CompTIA Security+ (Exam SY0-701) (CompTiaSec-SY0-701)

Modality: Virtual Classroom

Duration: 5 Days

"If you enroll in this course without the Master Subscription plan, you receive a Free Official Exam Voucher for SY0-701 Exam. This course does not include Exam Voucher if enrolled within the Master Subscription, however, you can request to purchase the Official Exam Voucher separately."

About the course:

Our Security+ Certification Prep Course provides the basic knowledge needed to plan, implement, and maintain information security in a vendor-neutral format. This includes risk management, host and network security, authentication and access control systems, cryptography, and organizational security. This course maps to the CompTIA Security+ certification exam (SY0-701). Our Classroom and Classroom Live courses utilize official CompTIA courseware and labs. Objective coverage is marked throughout the course.

A CompTIA Certified Information Security Analyst can earn up to **$95,829**/- per annum, on average.

Course Objectives:

With the help of this course, you will be able to deploy information security across varying contexts. Once the course is complete, it will allow you to:

- Proactively implement sound security protocols to mitigate security risks
- Quickly respond to security issues
- Retroactively identify where security breaches may have occurred
- Design a network, on-site or in the cloud, with security in mind

Audience:

This course is intended to be undertaken by those IT Professionals, having administrative and networking skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks. Additionally, those professionals who are familiar with operating systems like Unix, macOS®, Linux, and wish to further progress in their IT career by obtaining in-depth knowledge of security topics. It can also be undertaken by those opting to take the CompTIA Security+ certification examination or wish to use this as a means to attempt advanced level certifications related to security.

Prerequisites:

In order to be successful in this course, all students should have basic knowledge of Windows and

know how to use it, along with an understanding of networking and computer concepts.

Suggested Prerequisite course:

It is recommended to have cleared the following course prior to opting for this one.

- CompTIA A+ Certification: A Comprehensive Approach (Exams 220-1001 and 220-1002) (Comptia-A)
- CompTIA Network+ (Exam N10-008) (ComptiaNet)

Course Outline:

Lesson 1: Comparing Security Roles and Controls

Topic 1A: Compare and Contrast Information Security Roles
Topic 1B: Compare and Contrast Security Control and Framework Types

Lesson 2: Explaining Threat Actors and Threat Intelligence

Topic 2A: Explain Threat Actor Types and Attack Vectors

Lesson 3: Performing Security Assessments

Topic 3A: Assess Organizational Security with Network Reconnaissance Tools
Topic 3B: Explain Security Concerns with General Vulnerability Types
Topic 3C: Summarize Vulnerability Scanning Techniques
Topic 3D: Explain Penetration Testing Concepts

Lesson 4: Identifying Social Engineering and Malware

Topic 4A: Compare and Contrast Social Engineering Techniques
Topic 4B: Analyze Indicators of Malware-Based Attacks

Lesson 5: Summarizing Basic Cryptographic Concepts

Topic 5A: Compare and Contrast Cryptographic Ciphers
Topic 5B: Summarize Cryptographic Modes of Operation
Topic 5C: Summarize Cryptographic Use Cases and Weaknesses
Topic 5D: Summarize Other Cryptographic Technologies

Lesson 6: Implementing Public Key Infrastructure

Topic 6A: Implement Certificates and Certificate Authorities
Topic 6B: Implement PKI Management

Lesson 7: Implementing Authentication Controls

Topic 7A: Summarize Authentication Design Concepts

Topic 7B: Implement Knowledge-Based Authentication
Topic 7C: Implement Authentication Technologies
Topic 7D: Summarize Biometrics Authentication Concepts

Lesson 8: Implementing Identity and Account Management Controls

Topic 8A: Implement Identity and Account Types
Exam objectives covered:
Topic 8B: Implement Account Policies
Topic 8C: Implement Authorization Solutions
Topic 8D: Explain the Importance of Personnel Policies

Lesson 9: Implementing Secure Network Designs

Topic 9A: Implement Secure Network Designs
Topic 9B: Implement Secure Switching and Routing
Topic 9C: Implement Secure Wireless Infrastructure
Topic 9D: Implement Load Balancers

Lesson 10: Implementing Network Security Appliances

Topic 10A: Implement Firewalls and Proxy Servers
Topic 10B: Implement Network Security Monitoring
Topic 10C: Summarize the Use of SIEM

Lesson 11: Implementing Secure Network Protocols

Topic 11A: Implement Secure Network Operations Protocols
Topic 11B: Implement Secure Application Protocols
Topic 11C: Implement Secure Remote Access Protocols

Lesson 12: Implementing Host Security Solutions

Topic 12A: Implement Secure Firmware
Topic 12B: Implement Endpoint Security
Topic 12C: Explain Embedded System Security Implications

Lesson 13: Implementing Secure Mobile Solutions

Topic 13A: Implement Mobile Device Management
Topic 13B: Implement Secure Mobile Device Connections

Lesson 14: Summarizing Secure Application Concepts

Topic 14A: Analyze Indicators of Application Attacks
Topic 14B: Analyze Indicators of Web Application Attacks
Topic 14C: Summarize Secure Coding Practices
Topic 14D: Implement Secure Script Environments

Topic 14E: Summarize Deployment and Automation Concepts

Lesson 15: Implementing Secure Cloud Solutions

Topic 15A: Summarize Secure Cloud and Virtualization Services
Topic 15B: Apply Cloud Security Solutions
Topic 15C: Summarize Infrastructure as Code Concepts

Lesson 16: Explaining Data Privacy and Protection Concepts

Topic 16A: Explain Privacy and Data Sensitivity Concepts
Topic 16B: Explain Privacy and Data Protection Controls

Lesson 17: Performing Incident Response

Topic 17A: Summarize Incident Response Procedures
Topic 17B: Utilize Appropriate Data Sources for Incident Response
Topic 17C: Apply Mitigation Controls

Lesson 18: Explaining Digital Forensics

Topic 18A: Explain Key Aspects of Digital Forensics Documentation
Topic 18B: Explain Key Aspects of Digital Forensics Evidence Acquisition

Lesson 19: Summarizing Risk Management Concepts

Topic 19A: Explain Risk Management Processes and Concepts

Lesson 20: Implementing Cybersecurity Resilience

Topic 20A: Implement Redundancy Strategies
Topic 20B: Implement Backup Strategies
Topic 20C: Implement Cybersecurity Resiliency Strategies

Lesson 21: Explaining Physical Security

Topic 21A: Explain the Importance of Physical Site Security Controls
Topic 21B: Explain the Importance of Physical Host Security Controls?