CompTIA CySA+ LIVE Instructor-Led Cybersecurity Analyst Certification

Course Description

This extensive Virtual "Live" Instructor-Led CompTIA Cybersecurity Analyst (CySA+) course also prepares attendees for the exam. This exam is an intermediate-level credential for cybersecurity professionals.

As attackers have learned to evade traditional signature-based solutions, such as firewalls, an analytics-based approach within the IT security industry is increasingly important for most organizations. The behavioral analytics skills covered by CySA+ identify and combat malware, and advanced persistent threats (APTs), resulting in enhanced threat visibility across a broad attack surface.

The exam will certify that the successful candidate has the knowledge and skills required to

-Perform data analysis and interpret the results to identify vulnerabilities, threats, and risks to an organization
-Configure and use threat detection tools
-Secure and protect applications and systems within an organization

CompTIA CySA+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements. It is compliant with government regulations under the Federal Information Security Management Act (FISMA). Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program. Over 1.3 million CompTIA ISOANSI-accredited exams have been delivered since January 1, 2011.

This course meets the NEW DoD Directive 8140 requirements.

Will Department of Defense (DoD) Directive 8140 replace DoDD 8570? Yes.

When will DoD 8140 take effect? It is already in effect.

Why Change from 8570 to 8140?

DoD 8140 is designed to be more flexible and inclusive than DoD 8570. DoD 8140 includes initiatives such as NIST NICE (National Initiative for Cybersecurity Education), which identifies critical KSAs (Knowledge, Skills, and Abilities) and places cybersecurity positions into 7 categories (1. Security Provision, 2. Operate Maintain, 3. Protect Defend, 4. Analyze, 5. Operate Collect, 6. Oversight Development, and 7. Investigate) consisting of 31 specialty areas.

BTS works with clients to deliver appropriate material to become certified. Course design uses the latest texts and other materials over a one or two week period based on client needs. Time is allowed after each Instructor presentation and demonstration for student Hands-On work on labs, practice exams and Network+ related drills.

BTS offers On-Site or Virtual Test Administration for this course, or students can take the exam at their own leisure at a certified testing center of their choice and schedule.

Students Will Learn

- **The CompTIA CySA+ certification 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.**
- **The CompTIA CySA+ exam is based on these objectives**
- **-Threat Management**
- **-Vulnerability Management**
- **-Cyber Incident Response**
- **-Security Architecture**
- **-And More...**

Target Audience

The CompTIA Cybersecurity Analyst (CySA+) 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.

Prerequisites

While there is no required prerequisite, the CompTIA CySA+ certification is intended to follow CompTIA Security+ or equivalent experience. It is recommended for CompTIA CySA+ certification candidates to have the following
- 3 to 4 years of Hands-On information security or related experience Network+, Security+, or equivalent knowledge.

Course Outline

Module 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:
- 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

Module 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/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

Module 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
- 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

Module 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
- 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 ascenario, 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
- 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

Delivery Method

LIVE Virtual Instructor-led with numerous labs and exercises.

Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

5 Days