CO-SE+

COMPTIA SECURITY+

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
5 Days	Introduction	IT Security	Classroom	NA

INTRODUCTION

CompTIA Security+ is the certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management – making it an important stepping stone of an IT security career.

This course will further benefit delegates in two ways. If delegates intend to pass the CompTIA Security+ (Exam SY0-701) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of computer security. Today's job market demands individuals with demonstrable skills, and the information and activities in this course will help delegates build your computer security skill-set so that you can confidently perform your duties in any security-related role.

AUDIENCE PROFILE

This 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; familiarity with other operating systems, such as MacOS, Unix, or Linux; and who wants to further a career in IT by acquiring foundational knowledge of security topics; preparing for the CompTIA Security+ certification examination; or using Security+ as the foundation for advanced security certifications or career roles.

PREREQUISITES

Before attending this course delegates should possess basic Windows user skills and a fundamental understanding of computer and networking concepts. Additionally, delegates should have:

- Either attended the CompTIA Network+ course, or have equivalent knowledge or;
- Have a minimum of two years of technical networking experience, with an emphasis on security

COURSE OBJECTIVES

In this course, delegates will describe the major networking technologies and systems of modern networks, and configure, manage, and troubleshoot modern networks. In addition, delegates will be able to:

- 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 incident
- Ensure the continuity of business operations in the event of an incident

COURSE OUTLINE

COURSE CONTENT

Lesson 1: Summarize Fundamental Security Concepts
- Security Concepts
- Security Controls

Lesson 2: Compare Threat Types
- Threat Actors
- Attack surfaces
- Social Engineering

Lesson 3: Explain Cryptographic Solutions
- Cryptographic Algorithms
- Public Key Infrastructure
- Cryptographic Solutions

Lesson 4: Implement Identity and Access Management
- Authentication
- Authorization
- Identity Management

Lesson 5: Secure Enterprise Network Architecture
- Enterprise Network Architecture
- Network Security Appliances
- Secure Communications

Lesson 6: Secure Cloud Network Architecture
- Cloud Infrastructure
- Embedded Systems and Zero Trust Architecture

Module 7: Explain Resiliency and Site Security Concepts
- Asset Management
- Redundancy Strategies
- Physical Security

Lesson 8: Explain Vulnerability Management
- Device and OS Vulnerabilities
- Application and Cloud Vulnerabilities
- Vulnerability Identification Methods

Lesson 9: Evaluate Network Security Capabilities
- Network Security Baselines
- Network Security Capability Enhancement

Lesson 10: Assess Endpoint Security Capabilities
- Implement Endpoint Security
- Mobile Device Hardening

Lesson 11: Enhance Application Security Capabilities
- Application Protocol Security Baselines
- Cloud and Web Application Security Concepts

Lesson 12: Explain Incident Response and Monitoring Concepts
- Incident Response
- Data Sources

Lesson 13: Analyse Indicators of Malicious Activity
- Malware Attack Indicators
- Application Attack Indicators

Lesson 14: Summarize Security Governance Concepts
- Policies, Standards, and Procedures
- Change Management

Lesson 15: Explain Risk Management Processes
- Risk Management Processes and Concepts
- Vendor Management Concepts
- Audits and Assessments

Lesson 16: Summarize Data Protection and Compliance Concepts
- Data Classification and Compliance
- Personnel Policies

SKILLS AND COMPETENCIES COVERED

General Security Concepts
12%

- Compare and contrast various types of security controls.
- Summarize fundamental security concepts.
- Explain the importance of change management processes and the impact to security.
- Explain the importance of using appropriate cryptographic solutions.

Threats, Vulnerabilities & Mitigations
22%

- Compare and contrast common threat actors and motivations.
- Explain common threat vectors and attack surfaces.
- Explain various types of vulnerabilities.
- Given a scenario, analyze indicators of malicious activity.
- Explain the purpose of mitigation techniques used to secure the enterprise.

Security Architecture
18%

- Compare and contrast security implications of different architecture models.
- Given a scenario, apply security principles to secure enterprise infrastructure.
- Compare and contrast concepts and strategies to protect data.
- Explain the importance of resilience and recovery in security architecture.

Security Operations
28%

- Given a scenario, apply common security techniques to computing resources.
- Explain the security implications of proper hardware, software, and data asset management.
- Explain various activities associated with vulnerability management.
- Explain security alerting and monitoring concepts and tools.
- Given a scenario, modify Enterprise capabilities to enhance security.
- Given a scenario, implement and maintain identity and access management.
- Explain the importance of automation and orchestration related to secure operations.
- Explain appropriate incident response activities.
- Given a scenario, use data sources to support an investigation.

Security Program Management & Oversight
20%

- Summarize elements of effective security governance.
- Explain elements of the risk management process.
- Explain the processes associated with third-party risk assessment and management.
- Summarize elements of effective security compliance.
- Explain types and purposes of audits and assessments.
- Given a scenario, implement security awareness practices.

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the CompTIA Security+ Exam SY0-701. Successfully passing this exam will result in the attainment of the CompTIA Security+ certification.