



CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives

EXAM NUMBER: CS0-002



About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Cybersecurity Analyst (CySA+) CSO-002 certification exam. With the end goal of proactively defending and continuously improving the security of an organization, CySA+ will verify the successful candidate has the knowledge and skills required to:

- Leverage intelligence and threat detection techniques
- Analyze and interpret data
- Identify and address vulnerabilities
- Suggest preventative measures
- Effectively respond to and recover from incidents

This is equivalent to 4 years of hands-on experience in a technical cybersecurity job role.

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an 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 testing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	CS0-002
Number of questions	Maximum of 85
Type of questions	Multiple choice and performance-based
Length of test	165 minutes
Recommended experience	<ul style="list-style-type: none">• 4 years of hands-on experience in a technical cybersecurity job role• Security+ and Network+, or equivalent knowledge and experience
Passing score	750

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 Threat and Vulnerability Management	22%
2.0 Software and Systems Security	18%
3.0 Security Operations and Monitoring	25%
4.0 Incident Response	22%
5.0 Compliance and Assessment	13%
Total	100%



1.0 Threat and Vulnerability Management

1.1 Explain the importance of threat data and intelligence.

• Intelligence sources 02

- Open-source intelligence
- Proprietary/closed-source intelligence
- Timeliness
- Relevancy
- Accuracy

• Confidence levels 02

• Indicator management 05

- Structured Threat Information eXpression (STIX)
- Trusted Automated eXchange of Indicator Information (TAXII)
- OpenIoC

• Threat classification 04

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

• Threat actors 04

- Nation-state
- Hactivist
- Organized crime
- Insider threat
 - Intentional
 - Unintentional

• Intelligence cycle 01

- Requirements

- Collection

- Analysis
- Dissemination
- Feedback

• Commodity malware 04

• Information sharing and analysis communities 03

- Healthcare
- Financial
- Aviation
- Government
- Critical infrastructure

1.2 Given a scenario, utilize threat intelligence to support organizational security.

• Attack frameworks 06

- MITRE ATT&CK
- The Diamond Model of Intrusion Analysis
- Kill chain

• Threat research 05

- Reputational
- Behavioral
- Indicator of compromise (IoC)

- Common vulnerability scoring system (CVSS) 09

• Threat modeling methodologies 07

- Adversary capability
- Total attack surface
- Attack vector
- Impact
- Likelihood

• Threat intelligence sharing with supported functions 03

- Incident response
- Vulnerability management
- Risk management
- Security engineering
- Detection and monitoring



1.3 Given a scenario, perform vulnerability management activities.

- **Vulnerability identification**
 - Asset criticality 08
 - Active vs. passive scanning 08, 10
 - Mapping/enumeration 10
- **Validation 09**
 - True positive
 - False positive
 - True negative
 - False negative
- **Remediation/mitigation**
 - Configuration baseline 12
 - Patching 12
 - Hardening 12
 - Compensating controls 11, 51
- Risk acceptance 52
- Verification of mitigation 12
- **Scanning parameters and criteria**
 - Risks associated with scanning activities
 - Vulnerability feed
 - Scope
 - Credentialed vs. non-credentialed
 - Server-based vs. agent-based
 - Internal vs. external
 - Special considerations
 - Types of data
 - Technical constraints
 - Workflow
- Sensitivity levels
- Regulatory requirements
- Segmentation
- Intrusion prevention system (IPS), intrusion detection system (IDS), and firewall settings
- **Inhibitors to remediation 14**
 - Memorandum of understanding (MOU)
 - Service-level agreement (SLA)
 - Organizational governance
 - Business process interruption
 - Degrading functionality
 - Legacy systems
 - Proprietary systems

