CompTIA Security+ (SY0-801)

Course Overview

CompTIA's Security+ certification is a global certification that validates the foundational cybersecurity skills necessary to perform core security functions and pursue an IT security career.

Course Objectives

This course can benefit you in two ways. If you intend to pass the CompTIA Security+ (Exam SY0-801) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of IT security. Today's job market demands individuals with demonstrable skills, and the information and activities in this course can help you build your cybersecurity skill set so that you can confidently perform your duties in any entry-level security role.

On course completion, you will be able to achieve the following:

- Summarize fundamental security concepts.
- Compare threat types.
- Explain appropriate cryptographic solutions.
- Implement identity and access management.
- Secure enterprise network architecture.
- Secure cloud network architecture.
- Explain resiliency and site security concepts.
- Explain vulnerability management.
- Evaluate network security capabilities.
- Assess endpoint security capabilities.
- Enhance application security capabilities.
- Explain incident response and monitoring concepts.
- Analyze indicators of malicious activity.
- Summarize security governance concepts.
- Explain risk management processes.
- Summarize data protection and compliance concepts.

Target Student

The Official CompTIA Security+ (Exam SY0-801) is the primary course you will need to take if your job responsibilities include safeguarding networks, detecting threats, and securing data in your organization. You can take this course to prepare for the CompTIA Security+ (Exam SY0-801) certification examination.

Course Prerequisites

Security administrator with two years of hands-on experience . CompTIA A+ and CompTIA Network+, or the equivalent knowledge, is strongly recommended.

Associated Certifications

Security+

Table of Contents

1. Summarize Fundamental Security Concepts
    1.1 Security Concepts
    1.2 Security Controls

2. Identify Threats, Vulnerabilities, and Attacks
    2.1 Threat Actors
    2.2 Attack Vectors and Sources
    2.3 Social Engineering

3. Explain Cryptographic Solutions
    3.1 Cryptographic Algorithms
    3.2 Cryptographic Solutions
    3.3 Public Key Infrastructure

4. Implement Identity and Access Management
    4.1 Access Control Models
    4.2 Active Directory Overview
    4.3 Authentication
    4.4 Authorization
    4.5 Identity Management

5. Secure Enterprise Network Architecture
    5.1 Enterprise Network Architecture
    5.2 Network Security Appliances
    5.3 Secure Communications

6. Secure Cloud Network Architecture
    6.1 Cloud Infrastructure
    6.2 Embedded Systems and Zero Trust Architecture

7. Explain Resiliency and Site Security Concepts
    7.1 Asset Management
    7.2 Physical Security
    7.3 Redundancy Strategies

8. Explain Vulnerability Management
    8.1 Device and OS Vulnerabilities
    8.2 Application and Cloud Vulnerabilities
    8.3 Vulnerability Identification Methods
    8.4 Vulnerability Analysis and Remediation
    8.5 Artificial Intelligence

9. Evaluate Network Security Capabilities
    9.1 Network Security Baselines
    9.2 Network Security Capability Enhancement

10. Assess Endpoint Security Capabilities
    10.1 Endpoint Security
    10.2 Mobile Device Hardening

11. Enhance Application Security Capabilities
    11.1 Application Protocol Security Baselines
    11.2 Cloud and Web Application Security Concepts

12. Explain Incident Response and Monitoring Concepts
    12.1 Incident Response
    12.2 Digital Forensics
    12.3 Data Sources
    12.4 Alerting and Monitoring Tools

13. Analyze Indicators of Malicious Activity
    13.1 Malware Attack Indicators
    13.2 Physical and Network Attack Indicators
    13.3 Application Attack Indicators

14. Summarize Security Governance Concepts
    14.1 Policies, Standards, and Procedures
    14.2 Change Management
    14.3 Automation and Orchestration

15. Explain Risk Management Processes
    15.1 Risk Management Processes and Concepts
    15.2 Vendor Management Concepts
    15.3 Audits and Assessments

16. Summarize Data Protection and Compliance Concepts
    16.1 Data Classification and Compliance
    16.2 Personnel Policies