CompTIA Advanced Security Practitioner (CASP+)

Duration: 5 Days **Course Code: GK2951**

Overview:

CompTIA Advanced Security Practitioner (CASP+) is an advanced-level cybersecurity certification for security architects and senior security engineers charged with leading and improving an enterprise's cybersecurity readiness. CASP+ is an advanced-level cybersecurity certification covering technical skills in security architecture and senior security engineering in traditional, cloud, and hybrid environments, governance, risk, and compliance skills, assessing an enterprise's cybersecurity readiness, and leading technical teams to implement enterprise-wide cybersecurity solutions. Successful candidates will have the knowledge required to: Architect, engineer, integrate, and implement secure solutions across complex environments to support a resilient enterpriseUse monitoring, detection, incident response, and automation to proactively support ongoing security operations in an enterprise environmentApply security practices to cloud, on-premises, endpoint, and mobile infrastructure, while considering cryptographic technologies and techniquesConsider the impact of governance, risk, and compliance requirements throughout the enterprise
CASP+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

Target Audience:

Security ArchitectSenior Security EngineerSOC ManagerSecurity Analyst

Objectives:

- **Security Architecture**
- Expanded coverage to analyze security requirements in hybrid networks to work toward an enterprise-wide, zero trust security architecture with advanced secure cloud and virtualization solutions.
- **Governance, Risk, and Compliance**
- Expanded to support advanced techniques to prove an organization's overall cybersecurity resiliency metric and compliance to regulations, such as CMMC, PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, and CCPA.
- **Security Operations**
- Expanded emphasis on newer techniques addressing advanced threat management, vulnerability management, risk mitigation, incident response tactics, and digital forensics analysis.
- **Security Engineering and Cryptography**
- Expanded to focus on advanced cybersecurity configurations for endpoint security controls, enterprise mobility, cloud/hybrid environments, and enterprise-wide PKI and cryptographic solutions

Prerequisites:

Attendance in our Internetworking with TCP/IP and Switching in IP Networks courses is strongly recommended Security+ Prep Course

- G013 - CompTIA Security+ (SY0-601)

Testing and Certification

-

Content:

- Lesson 1: Perform Risk Management Activities
- Lesson 2: Summarizing Governance ; Compliance Strategies
- Lesson 3: Implementing Business Continuity ; Disaster Recovery
- Lesson 4: Identifying Infrastructure Services
- Lesson 5: Performing Software Integration
- Lesson 6: Explain Virtualization, Cloud and Emerging Technology
- Lesson 7: Exploring Secure Configurations and System Hardening
- Lesson 8: Understanding Security Considerations of Cloud and Specialized Platforms
- Lesson 9: Implementing Cryptography
- Lesson 10: Implementing Public Key Infrastructure (PKI)
- Lesson 11: Architecting Secure Endpoints
- Lesson 12: Summarizing IIoT ; IoT Concepts

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/