EDUSUM

#1 Online Certification Guide

COMPTIA CS0-002

CompTIA CySA Plus Certification Questions & Answers

Exam Summary – Syllabus –Questions

CS0-002

CompTIA Cybersecurity Analyst (CySA+)

85 Questions Exam – 750/900 Cut Score – Duration of 165 minutes

Table of Contents:

Know Your CS0-002 Certification Well:

The CS0-002 is best suitable for candidates who want to gain knowledge in the CompTIA Cybersecurity. Before you start your CS0-002 preparation you may struggle to get all the crucial CySA Plus materials like CS0-002 syllabus, sample questions, study guide.

But don't worry the CS0-002 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the CS0-002 syllabus?
- How many questions are there in the CS0-002 exam?
- Which Practice test would help me to pass the CS0-002 exam at the first attempt?

Passing the CS0-002 exam makes you CompTIA Cybersecurity Analyst (CySA+). Having the CySA Plus certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CompTIA CS0-002 CySA Plus Certification Details:

Exam Name	CompTIA Cybersecurity Analyst (CySA+)
Exam Code	CS0-002
Exam Price	$370 (USD)
Duration	165 mins
Number of Questions	85
Passing Score	750 / 900
Books / Training	**eLearning with CompTIA CertMaster Learn for CySA+** **Interactive Labs with CompTIA CertMaster Labs for CySA+**
Schedule Exam	**CompTIA Marketplace**
Sample Questions	**CompTIA CySA+ Sample Questions**
Practice Exam	**CompTIA CS0-002 Certification Practice Exam**

CS0-002 Syllabus:

Topic	Details
Threat and Vulnerability Management - 22%	
Explain the importance of threat data and intelligence.	1. Intelligence sources • Open-source intelligence • Proprietary/closed-source intelligence • Timeliness • Relevancy • Accuracy 2. Confidence levels 3. Indicator management • Structured Threat Information eXpression (STIX) • Trusted Automated eXchange of Indicator Information (TAXII) • OpenIoC 4. Threat classification • Known threat vs. unknown threat • Zero-day • Advanced persistent threat 5. Threat actors • Nation-state • Hacktivist • Organized crime • Insider threat Intentional Unintentional 6. Intelligence cycle • Requirements • Collection • Analysis • Dissemination • Feedback

Topic	Details
	7. Commodity malware 8. Information sharing and analysis communities • Healthcare • Financial • Aviation • Government • Critical infrastructure
Given a scenario, utilize threat intelligence to support organizational security.	1. Attack frameworks • MITRE ATT&CK • The Diamond Model of Intrusion Analysis • Kill chain 2. Threat research • Reputational • Behavioral • Indicator of compromise (IoC) • Common vulnerability scoring system (CVSS) 3. Threat modeling methodologies • Adversary capability • Total attack surface • Attack vector • Impact • Likelihood 3. Threat intelligence sharing with supported functions • Incident response • Vulnerability management • Risk management • Security engineering • Detection and monitoring
Given a scenario, perform vulnerability management activities.	1. Vulnerability identification • Asset criticality • Active vs. passive scanning • Mapping/enumeration

Topic	Details
	2. Validation • True positive • False positive • True negative • False negative 3. Remediation/mitigation • Configuration baseline • Patching • Hardening • Compensating controls • Risk acceptance • Verification of mitigation 4. 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 5. Inhibitors to remediation • Memorandum of understanding (MOU) • Service-level agreement (SLA) • Organizational governance • Business process interruption • Degrading functionality • Legacy systems • Proprietary systems

Topic	Details
Given a scenario, analyze the output from common vulnerability assessment tools.	1. Web application scanner • OWASP Zed Attack Proxy (ZAP) • Burp suite • Nikto • Arachni 2. Infrastructure vulnerability scanner • Nessus • OpenVAS • Qualys 3. Software assessment tools and techniques • Static analysis • Dynamic analysis • Reverse engineering • Fuzzing 4. Enumeration • Nmap • hping • Active vs. passive • Responder 5. Wireless assessment tools • Aircrack-ng • Reaver • oclHashcat 6. Cloud infrastructure assessment tools • ScoutSuite • Prowler • Pacu
Explain the threats and vulnerabilities associated with specialized technology.	1. Mobile 2. Internet of Things (IoT) 3. Embedded 4. Real-time operating system (RTOS) 5. System-on-Chip (SoC) 6. Field programmable gate array (FPGA)

Topic	Details
	7. Physical access control 8. Building automation systems 9. Vehicles and drones • CAN bus 10. Workflow and process automation systems 11. Industrial control system 12. Supervisory control and data acquisition (SCADA) • Modbus
Explain the threats and vulnerabilities associated with operating in the cloud.	1. Cloud service models • Software as a Service (SaaS) • Platform as a Service (PaaS) • Infrastructure as a Service (IaaS) 2. Cloud deployment models • Public • Private • Community • Hybrid 3. Function as a Service (FaaS)/serverless architecture 4. Infrastructure as code (IaC) 5. Insecure application programming interface (API) 6. Improper key management 7. Unprotected storage 8. Logging and monitoring • Insufficient logging and monitoring • Inability to access
Given a scenario, implement controls to mitigate attacks and software vulnerabilities.	1. Attack types • Extensible markup language (XML) attack • Structured query language (SQL) injection • Overflow attack Buffer Integer Heap • Remote code execution • Directory traversal • Privilege escalation

