

Topics Included

Taking It to The Next Level: Nmap Scripting

Chapter 1: Introduction

- The AI Revolution in Cybersecurity
- Navigating the Course
- The Threat Landscape
- AI vs. Cyber Threats
- From Reactive to Proactive
- Your Journey Begins
- Chapter 1 Quiz
- Preview

Chapter 2: Fundamentals of AI in Cybersecurity

- AI 101: Core Concepts
- Machine Learning Demystified
- Deep Learning in Cybersecurity
- Natural Language Processing
- Computer Vision in Security
- Predictive Analytics
- Artificial Neural Networks
- The AI Advantage
- Chapter 2 Quiz
- Preview

Chapter 3: AI-powered Threat Detection

- Real-time Network Analysis
- Behavioral Analytics
- Machine Learning in Action
- AI-enhanced SIEM
- Predictive Threat Intelligence
- Chapter 3 Quiz
- Preview

Chapter 4: Practical Implementation Strategies

- Assessing Your Security Posture
- Building Your AI Security Stack
- Data Preparation
- Overcoming Integration Challenges
- Chapter 4 Quiz

- Preview

Chapter 5: Emerging Trends in AI-driven Network Security

- Predictive Security
- AI-powered Threat Hunting
- Cloud Security Reinvented
- The Arms Race
- Chapter 5 Quiz
- Preview

Chapter 6: Best Practices and Ethical Considerations

- Balancing Act
- Ethical AI
- Privacy in the Age of AI
- Building Trust
- Chapter 6 Quiz
- Preview

Chapter 7: Real-world Applications and Case Studies

- Financial Sector Fortress
- Healthcare Shield
- Retail Defense
- Government-grade Security
- Chapter 7 Quiz
- Preview

Chapter 8: Conclusion and Q&A

- Your AI Security Toolkit

- Future-proofing Your Skills
- Q&A: Your Burning Questions Answered
- Course Conclusion
- Chapter 8 Quiz
- Preview

Chapter 9: Capstone Exercise

- Data Manipulation, Machine Learning, and Visualization with Python

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Generative AI for Cybersecurity

SKU: MISC-64

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Generative AI for Cybersecurity (Online OnDemand)

Course Bundle Description: The Generative AI for Cybersecurity course by EC-Council explores the role of artificial intelligence in enhancing cybersecurity defenses. It covers core concepts of generative AI and its applications in areas such as threat detection, vulnerability analysis, and security automation. Participants will gain hands-on experience with AI-driven tools to perform reconnaissance, generate phishing campaigns, and automate threat hunting tasks. The course also focuses on leveraging AI for predictive analysis, helping professionals stay ahead of emerging cyber threats. Designed for cybersecurity practitioners and managers, it offers practical insights into applying AI effectively within security frameworks.

Courses Included in the Gateway to Pen Testing Starter Pack

Taking It to The Next Level: Nmap Scripting

Chapter 1: Decoding Generative AI and Large Language Models

- Introduction to Generative AI (GenAI) and LLMs: A New Era in AI
- The Inner Workings of LLMs

- The Broad Application Spectrum of LLMs
- Chapter 1 Quiz
- Preview

Chapter 2: LLM Architecture: Design Patterns and Security Controls

- Architecture Design Patterns of LLM-powered Applications
- Security in LLM-powered Application Architecture
- Chapter 2 Quiz
- Preview

Chapter 3: LLM Technology Stacks and Security Considerations

- Choosing the Right Technology Stack for LLM Applications
- Maximizing Security in LLM Technology Stacks
- Chapter 3 Quiz
- Preview

Chapter 4: Open-sourced vs. Closed-sourced LLMs: Making the Choice

- Evaluating Open vs. Closed-sourced LLMs
- Tools for Evaluating Open-sourced LLMs
- Closed-sourced LLMs in Specific Use Cases
- Chapter 4 Lab
- Chapter 4 Quiz
- Preview

Chapter 5: Hands-on: Prompt Engineering and LLM Fine-tuning

- Prompt Engineering and LLM Fine-tuning
- Introduction to Fine-tuning
- Code Walkthrough Fine-tuning LLMs

