CompTIA Security+

Introduction

CompTIA Security+ certification is for those candidates aiming to make a career in IT and become a professional who has all the necessary networking and administrative skills in various protocols like TCP or IP networks. The candidate will also become familiar with operating systems, such as macOS, Unix, or Linux. This course is mandatory for those who want to acquire foundational knowledge of security aspects.

Course Highlights

This course teaches you about core aspects such as;

- 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 Outline

MODULE 1: Threats, Attacks, and Vulnerabilities

- Given a scenario, analyze indicators of compromise and determine the type of malware
- Compare and contrast types of attacks.
- Explain threat actor types and attributes.
- Explain penetration testing concepts.
- Explain vulnerability scanning concepts.
- Explain the impact associated with types of vulnerabilities.

MODULE 2: Technologies and Tools

- Install and configure network components, both hardware, and software-based, to support organizational security.
- Given a scenario, use appropriate software tools to assess the security posture of an organization
- Given a scenario, troubleshoot common security issues.
- Given a scenario, analyze and interpret output from security technologies.
- Given a scenario, deploy mobile devices securely.
- Given a scenario, implement secure protocols.

MODULE 3: Architecture and Design

- Explain use cases and purpose for frameworks, best practices, and secure configuration guides.
- Given a scenario, implement secure network architecture concepts.
- Given a scenario, implement the design of a secure system.
- Explain the importance of secure staging deployment concepts.
- Explain the security implications of embedded systems.
- Summarize secure application development and deployment concepts.
- Summarize cloud and virtualization concepts.
- Explain how resiliency and automation strategies reduce risk.
- Explain the importance of physical security controls.

MODULE 4: Identity and Access Management

- Compare and contrast identity and access management concepts
- Given a scenario, install and configure identity and access services.

- Given a scenario, implement identity and access management controls.
- Given a scenario, differentiate common account management practices.

MODULE 5: Risk Management

- Explain the importance of policies, plans, and procedures related to organizational security.
- Summarize business impact analysis concepts.
- Explain risk management processes and concepts.
- Given a scenario, follow incident response procedures.
- Summarize basic concepts of forensics.
- Explain disaster recovery and continuity of operation concepts.
- Compare and contrast various types of controls.
- Given a scenario, carry out data security and privacy practices.

MODULE 6: Cryptography and PKI

- Compare and contrast basic concepts of cryptography.
- Explain cryptography algorithms and their basic characteristics.
- Given a scenario, install and configure wireless security settings.
- Given a scenario, implement the public key infrastructure.

Prerequisites

CompTIA Network+ and two years of experience in IT administration with a security focus

Target Audience

This course is purposive for anyone preparing for an IT Security position or looking to upgrade their skills and become CompTIA Security+ Certified. Moreover, it will build new skills to deal wisely with the security of your organization.

Duration

16 hours training course