1.4 Given a scenario, analyze the output from common vulnerability assessment tools.

- **Web application scanner**
 - OWASP Zed Attack Proxy (ZAP)
 - Burp suite
 - Nikto
 - Arachni
- **Infrastructure vulnerability scanner**
 - Nessus
 - OpenVAS
 - Qualys
- **Software assessment tools and techniques**
 - Static analysis
 - Dynamic analysis
 - Reverse engineering
 - Fuzzing
- **Enumeration**
 - Nmap
 - hping
 - Active vs. passive
 - Responder
- **Wireless assessment tools**
 - Aircrack-ng
 - Reaver
 - oclHashcat
- **Cloud infrastructure assessment tools**
 - ScoutSuite
 - Prowler
 - Pacu

1.5 Explain the threats and vulnerabilities associated with specialized technology.

- Mobile
- Internet of Things (IoT)
- Embedded
- Real-time operating system (RTOS)
- System-on-Chip (SoC)
- Field programmable gate array (FPGA)
- Physical access control
- Building automation systems
- Vehicles and drones
 - CAN bus
- Workflow and process automation systems
- Industrial control system
- Supervisory control and data acquisition (SCADA)
 - Modbus



1.6

Explain the threats and vulnerabilities associated with operating in the cloud.

- **Cloud service models**
 - Software as a Service (SaaS)
 - Platform as a Service (PaaS)
 - Infrastructure as a Service (IaaS)
- **Cloud deployment models**
 - Public
 - Private
- Community
- Hybrid
- **Function as a Service (FaaS)/serverless architecture**
- **Infrastructure as code (IaC)**
- **Insecure application programming interface (API)**
- **Improper key management**
- **Unprotected storage**
- **Logging and monitoring**
 - Insufficient logging and monitoring
 - Inability to access

1.7

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

- **Attack types**
 - Extensible markup language (XML) attack
 - Structured query language (SQL) injection
 - Overflow attack
 - Buffer
 - Integer
 - Heap
 - Remote code execution
 - Directory traversal
 - Privilege escalation
- Password spraying
- Credential stuffing
- Impersonation
- On-path attack (previously known as man-in-the-middle attack)
- Session hijacking
- Rootkit
- Cross-site scripting
 - Reflected
 - Persistent
- Document object model (DOM)
- **Vulnerabilities**
 - Improper error handling
 - Dereferencing
 - Insecure object reference
 - Race condition
 - Broken authentication
 - Sensitive data exposure
 - Insecure components
 - Insufficient logging and monitoring
 - Weak or default configurations
 - Use of insecure functions
 - strcpy



2.0 Software and Systems Security

2.1 Given a scenario, apply security solutions for infrastructure management.

- **Cloud vs. on-premises**
- **Asset management**
 - Asset tagging
- **Segmentation**
 - Physical
 - Virtual
 - Jumpbox
 - System isolation
 - Air gap
- **Network architecture**
 - Physical
 - Software-defined
- Virtual private cloud (VPC)
- Virtual private network (VPN)
- Serverless
- **Change management**
- **Virtualization**
 - Virtual desktop infrastructure (VDI)
- **Containerization**
- **Identity and access management**
 - Privilege management
 - Multifactor authentication (MFA)
 - Single sign-on (SSO)
 - Federation
- Role-based
- Attribute-based
- Mandatory
- Manual review
- **Cloud access security broker (CASB)**
- **Honeypot**
- **Monitoring and logging**
- **Encryption**
- **Certificate management**
- **Active defense**

2.2 Explain software assurance best practices.

- **Platforms**
 - Mobile
 - Web application
 - Client/server
 - Embedded
 - System-on-chip (SoC)
 - Firmware
- **Software development life cycle (SDLC) integration**
- **DevSecOps**
- **Software assessment methods**
 - User acceptance testing
 - Stress test application
 - Security regression testing
 - Code review
- **Secure coding best practices**
 - Input validation
 - Output encoding
 - Session management
 - Authentication
 - Data protection
 - Parameterized queries
- **Static analysis tools**
- **Dynamic analysis tools**
- **Formal methods for verification of critical software**
- **Service-oriented architecture**
 - Security Assertions Markup Language (SAML)
 - Simple Object Access Protocol (SOAP)
 - Representational State Transfer (REST)
 - Microservices

