5 Days

# CompTIA Security+

CompTIA Security+ is a globally recognized certification that will help you in validating your foundational, vendor-neutral IT security knowledge and skills. This certification will help you in learning the principles required for network security and risk management. The Security+ certification will prove your skills to keep a network secure and to deter hackers.

This course will make you competent in the domains such as Network Security, Compliance and Operational Security, Threats and Vulnerabilities, Application, Data and Host Security, Access Control and Identity Management and Cryptography.

**Objectives:**

You should be able to meet the following objectives after the completion of the course:

- Identify access control and account management security measures
- Identify security threats and vulnerabilities
- Identify the fundamental concepts of computer security
- Manage application, data and host security

## Course Details

## Course Outline

**Part 1: Threats, Attacks and Vulnerabilities**
**Chapter 1:** Malware and Indicators of Compromise
**Chapter 2:** Attacks
**Chapter 3:** Threat Actors
**Chapter 4:** Vulnerability Scanning and Penetration Testing
**Chapter 5:** Vulnerabilities and Impacts

**Part 2: Technologies and Tools**
**Chapter 6:** Network Components
**Chapter 7:** Security Tools and Technologies
**Chapter 8:** Troubleshoot Common Security Issues
**Chapter 9:** Deploy Mobile Devices Securely
**Chapter 10:** Implementing Secure Protocols

**Part 3: Architecture and Design**
**Chapter 11:** Architecture Frameworks and Secure Network Architectures
**Chapter 12:** Secure Systems Design and Deployment
**Chapter 13:** Embedded Systems

**Chapter 14:** Application Development and Deployment
**Chapter 15:** Cloud and Virtualization
**Chapter 16:** Resiliency and Automation strategies
**Chapter 17:** Physical Security Controls

**Part 4: Identity and Access Management**
**Chapter 18:** Identity, Access and Accounts
**Chapter 19:** Identity and Access Services
**Chapter 20:** Identity and Access Management Controls

**Part 5: Risk Management**
**Chapter 21:** Policies, Plans and Procedures
**Chapter 22:** Risk Management and Business Impact Analysis Concepts
**Chapter 23:** Incident Response, Disaster Recovery and Continuity of Operation
**Chapter 24:** Digital forensics
**Chapter 25:** Compare and contrast various types of controls
**Chapter 26:** Data Security and Privacy Practices

**Part 6: Cryptography and PKI**
**Chapter 27:** Cryptography Concepts
**Chapter 28:** Cryptography Algorithms
**Chapter 29:** Wireless Security
**Chapter 30:** Public Key Infrastructure

## Who Should Attend

- Security personnel
- Information Technology (IT) professional

## Pre Requisite

The students should have completed the following, before attending this course:

- CompTIA Network+
- Two (2) years of experience in IT administration with a security focus.

## Exams

CompTIA Security+ [SY0-501]

464, Udyog Vihar Phase V,Gurgaon (Delhi NCR)-122016,India
+91 8882 233 777
training@mercury.co.in
www.mercurysolutions.co

Date - Nov 14, 2024