CompTIA Security+ (Exam SYO-501)

Modality: On Demand

Duration: 16 Hours

This course prepares you for the SY0-501 Exam leading to SY0-501 Certification. This course does not include the Official Exam Voucher, however, you can request to purchase the Official Exam Voucher separately.

About this course:

Through this CompTIA Security+ training online course, students will be equipped with the knowledge required to identify security fundamentals along with threats, conduct security assessments, analyze risks, deploy network, manage identity as well as access, operational host and software security, deploy cryptography, ensure business continuity, and address any security related issues.

On average, an individual having CompTIA Security+ certification can earn up to **$95,829**/- per annum.

Course Objective:

The CompTIA Security+ online classes have been designed to provide comprehensive information about CompTIA Security+ Certification (SY0-501) so that you can prepare for the exam and obtain this certification. With the skills learned throughout the course and the added certification details in your resume, you can be sure to catch the eye of the hiring manager. For those professionals, who are already working in any organization, this certification will be the push they need in order to progress through their career. Not only will you have this certification but also a surety of a successful IT career. It is a perfect study tool and a reference for on the job training.

Audience:

This course is designed to be undertaken by those professionals who are seeking a position in IT Security or want to upgrade their skill set and obtain the CompTIA Security+ Certification. At the same time, it will also equip you with the skills needed to excel in your job.

Prerequisite:

Prior to enrolling in this course, candidates should possess;

- Basic knowledge and understanding of networks and personal computers
- Apart from this there are no other pre-requisite courses that an individual should have done in order to enroll in this course.

Course Outline:

Course Introduction

- Instructor Bio
- Course Introduction
- Courseware

Chapter 01: Identifying Security Fundamentals

Topic A: Identify Information Security Concepts

- Identify Information Security Concepts - Part 1
- Identify Information Security Concepts - Part 2
- Information Security
- Goals of Information Security
- Risk
- Vulnerabilities
- Threats
- Attacks
- Controls
- Types of Controls
- The Security Management Process
- Demo - Identifying Information Security Basics

Topic B: Identify Basic Security Controls

- The CIA Triad - Part 1
- The CIA Triad - Part 2
- Non-repudiation
- Identification
- Authentication
- Authentication Factors
- Authorization
- Access Control
- Accounting and Auditing
- Principle of Least Privilege
- Privilege Management
- Demo - Identifying Basic Security Controls

Topic C: Identify Basic Authentication and Authorization Concepts

- Passwords
- Tokens
- Biometrics
- Geolocation
- Keystroke Authentication
- Multi-factor Authentication
- Mutual Authentication
- Demo - Identifying Basic Authentication and Authorization Concepts

Topic D: Identify Basic Cryptography Concepts

- Cryptography
- Encryption and Decryption - Part 1
- Encryption and Decryption - Part 2
- Encryption and Security Goals
- Ciphers
- A Key
- Symmetric Encryption
- Asymmetric Encryption - Part 1
- Asymmetric Encryption - Part 2
- Hashing
- Steganography
- Demo - Identifying Basic Cryptography Concepts
- Chapter 01 Review
- Review

Chapter 02: Analyzing Risk

Topic A: Analyze Organizational Risk

- Analyze Organizational Risk - Part 1
- Analyze Organizational Risk - Part 2
- Risk Management
- Components of Risk Analysis
- Phases of Risk Analysis
- Categories of Threat Types
- Risk Analysis Methods
- Risk Calculation
- Risk Response Techniques
- Risk Mitigation and Control Types
- Change Management - Part 1
- Change Management - Part 2
- Guidelines for Analyzing Risk
- Demo - Analyzing Risks to the Organization

Topic B: Analyze the Business Impact of Risk

- BIA
- Impact Scenarios - Part 1
- Impact Scenarios - Part 2
- Impact Scenarios - Part 3
- Privacy Assessments
- Critical Systems and Functions
- Maximum Tolerable Downtime
- Recovery Point Objective
- Recovery Time Objective
- Mean Time to Failure

- Mean Time to Repair
- Mean Time Between Failures
- Guidelines for Performing a Business Impact Analysis
- Demo - Performing a Business Impact Analysis
- Chapter 02 Review
- Review