2.3 Explain hardware assurance best practices.

- **Hardware root of trust**
 - Trusted platform module (TPM)
 - Hardware security module (HSM)
- **eFuse**
- **Unified Extensible Firmware Interface (UEFI)**
- **Trusted foundry**
- **Secure processing**
 - Trusted execution
 - Secure enclave
 - Processor security extensions
 - Atomic execution
- **Anti-tamper**
- **Self-encrypting drive**
- **Trusted firmware updates**
- **Measured boot and attestation**
- **Bus encryption**



3.0 Security Operations and Monitoring

3.1 Given a scenario, analyze data as part of security monitoring activities.

- **Heuristics**
- **Trend analysis**
- **Endpoint**
 - Malware
 - Reverse engineering
 - Memory
 - System and application behavior
 - Known-good behavior
 - Anomalous behavior
 - Exploit techniques
 - File system
 - User and entity behavior analytics (UEBA)
- **Network**
 - Uniform Resource Locator (URL) and domain name system (DNS) analysis
 - Domain generation algorithm
 - Flow analysis
 - Packet and protocol analysis
 - Malware
- **Log review**
 - Event logs
 - Syslog
 - Firewall logs
 - Web application firewall (WAF)
 - Proxy
 - Intrusion detection system (IDS)/Intrusion prevention system (IPS)
- **Impact analysis**
 - Organization impact vs. localized impact
 - Immediate vs. total
- **Security information and event management (SIEM) review**
 - Rule writing
 - Known-bad Internet protocol (IP)
 - Dashboard
- **Query writing**
 - String search
 - Script
 - Piping
- **E-mail analysis all in 35**
 - Malicious payload
 - Domain Keys Identified Mail (DKIM)
 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
 - Sender Policy Framework (SPF)
 - Phishing
 - Forwarding
 - Digital signature
 - E-mail signature block
 - Embedded links
 - Impersonation
 - Header

3.2 Given a scenario, implement configuration changes to existing controls to improve security.

- **Permissions**
- **Allow list (previously known as whitelisting)**
- **Blocklist (previously known as blacklisting)**
- **Firewall**
- **Intrusion prevention system (IPS) rules**
- **Data loss prevention (DLP)**
- **Endpoint detection and response (EDR)**
- **Network access control (NAC)**
- **Sinkholing**
- **Malware signatures**
 - Development/rule writing
- **Sandboxing**
- **Port security**



3.3 Explain the importance of proactive threat hunting.

- Establishing a hypothesis
 - Profiling threat actors and activities
 - Threat hunting tactics
 - Executable process analysis
 - Reducing the attack surface area
 - Bundling critical assets
 - Attack vectors
 - Integrated intelligence
 - Improving detection capabilities
-

3.4 Compare and contrast automation concepts and technologies.

- Workflow orchestration 45
 - Security Orchestration, Automation, and Response (SOAR) 42
- Scripting 45
- Application programming interface (API) integration
- Automated malware signature creation
- Data enrichment
- Threat feed combination
- Machine learning
- Use of automation protocols and standards
 - Security Content Automation Protocol (SCAP)
- Continuous integration
- Continuous deployment/delivery



4.0 Incident Response

4.1 Explain the importance of the incident response process.

• Communication plan 53

- Limiting communication to trusted parties
- Disclosing based on regulatory/legislative requirements
- Preventing inadvertent release of information
- Using a secure method of communication
- Reporting requirements

• Response coordination 53 with relevant entities

- Legal
- Human resources
- Public relations
- Internal and external
- Law enforcement
- Senior leadership
- Regulatory bodies

• Factors contributing to data criticality 53

- Personally identifiable information (PII)
- Personal health information (PHI)
- Sensitive personal information (SPI)
- High value asset
- Financial information
- Intellectual property
- Corporate information

4.2 Given a scenario, apply the appropriate incident response procedure. 53

• Preparation

- Training
- Testing
- Documentation of procedures

• Detection and analysis

- Characteristics contributing to severity level classification
- Downtime
- Recovery time
- Data integrity
- Economic
- System process criticality
- Reverse engineering
- Data correlation