- Summary and Final Thoughts
- Chapter 5 Lab
- Chapter 5 Quiz

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

EC-Council Practical Artificial Intelligence for Professionals

SKU: MISC-65

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Practical Artificial Intelligence for Professionals Bundle (Online OnDemand)

Course Bundle Description: The Practical Artificial Intelligence for Professionals learning path from EC-Council equips learners with hands-on knowledge to apply AI for automation, predictive analysis, and better decision-making. The course offers practical insights into using AI across various domains, combining videos, lab exercises, and real-world examples to build a strong foundation. It focuses on enabling professionals to harness AI tools for business and security applications, preparing them to implement AI-driven solutions effectively. Participants also receive shareable certificates for completed modules, enhancing their professional portfolio.

Courses Included (39+ Hours)

Advanced Machine Learning for Business Professionals
8 Chapters - Duration: 4 hrs
Learn how Machine Learning and AI can add real value to your organization and start your digital transformation.
Content

- Chapter 1: Introduction to Machine Learning
- Chapter 2: Supervised and Unsupervised Learning
- Chapter 3: Overview of the Machine Learning Workflow
- Chapter 4: Data Preprocessing Applications
- Chapter 5: Training, Testing, and Evaluating a ML Model

- Chapter 6: Deploying and Maintaining a Machine Learning Pipeline
- Chapter 7: When to Use Machine Learning and When Not To
- Chapter 8: Structure and Tools of a ML Team

Practical Applications of Machine Learning
7 Chapters - Duration: 4 hrs 12 mins
Everyone can learn linear algebra, but practical implementation of linear models is an essential skill for Machine Learning Engineers. This course covers various concepts with simultaneous practical applications.
Content

- Chapter 1: Overview of the Course
- Chapter 2: Deep Understanding of Regression Models
- Chapter 3: Optimizing Techniques
- Chapter 4: Analytical Visit of Classification Models
- Chapter 5: Practical Visit of Imbalance Classification
- Chapter 6: Dimensionality Reduction Techniques
- Chapter 7: Hands-on with the Project

Practical Visit to Data Mining
8 Chapters - Duration: 3 hrs
Data Mining is a vital tool in the industry today, and this course takes you from basic to advanced understanding of “Data Mining as a Tool.”
Content

- Chapter 1: Introduction to Data Mining
- Chapter 2: Essentials of Data Mining
- Chapter 3: Analyzing Mining Technique and Algorithm
- Chapter 4: Deep Dive into Clustering
- Chapter 5: Deep Dive into Tree Classification
- Chapter 6: Deep Dive into Handling Outlier and Effect

- Chapter 7: Understanding Project Pipeline
- Chapter 8: Advance Clustering Techniques

Advanced Deep Learning – Part 1
8 Chapters - Duration: 3 hrs 50 mins
Master Deep Learning by implementing algorithms such as CNN and LSTM. This part focuses on fundamentals like channels, kernels, and filters, preparing you for custom object detection using YOLO in Part 2.
Content

- Chapter 1: Overview of Course
- Chapter 2: Essential of Deep Learning
- Chapter 3: Introduction to CNN
- Chapter 4: Deep Dive into CNN
- Chapter 5: Activation Function & Gradient Descent
- Chapter 6: Hands-on with CNN
- Chapter 7: In-depth with Autoencoders
- Chapter 8: Hands-on with RNN

Advanced Deep Learning – Part 2
7 Chapters - Duration: 3 hrs 30 mins
Build on the foundational knowledge from Part 1 and explore real-time object detection using YOLO.
Content

- Chapter 1: Overview of Course
- Chapter 2: Data Collection and Annotation
- Chapter 3: Introduction to YOLO
- Chapter 4: Mathematics behind YOLO
- Chapter 5: Essentials of Model Training
- Chapter 6: Train Your Custom Object Detection

- Chapter 7: Test your Model

Applied Unsupervised Deep Learning
7 Chapters - Duration: 4 hrs 7 mins
Master complex tasks with unsupervised deep learning algorithms.
Content

- Chapter 1: Introduction
- Chapter 2: Principal Component Analysis
- Chapter 3: t-SNE
- Chapter 4: Autoencoders
- Chapter 5: Restricted Boltzmann Machines
- Chapter 6: Latent Semantic Analysis
- Chapter 7: Recommender System

