About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Cybersecurity Analyst (CySA+) CS0-002 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: Minimum of 85  
Type of questions: Multiple choice and performance-based  
Length of test: 165 minutes  
Recommended experience: • 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.

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Threat and Vulnerability Management</td>
<td>22%</td>
</tr>
<tr>
<td>2.0 Software and Systems Security</td>
<td>18%</td>
</tr>
<tr>
<td>3.0 Security Operations and Monitoring</td>
<td>25%</td>
</tr>
<tr>
<td>4.0 Incident Response</td>
<td>22%</td>
</tr>
<tr>
<td>5.0 Compliance and Assessment</td>
<td>13%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
1.0 Threat and Vulnerability Management

1.1 Explain the importance of threat data and intelligence.

- **Intelligence sources**
  - Open-source intelligence
  - Proprietary/closed-source intelligence
  - Timeliness
  - Relevancy
  - Accuracy

- **Confidence levels**

- **Indicator management**
  - Structured Threat Information eXpression (STIX)
  - Trusted Automated eXchange of Indicator Information (TAXII)
  - OpenIOC

- **Threat classification**
  - Known threat vs. unknown threat
  - Zero-day
  - Advanced persistent threat

- **Threat actors**
  - Nation-state
  - Hacktivist
  - Organized crime
  - Insider threat
    - Intentional
    - Unintentional

- **Intelligence cycle**
  - Requirements
  - Collection
  - Analysis
  - Dissemination
  - Feedback

- **Commodity malware**

- **Information sharing and analysis communities**
  - Healthcare
  - Financial
  - Aviation
  - Government
  - Critical infrastructure

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

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

- **Threat research**
  - Reputational
  - Behavioral
  - Indicator of compromise (IOC)

- **Threat modeling methodologies**
  - Adversary capability
  - Total attack surface
  - Attack vector
  - Impact
  - Likelihood

- **Common vulnerability scoring system (CVSS)**

- **Threat intelligence sharing with supported functions**
  - Incident response
  - Vulnerability management
  - Risk management
  - Security engineering
  - Detection and monitoring
1.3 Given a scenario, perform vulnerability management activities.

- **Vulnerability identification**
  - Asset criticality
  - Active vs. passive scanning
  - Mapping/enumeration
- **Validation**
  - True positive
  - False positive
  - True negative
  - False negative
- **Remediation/mitigation**
  - Configuration baseline
  - Patching
  - Hardening
  - Compensating controls
- **Risk acceptance**
- **Verification of mitigation**
- **Scanning parameters and criteria**
  - Risks associated with scanning activities
  - Vulnerability feed
  - Scope
  - Credentialled vs. non-credentialled
  - Server-based vs. agent-based
  - Internal vs. external
  - Special considerations
    - Types of data
    - Technical constraints
    - Workflow
- **Validation**
  - True positive
  - False positive
  - True negative
  - False negative
- **Remediation/mitigation**
  - Configuration baseline
  - Patching
  - Hardening
  - Compensating controls
- **Risk acceptance**
- **Verification of mitigation**
- **Scanning parameters and criteria**
  - Risks associated with scanning activities
  - Vulnerability feed
  - Scope
  - Credentialled vs. non-credentialled
  - Server-based vs. agent-based
  - Internal vs. external
  - Special considerations
    - Types of data
    - Technical constraints
    - Workflow
- **Risk acceptance**
- **Verification of mitigation**

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**
- **Incident command system (ICS)**
- **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
  - Man-in-the-middle attack
  - Session hijacking
  - Rootkit
  - Cross-site scripting
    - Reflected
    - Persistent
  - Document object model (DOM)
- Improper error handling
- Dereferencing
- Insecure object reference
- Race condition
- Broken authentication
- Insecure software
- 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
  - Dynamically generated algorithms
  - 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
  - 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
- Whitelisting
- 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
- Scripting
- 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
  - 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 with relevant entities
  - Legal
  - Human resources
  - Public relations
  - Internal and external
  - Law enforcement
  - Senior leadership
  - Regulatory bodies

- Factors contributing to data criticality
  - Personally identifiable information (PII)
  - Personal health information (PHI)
  - Special protected information (SPI)
  - High value asset
  - Financial information
  - Intellectual property
  - Corporate information

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

- 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
  - Indicator of compromise (IOC) generation
  - Monitoring
4.3 Given an incident, analyze potential indicators of compromise.

- **Network-related**
  - Bandwidth consumption
  - Beaconing
  - 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

- **Application-related**
  - 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

4.4 Given a scenario, utilize basic digital forensics techniques.

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

5.2 Given a scenario, apply security concepts in support of organizational risk mitigation.
- Business impact analysis
- Risk identification process
- Risk calculation
  - Probability
  - Magnitude
- Communication of risk factors
- Risk prioritization
  - Security controls
  - Engineering tradeoffs
- Systems assessment
- Documented compensating controls
- Training and exercises
  - Red team
  - Blue team
  - White team
  - Tabletop exercise
- Supply chain assessment
  - Vendor due diligence
  - Hardware source authenticity

5.3 Explain the importance of frameworks, policies, procedures, and controls.
- Frameworks
  - Risk-based
  - Prescriptive
- Policies and procedures
  - Code of conduct/ethics
  - Acceptable use policy (AUP)
  - Password policy
  - Data ownership
  - Preventative
  - Detective
  - Responsive
  - Corrective
- Control types
  - Managerial
  - Operational
  - Technical
- Audits and assessments
  - Regulatory
  - Compliance
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.
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTOS</td>
<td>Real-time Operating System</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertions Markup Language</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCAP</td>
<td>Security Content Automation Protocol</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SOAP</td>
<td>Simple Object Access Protocol</td>
</tr>
<tr>
<td>SOC</td>
<td>Security Operations Center</td>
</tr>
<tr>
<td>SoC</td>
<td>System on Chip</td>
</tr>
<tr>
<td>SPF</td>
<td>Sender Policy Framework</td>
</tr>
<tr>
<td>SPI</td>
<td>Special Protected Information</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-on</td>
</tr>
<tr>
<td>STIX</td>
<td>Structured Threat Information eXpression</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller</td>
</tr>
<tr>
<td>Access Control System Plus</td>
<td></td>
</tr>
<tr>
<td>TAXII</td>
<td>Trusted Automated eXchange of Intelligence Information</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>UEBA</td>
<td>User and Entity Behavior Analytics</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VPC</td>
<td>Virtual Private Cloud</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAF</td>
<td>Web Application Firewall</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>ZAP</td>
<td>Zed Attack Proxy</td>
</tr>
</tbody>
</table>
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
  - Greylog
  - ELK
  - Splunk
- Vulnerability scanner
  - OpenVAS
  - Nessus