



CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives

EXAM NUMBER: CS0-003



About the Exam

The CompTIA Cybersecurity Analyst (CySA+) certification exam will certify the successful 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

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an advanced IT professional.

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.

TEST DETAILS

Required exam	CS0-003
Number of questions	Maximum of 85
Types of questions	Multiple-choice and performance-based
Length of test	165 minutes
Recommended experience	4 years of hands-on experience as an incident response analyst or security operations center (SOC) analyst

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Security Operations	33%
2.0	Vulnerability Management	30%
3.0	Incident Response and Management	20%
4.0	Reporting and Communication	17%
Total		100%



1.0 Security Operations

1.1 Explain the importance of system and network architecture concepts in security operations.

- **Log ingestion**
 - Time synchronization
 - Logging levels
- **Operating system (OS) concepts**
 - Windows Registry
 - System hardening
 - File structure
 - Configuration file locations
 - System processes
 - Hardware architecture
- **Infrastructure concepts**
 - Serverless
 - Virtualization
 - Containerization
- **Network architecture**
 - On-premises
 - Cloud
 - Hybrid
 - Network segmentation
 - Zero trust
 - Secure access secure edge (SASE)
 - Software-defined networking (SDN)
- **Identity and access management**
 - Multifactor authentication (MFA)
 - Single sign-on (SSO)
 - Federation
- Privileged access management (PAM)
- Passwordless
- Cloud access security broker (CASB)
- **Encryption**
 - Public key infrastructure (PKI)
 - Secure sockets layer (SSL) inspection
- **Sensitive data protection**
 - Data loss prevention (DLP)
 - Personally identifiable information (PII)
 - Cardholder data (CHD)

1.2 Given a scenario, analyze indicators of potentially malicious activity.

- **Network-related**
 - Bandwidth consumption
 - Beaconsing
 - Irregular peer-to-peer communication
 - Rogue devices on the network
 - Scans/sweeps
 - Unusual traffic spikes
 - Activity on unexpected ports
- **Host-related**
 - Processor consumption
 - Memory consumption
 - Drive capacity consumption
- **Application-related**
 - Anomalous activity
 - Introduction of new accounts
- Unauthorized software
- Malicious processes
- Unauthorized changes
- Unauthorized privileges
- Data exfiltration
- Abnormal OS process behavior
- File system changes or anomalies
- Registry changes or anomalies
- Unauthorized scheduled tasks
- Unexpected output
- Unexpected outbound communication
- Service interruption
- Application logs
- **Other**
 - Social engineering attacks
 - Obfuscated links



1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.

- **Tools**
 - Packet capture
 - Wireshark
 - tcpdump
 - Log analysis/correlation
 - Security information and event management (SIEM)
 - Security orchestration, automation, and response (SOAR)
 - Endpoint security
 - Endpoint detection and response (EDR)
 - Domain name service (DNS) and Internet Protocol (IP) reputation
 - WHOIS
 - AbuseIPDB
 - File analysis
 - Strings
 - VirusTotal
 - Sandboxing
 - Joe Sandbox
 - Cuckoo Sandbox
 - Sender Policy Framework (SPF)
 - Embedded links
 - File analysis
 - Hashing
 - User behavior analysis
 - Abnormal account activity
 - Impossible travel
- **Common techniques**
 - Pattern recognition
 - Command and control
 - Interpreting suspicious commands
 - Email analysis
 - Header
 - Impersonation
 - DomainKeys Identified Mail (DKIM)
 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- **Programming languages/scripting**
 - JavaScript Object Notation (JSON)
 - Extensible Markup Language (XML)
 - Python
 - PowerShell
 - Shell script
 - Regular expressions

1.4 Compare and contrast threat-intelligence and threat-hunting concepts.

- **Threat actors**
 - Advanced persistent threat (APT)
 - Hacktivists
 - Organized crime
 - Nation-state
 - Script kiddie
 - Insider threat
 - Intentional
 - Unintentional
 - Supply chain
- **Tactics, techniques, and procedures (TTP)**
- **Confidence levels**
 - Timeliness
 - Relevancy
 - Accuracy
- **Collection methods and sources**
 - Open source
 - Social media
 - Blogs/forums
 - Government bulletins
 - Computer emergency response team (CERT)
 - Cybersecurity incident response team (CSIRT)
 - Deep/dark web
 - Closed source
 - Paid feeds
 - Information sharing organizations
 - Internal sources
- **Threat intelligence sharing**
 - Incident response
- Vulnerability management
- Risk management
- Security engineering
- Detection and monitoring
- **Threat hunting**
 - Indicators of compromise (IoC)
 - Collection
 - Analysis
 - Application
 - Focus areas
 - Configurations/misconfigurations
 - Isolated networks
 - Business-critical assets and processes
 - Active defense
 - Honeypot