Deep Learning: Masked Face Detection, Recognition
18 Chapters - Duration: 12 hrs 10 mins
Learn to detect faces, even with masks, using SSD and MTCNN models, and train custom recognition models.
Content

- Chapter 1: Set up the Environment
- Chapter 2: Jupyter Notebook Coding Environment
- Chapter 3: Image Process
- Chapter 4: Classification Model Explanation
- Chapter 5: TensorFlow Introduction and Quick Guide
- Chapter 6: Write a Classification Class Program
- Chapter 7: FaceNet Concepts
- Chapter 8: Create FaceNet Model
- Chapter 9: Face Alignment of CASIA Dataset using SSD Face Detection
- Chapter 10: Face Alignment of CASIA Dataset using MTCNN

- Chapter 11: CASIA Data Cleaning
- Chapter 12: Create a Dataset with Facial Masks
- Chapter 13: Train FaceNet Model
- Chapter 14: Training Skills
- Chapter 15: Evaluation of Recognizing Faces with Facial Masks
- Chapter 16: Training Skills Episode 2
- Chapter 17: Real-Time Face Detection, Facial Mask Detection, and Face Recognition
- Chapter 18: How to Train a Smaller Model

Computer Vision Face Recognition Quick Starter in Python
28 Chapters - Duration: 4 hrs 18 mins
Quickly develop Python-based systems for face detection, recognition, emotion analysis, and age/gender classification.
Content

- Chapter 1: Introduction to Face Recognition
- Chapter 2: Environment Setup: Installing Anaconda Package
- Chapter 3: Python Basics
- Chapter 4: Setting up Environment - Additional Dependencies (With DLib Fixes)
- Chapter 5: DLib Error: Downgrading Python and Fixing
- Chapter 6: Introduction to Face Detectors
- Chapter 7: Face Detection Implementation
- Chapter 8: cv2.imshow() Not Responding Issue Fix
- Chapter 9: Real-Time Face Detection from Webcam
- Chapter 10: Video Face Detection
- Chapter 11: Real-Time Face Detection - Face Blurring
- Chapter 12: Real-Time Facial Expression Detection - Installing Libraries

- Chapter 13: Real-Time Facial Expression Detection - Implementation
- Chapter 14: Video Facial Expression Detection
- Chapter 15: Image Facial Expression Detection
- Chapter 16: Real-Time Age and Gender Detection Introduction
- Chapter 17: Real-Time Age and Gender Detection Implementation
- Chapter 18: Image Age and Gender Detection Implementation
- Chapter 19: Introduction to Face Recognition
- Chapter 20: Face Recognition Implementation
- Chapter 21: Real-Time Face Recognition
- Chapter 22: Video Face Recognition
- Chapter 23: Face Distance
- Chapter 24: Face Landmarks Visualization
- Chapter 25: Multi Face Landmarks
- Chapter 26: Multi Face Landmarks from Real-Time and Pre-Saved Video
- Chapter 27: Face Makeup Using Face Landmarks
- Chapter 28: Real-Time Face Makeup

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

AWS Certified Machine Learning Specialist

SKU: MISC-66

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: ITI Partner Delivered AWS Certified Machine Learning Specialist (Online Live)

Course Bundle Description: This ITI Partner Delivered Machine Learning Pipeline on AWS course is a comprehensive four-day program that teaches participants to design, train, and deploy machine learning models using Amazon SageMaker to solve business problems, including fraud detection, recommendation engines, and flight delay prediction. The course includes hands-on labs, real-world case studies, and AWS Certified instructor guidance, preparing learners for the AWS Certified Machine Learning – Specialty exam. By the end, participants will have completed a full ML pipeline, equipping them with valuable AWS ML skills for tackling real-world scenarios

Course Topics:

1. Introduction to Machine Learning and the ML Pipeline

Learning Objective:

Upon completing this module, students will gain a foundational understanding of machine learning, including its core concepts, real-world applications, and the essential stages of a machine learning project. Additionally, they will be introduced to the course's structure and expectations.

