CompTIA Security+

Course Description

CompTIA has developed the Official CompTIA Security+ Study Guide (SY0-701) for the CompTIA certification candidate. Rigorously evaluated by third-party subject matter experts to validate adequate coverage of the Security+ exam objectives, the Official CompTIA Security+ Study Guide teaches the essential skills and information required for the CompTIA certification exam (SY0-701).

Course Duration:

5 days

Prerequisites:

To get the most out of the CompTIA Security+ Study Guide and be able to prepare for your exam, you should have successfully passed the CompTIA Network+ certification exam and have acquired 24 months of experience in networking support and IT administration. We also recommend the following skills and knowledge before starting this course:
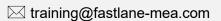
- Use a keyboard and mouse.
- Know the function and basic features of PC components.
- Able to use Windows to create and manage files and use basic administrative features (Explorer, Control Panel and Management Consoles).
- Know basic network terminology and functions (such as OSI Model, topology, Ethernet, TCP/IP, switches and routers).
- Understand TCP/IP addressing, core protocols and troubleshooting tools.

Objectives:

After you successfully complete this course, expect to be able to:

- 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.
- Compare and contrast common threat actors and motivations.
- Explain common threat vectors and attack surfaces.
- Explain various types of vulnerabilities.
- Analyze indicators of malicious activity.
- Explain the purpose of mitigation techniques used to secure the enterprise.
- Compare and contrast security implications of different architecture models.
- 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.
- 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.

- Modify enterprise capabilities to enhance security.
- Implement and maintain identity and access management.
- Explain the importance of automation and orchestration related to secure operations.
- Explain appropriate incident response activities.
- Use data sources to support an investigation.
- 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.
- Implement security awareness practices.

Course Outline:

- Lesson 1: Summarize Fundamental Security Concepts
- Lesson 2: Compare Threat Types
- Lesson 3: Explain Cryptographic Solutions
- Lesson 4: Implement Identity and Access Management
- Lesson 5: Secure Enterprise Network Architecture
- Lesson 6: Secure Cloud Network Architecture
- Lesson 7: Explain Resiliency and Site Security Concepts
- Lesson 8: Explain Vulnerability Management
- Lesson 9: Evaluate Network Security Capabilities
- Lesson 10: Assess Endpoint Security Capabilities
- Lesson 11: Enhance Application Security Capabilities
- Lesson 12: Explain Incident Response and Monitoring Concepts
- Lesson 13: Analyze Indicators of Malicious Activity
- Lesson 14: Summarize Security Governance Concepts
- Lesson 15: Explain Risk Management Processes
- Lesson 16: Summarize Data Protection and Compliance Concepts

Who Should Attend

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.