CompTIA Security+

Duration
***5* Days**

Course Overview

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and is the first security certification a candidate should earn.

CompTIA Security+ establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs.

Who Should Attend

This course is designed for people who are seeking to launch a career in cybersecurity.

Course Objectives

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, and IoT.
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

Course Prerequisites

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

Course Outline

LESSON 1: SUMMARIZE FUNDAMENTAL SECURITY CONCEPTS

- Security Concepts
- Security Controls

LESSON 2: COMPARE THREAT TYPES

- Threat Actors
- Attack Surfaces
- Social Engineering

LESSON 3: EXPLAIN CRYPTOGRAPHIC SOLUTIONS

- Cryptographic Algorithms
- Public Key Infrastructure
- Cryptographic Solutions

LESSON 4: IMPLEMENT IDENTITY AND ACCESS MANAGEMENT

- Authentication
- Authorization
- Identity Management

LESSON 5: SECURE ENTERPRISE NETWORK ARCHITECTURE

- Enterprise Network Architecture
- Network Security Appliances
- Secure Communications

LESSON 6: SECURE CLOUD NETWORK ARCHITECTURE

- Cloud Infrastructure
- Embedded Systems and Zero Trust Architecture

LESSON 7: EXPLAIN RESILIENCY AND SITE SECURITY CONCEPTS

- Asset Management
- Redundancy Strategies
- Physical Security

LESSON 8: EXPLAIN VULNERABILITY MANAGEMENT

- Device and OS Vulnerabilities
- Application and Cloud Vulnerabilities
- Vulnerability Identification Methods
- Vulnerability Analysis and Remediation

LESSON 9: EVALUATE NETWORK SECURITY CAPABILITIES

- Network Security Baselines
- Network Security Capability Enhancement

LESSON 10: ASSESS ENDPOINT SECURITY CAPABILITIES

- Implement Endpoint Security
- Mobile Device Hardening

LESSON 11: ENHANCE APPLICATION SECURITY CAPABILITIES

- Application Protocol Security Baselines
- Cloud and Web Application Security Concepts

LESSON 12: EXPLAIN INCIDENT RESPONSE AND MONITORING CONCEPTS

- Digital Forensics
- Data Sources
- Alerting and Monitoring Tools

LESSON 13: ANALYZE INDICATORS OF MALICIOUS ACTIVITY

- Malware Attack Indicators

- Physical and Network Attack Indicators
- Application Attack Indicators

LESSON 14: SUMMARIZE SECURITY GOVERNANCE CONCEPTS

- Policies, Standards, and Procedures
- Change Management
- Automation and Orchestration

LESSON 15: EXPLAIN RISK MANAGEMENT PROCESSES

- Risk Management Processes and Concepts
- Vendor Management Concepts
- Audits and Assessments

LESSON 16: SUMMARIZE DATA PROTECTION AND COMPLIANCE CONCEPTS

- Data Classification and Compliance
- Personnel Policies