Topics:

- Overview of machine learning, including use cases, types of machine learning, and key concepts
- Overview of the ML pipeline
- Introduction to course projects and approach

2. Introduction to Amazon SageMaker

Learning Objective:

Students will gain hands-on experience with Amazon SageMaker and Jupyter Notebooks, including launching instances, writing code, and exploring the platform's functionalities.

Topics:

- Introduction to Amazon SageMaker
- Demo: Amazon SageMaker and Jupyter notebooks
- Hands-on: Amazon SageMaker and Jupyter notebooks

3. Problem Formulation

Learning Objective:

Understand and apply the process of converting business problems into machine learning problems, including deciding when ML is the appropriate solution, with hands-on experience using Amazon SageMaker Ground Truth.

Topics:

- Overview of problem formulation and deciding if ML is the right solution
- Converting a business problem into an ML problem
- Demo: Amazon SageMaker Ground Truth
- Hands-on: Amazon SageMaker Ground Truth
- Practice problem formulation
- Formulate problems for projects

4. Pre-processing

Learning Objective:

Understand and apply data collection, integration, pre-processing, and visualization techniques to effectively prepare and analyze project data.

Topics:

- Overview of data collection and integration, and techniques for data pre-processing and visualization
- Practice pre-processing
- Pre-process project data
- Class discussion about projects

5. Model Training

Learning Objective:

By the end of this lesson, learners will be able to select appropriate algorithms, prepare and split data for training, apply loss functions and gradient descent for model optimization, and create a training job in Amazon SageMaker.

Topics:

- Choosing the right algorithm
- Formatting and splitting your data for training
- Loss functions and gradient descent for improving your model
- Demo: Create a training job in Amazon SageMaker

6. Model Evaluation

Learning Objective:

Develop skills in training, evaluating, and presenting classification and regression models through hands-on practice and initial project presentations.

Topics:

- How to evaluate classification models
- How to evaluate regression models
- Practice model training and evaluation
- Train and evaluate project models
- Initial project presentations

7. Feature Engineering and Model Tuning

Learning Objective:

Develop proficiency in feature engineering and hyperparameter tuning by practicing these techniques in real-world projects, culminating in a final project presentation that demonstrates the application of advanced machine learning optimization strategies.

Topics:

- Feature extraction, selection, creation, and transformation

- Hyperparameter tuning
- Demo: SageMaker hyperparameter optimization
- Practice feature engineering and model tuning
- Apply feature engineering and model tuning to projects
- Final project presentation

8. Deployment

Learning Objective:

Understand the process of deploying, performing inference, and monitoring machine learning models on Amazon SageMaker, including deploying models at the edge and creating SageMaker endpoints, and gain the ability to apply these skills in practical scenarios.

Topics:

- How to deploy, inference, and monitor your model on Amazon SageMaker
- Deploying ML at the edge
- Demo: Creating an Amazon SageMaker endpoint
- Post-assessment
- Course wrap-up

License Information: One license provides access to the course on the dates scheduled.

How to Access: Instructions for accessing the course will be emailed after purchase. To take the AWS Certified Machine Learning – Specialty exam (not included with the course) after completing the course, participants need to schedule it separately through AWS Training and Certification.

Microsoft Certified Azure AI Engineer Associate

SKU: MISC-67

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: ITI Partner Delivered Microsoft Certified Azure AI Engineer Associate (Online **Live**)

Course Bundle Description: The Designing and Implementing a Microsoft Azure AI Solution course, offered through an ITI partner, equips developers with the skills to build, deploy, and manage AI solutions on Azure. Tailored for those proficient in C# and Python, the course covers the use of Azure Cognitive Services, Azure Cognitive Search, and the Microsoft Bot Framework to create AI-powered applications. With a focus on real-world scenarios, participants gain hands-on experience in designing responsible AI solutions and deploying them effectively to meet enterprise needs. Note this course has specific prerequisites. ***Contact* us to schedule this live online course.**

Course Prerequisites

- Knowledge of Microsoft Azure
- Ability to navigate the Azure portal
- Knowledge of either C# or Python
- Familiarity with JSON and REST

Topics Included:

- Prepare to develop AI solutions on Azure: Understand core AI development principles and explore the capabilities Azure offers for AI solutions.
- Monitor Cognitive Services: Learn how to integrate AI into applications and monitor its performance effectively.
- Create and consume Cognitive Services: Build skills to develop and embed AI capabilities within your applications.
- Secure Cognitive Services: Implement security measures to prevent data loss and protect user privacy.
- Deploy Cognitive Services in containers: Explore container support to deploy Azure Cognitive Services APIs flexibly.
- Extract insights from text with the Language service: Create intelligent applications that analyze and extract meaningful information from text data.

