![QuickStart - Over 35 Years Of Technology Training]

**Document Generated: 02/19/2026**

**Learning Style: Virtual Classroom**

**Technology: CompTIA**

**Difficulty: Beginner**

**Course Duration: 5 Days**

**Next Course Date: March 23, 2026**

# CompTIA Security+ (Exam SY0-701) Instructor Led Training



Our Security+ Certification Prep Course provides the basic knowledge needed to plan, implement, and maintain information security in a vendor-neutral format. This includes risk management, host and network security, authentication and access

control systems, cryptography, and organizational security. This course maps to the CompTIA Security+ certification exam (SY0-701). Our Classroom and Classroom Live courses utilize official CompTIA courseware and labs. Objective coverage is marked throughout the course.

A CompTIA Certified Information Security Analyst can earn up to **$95,829**/- per annum, on average.

## Course Objectives:

With the help of this course, you will be able to deploy information security across varying contexts. Once the course is complete, it will allow you to:

- Proactively implement sound security protocols to mitigate security risks

- Quickly respond to security issues

- Retroactively identify where security breaches may have occurred

- Design a network, on-site or in the cloud, with security in mind

## Audience:

This course is intended to be undertaken by those IT Professionals, having administrative and networking skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks. Additionally, those professionals who are familiar with operating systems like Unix, macOS®, Linux, and wish to further progress in their IT career by obtaining in-depth knowledge of security topics. It can also be undertaken by those opting to take the CompTIA Security+ certification examination or wish to use this as a means to attempt advanced level certifications related to security.

## Prerequisites:

- In order to be successful in this course, all students should have basic knowledge of Windows and know how to use it, along with an understanding of networking and computer concepts.

## Course Outline:

- Lesson 1: Summarize Fundamental Security Concepts
    - 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
  - 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

## Credly Badge:



**Display your Completion Badge And Get The Recognition You Deserve.**

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges