CompTIA Security+

Course Description: This course maps to the CompTIA Security+ certification exam (SK0-601) and establishes the core knowledge required of any cybersecurity role, as well as providing a springboard to intermediate-level cybersecurity jobs. This course emphasizes both the practical and hands-on ability to identify and address security threats, attacks and vulnerabilities. CompTIA Security+ is a globally trusted, vendor-neutral certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career

Duration: Instructor-led, group-paced, classroom-delivery learning model with structured hands-on activities
35 hours (5 days)

Objectives: After completing this course, students will be able to:

- Prepare for the CompTIA Security+ exam
- Implement robust identity management and access control
- Confidently explain and define an array of security vulnerabilities
- Navigate the complexities of secure system and network design
- Explore the defensive measures like PKI, firewalls and IDS

Prerequisites: A+, Network+, 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.

Course Outline

Comparing Security Roles and Controls

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

Explaining Threat Actors and Threat Intelligence

- Compare and Contrast Security Control and Framework Types
- Follow Incident Response Procedures

Performing Security Assessments

- Explain Penetration Testing Concepts
- Assess Organizational Security with Network Reconnaissance Tools
- Explain Security Concerns with General Vulnerability Types
- Summarize Vulnerability Scanning Techniques

Identifying Social Engineering and Malware

- Compare and Contrast Social Engineering Techniques
- Analyze Indicators of Malware-Based Attacks

Summarizing Basic Cryptographic Concepts

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

Implementing Public Key Infrastructure

- Implement Certificates and Certificate Authorities
- Implement PKI Management

Implementing Authentication Controls

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

Implementing Identity and Account Management Controls

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

Implementing Secure Network Designs

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

CompTIA Security+

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

Implementing Secure Network Protocols
- Implement Secure Network Operations Protocols
- Implement Secure Applications Protocols
- Implement Secure Remote Access Protocols

Implementing Secure Mobile Solutions
- Implement Mobile Device Management
- Implement Secure Mobile Device Connections

Implementing Secure Application Concepts
- Analyze Indicators of Application Attacks
- Analyze Indicators of Web Application Attacks
- Implement Secure Script Environments
- Summarize Deployment and Automation Concepts

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

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

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

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

Summarizing Risk Management Concepts
- Explain Risk Management Processes and Concepts

Implementing Cybersecurity Resilience
- Implement Redundancy, Backup and Cybersecurity Strategies

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