CT-SECURITY+: CompTIA Security+ (Plus) Certification

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

OVERVIEW

The official ***CompTIA Security+ (Exam SY0-701)*** course is the primary curriculum you will need to take if your job responsibilities include securing network services, devices, and traffic in your organization. You can also take this course to prepare for the CompTIA Security+ certification examination.

As one of the top IT certifications for beginners globally, this course will provide guidance and expertise to build on your knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.

Funding Opportunity: Malaysian Bumiputera's aged 21-28 years old are eligible to apply for 100% funding for CompTIA Security+ under the Yayasan Peneraju Pendidikan Bumiputera funding program.

Are you currently retrenched? If yes, check out our PERKESO EIS: Get Back into the Workforce through Upskilling program.

SKILLS COVERED

By successfully completing this training course, you will be able to:

- General Security Concepts
- Threats, Vulnerabilities & Mitigations
- Security Architecture
- Security Operations
- Security Program Management & Oversight

WHO SHOULD ATTEND?

This CompTIA Security+ course is targeted toward the:

- Information technology (IT) professional who has networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks and familiarity with other operating systems, such as macOS®, Unix, or Linux
- Those who wants to further a career in IT by acquiring foundational knowledge of security topics
- Candidates preparing for the CompTIA Security+ certification examination
- Cybersecurity professionals using Security+ as the foundation for advanced security certifications or career roles

PREREQUISITES

To ensure your success in this course, you should possess basic Windows user skills and a fundamental understanding of computer and networking concepts.

CompTIA A+ and CompTIA Network+ certifications, or equivalent knowledge, and six to nine months' experience in networking, including configuring security parameters, are strongly recommended.

Additional introductory courses or work experience in application development and programming, or in network and operating system administration for any software platform or system, are helpful but not required. Note that the prerequisites for this course might differ

significantly from the prerequisites for the CompTIA certification exams.

MODULES

Module 1: Summarize Fundamental Security Concepts

Topic 1A: Security Concepts
Exam objectives covered:

1.2 Summarize fundamental security concepts

Topic 1B: Security Controls
Exam objectives covered:

1.1 Compare and contrast various types of security controls.

Module 2: Compare Threat Types

- 2.1 Compare and contrast common threat actors and motivations.

Topic 2B: Attack Surfaces
Exam objectives covered:

- 2.2 Explain common threat vectors and attack surfaces.

Topic 2C: Social Engineering
Exam objectives covered:

- 2.2 Explain common threat vectors and attack surfaces.

Module 3: Explain Cryptographic Solutions

Topic 3A: Cryptographic Algorithms
Exam objectives covered:

- 1.4 Explain the importance of using appropriate cryptographic solutions

Topic 3B: Public Key Infrastructure
Exam objectives covered:

- 1.4 Explain the importance of using appropriate cryptographic solutions.

Topic 3C: Cryptographic Solutions
Exam objectives covered:

- 1.4 Explain the importance of using appropriate cryptographic solutions

Module 4: Implement Identity and Access Management

- 4.6 Given a scenario, implement and maintain identity and access management.

Topic 4B: Authorization
Exam objectives covered:

- 4.6 Given a scenario, implement and maintain identity and access management.

Topic 4C: Identity Management
Exam objectives covered:

- 4.6 Given a scenario, implement and maintain identity and access management

Module 5: Secure Enterprise Network Architecture

- 3.1 Compare and contrast security implications of different architecture models.
- 3.2 Given a scenario, apply security principles to secure enterprise infrastructure

Topic 5B: Network Security Appliances
Exam objectives covered:

- 3.2 Given a scenario, apply security principles to secure enterprise infrastructure.

Topic 5C: Secure Communications
Exam objectives covered:

- 3.2 Given a scenario, apply security principles to secure enterprise infrastructure

Module 6: Secure Cloud Network Architecture

Topic 6A: Cloud Infrastructure
Exam objectives covered:

- 3.1 Compare and contrast security implications of different architecture models

Topic 6B: Embedded Systems and Zero Trust Architecture
Exam objectives covered:

- 1.2 Summarize fundamental security concepts.
- 3.1 Compare and contrast security implications of different architecture models

Module 7: Explain Resiliency and Site Security Concepts

Topic 7A: Asset Management
Exam objectives covered:

- 3.4 Explain the importance of resilience and recovery in security architecture.
- 4.2 Explain the security implications of proper hardware, software, and data asset management.

