CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives

EXAM NUMBER: CS0-004 V4

CompTIA CySA+ CS0-004 V4 Certification Exam
Exam Objectives Document Version 2.0

About the Exam

The CompTIA CySA+ CS0-004 V4 certification exam will certify the successful candidate has the knowledge and skills required to:

- Understand and perform incident response and vulnerability management processes.
- Detect and analyze indicators of malicious activity in support of security operations.
- Use appropriate tools, methods, and frameworks to prioritize and manage vulnerabilities and respond to incidents.
- Understand reporting and communication concepts related to vulnerability management and incident response activities.

This is the equivalent of approximately 4 years of hands-on experience in a SOC analyst (level 2) or a vulnerability analyst 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 ACCREDITATION

The CompTIA CySA+ exam is accredited by the ANSI National Accreditation Board (ANAB) to show compliance with the International Organization for Standardization (ISO) 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

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”), they 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	CySA+ CS0-004 V4
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 in a SOC analyst (level 2) or vulnerability analyst role
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.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Security Operations	34%
2.0	Vulnerability Management	26%
3.0	Incident Response and Management	24%
4.0	Reporting and Communication	16%
Total		**100%**

1.0 Security Operations

1.1 Explain concepts related to system and network architecture in security operations.

- Logging concepts
  - Ingestion
  - Configuration
  - Integrity and security
  - Time synchronization
  - Retention
- Operating system concepts
  - System hardening
  - File structure
    - Critical files
  - System processes
- Infrastructure/system architecture concepts
  - Cloud native
  - Virtualization
  - Containerization
  - Application programming interfaces (APIs)
- Device management concepts
  - Mobile
  - Endpoint
- Network architecture concepts
  - Zero Trust Network Architecture (ZTNA)
  - Secure access service edge (SASE)
  - Hybrid cloud
- Identity and access management (IAM)
  - Privileged access management (PAM)
  - Authentication and authorization methods
  - Secrets management
- Encryption techniques
- Data protection concepts
- Critical infrastructure concepts
  - Operational technology (OT)
  - Industrial control system (ICS)
  - Supervisory control and data acquisition (SCADA)

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

- Network-related indicators
  - Rogue devices
  - Enumeration
  - Anomalous activity
  - Activity on unexpected ports
- Host-related indicators
  - Resource consumption
  - Unauthorized software
  - Anomalous activity
    - Suspicious or rogue processes
    - Living Off the Land Binaries (LOLBins) and Scripts
    - File system changes
    - Data exfiltration
- Unauthorized configuration
- Application-related indicators
  - Service disruption
  - Anomalous activity
- Cloud-related indicators
  - Anomalous activity
  - Resource compromise
- Social engineering attacks
  - Typosquatting
  - URL shorteners
- Identity-based indicators
  - IAM account compromise
  - Unauthorized access
  - Impossible travel
- Email-related attacks
  - Business email compromise (BEC)

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

- Tools
  - Decoding/parsing
    - CyberChef
  - Packet analysis
    - Wireshark
    - tcpdump
    - Snort
    - Suricata
    - Zeek
  - Log analysis
    - Security information and event management (SIEM)
  - Threat-intelligence platforms
    - Open Threat Exchange (OTX)
    - Malware Information Sharing Platform (MISP)
    - Open Cyber Threat Intelligence (OpenCTI)
  - Endpoint security
    - Endpoint detection and response (EDR) and extended detection and response (XDR)
    - Mobile device management (MDM)
  - Domain and IP reputation
    - WHOIS
    - AbuseIPDB
    - Geolocation by IP Address (GEO-IP)
  - File analysis
    - Strings
    - VirusTotal
    - Yet another recursive acronym (YARA)
  - Sandboxing
    - Joe Sandbox
    - Cuckoo Sandbox
  - Pattern recognition
    - Regular expressions
    - Interpreting suspicious commands
  - Email analysis
    - MXToolbox
  - User and entity behavior analysis (UEBA)
    - Open User and Entity Behavior Analytics (OpenUBA)
- File formats
  - JSON
  - XML
  - YAML
  - EVTX
- Programming/scripting languages
  - Python
  - PowerShell
  - Shell script

1.4 Explain threat intelligence and threat-hunting concepts.

- Threat actors
  - Advanced persistent threat (APT)
  - Insider threat
- Tactics, techniques, and procedures (TTPs)
  - Heat maps
  - Pyramid of Pain
  - MITRE ATT&CK
  - Attribution
- Confidence-level impacts
  - Timeliness
  - Relevance
  - Accuracy
- Collection methods and sources
  - Open-source intelligence (OSINT)
  - Closed-source intelligence
  - Threat intelligence sharing
- Indicator of compromise (IoC)
  - Collection
  - Analysis
  - Application/usage
  - Types
    - Atomic
    - Behavioral
- Threat modeling
  - Spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege (STRIDE)
- Threat mapping
- Cyber deception

