

CompTIA CySA+ Cybersecurity Analyst

Duration: 5 Days Course Code: GK5867 Delivery Method: Company Event

Overview:

Company Events

These events can be delivered exclusively for your company at our locations or yours, specifically for your delegates and your needs. The Company Events can be tailored or standard course deliveries.

Target Audience:

The CompTIA Cybersecurity Analyst (CSA+) examination is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts. The exam will certify that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization.

Objectives:

- The CompTIA CSA+ certification is a vendor-neutral credential. The CompTIA CSA+ exam (Exam CS0-001) is an internationally targeted validation of intermediate-level security skills and knowledge. The course has a technical, "hands-on" focus on IT security analytics.
 - The CompTIA CSA+ exam is based on these objectives:
 - Threat Management
 - Vulnerability Management
 - Cyber Incident Response
 - Security Architecture and Tool Sets
-

Prerequisites:

While there is no required prerequisite, the CompTIA CSA+ certification is intended to follow CompTIA Security+ or equivalent experience. It is recommended for CompTIA CSA+ certification candidates to have the following:

- 3-4 years of hands-on information security or related experience
 - Network+, Security+, or equivalent knowledge
-

Content:

1. Threat Management

Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes

Procedures/common tasks:

- Topology discovery
- OS fingerprinting
- Service discovery
- Packet capture
- Log review
- Router/firewall ACLs review
- Email harvesting
- Social media profiling
- Social engineering
- DNS harvesting
- Phishing

Variables:

- Wireless vs. wired
- Virtual vs. physical
- Internal vs. external
- On-premises vs. cloud

Tools:

- NMAP
- Host scanning
- Network mapping
- NETSTAT
- Packet analyzer
- IDS/IPS
- HIDS/NIDS
- Firewall rule-based and logs
- Syslog
- Vulnerability scanner

Given a scenario, analyze the results of a network reconnaissance

Point-in-time data analysis:

- Packet analysis
- Protocol analysis
- Traffic analysis
- Netflow analysis
- Wireless analysis

Data correlation and analytics:

- Anomaly analysis
- Trend analysis
- Availability analysis
- Heuristic analysis
- Behavioral analysis

Data output:

Analyze reports from a vulnerability scan:

- Review and interpret scan results

Validate results and correlate other data points

- Compare to best practices or compliance
- Reconcile results
- Review related logs and/or other data sources
- Determine trends

Compare and contrast common vulnerabilities found in the following targets within an organization

Servers

Endpoints

Network infrastructure

Network appliances

Virtual infrastructure:

- Virtual hosts
- Virtual networks
- Management interface

Mobile devices

Interconnected networks

Virtual private networks (VPNs)

Industrial Control Systems (ICSs)

SCADA devices

3. Cyber Incident Response

Given a scenario, distinguish threat data or behavior to determine the impact of an incident

Threat classification:

- Known threats vs. unknown threats
- Zero day
- Advanced persistent threat

Eradication techniques:

- Sanitization
- Reconstruction/reimage
- Secure disposal

Validation:

- Patching
- Permissions
- Scanning
- Verify logging/communication to security monitoring

Corrective actions:

- Lessons learned report
- Change control process
- Update incident response plan

Incident summary report

4. Security Architecture and Tool Sets

Explain the relationship between frameworks, common policies, controls, and procedures

Regulatory compliance

Frameworks:

- NIST
- ISO
- COBIT
- SABSA
- TOGAF
- ITIL

Policies:

- Password policy
- Acceptable use policy
- Data ownership policy
- Data retention policy
- Account management policy
- Data classification policy

Controls:

- Control selection based on criteria
- Organizationally defined parameters
- Physical controls
- Logical controls
- Administrative controls

Procedures:

