APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

CompTIA Security+ Training

CompTIA Authorized Training · Applied Technology Academy

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

LEVEL	DURATION	EXAM	EXPERIENCE	AVERAGE SALARY
Beginner	**5 Days**	**SY0-701**	**2 years: Security/ systems admin (Network+ recommended)**	**$85,270**

Course Overview

The CompTIA Security+ certification exam will verify the successful candidate has 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 Internet of Things (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.

Course Outline

- **Lesson 1: Summarize**
  - Topic 1A: Security Concepts
  - Topic 1B: Security Controls
- **Lesson 2: Compare Threat Types**
  - Topic 2A: Threat Actors
  - Topic 2B: Attack Surfaces
  - Topic 2C: Social Engineering
- **Lesson 3: Explain Cryptographic Solutions**
  - Topic 3A: Cryptographic Algorithms
  - Topic 3B: Public Key Infrastructure

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

  - Topic 3C: Cryptographic Solutions
- **Lesson 4: Implement Identity and Access Management**
  - Topic 4A: Authentication
  - Topic 4B: Authorization
  - Topic 4C: Identity Management
- **Lesson 5: Secure Enterprise Network Architecture**
  - Topic 5A: Enterprise Network Architecture
  - Topic 5B: Network Security Appliances
  - Topic 5C: Secure Communications
- **Lesson 6: Secure Cloud Network Architecture**
  - Topic 6A: Cloud Infrastructure
  - Topic 6B: Embedded Systems and Zero Trust Architecture
- **Lesson 7: Explain Resiliency and Site Security Concepts**
  - Topic 7A: Asset Management
  - Topic 7B: Redundancy Strategies
  - Topic 7C: Physical Security
- **Lesson 8: Explain Vulnerability Management**
  - Topic 8A: Device and OS Vulnerabilities
  - Topic 8B: Application and Cloud Vulnerabilities
  - Topic 8C: Vulnerability Identification Methods
  - Topic 8D: Vulnerability Analysis and Remediation
- **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

Intended Audience

- Security Specialist
- Security Administrator
- Systems Administrator Help Desk Analyst
- Security Analyst
- Security Engineer

Prerequisites

CompTIA Network+ and two years of experience working in a security/systems administrator job role.

Follow-On Courses

- CompTIA CySA+
- CompTIA Linux+
- CISSP

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.