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

- Standardize processes
  - Manage and facilitate team coordination
  - Playbook/runbook creation
- Streamline operations
  - Automation and orchestration
    - Security orchestration, automation, and Response (SOAR)
    - Infrastructure as code (IaC)
  - Data enrichment
    - Rule/alert tuning
    - Dashboard creation
- Technology and tool integration
  - APIs
  - Webhooks
  - Plug-ins

1.6 Summarize concepts related to the use of AI in security operations.

- AI risks
  - Hallucinations
  - Data exposure
  - Model poisoning
  - Malicious prompts
- Governance
  - Legal or regulatory compliance
  - AI usage policies
- Use cases
  - Comparing artifacts
  - Analyzing log files
  - Document creation
  - Incident investigation
  - Event correlation
  - Automation and orchestration

2.0 Vulnerability Management

2.1 Given a scenario, implement the appropriate vulnerability scanning method.

- Asset inventory
- Planning considerations
  - Scheduling
  - Operations
  - Performance
  - Sensitivity levels
  - Segmentation
  - Regulatory requirements
- Scan types
  - Internal vs. external
  - Agent vs. agentless
  - Credentialed vs. non-credentialed
  - Passive vs. active
  - Discovery
    - Mapping scans
    - Device fingerprinting
  - Security baseline scanning
    - Payment Card Industry Data Security Standard (PCI DSS)
    - Center for Internet Security (CIS) benchmarks
    - International Organization for Standardization (ISO) 27000 series

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

- Network scanning and mapping
  - Angry IP Scanner
  - Masscan
- Multipurpose tools
  - Nmap
  - Metasploit Framework (MSF)
  - Maltego
  - Recon-ng
- Web application scanners
  - Burp Suite
  - Zed Attack Proxy (ZAP)
  - Nikto
- Vulnerability scanners
  - Nessus
  - Nuclei
  - Open Vulnerability Assessment Scanner (OpenVAS)
- Cloud infrastructure assessment tools
  - ScoutSuite
  - Prowler
  - Trivy
  - Checkov
- Breach attack simulation (BAS) tools
  - Atomic Red Team
  - Caldera

2.3 Given a scenario, analyze data to prioritize and mitigate vulnerabilities.

- Criteria
  - Exploitability
  - Active exploitation/threat intelligence
  - Asset value
  - Impact
  - Patch/remediation availability
  - True/false positives
  - True/false negatives
- Scoring methods
  - Common Vulnerability Scoring System (CVSS) metrics
  - First Exploitability Prediction Scoring System (EPSS)
- Context awareness
  - Internal
  - External
  - Isolated
- Mitigation strategies
  - Attack surface management
  - Secure coding best practices
  - Patching and configuration management
  - Exceptions
  - Compensating controls
- Validation of remediation

2.4 Explain concepts related to control types, risks, and vulnerability management.

- Control types
  - Administrative
  - Technical
  - Physical
- Control functions
  - Preventative
  - Detective
  - Responsive
  - Corrective
- Risk concepts
  - Risk appetite
  - Residual risk
  - Inherent risk
- Risk management strategies
  - Accept
  - Transfer
  - Avoid
  - Mitigate
- Policies, governance, and service-level objectives (SLOs)
- Application security
  - Static application security testing (SAST)
  - Dynamic application security testing (DAST)
  - Software Assurance Maturity Model (SAMM)
- Third-party risk
  - Supply chain
  - Software composition analysis (SCA)
  - Software bill of materials (SBOM)

3.0 Incident Response and Management

3.1 Summarize concepts related to attack methodology frameworks.

- Cyber Kill Chain
- Diamond Model of Intrusion Analysis
- MITRE ATT&CK

3.2 Summarize the incident response process.

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-incident

3.3 Given a scenario, implement incident response techniques.

- Developing plans
  - Incident response plan
  - Communication plan
- Creating playbooks
- Defining roles
- Performing training
  - Tabletop
  - Simulation
- Log collection
- Log correlation
- Log augmentation and enrichment
- Alerts and notifications
- Triage
- Establishment of a timeline
- Determining severity and impact
- Prioritization
- Evidence gathering
  - Chain of custody
  - Data integrity validation
  - Preservation
  - Legal hold
- Isolating affected targets
- Escalation
- Remediation and verification
- Release from isolation
- Performing restoration
- Root cause analysis (RCA)
- Corrective action development

