REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
*"Training You Can Really Use"*

# CompTIA® Security+™

## Duration: 5 Days

## Method: Instructor-Led Training (ILT) | Live Online Training

***Certification:*** *CompTIA Security+* — ***Exam****: SY0-701*

## Course Description

This course is designed to help participants prepare for the certification exam. Participants will implement and monitor security on networks, applications, and operating systems, and respond to security breaches.

## Target Audience

This course is intended for:

- Information Technology (IT) professionals who want to either:
  - Further their IT career by acquiring a foundational knowledge of security topics.
  - Prepare for the certification exam.
  - Use this course as the foundation for advanced security certifications or career roles.

## Prerequisites

To attend this course, candidates must have:

- Basic Windows® user skills.
- Fundamental understanding of computer and networking concepts or obtained the *CompTIA A+* and *Network+*® certifications.
- At least two (2) years of experience in IT administration with a security focus.

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
*"Training You Can Really Use"*

## Exam Details

| | |
|---|---|
| **Exam Code:** | • SY0-701 |
| **Length of Exam:** | • 90 Minutes |
| **Number of Questions:** | • 90 Questions Maximum |
| **Passing Score:** | • 750 out of 900 |
| **Question Format:** | • Multiple Choice and Performance Based Questions |

## Course Objectives

Upon successful completion of this course, attendees will be able to:

- Summarize fundamental security concepts.
- Compare threat types.
- Explain appropriate cryptographic solutions.
- Implement identity and access management.
- Secure enterprise network architecture.
- Secure cloud network architecture.
- Explain resiliency and site security concepts.
- Explain vulnerability management.
- Evaluate network security capabilities.
- Assess endpoint security capabilities.
- Enhance application security capabilities.
- Explain incident response and monitoring concepts.
- Analyse indicators of malicious activity.
- Summarize security governance concepts.
- Explain risk management processes.
- Summarize data protection and compliance concepts.

REAL WORLD
TECHNOLOGY TRAINING & SOLUTIONS
*"Training You Can Really Use"*

# Course Topics

## Module 1: Summarize Fundamental Security Concepts

- 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

## 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

## Course Topics *Continued*

### 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

### Module 13: Analyse 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

## LABS INCLUDED