CompTIA CySA+ Cybersecurity Analyst

Duration: 5 Days **Course Code: GK5867** **Version: CS0-003**

Overview:

CompTIA Cybersecurity Analyst (CySA+) is a certification for cyber professionals tasked with incident detection, prevention and response through continuous security monitoring.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

The course is aimed at Security Analysts, Security Operations Center (SOC) Analysts, Incident Response Analysts, Vulnerability Management Analysts and Security Engineers.

Objectives:

- **After completing this course, you should be able to:**
- Proactively Monitor and Detect. Demonstrate your skills in detecting and analyzing indicators of malicious activity using the most up-to-date methods and tools, such as threat intelligence, security information and event management (SIEM), endpoint detection and response (EDR) and extended detection and response (XDR).
- Respond to Threats, Attacks and Vulnerabilities. Prove your knowledge of incident response and vulnerability management processes and highlight the communication skills critical to security analysis and compliance.
- Demonstrate Competency of Current Trends. Valuable team members can show knowledge of current trends that affect the daily work of security analysts, such as cloud and hybrid environments.

Prerequisites:

Recommended Experience:

- Network+, Security+ or equivalent knowledge.
- Minimum of 4 years of hands-on experience as an incident response analyst or security operations center (SOC) analyst, or equivalent experience.

Testing and Certification

Recommended preparation for exam(s):

- CS0-003

The CompTIA Cybersecurity Analyst (CySA+) certification verifies that successful candidates have the knowledge and skills required to detect and analyze indicators of malicious activity, understand threat intelligence and threat management, respond to attacks and vulnerabilities, perform incident response, and report and communicate related activity.

- Number of Questions: Maximum of 85 questions
- Type of Questions: Multiple choice and performance-based
- Legth of Test: 165 minutes
- Passing Score: 750 (on a scale of 100-900)

Content:

CySA+ is a global, vendor-neutral certification covering intermediate-level knowledge and skills required by information security analyst job roles. It helps identify a cybersecurity professional's ability to proactively defend an organization using secure monitoring, threat identification, incident response and teamwork. The CompTIA CySA+ CS0-003 course and certification exam ensures the candidate has the knowledge and skills required to:

- Detect and analyze indicators of malicious activity
- Understand threat hunting and threat intelligence concepts
- Use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities
- Perform incident response processes
- Understand reporting and communication concepts related to vulnerability management and incident response activities

Technical Skills covered in the certification and training:

Security Operations

- Explain the importance of system and network architecture concepts in security operations.
- Analyze indicators of potentially malicious activity.
- Use appropriate tools or techniques to determine malicious activity.
- Compare and contrast threat-intelligence and threat-hunting concepts.
- Explain the importance of efficiency and process improvement in security operations.

Vulnerability Management

- Implement vulnerability scanning methods and concepts.
- Analyze output from vulnerability assessment tools.
- Analyze data to prioritize vulnerabilities.
- Recommend controls to mitigate attacks and software vulnerabilities.
- Explain concepts related to vulnerability response, handling and management.

Incident Response Management

- Explain concepts related to attack methodology frameworks.
- Perform incident response activities.
- Explain the preparation and post-incident activity phases of the incident management lifecycle.

Reporting and Communication

- Explain the importance of vulnerability management reporting and communication.
- Explain the importance of incident response reporting and communication.

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar