CompTIA Security+

Duration	Delivery Methods
5 Days	VILT, Private Group

In this course, students will build on their knowledge of and professional experience with security fundamentals, networks, and organizational security as you acquire the specific skills required to implement basic security services on any type of computer network.
Attendees will acquire the skills to implement basic security services on any computer network. This is the first security certification IT professionals should earn, as the knowledge earned in this course provides a springboard to intermediate-level cybersecurity jobs and advanced IT security certifications.

This course is also designed for students who are seeking the CompTIA Security+ certification and who want to prepare for the CompTIA Security+ SY0-601 Certification Exam.

Who Should Attend

This course is designed for information technology (IT) professionals who have networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks; familiarity with other operating systems, such as macOS®, Unix®, or Linux®; and who want to further a career in IT by acquiring foundational knowledge of security topics or using CompTIA Security+ as the foundation for advanced security certifications or career roles. This course is also designed for students seeking the CompTIA Security+ certification who want to prepare for the CompTIA Security+ SY0-601 Certification Exam.

Course Objectives

Through the CompTIA Security+ course, students learn how to identify and address security incidents. On course completion, participants will be able to:

- Scan and assess networks for vulnerabilities
- Monitor network traffic for unusual activity
- Investigate a network breach
- Compare and contrast attacks
- Compare and contrast security controls
- Use security assessment tools
- Explain basic cryptography concepts
- Implement a public key infrastructure
- Implement identity and access management controls
- Manage access services and accounts
- Implement a secure network architecture
- Install and configure security appliances
- Install and configure wireless and physical access security
- Deploy secure host, mobile, and embedded systems
- Implement secure network access protocols
- Implement secure network applications
- Explain risk management and disaster recovery concepts
- Describe secure application development concepts
- Explain organizational security concepts

Agenda

1 - COMPARING SECURITY ROLES AND SECURITY CONTROLS

- Compare and Contrast Information Security Roles
- Compare and Contrast Security Control and Framework Types

2 - EXPLAINING THREAT ACTORS AND THREAT INTELLIGENCE

- Explain Threat Actor Types and Attack Vectors
- Explain Threat Intelligence Sources

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 Concepts

4 - IDENTIFYING SOCIAL ENGINEERING AND MALWARE

- Compare and Contrast Social Engineering Techniques

- Analyze Indicators of Malware-Based Attacks

5 - SUMMARIZING BASIC CRYPTOGRAPHIC CONCEPTS

- Compare and Contrast Cryptographic Ciphers
- Summarize Cryptographic Modes of Operation
- Summarize Cryptographic Use Cases and Weaknesses
- Summarize Other Cryptographic Technologies

6 - IMPLEMENTING PUBLIC KEY INFRASTRUCTURE

- Implement Certificates and Certificate Authorities
- Implement PKI Management

7 - IMPLEMENTING AUTHENTICATION CONTROLS

- Summarize Authentication Design Concepts
- Implement Knowledge-Based Authentication
- Implement Authentication Technologies
- Summarize Biometrics Authentication Concepts

8 - IMPLEMENTING IDENTITY AND ACCOUNT MANAGEMENT CONTROLS

- Implement Identity and Account Types
- Implement Account Policies
- Implement Authorization Solutions
- Explain the Importance of Personnel Policies

9 - IMPLEMENTING SECURE NETWORK DESIGNS

- Implement Secure Network Designs
- Implement Secure Switching and Routing
- Implement Secure Wireless Infrastructure
- Implement Load Balancers

10 - IMPLEMENTING NETWORK SECURITY APPLIANCES

- Implement Firewalls and Proxy Servers
- Implement Network Security Monitoring
- Summarize the Use of SIEM

11 - IMPLEMENTING SECURE NETWORK PROTOCOLS

- Implement Secure Network Operations Protocols
- Implement Secure Application Protocols
- Implement Secure Remote Access Protocols

12 - IMPLEMENTING HOST SECURITY SOLUTIONS

- Implement Secure Firmware

- Implement Endpoint Security
- Explain Embedded System Security Implications

13 - IMPLEMENTING SECURE MOBILE SOLUTIONS

- Implement Mobile Device Management
- Implement Secure Mobile Device Connections

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

15 - IMPLEMENTING SECURE CLOUD SOLUTIONS

- Summarize Secure Cloud and Virtualization Services
- Apply Cloud Security Solutions
- Summarize Infrastructure as Code Concepts

16 - EXPLAINING DATA PRIVACY AND PROTECTION CONCEPTS

- Explain Privacy and Data Sensitivity Concepts
- Explain Privacy and Data Protection Controls

17 - PERFORMING INCIDENT RESPONSE

- Summarize Incident Response Procedures
- Utilize Appropriate Data Sources for Incident Response
- Apply Mitigation Controls

18 - EXPLAINING DIGITAL FORENSICS

- Explain Key Aspects of Digital Forensics Documentation
- Explain Key Aspects of Digital Forensics Evidence Acquisition

19 - SUMMARIZING RISK MANAGEMENT CONCEPTS

- Explain Risk Management Processes and Concepts
- Explain Business Impact Analysis Concepts

20 - IMPLEMENTING CYBERSECURITY RESILIENCE

- Implement Redundancy Strategies
- Implement Backup Strategies
- Implement Cybersecurity Resiliency Strategies

21 - EXPLAINING PHYSICAL SECURITY

- Explain the Importance of Physical Site Security Controls
- Explain the Importance of Physical Host Security Controls