BOOST
THE LEADING TRAINING PROVIDER

Information Technology

CompTIA CySA+Cybersecutiy Analyst

Course Introduction

The CompTIA CySA+ Cybersecurity Analyst training course is a vendor-neutral credential. The CompTIA CySA+ 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.

Target Audience

The training course is designed for IT professionals specifically those whose function mainly focused on security analysis, vulnerability analysis, or threat intelligence analysis.

Learning Objectives

- Threat Management
- Vulnerability Management
- Cyber Incident Response
- Security Architecture and Tool Sets

Course Outline

- **Day 01**

  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:**
- Firewall logs
- Packet captures
- NMAP scan results
- Event logs
- Syslogs
- IDS report
- **Tools:**
- SIEM
- Packet analyzer
- IDS
- Resource monitoring tool
- Netflow analyzer
- **Given a network-based threat, implement or recommend the appropriate response and countermeasure**
- **Network segmentation:**
- System isolation
- Jump box
- Honeypot
- Endpoint security
- Group policies
- **ACLs:**
- Sinkhole
- **Hardening:**
- Mandatory Access Control (MAC)
- Compensating controls
- Blocking unused ports/services
- Patching
- **Network Access Control (NAC):**
- Time-based
- Rule-based
- Role-based
- Location-based
- **Explain the purpose of practices used to secure a corporate environment**
- **Penetration testing:**
- Rules of engagement

- **Reverse engineering:**
- Isolation/sandboxing
- Hardware
- Software/malware
- **Training and exercises:**
- Red team
- Blue team
- White team
- **Risk evaluation:**
- Technical control review
- Operational control review
- Technical impact and likelihood

- **Day 02**

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/plug-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**
- **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

• **Day 03**

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
- Factors contributing to incident severity and prioritization:
- Scope of impact
- Types of data

- Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation
- **Forensics kit:**
- Digital forensics workstation
- Write blockers
- Cables
- Drive adapters
- Wiped removable media
- Cameras
- Crime tape
- Tamper-proof seals
- Documentation/forms
- **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
- **Explain the importance of communication during the incident response process**
- **Stakeholders:**
- HR
- Legal
- Marketing
- Management
- **Purpose of communication processes:**
- Limit communication to trusted parties
- Disclosure based on regulatory/legislative requirements
- Prevent inadvertent release of information
- Secure method of communication
- **Role-based responsibilities:**
- Technical
- Management
- Law enforcement
- Retain incident response provider

- **Given a scenario, analyze common symptoms to select the best course of action to support incident response**
- **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
- **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

- **Day 04**

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
- Compensating control development
- Control testing procedures
- Manage exceptions

- Remediation plans
- **Verifications and quality control:**
- Audits
- Evaluations
- Assessments
- Maturity model
- Certification
- **Given a scenario, use data to recommend remediation of security issues related to identity and access management**
- **Security issues associated with context-based authentication:**
- Time
- Location
- Frequency
- Behavioral
- **Security issues associated with identities:**
- Personnel
- Endpoints
- Servers
- Services
- Roles
- Applications
- **Security issues associated with identity repositories:**
- Directory services
- TACACS+
- RADIUS
- **Security issues associated with federation and single sign-on:**
- Manual vs. automatic provisioning/deprovisioning
- Self-service password reset
- **Exploits:**
- Impersonation
- Man-in-the-middle
- Session hijack
- Cross-site scripting
- Privilege escalation
- Rootkit
- **Given a scenario, review security architecture and make recommendations to implement compensating controls**
- **Security data analytics:**
- Data aggregation and correlation
- Trend analysis

- Historical analysis
- **Manual review:**
- Firewall log
- Syslogs
- Authentication logs
- Event logs
- **Defense in depth:**
- Personnel
- Processes
- Technologies
- Other security concepts

• **Day 05**

Security Architecture and Tool Sets (continuation)

- **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

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
April 14, 2025	April 18, 2025	5 days	4250.00 $	UAE - Dubai
July 14, 2025	July 18, 2025	5 days	4950.00 $	Spain - Madrid
Nov. 3, 2025	Nov. 7, 2025	5 days	4250.00 $	UAE - Abu Dhabi