CompTIA Security+

Duration: 5 Days   Course Code: G013

Overview:

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career. Gaining a CompTIA Security+ certification demonstrates your knowledge of industry-wide information assurance topics, like systems security, network infrastructure, access control, assessments and audits, cryptography, and organisational security.
Why is it different?
More choose Security+ - chosen by more corporations and defense organizations than any other certification on the market to validate baseline security skills and for fulfilling the DoD 8570 compliance.
Security+ proves hands-on skills – the only baseline cybersecurity certification emphasizing hands-on practical skills, ensuring the security professional is better prepared to problem solve a wider variety of today's complex issues.
More job roles turn to Security+ to supplement skills – baseline cybersecurity skills are applicable across more of today's job roles to secure systems, software and hardware.
Security+ is aligned to the latest trends and techniques – covering the most core technical skills in risk assessment and management, incident response, forensics, enterprise networks, hybrid/cloud operations, and security controls, ensuring high-performance on the job.
The CompTIA Security+ certification exam will verify 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 laws and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents

Target Audience:

Individuals whose job responsibilities include securing network services, devices, and data confidentiality/privacy in your organization and individuals who are preparing for the CompTIA Security+ certification exam.

Objectives:

- **After completing this course you should be able to:**
- Compare security roles and security controls
- Explain threat actors and threat intelligence
- Perform security assessments and identify social engineering attacks and malware types
- Summarize basic cryptographic concepts and implement public key infrastructure
- Implement authentication controls
- Implement identity and account management controls
- Implement secure network designs, network security appliances, and secure network protocols
- Implement host, embedded/Internet of Things, and mobile security solutions
- Implement secure cloud solutions
- Explain data privacy and protection concepts
- Perform incident response and digital forensics
- Summarize risk management concepts and implement cybersecurity resilience
- Explain physical security

Prerequisites:

Attendees should meet the following prerequisites:

- Basic Windows and Linux administrator skills
- The ability to implement fundamental networking appliances and IP addressing concepts
- Six to nine months' experience in networking, including configuring security parameters, are strongly recommended.

Testing and Certification

Recommended as preparartion for the following exams:

- SY0-601 Exam - CompTIA Security +

Follow-on-Courses:

The following courses are recommended for those students looks to expand their knowledge of cybersecurity.

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

Content:

Comparing Security Roles and Security Controls

- Compare and Contrast Information Security Roles
- Compare and Contrast Security Control and Framework Types

Explaining Threat Actors and Threat Intelligence

- Explain Threat Actor Types and Attack Vectors
- Explain Threat Intelligence Sources

Performing Security Assessments

- Assess Organizational Security with Network
- Reconnaissance Tools
- Explain Security Concerns with General Vulnerability Types
- Summarize Vulnerability Scanning Techniques
- Explain Penetration Testing Concepts

Identifying Social Engineering and Malware

- Compare and Contrast Social Engineering Techniques
- Analyze Indicators of Malware-Based Attacks

Summarizing Basic Cryptographic Concepts

- Compare and Contrast Cryptographic Ciphers
- Summarize Cryptographic Modes of Operation
- Summarize Cryptographic Use Cases and Weaknesses
- Summarize Other Cryptographic Technologies

Implementing Public Key Infrastructure

- Implement Certificates and Certificate Authorities
- Implement PKI Management

Implementing Authentication Controls

- Summarize Authentication Design Concepts
- Implement Knowledge-Based Authentication
- Implement Authentication Technologies
- Summarize Biometrics Authentication Concepts

Implementing Identity and Account Management Controls

- Implement Identity and Account Types
- Implement Account Policies
- Implement Authorization Solutions

Implementing Secure Network Designs

- Implement Secure Network Designs
- Implement Secure Switching and Routing
- Implement Secure Wireless Infrastructure
- Implement Load Balancers

Implementing Network Security Appliances

- Implement Firewalls and Proxy Servers
- Implement Network Security Monitoring
- Summarize the Use of SIEM

Implementing Secure Network Protocols

- Implement Secure Network Operations Protocols
- Implement Secure Application Protocols
- Implement Secure Remote Access Protocols

Implementing Host Security Solutions

- Implement Secure Firmware
- Implement Endpoint Security
- Explain Embedded System Security Implications

Implementing Secure Mobile Solutions

- Implement Mobile Device Management
- Implement Secure Mobile Device Connections

Summarizing Secure Application Concepts

- Analyze Indicators of Application Attacks
- Analyze Indicators of Web Application Attacks
- Summarize Secure Coding Practices
- Implement Secure Script Environments
- Summarize Deployment and Automation Concepts

Implementing Secure Cloud Solutions

- Summarize Secure Cloud and Virtualization Services
- Apply Cloud Security Solutions
- Summarize Infrastructure as Code Concepts

Explaining Data Privacy and Protection Concepts

- Explain Privacy and Data Sensitivity Concepts
- Explain Privacy and Data Protection Controls

Performing Incident Response

- Summarize Incident Response Procedures
- Utilize Appropriate Data Sources for Incident Response
- Apply Mitigation Controls

Explaining Digital Forensics

- Explain Key Aspects of Digital Forensics Documentation
- Explain Key Aspects of Digital Forensics Evidence Acquisition

Summarizing Risk Management Concepts

- Explain Risk Management Processes and Concepts
- Explain Business Impact Analysis Concepts

Implementing Cybersecurity Resilience

- Implement Redundancy Strategies
- Implement Backup Strategies
- Implement Cybersecurity Resiliency Strategies

Explaining Physical Security

- Explain the Importance of Physical Site Security Controls
- Explain the Importance of Physical Host Security Controls

Labs

- 01: Assisted Lab: Exploring the Lab Environment
- 02: Assisted Lab: Scanning and Identifying Network Nodes
- 03: Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools
- 04: Assisted Lab: Analyzing the Results of a Credentialed Vulnerability Scan
- 05: Assisted Lab: Installing, Using, and Blocking a Malware-based Backdoor
- 06: Applied Lab: Performing Network Reconnaissance and Vulnerability Scanning
- 07: Assisted Lab: Managing the Life Cycle of a Certificate
- 08: Assisted Lab: Managing Certificates with OpenSSL
- 09: Assisted Lab: Auditing Passwords with a Password Cracking Utility
- 10: Assisted Lab: Managing Centralized Authentication
- 11: Assisted Lab: Managing Access Controls in Windows Server
- 12: Assisted Lab: Configuring a System for Auditing Policies

- Explain the Importance of Personnel Policies

- 13: Assisted Lab: Managing Access Controls in Linux
- 14: Applied Lab: Configuring Identity and Access Management Controls
- 15: Assisted Lab: Implementing a Secure Network Design
- 16: Assisted Lab: Configuring a Firewall
- 17: Assisted Lab: Configuring an Intrusion Detection System
- 18: Assisted Lab: Implementing Secure Network Addressing Services
- 19: Assisted Lab: Implementing a Virtual Private Network
- 20: Assisted Lab: Implementing a Secure SSH Server
- 21: Assisted Lab: Implementing Endpoint Protection
- 22: Applied Lab: Securing the Network Infrastructure
- 23: Assisted Lab: Identifying Application Attack Indicators
- 24: Assisted Lab: Identifying a Browser Attack
- 25: Assisted Lab: Implementing PowerShell Security
- 26: Assisted Lab: Identifying Malicious Code

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