CompTIA Security+

Duration: 5 Days Course Code: G013 Version: SY0-701

Overview:

The CompTIA Security+ course is designed to help you prepare for the SY0-701 exam. The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations

Target Audience:

CompTIA Security+ is aimed at IT professionals with job roles such as: Security Administrator Security Specialist Systems Administrator

Objectives:

- **By the end of the course, you should be able to meet the following objectives:**
- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, Internet of Things (IoT), and operational technology.
- 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.

Prerequisites:

Networking and administrative skills in Windows-based TCP/IP networks and familiarity with other operating systems, such as OS X, Unix, or Linux.

- G005 - CompTIA Network+

Testing and Certification

CompTIA Security+ is the first early career cybersecurity certification a candidate should earn. It equips cybersecurity professionals with the foundational security skills necessary to safeguard networks, detect threats, and secure data through performance-based questions—helping them open the door to a cybersecurity career and become a trusted defender of digital environments.

- **Required exam:** SY0-701
- **Number of questions**: Maximum of 90
- **Types of questions:** Multiple-choice and performance-based
- **Length of test:** 90 minutes
- **Recommended experience:** A minimum of 2 years of experience in IT administration with a focus on security, hands-on experience with technical information security, and broad knowledge of security concepts

Follow-on-Courses:

- GK5867 - CompTIA CySA+ Cybersecurity Analyst
- G015 - CompTIA PenTest+
- GK2951 - CompTIA Advanced Security Practitioner (CASP+)

Content:

General Security Concepts 12%

- Compare and contrast various types of security controls.
- Summarize fundamental security concepts.
- Explain the importance of change management processes and the impact to security.
- Explain the importance of using appropriate cryptographic solutions.

Threats, Vulnerabilities ; Mitigations 22%

- Compare and contrast common threat actors and motivations.
- Explain common threat vectors and attack surfaces.
- Explain various types of vulnerabilities.
- Given a scenario, analyze indicators of malicious activity.
- Explain the purpose of mitigation techniques used to secure the enterprise.

Security Architecture 18%

- Compare and contrast security implications of different architecture models.
- Given a scenario, apply security principles to secure enterprise infrastructure.
- Compare and contrast concepts and strategies to protect data.
- Explain the importance of resilience and recovery in security architecture.

Security Operations 28%

- Given a scenario, apply common security techniques to computing resources.
- Explain the security implications of proper hardware, software, and data asset management.
- Explain various activities associated with vulnerability management.
- Explain security alerting and monitoring concepts and tools.
- Given a scenario, modify Enterprise capabilities to enhance security.
- Given a scenario, implement and maintain identity and access management.
- Explain the importance of automation and orchestration related to secure operations.
- Explain appropriate incident response activities.
- Given a scenario, use data sources to support an investigation.

Security Program Management ; Oversight 20%

- Summarize elements of effective security governance.
- Explain elements of the risk management process.
- Explain the processes associated with third-party risk assessment and management.
- Summarize elements of effective security compliance.
- Explain types and purposes of audits and assessments.
- Given a scenario, implement security awareness practices.

Additional Information:

Accredited by ANSI to show compliance with the ISO 17024 Standard.

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo