CompTIA Security+

Course Duration: 5 Days
Exam Reference: SYO-701

Course Overview

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

The new CompTIA Security+ (SY0-701) represents the latest and greatest in cybersecurity, covering the most in-demand skills related to current threats, automation, zero trust, IoT, risk – and more. Once certified, you'll understand the core skills needed to succeed on the job – and employers will notice too. The Security+ exam verifies you have 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, Internet of Things (IoT), and operational technology.
- 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.

CompTIA Security+ is compliant with ISO 17024 standards and approved by the U.S. DoD to meet Directive 8140.03M requirements. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program. Over 3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

Prerequisites

- CompTIA Network+
- 2 years of experience working in a security/systems administrator job role

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

CompTIA Security+

Course Objectives

Students will be able to understand and explain:

- General Security Concepts: Understand foundational security principles like the CIA triad (Confidentiality, Integrity, Availability), Zero Trust, and basic cryptography to build a strong security mindset.
- Threats, Vulnerabilities, and Mitigations: Identify common cybersecurity threats, recognize system vulnerabilities, and learn effective techniques to prevent, detect, and respond to various attacks.
- Security Architecture: Design and implement secure enterprise environments by applying security principles to infrastructure, data protection, and resilience across various platforms, including cloud and mobile.
- Security Operations: Perform practical security tasks, including incident response, vulnerability management, security monitoring, and implementing identity and access management solutions.
- Security Program Management and Oversight: Grasp the importance of security governance, risk management, compliance with regulations, and fostering security awareness within an organization.

Course Outline

Module 1: Summarize
- Security Concepts
- Security Controls

Module 2: Compare Threat Types
- Threat Actors
- Attack Surfaces
- Social Engineering

Module 3: Explain Cryptographic Solutions
- Cryptographic Algorithms
- Public Key Infrastructure
- Cryptographic Solutions

CompTIA Security+

Module 4: Implement Identity and Access Management
- Authentication
- Authorization
- Identity Management

Module 5: Secure Enterprise Network Architecture
- Enterprise Network Architecture
- Network Security Appliances
- Secure Communications

Module 6: Secure Cloud Network Architecture
- Cloud Infrastructure
- Embedded Systems and Zero Trust Architecture

Module 7: Explain Resiliency and Site Security Concepts
- Asset Management
- Redundancy Strategies
- Physical Security

Module 8: Explain Vulnerability Management
- Device and OS Vulnerabilities
- Application and Cloud Vulnerabilities
- Vulnerability Identification Methods
- Vulnerability Analysis and Remediation

Module 9: Evaluate Network Security Capabilities
- Network Security Baselines
- Network Security Capability Enhancement

Module 10: Assess Endpoint Security Capabilities
- Implement Endpoint Security
- Mobile Device Hardening

Module 11: Enhance Application Security Capabilities
- Application Protocol Security Baselines
- Cloud and Web Application Security Concepts

Module 12: Explain Incident Response and Monitoring Concepts
- Incident Response
- Digital Forensics
- Data Sources
- Alerting and Monitoring Tools

CompTIA Security+

Module 13: Analyze Indicators of Malicious Activity
- Malware Attack Indicators
- Physical and Network Attack Indicators
- Application Attack Indicators

Module 14: Summarize Security Governance Concepts
- Policies, Standards, and Procedures
- Change Management
- Automation and Orchestration

Module 15: Explain Risk Management Processes
- Risk Management Processes and Concepts
- Vendor Management Concepts
- Audits and Assessments

Module 16: Summarize Data Protection and Compliance Concepts
- Data Classification and Compliance
- Personnel Policies