- Continuous monitoring
- Evidence production
- Patching

- Firewall logs - Packet captures - NMAP scan results - Event logs - Syslogs - IDS report	Factors contributing to incident severity and prioritization: - Scope of impact - Types of data	- Compensating control development - Control testing procedures - Manage exceptions - Remediation plans
Tools: - SIEM - Packet analyzer - IDS - Resource monitoring tool - Netflow analyzer	Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation	Verifications and quality control: - Audits - Evaluations - Assessments - Maturity model - Certification
Given a network-based threat, implement or recommend the appropriate response and countermeasure	Forensics kit: - Digital forensics workstation - Write blockers - Cables - Drive adapters - Wiped removable media - Cameras - Crime tape - Tamper-proof seals - Documentation/forms	Given a scenario, use data to recommend remediation of security issues related to identity and access management
Network segmentation: - System isolation - Jump box - Honeypot - Endpoint security	Forensic investigation suite: - Imaging utilities - Analysis utilities - Chain of custody - Hashing utilities - OS and process analysis - Mobile device forensics - Password crackers - Cryptography tools - Log viewers	Security issues associated with context-based authentication: - Time - Location - Frequency - Behavioral
Group policies		Security issues associated with identities: - Personnel - Endpoints - Servers - Services - Roles - Applications
ACLs: Sinkhole		Security issues associated with identity repositories: - Directory services - TACACS+ - RADIUS
Hardening: - Mandatory Access Control (MAC) - Compensating controls - Blocking unused ports/services - Patching	Explain the importance of communication during the incident response process	Security issues associated with federation and single sign-on: - Manual vs. automatic provisioning/deprovisioning - Self-service password reset
Network Access Control (NAC): - Time-based - Rule-based - Role-based - Location-based	Stakeholders: - HR - Legal - Marketing - Management	Exploits: - Impersonation - Man-in-the-middle - Session hijack - Cross-site scripting - Privilege escalation - Rootkit
Explain the purpose of practices used to secure a corporate environment	Purpose of communication processes: - Limit communication to trusted parties - Disclosure based on regulatory/legislative requirements - Prevent inadvertent release of information - Secure method of communication	Given ascenario, review security architecture and make recommendations to implement compensating controls
Penetration testing: Rules of engagement	Role-based responsibilities: - Technical - Management - Law enforcement - Retain incident response provider	Security data analytics: Data aggregation and correlation
Reverse engineering: - Isolation/sandboxing - Hardware - Software/malware	Given a scenario, analyze common symptoms to select the best course of action to support incident response	
Training and exercises: - Red team - Blue team		

■ White team

Risk evaluation:

- Technical control review
- Operational control review
- Technical impact and likelihood

2. Vulnerability Management

Given a scenario, implement an information security vulnerability management process

Identification of requirements:

- Regulatory environments
- Corporate policy
- Data classification
- Asset inventory

Establish scanning frequency:

- Risk appetite
- Regulatory requirements
- Technical constraints
- Workflow

Configure tools to perform scans according to specification:

- Determine scanning criteria
- Tool updates/plugin-ins
- Permissions and access

Execute scanning

Generate reports:

- Automated vs. manual distribution

Remediation:

- Prioritizing
- Communication/change control
- Sandboxing/testing
- Inhibitors to remediation
- Ongoing scanning and continuous monitoring

Given a scenario, analyze the output resulting from a vulnerability scan

Common network-related symptoms:

- Bandwidth consumption
- Beaconing
- Irregular peer-to-peer communication
- Rogue devices on the network
- Scan sweeps
- Unusual traffic spikes

Common host-related symptoms:

- Processor consumption
- Memory consumption
- Drive capacity consumption
- Unauthorized software
- Malicious processes
- Unauthorized changes
- Unauthorized privileges
- Data exfiltration

Common application-related symptoms:

- Anomalous activity
- Introduction of new accounts
- Unexpected output
- Unexpected outbound communication
- Service interruption
- Memory overflows

Summarize the incident recovery and post-incident response process

Containment techniques:

- Segmentation
- Isolation
- Removal
- Reverse engineering

- Trend analysis
- Historical analysis

Manual review:

- Firewall log
- Syslogs
- Authentication logs
- Event logs

Defense in depth:

- Personnel
- Processes
- Technologies
- Other security concepts

Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC)

Best practices during software development:

- Security requirements definition
- Security testing phases
- Manual peer reviews
- User acceptance testing
- Stress test application
- Security regression testing
- Input validation
- Secure coding best practices:
- OWASP
- SANS
- Center for Internet Security

Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies

Preventative:

- IPS
- HIPS
- Firewall
- Antivirus
- Anti-malware
- EMET
- Web proxy
- Web Application Firewall (WAF)

Collective:

- SIEM
- Network scanning
- Vulnerability scanning
- Packet capture
- Command line/IP utilities
- IDS/HIDS

Analytical:

- Vulnerability scanning
- Monitoring tools
- Interception proxy

Exploit:

- Interception proxy
- Exploit framework
- Fuzzers

Forensics:

- Forensic suites
- Hashing
- Password cracking
- Imaging

Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

info@globalknowledge.ie

www.globalknowledge.com/en-ie/

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1