• Containment

- Segmentation

- Isolation

• Eradication and recovery

- Vulnerability mitigation
- Sanitization
- Reconstruction/reimaging
- Secure disposal
- Patching
- Restoration of permissions
- Reconstitution of resources
- Restoration of capabilities and services
- Verification of logging/communication to security monitoring

• Post-incident activities

- Evidence retention

- Lessons learned report
- Change control process
- Incident response plan update
- Incident summary report
- IoC generation
- Monitoring

**4.3** Given an incident, analyze potential indicators of compromise. 24

- **Network-related**
 - Bandwidth consumption
 - Beaconsing
 - Irregular peer-to-peer communication
 - Rogue device on the network
 - Scan/sweep
 - Unusual traffic spike
 - Common protocol over non-standard port
 - **Host-related**
 - Processor consumption
 - Memory consumption
 - Drive capacity consumption
 - Unauthorized software
 - Malicious process
 - Unauthorized change
 - Unauthorized privilege
 - Data exfiltration
 - Abnormal OS process behavior
 - File system change or anomaly
 - Registry change or anomaly
 - Unauthorized scheduled task
 - **Application-related**
 - Anomalous activity
 - Introduction of new accounts
 - Unexpected output
 - Unexpected outbound communication
 - Service interruption
 - Application log
-

4.4 Given a scenario, utilize basic digital forensics techniques. 49

- **Network**
 - Wireshark
 - tcpdump
- **Endpoint**
 - Disk
 - Memory
- **Mobile**
- **Cloud**
- **Virtualization**
- **Legal hold**
- **Procedures**
- **Hashing**
 - Changes to binaries
- **Carving**
- **Data acquisition**



5.0 Compliance and Assessment

5.1 Understand the importance of data privacy and protection. 50 & as noted additionally

- **Privacy vs. security**
- **Non-technical controls**
 - Classification
 - Ownership
 - Retention
 - Data types
 - Retention standards **also 51**
 - Confidentiality
- **Legal requirements**
 - Data sovereignty
 - Data minimization
 - Purpose limitation
 - Non-disclosure agreement (NDA)
- **Technical controls**
 - Encryption
 - Data loss prevention (DLP)
- **Data masking**
- **Deidentification**
- **Tokenization**
- **Digital rights management (DRM)**
 - Watermarking
- **Geographic access requirements**
- **Access controls**

5.2 Given a scenario, apply security concepts in support of organizational risk mitigation. 52 unless noted otherwise

- **Business impact analysis**
- **Risk identification process**
- **Risk calculation**
 - Probability
 - Magnitude
- **Communication of risk factors**
- **Risk prioritization**
 - Security controls **11**
 - Engineering tradeoffs **16**
- **Systems assessment**
- **Documented compensating controls**
- **Training and exercises**
 - Red team **27**
 - Blue team **27**
 - White team **27**
 - Tabletop exercise
- **Supply chain assessment 38**
 - Vendor due diligence
 - Hardware source authenticity

5.3 Explain the importance of frameworks, policies, procedures, and controls.

- **Frameworks 51**
 - Risk-based
 - Prescriptive
- **Policies and procedures 51**
 - Code of conduct/ethics
 - Acceptable use policy (AUP)
 - Password policy
 - Data ownership
- **Data retention**
- **Account management**
- **Continuous monitoring**
- **Work product retention**
- **Preventative**
- **Detective**
- **Responsive**
- **Corrective**
- **Control types 11**
 - Managerial
 - Operational
 - Technical
- **Audits and assessments 51**
 - Regulatory
 - Compliance