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

CTI AI Fundamentals

SKU: MISC-68

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: CTI AI Fundamentals (Online OnDemand)

Course Description: This introductory course offers a comprehensive foundation in artificial intelligence (AI). Participants will explore the basics of AI, including machine learning, natural language processing, computer vision, and neural networks. The course emphasizes practical applications across various industries, equipping learners with the skills to understand AI trends and implement solutions within their organizations. Ideal for beginners, it provides hands-on insights and real-world examples to demystify the AI landscape and foster future innovation.

Course Outline (2 hours)

- Module 1 - Getting Started With AI
  - Module 1.1 Introduction To AI
  - Module 1.2 Understanding The Types of AI
- Module 2 - Programming Lanaguages, Tools and Platforms For AI Solutions
  - Module 2.1 AI and Programming Languages
  - Module 2.2 AI, Machine Learning and Deep Learning
  - Module 2.3 AI Models
  - Module 2.4 AI Services in the Cloud
- Module 3 - Data Science Fundamentals for AI
  - Module 3.1 Introduction to Data Science
  - Module 3.2 Data Preparation Techniques
  - Module 3.3 Exploratory Data Analysis (EDA)
- Module 4 - AI In the Modern Workplace
  - Module 4.1 AI In The Workplace
  - Module 4.2 Data Analysis and Business Intelligence AI Tools
  - Module 4.3 Automation and Workflow Management Tools
  - Module 4.4 Natural Language Processing (NLP) Tools
  - Module 4.5 Virtual Assistants and Chatbots
- Module 5 - Ethical AI and Future Trends
  - Module 5.1 Understanding Bias, Fairness, Privacy, and Security
  - Module 5.2 Impact of AI on Jobs and Society
  - Module 5.3 Emerging Trends in AI
  - Module 5.4 AI Governance and Regulation
- Module 6 - Monumental Leaps Forward With AI

    - Module 6.1 AI for Social Good
    - Module 6.2 AI in Creative Industries
    - Module 6.3 AI in Cybersecurity
    - Module 6.4 AI in Smart Cities and Infrastructure
- Module 7 - AI Project Lifecycle Management
    - Module 7.1 AI Project Lifecycle Management
    - Module 7.2 Development and Implementation
    - Module 7.3 Maintenance, Evaluation, and Scaling
- Module 8 - AI Fundamentals Course Closeout
    - Module 8.1 Course Closeout

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

CTI AWS Cloud Practitioner

SKU: MISC-69

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: CTI AWS Certified Cloud Practitioner Course (Online OnDemand)

Course Description: The course provides a comprehensive introduction to AWS cloud services, focusing on core concepts like identity management (IAM), EC2, S3 storage, databases, scaling, security, and compliance. It covers essential tools such as CloudWatch for monitoring, Route 53 for global applications, and Lambda for serverless computing. Learners will explore best practices through the Well-Architected Framework, preparing for AWS certification with hands-on experience. This course includes over 8 hours of labs.

Course Outline (17+ hours)

- **Module 1: Intro to Cloud Computing**
  Covers cloud models and AWS services, with AWS Console basics.
- **Module 2: IAM**
  Manage users, groups, roles, MFA, and policies for secure access.
- **Module 3: EC2**
  Set up instances, security groups, SSH access, and budgets.
- **Module 4: EC2 Storage**
  Work with EBS, AMIs, snapshots, and EFS.
- **Module 5: ELB & ASG**
  Implement load balancing and auto-scaling.

- **Module 6: Amazon S3**
  Explore buckets, policies, versioning, and Snowball.
- **Module 7: Databases & Analytics**
  Learn RDS, DynamoDB, RedShift, and Glue.
- **Module 8: Other Compute Services**
  Explore ECS, Lambda, and Lightsail.
- **Module 9: Scaling Infrastructure**
  Use CloudFormation, Beanstalk, and OpsWorks.
- **Module 10: Global Applications**
  Manage Route 53, CloudFront, and Global Accelerator.
- **Module 11: Cloud Integration**
  Work with SQS, SNS, and distributed messaging.
- **Module 12: Monitoring & Troubleshooting**
  Use CloudWatch, CloudTrail, and X-Ray.
- **Module 13: VPN & Networking**
  Set up VPCs, subnets, gateways, and VPNs.
- **Module 14: Security & Compliance**
  Cover GuardDuty, KMS, Macie, and compliance tools.
- **Module 15: Machine Learning**
  Explore SageMaker, Polly, Lex, and Rekognition.
- **Module 16: Advanced Identity**
  Use Cognito, Directory Services, and SSO.
- **Module 17: Well-Architected Framework**
  Review AWS architecture best practices.
- **Module 18: Exam Prep**
  Finalize learning and prep for the certification exam.

Labs Included (8+ hours)

- AWS Fundamentals
- AWS Security & Compliance Concepts
- AWS Security Services
- AWS Deployment Methods
- AWS Global Infrastructure
- AWS Computing Services
- AWS Storage Services
- AWS Networking Services
- AWS Database Services

License Information: One license provides access to the curriculum for 12 months.

How to Access: Instructions for accessing the course will be emailed after purchase.

PECB Chief Information Security Officer certification

SKU: MISC-70

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: PECB Chief Information Security Officer (Online OnDemand)

PECB CISO Description: By obtaining the PECB Chief Information Security Officer certification, you will develop the professional knowledge to plan and oversee the implementation of an information security program, and, in turn, ensure that an organization's confidential information is protected from disclosure.

Topics Covered:

1. **Day 1 Fundamentals of information security and the role of a CISO**
    - Training course objectives and structure
    - Fundamentals of information security
    - Chief information security officer (CISO)
    - Information security program
2. **Day 2 Information security compliance program, risk management, and security architecture and design**
    - Information security compliance program
    - Analysis of the existing information security capabilities
    - Information security risk management
    - Security architecture and design
3. **Day 3 Security controls, incident management, and change management**
    - Information security controls
    - Information security incident management
    - Change management
4. **Day 4 Information security awareness, monitoring and measurement, and continual improvement**
    - Awareness and training programs
    - Monitoring and measurement h
    - Assurance program
    - Continual improvement
    - Closing of the training course
5. **Day 5 Certification Exam**

Exam Information: The PECB CISO course comes with the exam.

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course and taking the exams will be emailed after purchase.

Link to PECB Brochure: https://pecb.com/pdf/brochures/4/chief-information-security-officer-4p.pdf

EC-Council Industrial Cybersecurity: Healthcare

SKU: MISC-71

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Industrial Cybersecurity: Healthcare (Online OnDemand)

Course Description: The Industrial Cybersecurity for Healthcare course by EC-Council provides specialized training focused on securing industrial control systems (ICS) and critical infrastructure within the healthcare sector. This program addresses the unique challenges of protecting medical devices, operational technology, and healthcare networks from cyber threats. Participants gain a comprehensive understanding of ICS vulnerabilities, threat mitigation strategies, and compliance requirements specific to healthcare environments. Through hands-on labs and real-world case studies, learners develop the skills necessary to safeguard patient safety and ensure the resilience of healthcare operations

Topics Covered:

1. Introduction to Cybersecurity

11 Chapters – Duration: 4 hrs 11 mins
A comprehensive dive into the world of cybersecurity for beginners and intermediate learners.
Content:
Chapter 1: Introduction to Physical Security
Chapter 2: Securing Operating Systems
Chapter 3: Clear Desk and Removable Media Policy
Chapter 4: Internet Security
Chapter 5: Diving into Malware and Viruses
Chapter 6: Security on Social Networking Sites
Chapter 7: Securing E-mail Communication
Chapter 8: Securing Mobile Devices
Chapter 9: Securing the Cloud

Chapter 10: Network Connections
Chapter 11: Data Backup and Disaster Recovery

2. Cybersecurity for Healthcare – Part 1

4 Chapters – Duration: 3 hrs 12 mins
Healthcare organizations are increasingly under attack by bad actors, which has only gotten worse during the pandemic. Explore the reasons and methods of attack, and how to defend these vulnerable and critical systems.
Content:
Chapter 1: Healthcare vs. Traditional IT Environment
Chapter 2: The Attack Surface
Chapter 3: Connected Medical Devices – The Nightmare
Chapter 4: Cybercrime Faced by Healthcare Industry

3. Cybersecurity for Healthcare – Part 2

5 Chapters – Duration: 4 hrs
Defending healthcare organizations from cyber attacks.
Content:
Chapter 1: How to Secure a Healthcare Environment?
Chapter 2: How to Recover from a Cyber Attack?
Chapter 3: Healthcare Digitalization – The Opportunities
Chapter 4: Healthcare Compliance: HIPAA
Chapter 5: Healthcare Compliance: HITECH

4. Implementing Information Security in Your Enterprise

8 Chapters – Duration: 1 hr 52 mins
Protecting information, mitigating data risks, and reducing the probability of unauthorized access to data assets.
Content:
Chapter 1: Introduction to Information Security
Chapter 2: Implementing ISO27001 – Information Security Standards
Chapter 3: Establishing Information Security Roles, Responsibilities, and Governance
Chapter 4: Best Practice Document Management and International Records Management Based on ISO15489
Chapter 5: Data Protection, Data Privacy, and GDPR
Chapter 6: Compliance and Regulations Including Cyber Security
Chapter 7: Hybrid Cloud Computing Model
Chapter 8: Conclusion

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course and taking the exams will be emailed after purchase.

EC-Council Applied Secure Smart City

SKU: MISC-72

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Applied Secure Smart City (Online OnDemand)

Course Description: The Applied Secure Smart City course by EC-Council delivers advanced training on securing smart city infrastructures against evolving cyber threats. This course focuses on the integration of cybersecurity strategies into the interconnected systems that power smart cities, including IoT devices, critical infrastructure, and intelligent networks. Participants will explore the vulnerabilities and risks unique to smart city environments, learning to design and implement robust security measures to protect data, privacy, and public safety. Through practical labs and real-world scenarios, this program equips professionals with the knowledge and skills needed to safeguard smart city ecosystems effectively.

Topics Covered:

6 Chapters – Duration: 4 hours

Explore the essential components, sectors, and cybersecurity measures for safeguarding smart city infrastructures.

Chapter 1: Quick Introduction to Smart Cities

- Intro to Smart Cities
- Examples of Smart Cities
- Intro to Smart Cities Sectors
- Overview of Cyber Security for Smart Cities
- $7 Million Cybersecurity Scholarship by EC-Council
- Chapter 1 Quiz

Chapter 2: Introduction to Smart Energy

- Smart Energy Concepts & Solutions

- Real World Examples of Smart Energy Solutions
- Overview of Smart Energy Security Systems
- Chapter 2 Quiz

Chapter 3: Introduction to Future Mobility

- Future Mobility Concepts & Solutions
- Real World Examples of Future Mobility Solutions
- Overview of Future Mobility Security
- Chapter 3 Quiz

Chapter 4: Internet of Things (IoT)

- Introduction to IoT Concepts & Solutions
- Real World Examples of IoT Solutions
- Overview of IoT Security
- Chapter 4 Quiz

Chapter 5: Open Data

- Introduction to Open Data Concepts & Solutions
- Real World Examples of Open Data Solutions
- Overview of Open Data Security
- Chapter 5 Quiz

Chapter 6: Conclusion

- Secure Your Smart City
- Key Take-aways of Smart City Security
- How to Help Secure Your Own Smart City?
- Chapter 6 Quiz

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course and taking the exams will be emailed after purchase.

