CompTIA Security+

Course Description

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations and its industry-leading IT certifications are an important part of that mission. CompTIA's Security+ certification is a foundation-level certificate designed for IT administrators with two years' experience whose job role is focused on system security. The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to assist with cybersecurity duties in small and large organizations. These duties include assessments and monitoring; secure network, host, app, and cloud provisioning; data governance; and incident analysis and response.

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on troubleshooting to ensure security professionals have practical security problem solving skills. Cybersecurity professionals with Security+ know how to address security incidents—not just identify them. Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and the government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program

Course Duration:

5 days

Prerequisites:

To ensure your success in this course, you should have basic Windows and Linux administrator skills and the ability to implement fundamental networking appliances and IP addressing concepts. CompTIA A+ and Network+ certifications, or equivalent knowledge, and six to nine months' experience in networking, including configuring security parameters, are strongly recommended.

Objectives:

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

- Compare security roles and security controls
- Explain threat actors and threat intelligence
- Perform security assessments and identify social engineering attacks and malware types
- Summarize basic cryptographic concepts and implement public key infrastructure
- Implement authentication controls
- Implement identity and account management controls
- Implement secure network designs, network security appliances, and secure network protocols
- Implement host, embedded/Internet of Things, and mobile security solutions
- Implement secure cloud solutions
- Explain data privacy and protection concepts
- Perform incident response and digital forensics
- Summarize risk management concepts and implement cybersecurity resilience
- Explain physical security

Course Outline:

- Comparing Security Roles and Security Controls
- Explaining Threat Actors and Threat Intelligence
- Performing Security Assessments
- Identifying Social Engineering and Malware
- Summarizing Basic Cryptographic Concepts
- Implementing Public Key Infrastructure
- Implementing Authentication Controls
- Implementing Identity and Account Management Controls
- Implementing Secure Network Designs
- Implementing Network Security Appliances
- Implementing Secure Network Protocols
- Implementing Host Security Solutions
- Implementing Secure Mobile Solutions
- Summarizing Secure Application Concepts
- Implementing Secure Cloud Solutions
- Explaining Data Privacy and Protection Concepts
- Performing Incident Response
- Explaining Digital Forensics
- Summarizing Risk Management Concepts
- Implementing Cybersecurity Resilience
- Explaining Physical Security

Who Should Attend

The Official CompTIA Security+ Guide (Exam SY0-601) is the primary course you will need to take if your job responsibilities include securing network services, devices, and data confidentiality/privacy in your organization. You can take this course to prepare for the CompTIA Security+ (Exam SY0-601) certification examination.