Topic 7B: Redundancy Strategies
Exam objectives covered:

- 1.2 Summarize fundamental security concepts.
- 3.4 Explain the importance of resilience and recovery in security architecture.

Topic 7C: Physical Security
Exam objectives covered:

- 1.2 Summarize fundamental security concepts.

Module 8: Explain Vulnerability Management

Topic 8A: Device and OS Vulnerabilities
Exam objectives covered:

- 2.3 Explain various types of vulnerabilities.

Topic 8B: Application and Cloud Vulnerabilities
Exam objectives covered:

- 2.3 Explain various types of vulnerabilities

Topic 8C: Vulnerability Identification Methods
Exam objectives covered:

- 4.3 Explain various activities associated with vulnerability management.

Topic 8D: Vulnerability Analysis and Remediation

Exam objectives covered:

- 4.3 Explain various activities associated with vulnerability management

Module 9: Evaluate Network Security Capabilities

Topic 9A: Network Security Baselines
Exam objectives covered:

- 4.1 Given a scenario, apply common security techniques to computing resources.
- 4.5 Given a scenario, modify enterprise capabilities to enhance security.

Topic 9B: Network Security Capability Enhancement
Exam objectives covered:

- 4.5 Given an scenario, modify enterprise capabilities to enhance security.

Module 10: Assess Endpoint Security Capabilities

Topic 10A: Implement Endpoint Security
Exam objectives covered:

- 2.5 Explain the purpose of mitigation techniques used to secure the enterprise.
- 4.1 Given a scenario, apply common security techniques to computing resources.
- 4.5 Given a scenario, modify enterprise capabilities to enhance security.

Topic 10B: Mobile Device Hardening
Exam objectives covered:

- 4.1 Given a scenario, apply common security techniques to computing resources.

Module 11: Enhance Application Security Capabilities

Topic 11A: Application Protocol Security Baselines
Exam objectives covered:

- 4.5 Given a scenario, modify enterprise capabilities to enhance security.

Topic 11B: Cloud and Web Application Security Concepts
Exam objectives covered:

- 4.1 Given a scenario, apply common security techniques to computing resources

Topic 11B: Cloud and Web Application Security Concepts
Exam objectives covered:

- 4.1 Given a scenario, apply common security techniques to computing resources

Module 12: Explain Incident Response and Monitoring Concepts

Topic 12A: Incident Response
Exam objectives covered:

- 4.8 Explain appropriate incident response activities.

Topic 12B: Digital Forensics
Exam objectives covered:

- 4.8 Explain appropriate incident response activities.

Topic 12C: Data Sources
Exam objectives covered:

- 4.9 Given a scenario, use data sources to support an investigation

Topic 12D: Alerting and Monitoring Tools
Exam objectives covered:

- 4.4 Explain security alerting and monitoring concepts and tools

Module 13: Analyze Indicators of Malicious Activity

Topic 13A: Malware Attack Indicators
Exam objectives covered:

- 2.4 Given a scenario, analyze indicators of malicious activity.

Topic 13B: Physical and Network Attack Indicators

Exam objectives covered:

- 2.4 Given a scenario, analyze indicators of malicious activity.

Topic 13C: Application Attack Indicators
Exam objectives covered:

- 2.4 Given a scenario, analyze indicators of malicious activity.

Module 14: Summarize Security Governance Concepts

Topic 14A: Policies, Standards, and Procedures
Exam objectives covered:

- 5.1 Summarize elements of effective security governance.

Topic 14B: Change Management
Exam objectives covered:

- 1.3 Explain the importance of change management processes and the impact to security.

Topic 14C: Automation and Orchestration

Exam objectives covered:

- 4.7 Explain the importance of automation and orchestration related to secure operations.

Module 15: Explain Risk Management Processes

Topic 15A: Risk Management Processes and Concepts
Exam objectives covered:

- 5.2 Explain elements of the risk management process.

Topic 15B: Vendor Management Concepts
Exam objectives covered:

- 5.3 Explain the processes associated with third party risk assessment and management

Topic 15C: Audits and Assessments
Exam objectives covered:

- 5.5 Explain types and purposes of audits and assessments

Module 16: Summarize Data Protection and Compliance Concepts

Topic 16A: Data Classification and Compliance
Exam objectives covered:

- 3.3 Compare and contrast concepts and strategies to protect data.
- 5.4 Summarize elements of effective security compliance.

Topic 16B: Personnel Policies
Exam objectives covered:

- 5.6 Given a scenario, implement security awareness practices

END OF PAGE