EC-Council Cybersecurity for Telecommunications

SKU: MISC-73

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Cybersecurity for Telecommunications (Online OnDemand)

Course Description: This the Cybersecurity for Telecommunications course by EC-Council provides specialized training in securing telecommunications infrastructure against modern cyber threats. This course covers the unique challenges faced by telecom networks, including securing mobile communications, VoIP, and next-generation networks (5G). Participants will gain in-depth knowledge of telecom-specific vulnerabilities, threat mitigation techniques, and compliance requirements. Through practical exercises and real-world case studies, learners will develop the skills necessary to protect critical telecommunications systems and ensure secure communication channels in dynamic environments.

Topics Covered:

6 Chapters – Duration: Varies

Gain an in-depth understanding of telecommunications networks, their vulnerabilities, and cybersecurity measures to protect them.

Chapter 1: Introduction and Overview

- Course Outline and Description of Sections

Chapter 2: Telecom Networks

- Analog, Digital, and Mobile Networks
- The PSTN and Circuit Switching
- IP Networks and Packet-switching
- VoIP and IoT Networks
- Chapter 2 Quiz

Chapter 3: Telecom Standards

- GSM
- TCP/IP Standards
- Wireless Network Standards
- Standards Compatibility and Interoperability

- Chapter 3 Quiz

Chapter 4: Network Access Control and Transport Formats

- Network Access Control
- Transfer Formats
- SONET
- Signaling System 7 (SS7)
- Chapter 4 Quiz

Chapter 5: Vulnerabilities, Threats, and Countermeasures

- Common Telecom Network Vulnerabilities
- Common Telecom Network Threats
- Telecom Network Attacks and Attackers
- Mitigations to Cybersecurity Vulnerabilities and Attacks
- Chapter 5 Quiz

Chapter 6: Course Summary

- Network Standards
- Telecom Standards
- Transmission Standards, Formats, and Vulnerabilities
- Vulnerabilities, Threats, and Mitigation

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course and taking the exams will be emailed after purchase.

EC-Council Cybersecurity for FinTech

SKU: MISC-74

MSRP: Not for individual Sale, for bundles only

Sales Price: Not for individual Sale, for bundles only

Courses Include: EC-Council Cybersecurity for FinTech (Online OnDemand)

Course Description: The Cybersecurity for FinTech course by EC-Council offers targeted training on protecting financial technology ecosystems from cyber threats. This

program addresses the unique security challenges of the FinTech sector, including securing digital payment systems, blockchain technology, and financial data. Participants will explore critical vulnerabilities, compliance frameworks, and threat mitigation strategies specific to FinTech applications. With a focus on practical implementation, this course equips professionals with the skills needed to safeguard financial transactions, protect sensitive data, and ensure regulatory compliance in the fast-evolving FinTech landscape

Topics Covered:

4 Chapters – Duration: 4 Hours

Explore the unique security challenges of the FinTech industry and learn to design, deploy, and maintain secure FinTech systems.

Chapter 1: Applied FinTech with Gaps and Challenges

- What and Why of FinTech?
- FinTech Ecosystem Overview
- How FinTech is Changing Traditional Finance?
- Reinventing the Wheel
- The Role of Technology
- Security Gaps in the Use Cases with Architecture Review
- $7 Million Cybersecurity Scholarship by EC-Council
- Chapter 1 Quiz

Chapter 2: Building FinTech Security Architecture

- Security Fundamentals
- Understanding Public Cryptography
- FinTech Architecture Vulnerabilities and Attack Vectors
- Data Flow with Threat Modeling
- Designing FinTech Security Architecture for Mitigating Risk
- Chapter 2 Quiz

Chapter 3: How to Deploy FinTech Application Securely

- Assessing FinTech Development Lifecycle
- Security Checkpoints in Coding

- FinTech Security Solution
- FinTech Risk Management Framework (DevSecOps)
- FinTech Incident Management
- Chapter 3 Quiz

Chapter 4: Legal Ecosystem with Security Best Practices

- FinTech Legal Guidelines and Controls (GDPR, PCISS, ISO27X)
- FinTech Compliance Check
- RegTech Focus Areas for FinTech
- Designing FinTech Sandbox
- Considerations for Solid Legal Foundation

License Information: One license provides access to each course for 12 months. Access keys must be redeemed within 12 months of purchase.

How to Access: Instructions for accessing the course and taking the exams will be emailed after purchase.