1.5 Explain the importance of efficiency and process improvement in security operations.

- **Standardize processes**
 - Identification of tasks suitable for automation
 - Repeatable/do not require human interaction
 - Team coordination to manage and facilitate automation
- **Streamline operations**
 - Automation and orchestration
 - Security orchestration, automation, and response (SOAR)
 - Orchestrating threat intelligence data
 - Data enrichment
 - Threat feed combination
 - Minimize human engagement
- **Technology and tool integration**
 - Application programming interface (API)
 - Webhooks
 - Plugins
- **Single pane of glass**



2.0 Vulnerability Management

2.1 Given a scenario, implement vulnerability scanning methods and concepts.

- **Asset discovery**
 - Map scans
 - Device fingerprinting
- **Special considerations**
 - Scheduling
 - Operations
 - Performance
 - Sensitivity levels
 - Segmentation
 - Regulatory requirements
- **Internal vs. external scanning**
- **Agent vs. agentless**
- **Credentialed vs. non-credentialed**
- **Passive vs. active**
- **Static vs. dynamic**
 - Reverse engineering
 - Fuzzing
- **Critical infrastructure**
 - Operational technology (OT)
 - Industrial control systems (ICS)
 - Supervisory control and data acquisition (SCADA)
- **Security baseline scanning**
- **Industry frameworks**
 - Payment Card Industry Data Security Standard (PCI DSS)
 - Center for Internet Security (CIS) benchmarks
 - Open Web Application Security Project (OWASP)
 - International Organization for Standardization (ISO) 27000 series

2.2 Given a scenario, analyze output from vulnerability assessment tools.

- **Tools**
 - Network scanning and mapping
 - Angry IP Scanner
 - Maltego
 - Web application scanners
 - Burp Suite
 - Zed Attack Proxy (ZAP)
 - Arachni
 - Nikto
 - Vulnerability scanners
 - Nessus
 - OpenVAS
 - Debuggers
 - Immunity debugger
 - GNU debugger (GDB)
 - Multipurpose
 - Nmap
 - Metasploit framework (MSF)
 - Recon-ng
 - Cloud infrastructure assessment tools
 - Scout Suite
 - Prowler
 - Pacu



2.3 Given a scenario, analyze data to prioritize vulnerabilities.

- **Common Vulnerability Scoring System (CVSS) interpretation**
 - Attack vectors
 - Attack complexity
 - Privileges required
 - User interaction
 - Scope
- Impact
 - Confidentiality
 - Integrity
 - Availability
- **Validation**
 - True/false positives
 - True/false negatives
- **Context awareness**
 - Internal
 - External
 - Isolated
- **Exploitability/weaponization**
- **Asset value**
- **Zero-day**

2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities.

- **Cross-site scripting**
 - Reflected
 - Persistent
- **Overflow vulnerabilities**
 - Buffer
 - Integer
 - Heap
 - Stack
- **Data poisoning**
- **Broken access control**
- **Cryptographic failures**
- **Injection flaws**
- **Cross-site request forgery**
- **Directory traversal**
- **Insecure design**
- **Security misconfiguration**
- **End-of-life or outdated components**
- **Identification and authentication failures**
- **Server-side request forgery**
- **Remote code execution**
- **Privilege escalation**
- **Local file inclusion (LFI)/remote file inclusion (RFI)**