Chapter 03: Identifying Security Threats

Topic A: Identify Types of Attackers

- Identify Types of Attackers - Part 1
- Identify Types of Attackers - Part 2
- Hackers and Attackers - Part 1
- Hackers and Attackers - Part 2
- Threat Actors - Part 1
- Threat Actors - Part 2
- Threat Actor Attributes - Part 1
- Threat Actor Attributes - Part 2
- Open-Source Intelligence
- Demo - Identifying Types of Attackers

Topic B: Identify Social Engineering Attacks

- Social Engineering - Part 1
- Social Engineering - Part 2
- Effectiveness
- Impersonation
- Phishing and Related Attacks - Part 1
- Phishing and Related Attacks - Part 2
- Hoaxes
- Physical Exploits
- Watering Hole Attacks
- Demo - Identifying Social Engineering Attacks

Topic C: Identify Malware

- Malicious Code - Part 1
- Malicious Code - Part 2
- Viruses
- Worms
- Adware
- Spyware
- Trojan Horses
- Keyloggers
- Remote Access Trojans
- Logic Bombs
- Botnets - Part 1

- Botnets - Part 2
- Ransomware - Part 1
- Ransomware - Part 2
- Advance Persistent Threats
- Demo - Identifying Types of Malware

Topic D: Identify Software-Based Threats

- Software Attacks
- Password Attacks
- Types of Password Attacks - Part 1
- Types of Password Attacks - Part 2
- Cryptographic Attacks
- Types of Cryptographic Attacks - Part 1
- Types of Cryptographic Attacks - Part 2
- Backdoor Attacks - Part 1
- Backdoor Attacks - Part 2
- Application Attacks - Part 1
- Application Attacks - Part 2
- Types of Application Attacks
- Driver Manipulation
- Privilege Escalation - Part 1
- Privilege Escalation - Part 2
- Demo - Identifying Password Attacks

Topic E: Identify Network-Based Threats

- TCP/IP Basics - Part 1
- TCP/IP Basics - Part 2
- Spoofing Attacks
- IP and MAC Address Spoofing - Part 1
- IP and MAC Address Spoofing - Part 2
- ARP Poisoning
- DNS Poisoning
- Port Scanning Attacks - Part 1
- Port Scanning Attacks - Part 2
- Scan Types - Part 1
- Scan Types - Part 2
- Eavesdropping Attacks
- Man-in-the-Middle Attacks - Part 1
- Man-in-the-Middle Attacks - Part 2
- Man-in-the-Browser Attacks
- Replay Attacks - Part 1
- Replay Attacks - Part 2
- DoS Attacks
- DDoS Attacks
- Hijacking Attacks - Part 1
- Hijacking Attacks - Part 2

- Amplification Attacks - Part 1
- Amplification Attacks - Part 2
- Pass the Hash Attacks
- Demo - Identifying Threats to DNS
- Demo - Identifying Port Scanning Threats

Topic F: Identify Wireless Threats

- Rogue Access Points
- Evil Twins
- Jamming
- Bluejacking
- Bluesnarfing
- Near Field Communication Attacks
- RFID System Attacks
- War Driving, War Walking, and War Chalking
- Packet Sniffing
- IV Attacks
- Wireless Replay Attacks
- WEP and WPA Attacks
- WPS Attacks
- Wireless Disassociation
- Demo - Identifying Wireless Threats

Topic G: Identify Physical Threats

- Physical Threats and Vulnerabilities
- Hardware Attacks
- Environmental Threats and Vulnerabilities - Part 1
- Environmental Threats and Vulnerabilities - Part 2
- Demo - Identifying Physical Threats
- Chapter 03 Review
- Review

Chapter 04: Conducting Security Assessments

Topic A: Identify Vulnerabilities

- Identify Vulnerabilities - Part 1
- Identify Vulnerabilities - Part 2
- Host Vulnerabilities
- Software Vulnerabilities
- Encryption Vulnerabilities
- Network Architecture Vulnerabilities
- Account Vulnerabilities
- Operations Vulnerabilities
- Demo - Identifying Vulnerabilities

Topic B: Assess Vulnerabilities

- Security Assessment
- Security Assessment Techniques
- Vulnerability Assessment Tools
- Types of Vulnerability Scans
- False Positives
- Guidelines for Assessing Vulnerabilities
- Demo - Capturing Network Data with Wireshark
- Demo - Scanning for General Vulnerabilities

