CompTIA Security+

Overview:

CompTIA Security+ (SY0-601) is a course designed to teach IT professionals the fundamentals of information security. The course covers everything from basic security concepts to advanced topics like identity management and vulnerability management. It provides a solid foundation in the essential security knowledge and skills necessary to develop and maintain a successful security program. The course can be used to prepare for the corresponding CompTIA Security+ certification exam and provide an understanding of security concepts that can be applied in any job.

Target Audience:

The CompTIA Security+ SY0-601 training is designed for IT professionals who are looking to gain in-depth knowledge and expertise in the field of cybersecurity.
This training is ideal for IT support professionals, system administrators, software developers, hardware engineers, and other individuals working in the security field or performing related IT activities.
It is also a great option for those who are looking to gain official recognition of their cybersecurity skillset and become certified in security principles.
The training provides an excellent introduction to the important principles and practices within the context of the CompTIA Security+ certification exam, ensuring that all candidates have the proper foundation to fully understand and be able to apply their knowledge when in a work environment.

Learning Objectives of CompTIA-SY0-601-Security+

- Identify threats, attacks and technologies used to mitigate their impact.
- Understand how to design, implement and manage network security.
- Comprehend how to use authentication, authorization and access control mechanisms.
- Gain knowledge of risk mitigation methods and to identify appropriate mitigation techniques.
- Understand how to secure cloud, virtualization and information technologies.
- Recognize secure software development principles, policies and procedures.
- Become familiar with protocols and technologies associated with cryptography.
- Learn to identify secure networks and systems using monitoring and logging tools.
- Gain knowledge of organizational security strategies and incident response processes.
- Understand the different principles, methods and tools used to support operations security.

Course Contents:

Attacks, Threats, and Vulnerabilities

- Compare and contrast different types of social engineering techniques.

- Given a scenario, analyze potential indicators to determine the type of attack.
- Given a scenario, analyze potential indicators associated with application attacks.
- Given a scenario, analyze potential indicators associated with network attacks.
- Explain different threat actors, vectors, and intelligence sources.
- Explain the security concerns associated with various types of vulnerabilities.
- Summarize the techniques used in security assessments.
- Explain the techniques used in penetration testing.

Architecture and Design

- Explain the importance of security concepts in an enterprise environment.
- Summarize virtualization and cloud computing concepts.
- Summarize secure application development, deployment, and automation concepts.
- Summarize authentication and authorization design concepts.
- Given a scenario, implement cybersecurity resilience.
- Explain the security implications of embedded and specialized systems.
- Explain the importance of physical security controls.
- Summarize the basics of cryptographic concepts.

Implementation

- Given a scenario, implement secure protocols.
- Given a scenario, implement host or application security solutions
- Given a scenario, implement secure network designs.
- Given a scenario, install and configure wireless security settings.
- Given a scenario, implement secure mobile solutions.
- Given a scenario, apply cybersecurity solutions to the cloud.
- Given a scenario, implement identity and account management controls.
- Given a scenario, implement authentication and authorization solutions.
- Given a scenario, implement public key infrastructure.

Operations and Incident Response

- Given a scenario, use the appropriate tool to assess organizational security.
- Summarize the importance of policies, processes, and procedures for incident response.
- Given an incident, utilize appropriate data sources to support an investigation.
- Given an incident, apply mitigation techniques or controls to secure an environment.
- Explain the key aspects of digital forensics.

Governance, Risk, and Compliance

- Compare and contrast various types of controls.
- Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.
- Explain the importance of policies to organizational security
- Summarize risk management processes and concepts.
- Explain privacy and sensitive data concepts in relation to security