2.5 Explain concepts related to vulnerability response, handling, and management.

- **Compensating control**
- **Control types**
 - Managerial
 - Operational
 - Technical
 - Preventative
 - Detective
 - Responsive
 - Corrective
- **Patching and configuration management**
 - Testing
 - Implementation
 - Rollback
 - Validation
- **Maintenance windows**
- **Exceptions**
- **Risk management principles**
 - Accept
 - Transfer
 - Avoid
 - Mitigate
- **Policies, governance, and service-level objectives (SLOs)**
- **Prioritization and escalation**
- **Attack surface management**
 - Edge discovery
 - Passive discovery
 - Security controls testing
 - Penetration testing and adversary emulation
 - Bug bounty
- Attack surface reduction
- **Secure coding best practices**
 - Input validation
 - Output encoding
 - Session management
 - Authentication
 - Data protection
 - Parameterized queries
- **Secure software development life cycle (SDLC)**
- **Threat modeling**



3.0 Incident Response and Management

3.1 Explain concepts related to attack methodology frameworks.

- Cyber kill chains
- Diamond Model of Intrusion Analysis
- MITRE ATT&CK
- Open Source Security Testing Methodology Manual (OSS TMM)
- OWASP Testing Guide

3.2 Given a scenario, perform incident response activities.

- **Detection and analysis**
 - IoC
 - Evidence acquisitions
 - Chain of custody
 - Validating data integrity
 - Preservation
 - Legal hold
 - Data and log analysis
- **Containment, eradication, and recovery**
 - Scope
 - Impact
 - Isolation
 - Remediation
 - Re-imaging
 - Compensating controls

3.3 Explain the preparation and post-incident activity phases of the incident management life cycle.

- **Preparation**
 - Incident response plan
 - Tools
 - Playbooks
- **Post-incident activity**
 - Forensic analysis
 - Root cause analysis
 - Lessons learned
- Tabletop
- Training
- Business continuity (BC)/disaster recovery (DR)



4.0 Reporting and Communication

4.1 Explain the importance of vulnerability management reporting and communication.

- **Vulnerability management reporting**
 - Vulnerabilities
 - Affected hosts
 - Risk score
 - Mitigation
 - Recurrence
 - Prioritization
- **Comppliance reports**
- **Action plans**
 - Configuration management
 - Patching
- Compensating controls
- Awareness, education, and training
- Changing business requirements
- **Inhibitors to remediation**
 - Memorandum of understanding (MOU)
 - Service-level agreement (SLA)
 - Organizational governance
 - Business process interruption
 - Degrading functionality
 - Legacy systems
- Proprietary systems
- **Metrics and key performance indicators (KPIs)**
 - Trends
 - Top 10
 - Critical vulnerabilities and zero-days
 - SLOs
- **Stakeholder identification and communication**

4.2 Explain the importance of incident response reporting and communication.

- **Stakeholder identification and communication**
- **Incident declaration and escalation**
- **Incident response reporting**
 - Executive summary
 - Who, what, when, where, and why
 - Recommendations
 - Timeline
- Impact
- Scope
- Evidence
- **Communications**
 - Legal
 - Public relations
 - Customer communication
 - Media
 - Regulatory reporting
 - Law enforcement
- **Root cause analysis**
- **Lessons learned**
- **Metrics and KPIs**
 - Mean time to detect
 - Mean time to respond
 - Mean time to remediate
 - Alert volume

CompTIA CySA+ CS0-003 Acronym List

The following is a list of acronyms that appears on the CompTIA CySA+ CS0-003 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