Topic C: Implement Penetration Testing

- Penetration Testing
- Penetration Testing Techniques
- Box Testing Methods
- Penetration Testing Tools
- Guidelines for Implementing Penetration Testing
- Demo - Implementing Penetration Testing
- Chapter 04 Review
- Review

Chapter 05: Implementing Host and Software Security

Topic A: Implement Host Security

- Implement Host Security - Part 1
- Implement Host Security - Part 2
- Hardening
- Operating System Security
- Operating System Hardening Techniques
- Trusted Computing Base
- Hardware and Firmware Security - Part 1
- Hardware and Firmware Security - Part 2
- Security Baselines
- Software Updates
- Application Blacklisting and Whitelisting
- Logging
- Auditing
- Anti-malware Software
- Types of Anti-malware Software
- Hardware Peripheral Security
- Embedded Systems
- Security Implications for Embedded Systems - Part 1
- Security Implications for Embedded Systems - Part 2
- Guidelines for Securing Hosts
- Demo - Implementing Auditing
- Demo - Hardening a Server

Topic B: Implement Cloud and Virtualization Security

- Virtualization
- Hypervisors - Part 1
- Hypervisors - Part 2
- Virtual Desktop Infrastructure
- Virtualization Security
- Cloud Computing
- Cloud Deployment Models
- Cloud Service Types
- Guidelines for Securing Virtualized and Cloud-Based Resources
- Demo - Securing Virtual Machine Networking

Topic C: Implement Mobile Device Security

- Mobile Device Connection Methods - Part 1
- Mobile Device Connection Methods - Part 2
- Mobile Device Management
- Mobile Device Security Controls - Part 1
- Mobile Device Security Controls - Part 2
- Mobile Device Monitoring and Enforcement - Part 1
- Mobile Device Monitoring and Enforcement - Part 2
- Mobile Deployment Models
- BYOD Security Controls
- Guidelines for Implementing Mobile Device Security
- Demo - Implementing Mobile Device Security

Topic D: Incorporate Security in the Software Development Lifecycle

- Software Development Lifecycle
- Software Development Models
- DevOps
- Versioning
- Secure Coding Techniques - Part 1
- Secure Coding Techniques - Part 2
- Code Testing Methods
- Guidelines for Incorporating Security in the Software Development Lifecycle
- Demo - Performing Static Code Analysis
- Chapter 05 Review
- Review

Chapter 06: Implementing Network Security

Topic A: Configure Network Security Technologies

- Configure Network Security Technologies - Part 1
- Configure Network Security Technologies - Part 2
- Network Components

- Network Devices
- Routers
- Switches
- Proxies
- Firewalls
- Load Balancer
- Network Scanners and Analysis Tools
- Intrusion Detection Systems
- Network IDS
- Intrusion Prevention Systems
- Network IPS
- Types of Network Monitoring Systems
- Security Information and Event Management
- Data Loss/Leak Prevention
- Virtual Private Networks
- VPN Concentrators
- Security Gateways
- Unified Threat Management
- Guidelines for Configuring Network Security Technologies
- Demo - Configuring a Network IDS

Topic B: Secure Network Design Elements

- Network Access Control
- Demilitarized Zones
- Network Isolation - Part 1
- Network Isolation - Part 2
- Virtual Local Area Networks - Part 1
- Virtual Local Area Networks - Part 2
- Network Security Device Placement
- Network Address Translation
- Software-Defined Networking
- Guidelines for Securing Network Design Elements
- Demo - Securing Network Design Elements

Topic C: Implement Secure Networking Protocols and Services

- The Open Systems Interconnection Model
- OSI Model and Security
- Internet Protocol Suite
- Domain Name System
- Hypertext Transfer Protocol
- Secure Sockets Layer/Transport Layer Security - Part 1
- Secure Sockets Layer/Transport Layer Security - Part 2
- HTTP Secure
- Secure Shell
- Simple Network Management Protocol
- Real-Time Transport Protocol

- Internet Control Message Protocol
- Internet Protocol Security
- Network Basic Input/Output System
- File Transfer Protocols
- Email Protocols
- Additional Networking Protocols and Services
- Ports and Port Ranges
- Demo - Installing an Internet Information Services Web Server with Basic Security
- Demo - Securing Network Traffic Using IPSec

