CompTIA Security+ (Exam SYO-701)

Duration: *5 Day(s)*

Course Overview

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations; its industry-leading IT certifications are an important part of that mission. 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.

This exam will certify the successful candidate has the knowledge and skills required 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 regulations and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents.

Security+ is compliant with ISO 17024 standards. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program.

Review this course online at https://www.alta3.com/courses/SEC+701

Objectives

- Design comprehensive security frameworks for enterprise environments.
- Implement effective security measures across cloud, mobile, and IoT platforms.
- Understand regulatory compliance and governance in cybersecurity.
- Respond to and manage security incidents efficiently.

Who Should Attend

- Network Administrators
- Security Analysts
- IT Support Technicians
- Entry-Level Security Professionals

Prerequisites

To ensure your success in this course, you should have a minimum of two years of experience in IT administration with a focus on security, hands-on experience with technical information security, and a broad knowledge of security concepts. CompTIA A+ and CompTIA Network+, or the equivalent knowledge, is strongly recommended.

Course Outline

Lesson 1: Summarize Fundamental Security Concepts

1. Security Concepts
2. Security Controls

Lesson 2: Compare Threat Types

3. Threat Actors
4. Attack Surfaces

5. Social Engineering

Lesson 3: Explain Cryptographic Solutions

6. Cryptographic Algorithms
7. Public Key Infrastructure
8. Cryptographic Solutions

Lesson 4: Implement Identity and Access Management

9. Authentication
10. Authorization
11. Identity Management

Lesson 5: Secure Enterprise Network Architecture

12. Enterprise Network Architecture
13. Network Security Appliances
14. Secure Communications

Lesson 6: Secure Cloud Network Architecture

15. Cloud Infrastructure
16. Embedded Systems and Zero Trust Architecture

Lesson 7: Explain Resiliency and Site Security Concepts

17. Asset Management
18. Redundancy Strategies
19. Physical Security

Lesson 8: Explain Vulnerability Management

20. Device and OS Vulnerabilities
21. Application and Cloud Vulnerabilities
22. Vulnerability Identification Methods
23. Vulnerability Analysis and Remediation

Lesson 9: Evaluate Network Security Capabilities

24. Network Security Baselines
25. Network Security Capability Enhancement

Lesson 10: Assess Endpoint Security Capabilities

26. Implement Endpoint Security

27. Mobile Device Hardening

Lesson 11: Enhance Application Security Capabilities

28. Application Protocol Security Baselines
29. Cloud and Web Application Security Concepts

Lesson 12: Explain Incident Response and Monitoring Concepts

30. Incident Response
31. Digital Forensics
32. Data Sources
33. Alerting and Monitoring Tools

Lesson 13: Analyze Indicators of Malicious Activity

34. Malware Attack Indicators
35. Physical and Network Attack Indicators
36. Application Attack Indicators

Lesson 14: Summarize Security Governance Concepts

37. Policies, Standards, and Procedures
38. Change Management
39. Automation and Orchestration

Lesson 15: Explain Risk Management Processes

40. Risk Management Processes and Concepts
41. Vendor Management Concepts
42. Audits and Assessments

Lesson 16: Summarize Data Protection and Compliance Concepts

43. Data Classification and Compliance
44. Personnel Policies