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 SY0-501) 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: Identifying Security Fundamentals

- Identify Information
- Security Concepts
- Identify Basic Security Controls
- Identify Basic Authentication and Authorization Concepts
- Identify Basic Cryptography Concepts

Lesson 2: Analysing Risk

- Analyse Organizational Risk
- Analyse the Business
- Impact of Risk

Lesson 3: Identifying Security Threats

- Identify Types of Attackers
- Identify Social Engineering Attacks
- Identify Malware
- Identify Software-Based Threats
- Identify Network-Based Threats
- Identify Wireless Threats
- Identify Physical Threats

Lesson 4: Conducting Security Assessments

- Identify Vulnerabilities
- Assess Vulnerabilities
- Implement Penetration Testing

Lesson 5: Implementing Host and Software Security

- Implement Host Security
- Implement Cloud and Virtualization Security
- Implement Mobile Device Security
- Incorporate Security in the Software Development Lifecycle

Module 6: Implementing Network Security

- Configure Network Security Technologies
- Secure Network Design Elements
- Implement Secure Networking Protocols and Services
- Secure Wireless Traffic

Module 7: Managing Identity and Access

- Implement Identity and Access Management
- Configure Directory Services
- Configure Access Services
- Manage Accounts

Lesson 8: Implementing Cryptography

- Identify Advanced Cryptography Concepts
- Select Cryptographic Algorithms
- Configure a Public Key Infrastructure
- Enrol Certificates
- Back Up and Restore Certificates and Private Keys
- Revoke Certificate

Lesson 9: Implementing Operational Security

- Evaluate Security Frameworks and Guidelines
- Incorporate Documentation in Operational Security
- Implement Security Strategies
- Manage Data Security Processes
- Implement Physical Controls

Lesson 10: Addressing Security Incidents

- Troubleshoot Common Security Issues
- Respond to Security Incidents
- Investigate Security Incidents

Lesson 11: Ensuring Business Continuity

- Select Business Continuity and Disaster Recovery Processes
- Develop a Business Continuity Plan

SKILLS AND COMPETENCIES COVERED

ASSOCIATED CERTIFICATIONS & EXAM

This course will prepare delegates to write the CompTIA Security+ Exam SY0-501. Successfully passing this exam will result in the attainment of the CompTIA Security+ certification.