COMPTIA SECURITY+ TRAINING

Duration: 5 Days

Overview:
CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

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.

You Will Learn How To:

- Attacks, Threats and Vulnerabilities
  - Focusing on more threats, attacks, and vulnerabilities on the Internet from newer custom devices that must be mitigated, such as IoT and embedded devices, newer DDoS attacks, and social engineering attacks based on current events.
- Architecture and Design
  - Includes coverage of enterprise environments and reliance on the cloud, which is growing quickly as organizations transition to hybrid networks.
- Implementation
  - Expanded to focus on administering identity, access management, PKI, basic cryptography, wireless, and end-to-end security.
- Operations and Incident Response
  - Covering organizational security assessment and incident response procedures, such as basic threat detection, risk mitigation techniques, security controls, and basic digital forensics.
- Governance, Risk and Compliance
  - Expanded to support organizational risk management and compliance to regulations, such as PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.

Course Outline

Lesson 1: Comparing Security Roles and Security Controls
Lesson 2: Explaining Threat Actors and Threat Intelligence
Lesson 3: Performing Security Assessments
Lesson 4: Identifying Social Engineering and Malware
Lesson 5: Summarizing Basic Cryptographic Concepts
Lesson 6: Implementing Public Key Infrastructure
Lesson 7: Implementing Authentication Controls
Lesson 8: Implementing Identity and Account Management Controls
Lesson 9: Implementing Secure Network Designs
Lesson 10: Implementing Network Security Appliances
Lesson 11: Implementing Secure Network Protocols
Lesson 12: Implementing Host Security Solutions
Lesson 13: Implementing Secure Mobile Solutions
Lesson 14: Summarizing Secure Application Concepts
Lesson 15: Implementing Secure Cloud Solutions
Lesson 16: Explaining Data Privacy and Protection Concepts
Lesson 17: Performing Incident Response
Lesson 18: Explaining Digital Forensics
Lesson 19: Summarizing Risk Management Concepts
Lesson 20: Implementing Cybersecurity Resilience
Lesson 21: Explaining Physical Security

Ways to Register:
Call (+63) 917-307-3822 **Email**: Sandra@gkphilippines.com