CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives

EXAM NUMBER: CS0-001

CompTIA

About the Exam

The CompTIA Cybersecurity Analyst (CySA+) certification is a vendor-neutral credential. The CompTIA CySA+ exam is an internationally targeted validation of intermediate-level security skills and knowledge. While there is no required prerequisite, the CompTIA CySA+ certification is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus on IT security analytics.

The CompTIA 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.

It is recommended for CompTIA CySA+ certification candidates to have the following:

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

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the **CompTIA Certification Exam Policies**. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the **CompTIA Candidate Agreement**. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid. y

TEST DETAILS

Required exam	CS0-001
Number of questions	Maximum of 85
Types of questions	Multiple choice and performance-based
Length of test	165 Minutes
Recommended experience	Network+, Security+, or equivalent knowledge. Minimum of 3-4 years of hands-on information security or related experience. While there is no required prerequisite, CySA+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, "hands-on" focus.
Passing score	750 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented. The CompTIA CySA+ exam is based on these objectives.

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Threat Management	27%
2.0 Vulnerability Management	26%
3.0 Cyber Incident Response	23%
4.0 Security Architecture and Tool Sets	24%
Total	**100%**

1.0 Threat Management

1.1 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

1.2 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

1.3 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

1.4 Explain the purpose of practices used to secure a corporate environment.

- **Penetration testing**
  - Rules of engagement
    - Timing
    - Scope
    - Authorization
    - Exploitation
    - Communication
    - Reporting
- **Reverse engineering**
  - Isolation/sandboxing
  - Hardware
    - Source authenticity of hardware
    - Trusted foundry
    - OEM documentation
  - Software/malware
    - Fingerprinting/hashing
    - Decomposition
- **Training and exercises**
  - Red team
  - Blue team
  - White team
- **Risk evaluation**
  - Technical control review
  - Operational control review
  - Technical impact and likelihood
    - High
    - Medium
    - Low

2.0 Vulnerability Management

2.1 Given a scenario, implement an information security vulnerability management process.

- **Identification of requirements**
  - Regulatory environments
  - Corporate policy
  - Data classification
  - Asset inventory
    - Critical
    - Non-critical
- **Establish scanning frequency**
  - Risk appetite
  - Regulatory requirements
  - Technical constraints
  - Workflow
- **Configure tools to perform scans according to specification**
  - Determine scanning criteria
    - Sensitivity levels
    - Vulnerability feed
    - Scope
    - Credentialed vs. non-credentialed
    - Types of data
    - Server-based vs. agent-based
  - Tool updates/plug-ins
    - SCAP
  - Permissions and access
- **Execute scanning**
- **Generate reports**
  - Automated vs. manual distribution
- **Remediation**
  - Prioritizing
    - Criticality
    - Difficulty of implementation
  - Communication/change control
  - Sandboxing/testing
  - Inhibitors to remediation
    - MOUs
    - SLAs
    - Organizational governance
    - Business process interruption
    - Degrading functionality
- **Ongoing scanning and continuous monitoring**

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

- **Analyze reports from a vulnerability scan**
  - Review and interpret scan results
    - Identify false positives
    - Identify exceptions
    - Prioritize response actions
- **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

2.3 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**

3.0 Cyber Incident Response

3.1 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
    - Downtime
    - Recovery time
    - Data integrity
    - Economic
    - System process criticality
  - Types of data
    - Personally Identifiable Information (PII)
    - Personal Health Information (PHI)
    - Payment card information
    - Intellectual property
    - Corporate confidential
      - Accounting data
      - Mergers and acquisitions

3.2 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
    - Chain of custody form
    - Incident response plan
    - Incident form
    - Call list/escalation list
- **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

3.3 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

3.4 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

3.5 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**

4.0 Security Architecture and Tool Sets

4.1 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

4.2 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

4.3 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
    - Training
    - Dual control
    - Separation of duties
    - Third party/consultants
    - Cross training
    - Mandatory vacation
    - Succession planning
  - Processes
    - Continual improvement
    - Scheduled reviews
    - Retirement of processes
  - Technologies
    - Automated reporting
    - Security appliances
    - Security suites
    - Outsourcing
      - Security as a Service
    - Cryptography
  - Other security concepts
    - Network design
    - Network segmentation

4.4 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
    - Static code analysis
    - Web app vulnerability scanning
    - Fuzzing
    - Use interception proxy to crawl application
  - Manual peer reviews
  - User acceptance testing
  - Stress test application
  - Security regression testing
  - Input validation
- **Secure coding best practices**
  - OWASP
  - SANS
  - Center for Internet Security
    - System design recommendations
    - Benchmarks

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

(**The intent of this objective is NOT to test specific vendor feature sets.)