Acronym	Spelled Out	Acronym	Spelled Out
ACL	Access Control List	HIDS	Host-based Intrusion Detection System
API	Application Programming Interface	HIPS	Host-based Intrusion Prevention System
APT	Advanced Persistent Threat	HTTP	Hypertext Transfer Protocol
ARP	Address Resolution Protocol	HTTPS	Hypertext Transfer Protocol Secure
AV	Antivirus	IaaS	Infrastructure as a Service
BC	Business Continuity	ICMP	Internet Control Message Protocol
BCP	Business Continuity Plan	ICS	Industrial Control Systems
BGP	Border Gateway Protocol	IDS	Intrusion Detection System
BIA	Business Impact Analysis	IoC	Indicators of Compromise
C2	Command and Control	IP	Internet Protocol
CA	Certificate Authority	IPS	Intrusion Prevention System
CASB	Cloud Access Security Broker	IR	Incident Response
CDN	Content Delivery Network	ISO	International Organization for Standardization
CERT	Computer Emergency Response Team	IT	Information Technology
CHD	Cardholder Data	ITIL	Information Technology Infrastructure Library
CI/CD	Continuous Integration and Continuous Delivery	JSON	JavaScript Object Notation
CIS	Center for Internet Security	KPI	Key Performance Indicator
COBIT	Control Objectives for Information and Related Technologies	LAN	Local Area Network
CSIRT	Cybersecurity Incident Response Team	LDAPS	Lightweight Directory Access Protocol
CSRF	Cross-site Request Forgery	LFI	Local File Inclusion
CVE	Common Vulnerabilities and Exposures	LOI	Letter of Intent
CVSS	Common Vulnerability Scoring System	MAC	Media Access Control
DDoS	Distributed Denial of Service	MFA	Multifactor Authentication
DoS	Denial of Service	MOU	Memorandum of Understanding
DKIM	Domain Keys Identified Mail	MSF	Metasploit Framework
DLP	Data Loss Prevention	MSP	Managed Service Provider
DMARC	Domain-based Message Authentication, Reporting, and Conformance	MSSP	Managed Security Service Provider
DNS	Domain Name Service	MTTD	Mean Time to Detect
DR	Disaster Recovery	MTTR	Mean Time to Repair
EDR	Endpoint Detection and Response	NAC	Network Access Control
FIM	File Integrity Monitoring	NDA	Non-disclosure Agreement
FTP	File Transfer Protocol	NGFW	Next-generation Firewall
GDB	GNU Debugger	NIDS	Network-based Intrusion Detection System
GPO	Group Policy Objects	NTP	Network Time Protocol
		OpenVAS	Open Vulnerability Assessment Scanner

Acronym	Spelled Out	Acronym	Spelled Out
OS	Operating System	SMB	Server Message Block
OSSTMM	Open Source Security Testing Methodology Manual	SMTP	Simple Mail Transfer Protocol
OT	Operational Technology	SNMP	Simple Network Management Protocol
OWASP	Open Web Application Security Project	SOC	Security Operations Center
PAM	Privileged Access Management	SPF	Sender Policy Framework
PCI DSS	Payment Card Industry Data Security Standard	SQL	Structured Query Language
PHP	Hypertext Preprocessor	SSL	Secure Sockets Layer
PID	Process Identifier	SSO	Single Sign-on
PII	Personally Identifiable Information	SSRF	Server-side Request Forgery
PKI	Public Key Infrastructure	STIX	Structured Threat Information Expression
PLC	Programmable Logic Controller	SWG	Secure Web Gateway
POC	Proof of Concept	TCP	Transmission Control Protocol
RCE	Remote Code Execution	TFTP	Trivial File Transfer Protocol
RDP	Remote Desktop Protocol	TLS	Transport Layer Security
REST	Representational State Transfer	TRACE	Trade Reporting and Compliance Engine
RFI	Remote File Inclusion	TTP	Tactics, Techniques, and Procedures
RXSS	Reflected Cross-site Scripting	UEBA	User and Entity Behavior Analytics
SaaS	Software as a Service	URI	Uniform Resource Identifier
SAML	Security Assertion Markup Language	URL	Uniform Resource Locator
SASE	Secure Access Secure Edge	USB	Universal Serial Bus
SCADA	Supervisory Control and Data Acquisition	VLAN	Virtual LAN
SDLC	Software Development Life Cycle	VM	Virtual Machine
SDN	Software-defined Networking	VPN	Virtual Private Network
SFTP	Secure File Transfer Protocol	WAF	Web Application Firewall
SIEM	Security Information and Event Management	WAN	Wide Area Network
SLA	Service-level Agreement	XDR	Extended Detection Response
SLO	Service-level Objective	XML	Extensible Markup Language
SOAR	Security Orchestration, Automation, and Response	XSS	Cross-site Scripting
		XXE	XML External Entity
		ZAP	Zed Attack Proxy
		ZTNA	Zero Trust Network Access

CompTIA CySA+ CS0-003 Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CySA+ CS0-003 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

Equipment

- Workstations (or laptop) with ability to run VM
- Firewall
- IDS/IPS
- Servers

Software

- Windows operating systems
 - Commando VM
- Linux operating systems
 - Kali
- Open-source UTM appliance
- Metasploitable
- SIEM
 - Greylog
 - ELK
 - Splunk
- TCPDump
- Wireshark
- Vulnerability scanner (i.e., OpenVAS)
- Nessus
- Access to cloud instances
 - Azure
 - AWS
 - GCP