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	ACRONYM	SPELLED OUT
3DES	Triple Data Encryption Algorithm	ELK	Elasticsearch, Logstash, Kibana
ACL	Access Control List	ERP	Enterprise Resource Planning
AES	Advanced Encryption Standard	FaaS	Function as a Service
API	Application Programming Interface	FPGA	Field-programmable Gate Array
ARP	Address Resolution Protocol	FTK	Forensic Toolkit
APT	Advanced Persistent Threat	FTP	File Transfer Protocol
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	HIDS	Host Intrusion Detection System
AUP	Acceptable Use Policy	HIPS	Host-based Intrusion Prevention System
BEC	Business Email Compromise	HSM	Hardware Security Module
BYOD	Bring Your Own Device	HTTP	Hypertext Transfer Protocol
CA	Certificate Authority	IaaS	Infrastructure as a Service
CAN	Controller Area Network	IaC	Infrastructure as Code
CASB	Cloud Access Security Broker	ICMP	Internet Control Message Protocol
CI/CD	Continuous Integration/Continuous Delivery	IDS	Intrusion Detection System
CIS	Center for Internet Security	IMAP	Internet Message Access Protocol
COBIT	Control Objectives for Information and Related Technology	IoC	Indicator of Compromise
CPU	Central Processing Unit	IoT	Internet of Things
CRM	Customer Relations Management	IP	Internet Protocol
CVSS	Common Vulnerability Scoring System	IPS	Intrusion Prevention System
DDoS	Distributed Denial of Service	ISAC	Information Sharing and Analysis Center
DGA	Domain Generation Algorithm	ISO	International Organization for Standardization
DHCP	Dynamic Host Configuration Protocol	ITIL	Information Technology Infrastructure Library
DKIM	Domain Keys Identified Mail	LAN	Local Area Network
DLP	Data Loss Prevention	LDAP	Lightweight Directory Access Protocol
DMARC	Domain-based Message Authentication, Reporting, and Conformance	MaaS	Monitoring as a Service
DMZ	Demilitarized Zone	MAC	Mandatory Access Control
DNS	Domain Name System	MD5	Message Digest 5
DNSSEC	Domain Name System Security Extensions	MDM	Mobile Device Management
DOM	Document Object Model	MFA	Multifactor Authentication
DRM	Digital Rights Management	MOA	Memorandum of Agreement
EDR	Endpoint Detection and Response	MOU	Memorandum of Understanding
		MRTG	Multi Router Traffic Grapher
		NAC	Network Access Control
		NAS	Network-attached Storage

ACRONYM	SPELLED OUT
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NIC	Network Interface Card
NIDS	Network Intrusion Detection Systems
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OSSIM	Open Source Security Information Management
OWAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Pluggable Authentication Module
PCAP	Packet Capture
PCI	Payment Card Industry
PHI	Personal Health Information
PID	Process Identification Number
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-in User Service
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RTOS	Real-time Operating System
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDLC	Software Development Life Cycle
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMB	Server Message Block
SOAP	Simple Object Access Protocol
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SoC	System on Chip
SPF	Sender Policy Framework
SPI	Sensitive Personal Information
SQL	Structured Query Language
SSH	Secure Shell
SSHD	Solid-state Hybrid Drive
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STIX	Structured Threat Information eXpression
TACACS+	Terminal Access Controller Access Control System Plus

ACRONYM	SPELLED OUT
TAXII	Trusted Automated eXchange of Intelligence Information
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
UEBA	User and Entity Behavior Analytics
UEFI	Unified Extensible Firmware Interface
UEM	Unified Endpoint Management
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPC	Virtual Private Cloud
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
XML	Extensible Markup Language
XSS	Cross-site Scripting
ZAP	Zed Attack Proxy

CySA+ Proposed Hardware and Software List

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 that wish to create a lab component for their training offering. The bulleted lists below each topic are samples and are not exhaustive.

IT HARDWARE

- Workstation (or laptop)
with ability to run VM
- Managed switch
- Firewall
- Mobile phones
- VoIP Phone
- WAP
- IDS/ IPS
- IoT Devices
- Servers

SOFTWARE

- VM images for attack targets
- Windows Server
- Windows Client
 - Commando VM
- Linux
 - Kali
 - ParrotOS
 - Security Onion
- Chrome OS
- UTM Appliance
- pfSense
- Metasploitable

- Access to cloud instances
 - Azure
 - AWS
 - GCP
- SIEM
 - Graylog
 - ELK
 - Splunk
- Vulnerability scanner
 - OpenVAS
 - Nessus