Topic D: Secure Wireless Traffic

- Wireless Networks
- Wireless Antenna Types
- 802.11 Protocols
- Wireless Cryptographic Protocols
- Wireless Authentication Protocols
- VPNs and Open Wireless
- Wireless Client Authentication Methods
- Wireless Access Point Security
- Captive Portals
- Site Surveys
- Guidelines for Securing Wireless Traffic
- Demo - Securing Wireless Traffic
- Chapter 06 Review
- Review

Chapter 07: Managing Identity and Access

Topic A: Implement Identity and Access Management

- Implement Identity and Access Management - Part 1
- Implement Identity and Access Management - Part 2
- Identity and Access Management
- Access Control Models
- Physical Access Control Devices
- Biometric Devices
- Certificate-Based Authentication
- File System and Database Access
- Guidelines for Implementing IAM
- Demo - Implementing DAC for a File Share

Topic B: Configure Directory Services

- Directory Services - Part 1
- Directory Services - Part 2
- Lightweight Directory Access Protocol
- Secure LDAP

- Common Directory Services
- Demo - Backing Up Active Directory
- **Topic C: Configure Access Services**
- Remote Access Methods
- Tunneling
- Remote Access Protocols
- HMAC-Based One-Time Password
- Time-Based OTP
- Password Authentication Protocol
- Challenge-Handshake Authentication Protocol
- NT LAN Manager
- Authentication, Authorization, and Accounting
- Remote Authentication Dial-In User Service - Part 1
- Remote Authentication Dial-In User Service - Part 2
- Terminal Access Controller Access-Control System
- Kerberos - Part 1
- Kerberos - Part 2
- Demo - Configuring a Remote Access Server
- Demo - Setting Up Remote Access Authentication

Topic D: Manage Accounts

- Account Management
- Account Privileges
- Account Types
- Account Policy
- Password Policy
- Multiple Accounts
- Shared Accounts
- Account Management Security Controls
- Credential Management
- Group Policy
- Identity Federation
- Identity Federation Methods
- Guidelines for Managing Accounts
- Demo - Managing Accounts
- Chapter 07 Review
- Review

Chapter 08: Implementing Cryptography

Topic A: Identify Advanced Cryptography Concepts

- Identify Advanced Cryptography Concepts - Part 1
- Identify Advanced Cryptography Concepts - Part 2
- Cryptography Elements
- Hashing Concepts
- Data States

- Key Exchange - Part 1
- Key Exchange - Part 2
- Digital Signatures - Part 1
- Digital Signatures - Part 2
- Cipher Suites
- Session Keys
- Key Stretching
- Special Considerations for Cryptography
- Demo - Identifying Advanced Cryptographic Concepts

Topic B: Select Cryptographic Algorithms

- Types of Ciphers
- Types of Hashing Algorithms
- Types of Symmetric Encryption Algorithms
- Types of Asymmetric Encryption Techniques
- Types of Key Stretching Algorithms
- Substitution Ciphers
- Exclusive Or
- Cryptographic Modules
- Demo - Selecting Cryptographic Algorithms

Topic C: Configure a Public Key Infrastructure

- Public Key Infrastructure
- PKI Components
- CA Hierarchies
- The Root CA
- Subordinate CAs
- Offline Root CAs
- Types of Certificates - Part 1
- Types of Certificates - Part 2
- X.509
- Certificate File Formats
- CA Hierarchy Design Options
- Demo - Installing a CA
- Demo - Securing a Windows Server 2016 CA

Topic D: Enroll Certificates

- The Certificate Enrollment Process
- The Certificate Lifecycle
- Certificate Lifecycle Management
- The SSL/TLS Connection Process
- Demo - Enrolling Certificates
- Demo - Securing Network Traffic with Certificates

Topic E: Back Up and Restore Certificates and Private Keys

- Private Key Protection Methods
- Key Escrow
- Private Key Restoration Methods
- Private Key Replacement
- Demo - Backing Up a Certificate and Private Key
- Demo - Restoring a Certificate and Private Key
- **Topic F: Revoke Certificates**
- Certificate Revocation
- Certificate Revocation List - Part 1
- Certificate Revocation List - Part 2
- Online Certificate Status Protocol
- Demo - Revoking Certificates
- Chapter 08 Review
- Review

