CompTIA Security+ Certification Training (SY0-701)

Course Overview

The Official CompTIA Security+ Instructor and Student Guides teach students the knowledge and 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 regulations and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents; and to take the CompTIA Security+ certification exam.

Course Objectives

This course can benefit you in two ways. If you 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 IT security. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your cybersecurity skill set so that you can confidently perform your duties in any entry-level security role.

On course completion, you will be able to do the following:

- Summarize fundamental security concepts.
- Compare threat types.
- Explain appropriate cryptographic solutions.
- Implement identity and access management.
- Secure enterprise network architecture.
- Secure cloud network architecture.
- Explain resiliency and site security concepts.
- Explain vulnerability management.
- Evaluate network security capabilities.
- Assess endpoint security capabilities.
- Enhance application security capabilities.
- Explain incident response and monitoring concepts.
- Analyze indicators of malicious activity.
- Summarize security governance concepts.
- Explain risk management processes.
- Summarize data protection and compliance concepts.

Target Student

The Official CompTIA Security+ (Exam SY0-701) is the primary course you will need to take if your job responsibilities include safeguarding networks, detecting threats, and securing data in your organization. You can take this course to prepare for the CompTIA Security+ (Exam SY0-701) certification examination.

Course Prerequisites

To ensure your success in this course, you should have a minimum of two years of experience in IT administration with a focus on security, hands-on experience with technical information security, and a broad knowledge of security concepts. CompTIA A+ and CompTIA Network+, or the equivalent knowledge, is strongly recommended.

Associated Certifications

Security+

Table of Contents

Lesson 9 : Evaluate Network Security Capabilities

- Topic 9A: Network Security Baselines
- Topic 9B: Network Security Capability Enhancement

Lesson 10: Assess Endpoint Security Capabilities

- Topic 10A: Implement Endpoint Security
- Topic 10B: Mobile Device Hardening

Lesson 11: Enhance Application Security Capabilities

- Topic 11A: Application Protocol Security Baselines
- Topic 11B: Cloud and Web Application Security Concepts

Lesson 12: Explain Incident Response and Monitoring Concepts

- Topic 12A: Incident Response
- Topic 12B: Digital Forensics
- Topic 12C: Data Sources
- Topic 12D: Alerting and Monitoring Tools

Lesson 13: Analyze Indicators of Malicious Activity

- Topic 13A: Malware Attack Indicators
- Topic 13B: Physical and Network Attack Indicators
- Topic 13C: Application Attack Indicators

Lesson 14: Summarize Security Governance Concepts

- Topic 14A: Policies, Standards, and Procedures
- Topic 14B: Change Management
- Topic 14C: Automation and Orchestration

Lesson 15: Explain Risk Management Processes

- Topic 15A: Risk Management Processes and Concepts
- Topic 15B: Vendor Management Concepts
- Topic 15C: Audits and Assessments

Lesson 16: Summarize Data Protection and Compliance Concepts

- Topic 16A: Data Classification and Compliance
- Topic 16B: Personnel Policies

Appendix A: Mapping Course Content to CompTIA Security