Security+

Price	Duration	Delivery Methods
$1,295.00	5 Daytime Classes or 10 Evening Classes	Virtual, Private Group,

CAREER SKILLS+™

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.)

Agenda

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
Incident Response
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