CompTIA Security+ (Exam SY0-501) (CompTiaSec-SY0-501) (Flex)

Modality: Virtual Classroom

Duration: 20 Days (2 hrs/day)

"If you enroll in this course without the Master Subscription plan, you receive a Free Official Exam Voucher (excluding purchases using Training Vouchers / SATV) for SY0-501 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:

The CompTIA® Security+® (Exam SY0-501) is one of the most important courses which you will be required to complete if your job responsibilities are inclusive of securing devices, network services, and incoming as well as outgoing traffic in your respective organization. It can also be undertaken if you are planning to take the CompTIA Security+ certification examination. This course will enhance your knowledge about networks, security fundamentals, and organizational security and will also provide professional experience with the same. Throughout the course, you will learn new skills which will enable you to deploy basic security services on all kinds of computer networks.

Taking this course will be advantageous for you in two different ways. It will help you in preparing for and attempting the CompTIA Security+ certification exam (Exam SY0-501). However, if you wish to have a successful career in the field of cyber security, then the course will also help you in developing and further enhancing your skill set to demonstrate the capabilities needed to excel in computer security. The information obtained vi this course will allow you to confidently tackle all tasks given to you in a security related role.

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:

- Analyze risk
- Identify the essential components of information security
- Identify numerous threats which affect information security
- Deploy security for networks
- Deploy Security for hosts and software
- Detect vulnerability by conducting security assessments
- Manage identity and access
- Address security incidents
- Deploy operational level security
- Deploy cryptographic solutions within the organization
- In the event of an unforeseen incident, ensure smooth running of business operations.

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 220-901 and 220-902) (Comptia-A)
- CompTIA Network+ (Exam N10-006) (ComptiaNet)

Course Outline:

Module 1: Identifying Security Fundamentals

- **Lesson A:** Identify Information Security Concepts
- **Lesson B:** Identify Basic Security Controls
- **Lesson C:** Identify Basic Authentication and Authorization Concepts
- **Lesson D:** Identify Basic Cryptography Concepts

Module 2: Analyzing Risk

- **Lesson A:** Analyze Organizational Risk
- **Lesson B:** Analyze the Business Impact of Risk

Module 3: Identifying Security Threats

- **Lesson A:** Identify Types of Attackers
- **Lesson B:** Identify Social Engineering Attacks
- **Lesson C:** Identify Malware
- **Lesson D:** Identify Software-Based Threats
- **Lesson E:** Identify Network-Based Threats
- **Lesson F:** Identify Wireless Threats
- **Lesson G:** Identify Physical Threats

Module 4: Conducting Security Assessments

- **Lesson A:** Identify Vulnerabilities
- **Lesson B:** Assess Vulnerabilities
- **Lesson C:** Implement Penetration Testing

Module 5: Implementing Host and Software Security

- **Lesson A:** Implement Host Security
- **Lesson B:** Implement Cloud and Virtualization Security
- **Lesson C:** Implement Mobile Device Security
- **Lesson D:** Incorporate Security in the Software Development Lifecycle

Module 6: Implementing Network Security

- **Lesson A:** Configure Network Security Technologies
- **Lesson B:** Secure Network Design Elements
- **Lesson C:** Implement Secure Networking Protocols and Services
- **Lesson D:** Secure Wireless Traffic

Module 7: Managing Identity and Access

- **Lesson A:** Implement Identity and Access Management
- **Lesson B:** Configure Directory Services
- **Lesson C:** Configure Access Services
- **Lesson D:** Manage Accounts

Module 8: Implementing Cryptography

- **Lesson A:** Identify Advanced Cryptography Concepts
- **Lesson B:** Select Cryptographic Algorithms
- **Lesson C:** Configure a Public Key Infrastructure
- **Lesson D:** Enroll Certificates
- **Lesson E:** Back Up and Restore Certificates and Private Keys
- **Lesson F:** Revoke Certificates

Module 9: Implementing Operational Security

- **Lesson A:** Evaluate Security Frameworks and Guidelines
- **Lesson B:** Incorporate Documentation in Operational Security
- **Lesson C:** Implement Security Strategies
- **Lesson D:** Manage Data Security Processes
- **Lesson E:** Implement Physical Controls

Module 10: Addressing Security Incidents

- **Lesson A:** Troubleshoot Common Security Issues

- **Lesson B:** Respond to Security Incidents
- **Lesson C:** Investigate Security Incidents

Module 11: Ensuring Business Continuity

- **Lesson A:** Select Business Continuity and Disaster Recovery Processes
- **Lesson B:** Develop a Business Continuity Plan

Appendix A: Mapping Course Content to CompTIA® Security+® (Exam SY0-501)

Appendix B: Linux Essentials

Appendix C: Log File Essentials

Appendix D: Programming Essentials