- **Preventative**
  - IPS
    - Sourcefire
    - Snort
    - Bro
  - HIPS
  - Firewall
    - Cisco
    - Palo Alto
    - Check Point
  - Antivirus
  - Anti-malware
  - EMET
  - Web proxy
  - Web Application Firewall (WAF)
    - ModSecurity
    - NAXSI
    - Imperva
- **Collective**
  - SIEM
    - ArcSight
    - QRadar
    - Splunk
    - AlienVault
    - OSSIM
    - Kiwi Syslog
  - Network scanning
    - NMAP
  - Vulnerability scanning
    - Qualys
    - Nessus
    - OpenVAS
    - Nexpose
    - Nikto
    - Microsoft Baseline Security Analyzer
  - Packet capture
    - Wireshark
    - tcpdump
    - Network General
    - Aircrack-ng
  - Command line/IP utilities
    - netstat
    - ping
    - tracert/traceroute
    - ipconfig/ifconfig
    - nslookup/dig
    - Sysinternals
    - OpenSSL
  - IDS/HIDS
    - Bro
- **Analytical**
  - Vulnerability scanning
    - Qualys
    - Nessus
    - OpenVAS
    - Nexpose
    - Nikto
    - Microsoft Baseline Security Analyzer
  - Monitoring tools
    - MRTG
    - Nagios
    - SolarWinds
    - Cacti
    - NetFlow Analyzer
  - Interception proxy
    - Burp Suite
    - Zap
    - Vega
- **Exploit**
  - Interception proxy
    - Burp Suite
    - Zap
    - Vega
  - Exploit framework
    - Metasploit
    - Nexpose
  - Fuzzers
    - Untidy
    - Peach Fuzzer
    - Microsoft SDL File/Regex Fuzzer
- **Forensics**
  - Forensic suites
    - EnCase
    - FTK
    - Helix
    - Sysinternals
    - Cellebrite
  - Hashing
    - MD5sum
    - SHAsum
  - Password cracking
    - John the Ripper
    - Cain & Abel
  - Imaging
    - DD

CompTIA Cybersecurity Analyst (CySA+) Acronym List

The following is a list of acronyms that appear on the CompTIA CySA+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
ACL	Access Control List
ARP	Address Resolution Protocol
BYOD	Bring Your Own Device
CIS	Center for Internet Security
CoBiT	Control Objectives for Information and Related Technology
CCTV	Closed-Circuit Television
CRM	Customer Relations Management
DDoS	Distributed Denial of Service
DNS	Domain Name Service
EMET	Enhanced Mitigation Experience Toolkit
FISMA	Federal Information Security Management Act
FTK	Forensic Tool Kit
FTP	File Transfer Protocol
HBSS	Host Based Security System
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
HR	Human Resources
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
IOC	Indicator of Compromise
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MD5	Message Digest 5
MOA	Memorandum Of Agreement
MOU	Memorandum Of Understanding
MRTG	Multi Router Traffic Grapher
NAC	Network Access Control
NAXSI	Nginx Anti XSS & SQL Injection
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards & Technology
OEM	Original Equipment Manufacturer
OSSIM	Open Source Security Information Management
OWASP	Open Web Application Security Project
PAM	Pluggable Authentication Module

ACRONYM	SPELLED OUT
PCA	Prinicpal Component Analysis
PCI	Payment Card Industry
PHI	Protected Health Information
PII	Personally Identifiable Information
RACI	Responsible, Accountable, Consulted and Informed
RADIUS	Remote Authentication Dial-In User Service
SABSA	Sherwood Applied Business Security Architecture
SANS	System Administration, Networking, and Security Institute
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDLC	Software Development Life Cycle
SEO	Search Engine Optimization
SHA	Secure Hash Algorithm
SIEM	Security Incident and Event Manager
SLA	Service Level Agreement
SOC	Security Operations Center
SPF	Sender Policy Framework
SSH	Secure Shell
SSL	Secure Sockets Layer
TACACS+	Terminal Access Controller Access Control System Plus
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOGAF	The Open Group Architecture Framework
USB	Universal Serial Bus
VAS	Vulnerability Assessment System
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	Web Application Firewall

Suggested Classroom Equipment for CySA+ Certification Training

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CySA+ exam. This list may also be helpful for training companies who wish to create a lab component for their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

IT HARDWARE

- Router
- Switch
- Firewall
- Workstations/laptops
- IDS/IPS
- Servers
- Write blocker
- Pelican cases
- Wireless access point
- Drive adapters
- VoIP phone
- Mobile phone

TOOLS

- Screw driver
- PC service toolkit

CONSUMABLES

- Cat 5/6 cables
- Spare drives/flash drives

SOFTWARE

- Virtualization platform
- Kali Linux/BackTrack
- Virtualized attack targets
  - Web servers
  - Database servers
  - Time servers
  - DNS servers
  - PC workstations

CompTIA