Chapter 09: Implementing Operational Security

Topic A: Evaluate Security Frameworks and Guidelines

- Evaluate Security Frameworks and Guidelines - Part 1
- Evaluate Security Frameworks and Guidelines - Part 2
- Security Frameworks
- Security Framework Examples
- Security Configuration Guides
- Compliance
- Layered Security
- Defense in Depth
- Demo - Evaluating Security Frameworks and Guidelines

Topic B: Incorporate Documentation in Operational Security

- Security Policies - Part 1
- Security Policies - Part 2
- Common Security Policy Types
- Personnel Management
- Separation of Duties
- Job Rotation
- Mandatory Vacation
- Additional Personnel Management Tasks
- Training and Awareness
- Business Agreements
- Guidelines for Incorporating Documentation in Operational Security
- Demo - Incorporating Documentation in Operational Security

Topic C: Implement Security Strategies

- Security Automation
- Scalability

- Elasticity
- Redundancy
- Fault Tolerance
- Redundant Array of Independent Disks
- Non-persistence
- High Availability
- Deployment Environments
- Guidelines for Implementing Security Strategies
- Demo - Implementing Virtual Machine Snapshots

Topic D: Manage Data Security Processes

- Data Security
- Data Security Vulnerabilities
- Data Storage Methods
- Data Encryption Methods
- Data Sensitivity
- Data Management Roles
- Data Retention
- Data Disposal
- Guidelines for Managing Data Security
- Demo - Destroying Data Securely
- Demo - Encrypting a Storage Device

Topic E: Implement Physical Controls

- Physical Security Controls
- Physical Security Control Types - Part 1
- Physical Security Control Types - Part 2
- Physical Security Control Types - Part 3
- Physical Security Control Types - Part 4
- Environmental Exposures
- Environmental Controls - Part 1
- Environmental Controls - Part 2
- Environmental Monitoring
- Safety
- Guidelines for Implementing Physical Controls
- Demo - Implementing Physical Controls
- Chapter 09 Review
- Review

Chapter 10: Addressing Security Issues

Topic A: Troubleshoot Common Security Issues

- Troubleshoot Common Security Issues - Part 1
- Troubleshoot Common Security Issues - Part 2
- Access Control Issues

- Encryption Issues
- Data Exfiltration
- Anomalies in Event Logs
- Security Configuration Issues
- Baseline Deviations
- Software Issues
- Personnel Issues
- Asset Management Issues
- Demo - Identifying Event Log Anomalies

Topic B: Respond to Security Incidents

- Incident Response
- Incident Preparation
- Incident Detection and Analysis
- Incident Containment
- Incident Eradication
- Incident Recovery
- Lessons Learned
- Incident Response Plans
- First Responders
- An Incident Report
- Guidelines for Responding to Security Incidents
- Demo - Responding to a Security Incident

Topic C: Investigate Security Incidents

- Computer Forensics
- The Basic Forensic Process
- Preservation of Forensic Data
- Basic Forensic Response Procedures - Part 1
- Basic Forensic Response Procedures - Part 2
- Order of Volatility
- Chain of Custody
- Guidelines for Investigating Security Incidents
- Demo - Implementing Forensic Procedures
- Chapter 10 Review
- Review

Chapter 11: Ensuring Business Continuity

Topic A: Select Business Continuity and Disaster Recovery Processes

- Select Business Continuity and Disaster Recovery Processes - Part 1
- Select Business Continuity and Disaster Recovery Processes - Part 2
- Business Continuity and Disaster Recovery
- The Disaster Recovery Process
- Recovery Team

- Order of Restoration
- Recovery Sites
- Secure Recovery
- Backup Types (Full)
- Backup Types (Differential vs. Incremental)
- Secure Backups
- Geographic Considerations
- Guidelines for Selecting Business Continuity and Disaster Recovery Processes
- Demo - Selecting Business Continuity and Disaster Recovery Processes

Topic B: Develop a Business Continuity Plan

- Business Continuity Plans - Part 1
- Business Continuity Plans - Part 2
- Disaster Recovery Plans - Part 1
- Disaster Recovery Plans - Part 2
- IT Contingency Plans
- Succession Plans
- Failover
- Alternate Business Practices
- Testing Exercises
- After-Action Reports
- Guidelines for Developing a BCP
- Demo - Developing a BCP
- Chapter 11 Review
- Review

Course Summary

- Course Closure
- Course Summary