CompTIA Security+

Overview

The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations.

Course Objectives

This course will teach you the fundamental principles of installing and configuring cybersecurity controls and participating in incident response and risk mitigation. It will prepare you to take the CompTIA Security+ SY0-601 exam by providing 100% coverage of the objectives and content examples listed on the syllabus. Study of the course can also help to build the prerequisites to study more advanced IT security qualifications, such as CompTIA Cybersecurity Analyst (CSA)+, CompTIA Advanced Security Practitioner (CASP), and ISC's CISSP (Certified Information Systems Security Professional).

On course completion, you will be able to:

- Identify strategies developed by cyber adversaries to attack networks and hosts and the counter measures deployed to defend them.
- Understand the principles of organizational security and the elements of effective security policies.
- Know the technologies and uses of cryptographic standards and products.
- Install and configure network- and host-based security technologies.
- Describe how wireless and remote access security is enforced.
- Describe the standards and products used to enforce security on web and communications technologies.
- Identify strategies for ensuring business continuity, fault tolerance, and disaster recovery.
- Summarize application and coding vulnerabilities and identify development and deployment methods designed to mitigate them.

Duration

5 Days

CompTIA Security+

Who Should Attend

CompTIA Security+ is aimed at IT professionals with job roles such as security engineer, security consultant / specialist, information assurance technician, junior auditor / penetration tester, security administrator, systems administrator, and network administrator.

Prerequisites

Networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems, such as OS X, Unix, or Linux.

Recommended prerequisites:

- CompTIA Network+

CompTIA Security+

Course Topics

Module 1	**Comparing Security Roles and Controls** • Compare and Contrast Information Security Roles • Compare and Contrast Security Control and Framework
Module 2	**Explaining Threat Actors and Threat Intelligence** • Explain Threat Actor Types and Attack
Module 3	**Performing Security Assessments** • Assess Organizational Security with Network Reconnaissance Tools • Explain Security Concerns with General Vulnerability Types • Summarize Vulnerability Scanning Techniques • Explain Penetration Testing
Module 4	**Identifying Social Engineering and Malware** • Compare and Contrast Social Engineering Techniques • Analyze Indicators of Malware-Based
Module 5	**Summarizing Basic Cryptographic Concepts** • Compare and Contrast Cryptographic Ciphers • Summarize Cryptographic Modes of Operation • Summarize Cryptographic Use Cases and Weaknesses • Summarize Other Cryptographic
Module 6	**Implementing Public Key Infrastructure** • Implement Certificates and Certificate Authorities • Implement PKI.
Module 7	**Implementing Authentication Controls** • Summarize Authentication Design Concepts • Implement Knowledge-Based Authentication • Implement Authentication Technologies • Summarize Biometrics Authentication Concepts

CompTIA Security+

Module 8	**Implementing Identity and Account Management Controls** • Implement Identity and Account Types • Implement Account Policies • Implement Authorization Solutions • Explain the Importance of Personnel Policies
Module 9	**Implementing Secure Network Designs** • Implement Secure Network Designs • Implement Secure Switching and Routing • Implement Secure Wireless Infrastructure • Implement Load Balancers
Module 10	**Implementing Network Security Appliances** • Implement Firewalls and Proxy Servers • Implement Network Security Monitoring • Summarize the Use of SIEM
Module 11	**Implementing Secure Network Protocols** • Implement Secure Network Operations Protocols • Implement Secure Application Protocols • Implement Secure Remote Access Protocols
Module 12	**Implementing Host Security Solutions** • Implement Secure Firmware • Implement Endpoint Security • Explain Embedded System Security Implications
Module 13	**Implementing Secure Mobile Solutions** • Implement Mobile Device Management • Implement Secure Mobile Device Connections
Module 14	**Summarizing Secure Application Concepts** • Analyze Indicators of Application Attacks • Analyze Indicators of Web Application Attacks • Summarize Secure Coding Practices • Implement Secure Script Environments • Summarize Deployment and Automation Concepts

CompTIA Security+

Module 15	**Implementing Secure Cloud Solutions** • Summarize Secure Cloud and Virtualization Services • Apply Cloud Security Solutions • Summarize Infrastructure as Code Concepts
Module 16	**Explaining Data Privacy and Protection Concepts** • Explain Privacy and Data Sensitivity Concepts • Explain Privacy and Data Protection Controls
Module 17	**Performing Incident Response** • Summarize Incident Response Procedures • Utilize Appropriate Data Sources for Incident Response • Apply Mitigation Controls
Module 18	**Explaining Digital Forensics** • Explain Key Aspects of Digital Forensics Documentation • Explain Key Aspects of Digital Forensics Evidence Acquisition
Module 19	**Summarizing Risk Management Concepts**
Module 20	**Implementing Cybersecurity Resilience** • Implement Redundancy Strategies • Implement Backup Strategies • Implement Cybersecurity Resiliency Strategies
Module 21	**Explaining Physical Security** • Explain the Importance of Physical Site Security Controls • Explain the Importance of Physical Host Security Controls