CT-SECURITY+: CompTIA® Security+ (701)

Course Code: CT-SECURITY+
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor- led Training (VILT)

OVERVIEW

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and is the first security certification a candidate should earn.
Security+ establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs.
Security+ incorporates best practices in hands-on troubleshooting, ensuring candidates have practical security problem-solving skills required to:

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions;
- Monitor and secure hybrid environments, including cloud, mobile, and IoT;
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance;
- Identify, analyze, and respond to security events and incidents.

CompTIA Security+ is compliant with ISO 17024 standards and approved by the U.S. DoD to meet Directive 8140.03M requirements. Security+ also maps to the core objectives required for 20 NICE work roles.
Security+ is good for three years from the day of achievement, and the CompTIA Continuing Education program enables Security+ credentialed individuals to extend their certification in three-year intervals.

SKILLS COVERED

In this course, you will implement information security across a variety of different contexts.

You will:

- Identify the fundamental components of information security.
- Analyze risk.
- Identify various threats to information security.
- Conduct security assessments to detect vulnerabilities.
- Implement security for hosts and software.
- Implement security for networks.
- Manage identity and access.
- Implement cryptographic solutions in the organization.
- Implement security at the operational level.
- Address security incidents.
- Ensure the continuity of business operations in the event of an incident

WHO SHOULD ATTEND?

Job roles that Security+ maps to:

- Security Specialist
- Security Administrator
- Systems Administrator
- Help Desk Analyst
- Security Analyst
- Security Engineer

PREREQUISITES

CompTIA Network+ and a minimum of 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts.

MODULES

Lesson 1: Summarize Fundamental Security Concepts

Lesson content is aligned to the following exam objective(s): 1.1, 1.2

- Lesson Topics
  - 1A: Security Concepts
  - 1B: Security Controls
- Training Activities
  - CML Lesson 1: Study Materials
  - Assisted Lab: Exploring the Lab Environment
  - Assisted Lab: Perform System Configuration Gap Analysis

Lesson 2: Compare Threat Types

Lesson content is aligned to the following exam objective(s): 2.1, 2.2

- Lesson Topics
  - 2A: Threat Actors
  - 2B: Attack Surfaces
  - 2C: Social Engineering
- Training Activities
  - CML Lesson 2: Study Materials
  - CML Lesson 2: PBQ – Compare and Contrast Social Engineering Techniques
  - Assisted Lab: Finding Open Service Ports
  - Skills Quiz Lessons 1 & 2

Lesson 3: Explain Cryptographic Solutions

Lesson content is aligned to the following exam objective(s): 1.4

- Lesson Topics
  - 3A: Cryptographic Algorithms
  - 3B: Public Key Infrastructure
  - 3C: Cryptographic Solutions
- Training Activities
  - CML Lesson 3: Study Materials
  - CML Lesson 3: PBQ –Implement Certificates and Certificate Authorities

Lesson 4: Implement Identity and Access Management

Lesson content is aligned to the following exam objective(s): 4.6

- Lesson Topics
  - 4A: Authentication
  - 4B: Authorization
  - 4C: Identity Management
- Training Activities
  - CML Lesson 4: Study Materials
  - Assisted Lab: Managing Permissions
  - Skills Quiz Lessons 3 & 4

Lesson 5: Secure Enterprise Network Architecture

Lesson content is aligned to the following exam objective(s): 3.1, 3.2

- Lesson Topics

  - 5A: Enterprise Network Architecture
  - 5B: Network Security Appliances
  - 5C: Secure Communications
- Training Activities
  - CML Lesson 5: Study Materials
  - Assisted Lab: Setting up Remote Access

Lesson 6: Secure Cloud Network Architecture

Lesson content is aligned to the following exam objective(s): 1.2, 3.1, 3.2

- Lesson Topics
  - 6A: Cloud Infrastructure
  - 6B: Embedded Systems and Zero Trust Architecture
- Training Activities
  - CML Lesson 6: Study Materials
  - CML Lesson 6: PBQ – Analyze Infrastructure Types and Functions
  - Assisted Lab: Using Containers
  - Assisted Lab: Using Virtualization
  - Skills Quiz Lessons 5 & 6

Lesson 7: Explain Resiliency and Site Security Concepts

Lesson content is aligned to the following exam objective(s): 1.2, 3.4, 4.2

- Lesson Topics
  - 7A: Asset Management
  - 7B: Redundancy Strategies
  - 7C: Physical Security
- Training Activities
  - CML Lesson 7: Study Materials
  - CML Lesson 7: PBQ – Incorporate Redundancy Strategies
  - Applied Lab: Implement Backups
  - Skills Quiz Lesson 7

Lesson 8: Explain Vulnerability Management

Lesson content is aligned to the following exam objective(s): 2.3, 4.3

- Lesson Topics
  - 8A: Device and OS Vulnerabilities
  - 8B: Application and Cloud Vulnerabilities
  - 8C: Vulnerability Identification Methods
  - 8D: Vulnerability Analysis and Remediation
- Training Activities
  - CML Lesson 8: Study Materials
  - CML Lesson 8: PBQ – Identify Types of Vulnerabilities
  - Assisted Lab: Working with Threat Feeds
  - Assisted Lab: Performing Vulnerability Scans
  - Skills Quiz Lesson 8

Mid-term Assessment

Lesson 9: Evaluate Network Security Capabilities

Lesson content is aligned to the following exam objective(s): 4.1, 4.5

- Lesson Topics
  - 9A: Network Security Baselines
  - 9B: Network Security Capability Enhancement
- Training Activities
  - CML Lesson 9: Study Materials
  - Assisted Lab: Understanding Security Baselines

Lesson 10: Assess Endpoint Security Capabilities

Lesson content is aligned to the following exam objective(s): 2.5, 4.1, 4.5

- Lesson Topics
  - 10A: Implement Endpoint Security
  - 10B: Mobile Device Hardening
- Training Activities
  - CML Lesson 10: Study Materials
  - CML Lesson 10: PBQ –Implement Mobile Device Management

Lesson 11: Enhance Application Security Capabilities

Lesson content is aligned to the following exam objective(s): 4.1, 4.5

- Lesson Topics
  - 11A: Application Protocol Security Baselines
  - 11B: Cloud and Web Application Security Concepts
- Training Activities
  - CML Lesson 11: Study Materials
  - CML Lesson 11: PBQ – Modify Enterprise Capabilities to Enhance Security
  - Assisted Lab: Configuring System Monitoring
  - Skills Quiz Lessons 9, 10, & 11

Lesson 12: Explain Incident Response and Monitoring Concepts

Lesson content is aligned to the following exam objective(s): 4.4, 4.8, 4.9

- Lesson Topics
  - 12A: Incident Response
  - 12B: Digital Forensics
  - 12C: Data Sources
  - 12D: Alerting and Monitoring Tools
- Training Activities
  - CML Lesson 12: Study Materials
  - Applied Lab: Using Network Sniffers
  - Assisted Lab: Performing Root Cause Analysis
  - Skills Quiz Lesson 12

Lesson 13: Analyze Indicators of Malicious Activity

Lesson content is aligned to the following exam objective(s): 2.4

- Lesson Topics
  - 13A: Malware Attack Indicators
  - 13B: Physical and Network Attack Indicators
  - 13C: Application Attack Indicators
- Training Activities
  - CML Lesson 13: Study Materials
  - Assisted Lab: Detecting and Responding to Malware
  - Skills Quiz Lesson 13

Lesson 14: Summarize Security Governance Concepts

Lesson content is aligned to the following exam objective(s): 1.3, 4.7, 5.1

- Lesson Topics
  - 14A: Policies, Standards, and Procedures
  - 14B: Change Management
  - 14C: Automation and Orchestration
- Training Activities
  - CML Lesson 14: Study Materials

    - CML Lesson 14: PBQ – Apply Appropriate Polices and Regulations
    - Adaptive Lab: Using a Playbook
    - Skills Quiz Lesson 14

Lesson 15: Explain Risk Management Processes

Lesson content is aligned to the following exam objective(s): 5.2, 5.3, 5.5

- Lesson Topics
    - 15A: Risk Management Processes and Concepts
    - 15B: Vendor Management Concepts
    - 15C: Audits and Assessments
- Training Activities
    - CML Lesson 15: Study Materials
    - Assisted Lab: Performing Penetration Testing
    - Assisted Lab: Performing Reconnaissance

Lesson 16: Summarize Data Protection and Compliance Concepts

Lesson content is aligned to the following exam objective(s): 3.3, 5.4, 5.6

- Lesson Topics
    - 16A: Data Classification and Compliance
    - 16B: Personnel Policies
- Training Activities
    - CML Lesson 16: Study Materials
    - CML Lesson 16: PBQ – Apply Appropriate Techniques to Secure Data
    - Assisted Lab: Training and Awareness through Simulation
    - Skills Quiz Lessons 15 & 16