CompTIA Security+
Exam Number: SYO-601

What is CompTIA Security +?

CompTIA Security+ is the certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this official course helps students prepare to write the actual CompTIA Security+ certification which covers the essential principles for network security and risk management – making it an important stepping stone to an IT security career.

Led by a CompTIA authorized instructor, the training and course material for this official Security+ training program will provide students with a comprehensive review of network security, compliance and operation security, threats and vulnerabilities as well as application, data and host security. Additionally, this course will also help students successfully prepare for the CompTIA Security+ exam.

Course Breakdown

Module 1	Threats, Attacks and Vulnerabilities
Module 2	Architecture and Design
Module 3	Implementation
Module 4	Operations and Incident Response
Module 5	Governance, Risk, and Compliance

https://learnersone.com
(240) 930-4053

Table of **Contents:**

Program **Overview:**

CompTIA Security+ 601 is a globally trusted certification that validates foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification training covers the essential principles of network security and risk management.

Program **Features:**

- 40 hours of instructor-led learning
- Covers 6 domains required to become an IT security professional
- Industry-recognized course completion certificate
- Hands-on based learning
- Exam Voucher as applicable

Delivery **Mode:**

Onsite Boot Camp and Live Virtual Classroom

Prerequisites:

There are no specific prerequisites to take up this certification but it is recommended that individuals take the Network+ certification before taking the CompTIA Security+ 601 training and certification exam.

Target **Audience:**

The CompTIA Security+ 601 course is ideal for professionals who are working in the roles of system administrators, network administrators, security administrators, and IT auditors.

Key Learning **Outcomes:**

By the end of this online CompTIA Security+ training, you will be able to:

- 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 **Curriculum:**

Lesson 01 - Threats, Attacks, and Vulnerabilities

Comparing Security Roles and Controls

- Compare and Contrast Information Security Roles
- Compare and Contrast Security Control and Framework Types
- Q&A with Knowledge Checks

Threat Actors and Threat

- Threat Actor Types and Attack Vectors
- Threat Intelligence Sources
- Q&A with Knowledge Checks

Performing Security Assessments

- Assess Organizational Security with Network Reconnaissance Tools
- Security Concerns with General Vulnerability Types
- Vulnerability Scanning Techniques
- Penetration Testing Concepts
- Q&A with Knowledge Checks

Identifying Social Engineering and Malware

- Compare and Contrast Social Engineering Techniques.
- Analyze Indicators of Malware-Based Attacks
- Q&A with Knowledge Checks

Lesson 02 - Architecture and Design

Summarizing Basic Cryptographic Concepts

- Compare and Contrast Cryptographic Ciphers
- Summarize Cryptographic Modes of Operation
- Summarize Cryptographic Use Cases and Weaknesses
- Summarize Other Cryptographic Technologies
- Q&A with Knowledge Checks

Implementing Public Key Infrastructure

- Certificates and Certificate Authorities
- PKI Management
- Q&A with Knowledge Checks

Implementing Authentication Controls

- Authentication Design Concepts
- Knowledge-Based Authentication
- Authentication Technologies
- Biometrics Authentication Concepts
- Q&A with Knowledge Checks

Implementing Identity and Account Management Controls

- Identity and Account Types
- Account Policies
- Authorization Solutions
- Importance of Personnel Policies
- Q&A with Knowledge Checks

Lesson 03 - Implementation

Implementing Secure Network Designs

- Secure Network Designs
- Secure Switching and Routing
- Secure Wireless Infrastructure
- Load Balancers

Q&A with Knowledge Checks

Implementing Network Security Appliances

- Firewalls and Proxy Servers
- Network Security Monitoring
- Use of SIEM

Q&A with Knowledge Checks

Implementing Secure Network Protocols

- Secure Network Operations Protocols
- Secure Application Protocols
- Secure Remote Access Protocols
- Q&A with Knowledge Checks

Implementing Host Security Solutions

- Secure Firmware
- Endpoint Security
- Embedded System Security Implications
- Q&A with Knowledge Checks

Implementing Secure Mobile Solutions

- Mobile Device Management
- Secure Mobile Device Connections
- Q&A with Knowledge Checks

Lesson 04 - Operations and Incident Response

Secure Application Concepts

- Analyze Indicators of Application Attacks
- Analyze Indicators of Web Application Attacks
- Secure Coding Practices
- Secure Script Environments
- Deployment and Automation Concepts

Q&A with Knowledge Checks

Implementing Secure Cloud Solutions

- Secure Cloud and Virtualization Services
- Apply Cloud Security Solutions
- Infrastructure as Code Concepts
- Q&A with Knowledge Checks

Explaining Data Privacy and Protection Concepts

- Privacy and Data Sensitivity Concepts
- Privacy and Data Protection Controls

Q&A with Knowledge Checks

Performing Incident Response

Incident Response Procedures

- Utilize Appropriate Data Sources for Incident Response
- Apply Mitigation Controls

Q&A with Knowledge Checks

Explaining Digital Forensics

- Key Aspects of Digital Forensics Documentation
- Key Aspects of Digital Forensics Evidence Acquisition Q&A
- with Knowledge Checks

Lesson 05 - Governance, Risk, and Compliance

Summarizing Risk Management Concepts

- Risk Management Processes and Concepts
- Business Impact Analysis Concepts
- Q&A with Knowledge Checks

Implementing Cybersecurity Resilience

- Redundancy Strategies
- Backup Strategies
- Cybersecurity Resilience Strategies
- Q&A with Knowledge Checks

Explaining Physical Security

- Importance of Physical Site Security Controls
- Importance of Physical Host Security Controls
- Q&A with Knowledge Checks

About **Us:**

Trusted by hundreds of satisfied students and organizations, we are a top-notch educator providing the most complete training complete training programs to help you stay informed, engaged and a step ahead.