4.0 Reporting and Communication

4.1 Explain the importance of vulnerability management reporting and communication.

- Vulnerability scan reports
- Compliance findings
- Risk scorecards
- Action plans
  - Escalation
  - Dependencies
- Inhibitors to remediation
  - Contractual agreements
  - Organizational governance
  - Business process interruption
  - Degrading functionality
  - Legacy systems
  - Proprietary systems
  - Patch availability
- Stakeholder identification and communication
- Metrics and key performance indicators (KPIs)
  - Trends
  - Top risks
  - Service-level agreement (SLA)

4.2 Explain the importance of security operations and incident response reporting and communication.

- Incident declaration and escalation
- Executive summary
- Communication plan
  - Stakeholder identification
  - Legal team
  - Public relations
  - Regulatory reporting agencies
  - Law enforcement
  - Customers
- Operational security awareness
  - Communication channels
- Post-incident reporting
  - After action report
  - Lessons learned
  - Root cause analysis
- Shift/incident handover
- Internal threat intelligence report
  - Tailored to organization/environment
- Metrics and KPIs
  - Alert volume
  - False-positive rate
  - True-positive rate
  - Mean time to close
  - Mean time to detect
  - Mean time to respond
  - Mean time to remediate
  - Phishing campaign click rate

CompTIA CySA+ Acronym List

The following is a list of acronyms that appear on the CompTIA CySA+ CS0-004 V4 certification 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	DEFINITION
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ASN	Anonymous System Number
AWS	Amazon Web Services
BAS	Breach Attack Simulation
BC	Business Continuity
BEC	Business Email Compromise
CASB	Cloud Access Security Broker
CERT	Computer Emergency Response Team
CHD	Cardholder Data
CIS	Center for Internet Security
CSIRT	Cybersecurity Incident Response Team
CVSS	Common Vulnerability Scoring System
DAST	Dynamic Application Security Testing
DKIM	Domain Keys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name Service
DR	Disaster Recovery
EDR	Endpoint Detection and Response
EPSS	Exploitability Predication Scoring System
GCP	Google Cloud Platform
GDB	GNU Debugger
GeoIP	Geolocation by IP
IaC	Infrastructure as Code
IAM	Identity and Access Management
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IoC	Indicator of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
KPI	Key Performance Indicator

ACRONYM	DEFINITION
LFI	Local File Inclusion
MDM	Mobile Device Management
MFA	Multifactor Authentication
MISP	Malware Information Sharing Platform
MOU	Memorandum of Understanding
MSF	Metasploit Framework
OpenCTI	Open Cyber Threat Intelligence
OpenUBA	Open User Behavior Analytics
OpenVAS	Open Vulnerability Assessment Scanner
OSINT	Open-Source Intelligence
OSSTMM	Open Source Security Testing Methodology Manual
OT	Operational Technology
OTX	Open Threat Exchange
OWASP	Open Web Application Security Project
PAM	Privileged Access Management
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RFI	Remote File Inclusion
SAMM	Software Assurance Maturity Model
SASE	Secure Access Service Edge
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SCA	Software Composition Analysis
SCADA	Supervisory Control and Data Acquisition
SDLC	Software Development Life Cycle
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SLA	Service-level Agreement
SLO	Service-level Objective
SOAR	Security Orchestration, Automation, and Response
SPF	Sender Policy Framework
SSL	Secure Sockets Layer
SSO	Single Sign-on
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege
TCP	Transmission Control Protocol
TTPs	Tactics, Techniques, and Procedures
UEBA	User and Entity Behavior Analysis
UTM	Unified Threat Management
VM	Virtual Machine
XDR	Extended Detection and Response
XML	Extensible Markup Language
YAML	Yet Another Markup Language

ACRONYM	DEFINITION
YARA	Yet Another Recursive Acronym
ZAP	Zed Attack Proxy
ZTNA	Zero Trust Network Access

CompTIA CySA+ Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CySA+ CS0-004 V4 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 laptops) with ability to run a virtual machine (VM)
- Firewall
- Intrusion detection system/intrusion prevention system (IDS/IPS)
- Servers

SOFTWARE

- Windows operating systems
  - Commando VM
- Linux operating systems
  - Kali
- Open-source unified thread management (UTM) appliance
- Metasploitable
- SIEM
  - Greylog
  - Elasticsearch, Logstash, and Kibana (ELK)
  - Splunk
- tcpdump
- Wireshark
- Vulnerability scanner
  - OpenVAS
  - Nessus
- Access to cloud instances
  - Azure
  - Amazon Web Services (AWS)
  - Google Cloud Platform (GCP)

CompTIA