Topic	Details
	• Password spraying • Credential stuffing • Impersonation • Man-in-the-middle attack • Session hijacking • Rootkit • Cross-site scripting Reflected Persistent Document object model (DOM) 2. 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
Software and Systems Security - 18%	
Given a scenario, apply security solutions for infrastructure management.	1. Cloud vs. on-premises 2. Asset management • Asset tagging 3. Segmentation • Physical • Virtual • Jumpbox • System isolation Air gap 4. Network architecture • Physical

Topic	Details
	• Software-defined • Virtual private cloud (VPC) • Virtual private network (VPN) • Serverless 5. Change management 6. Virtualization • Virtual desktop infrastructure (VDI) 7. Containerization 8. Identity and access management • Privilege management • Multifactor authentication (MFA) • Single sign-on (SSO) • Federation • Role-based • Attribute-based • Mandatory • Manual review 9. Cloud access security broker (CASB) 10. Honeypot 11. Monitoring and logging 12. Encryption 13. Certificate management 14. Active defense
Explain software assurance best practices.	1. Platforms Mobile Web application Client/server Embedded System-on-chip (SoC) Firmware 2. Software development life cycle (SDLC) integration 3. DevSecOps 4. Software assessment methods User acceptance testing Stress test application Security regression testing Code review 5. Secure coding best practices

Topic	Details
	Input validation Output encoding Session management Authentication Data protection Parameterized queries 6. Static analysis tools 7. Dynamic analysis tools 8. Formal methods for verification of critical software 9. Service-oriented architecture • Security Assertions Markup Language (SAML) • Simple Object Access Protocol (SOAP) • Representational State Transfer (REST) • Microservices
Explain hardware assurance best practices.	1. Hardware root of trust Trusted platform module (TPM) Hardware security module (HSM) 2. eFuse 3. Unified Extensible Firmware Interface (UEFI) 4. Trusted foundry 5. Secure processing • Trusted execution • Secure enclave • Processor security extensions • Atomic execution 6. Anti-tamper 7. Self-encrypting drive 8. Trusted firmware updates 9. Measured boot and attestation 10. Bus encryption
Security Operations and Monitoring - 25%	
Given a scenario, analyze data as part of security monitoring activities.	1. Heuristics 2. Trend analysis 3. Endpoint • Malware Reverse engineering

Topic	Details
	• Memory • System and application behavior Known-good behavior Anomalous behavior Exploit techniques • File system • User and entity behavior analytics (UEBA) 4. Network • Uniform Resource Locator (URL) and domain name system (DNS) analysis Domain generation algorithm • Flow analysis • Packet and protocol analysis Malware 5. Log review • Event logs • Syslog • Firewall logs • Web application firewall (WAF) • Proxy • Intrusion detection system (IDS)/Intrusion prevention system (IPS) 6. Impact analysis • Organization impact vs. localized impact • Immediate vs. total 7. Security information and event management (SIEM) review • Rule writing • Known-bad Internet protocol (IP) • Dashboard 8. Query writing • String search • Script • Piping 9. E-mail analysis

Topic	Details
	- 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
Given a scenario, implement configuration changes to existing controls to improve security.	1. Permissions 2. Whitelisting 3. Blacklisting 4. Firewall 5. Intrusion prevention system (IPS) rules 6. Data loss prevention (DLP) 7. Endpoint detection and response (EDR) 8. Network access control (NAC) 9. Sinkholing 10. Malware signatures - Development/rule writing 11. Sandboxing 12. Port security
Explain the importance of proactive threat hunting.	1. Establishing a hypothesis 2. Profiling threat actors and activities 3. Threat hunting tactics - Executable process analysis 4. Reducing the attack surface area 5. Bundling critical assets 6. Attack vectors 7. Integrated intelligence 8. Improving detection capabilities
Compare and contrast automation concepts and technologies.	1. Workflow orchestration

Topic	Details
	• Security Orchestration, Automation, and Response (SOAR) 2. Scripting 3. Application programming interface (API) integration 4. Automated malware signature creation 5. Data enrichment 6. Threat feed combination 7. Machine learning 8. Use of automation protocols and standards • Security Content Automation Protocol (SCAP) 9. Continuous integration 10. Continuous deployment/delivery
Incident Response - 22%	
Explain the importance of the incident response process.	1. 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 2. Response coordination with relevant entities • Legal • Human resources • Public relations • Internal and external • Law enforcement • Senior leadership • Regulatory bodies 3. Factors contributing to data criticality • Personally identifiable information (PII) • Personal health information (PHI) • Sensitive personal information (SPI) • High value asset • Financial information

Topic	Details
	• Intellectual property • Corporate information
Given a scenario, apply the appropriate incident response procedure.	1. Preparation • Training • Testing • Documentation of procedures 2. Detection and analysis • Characteristics contributing to severity level classification • Downtime • Recovery time • Data integrity • Economic • System process criticality • Reverse engineering • Data correlation 3. Containment • Segmentation • Isolation 4. 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 5. Post-incident activities • Evidence retention • Lessons learned report

Topic	Details
	- Change control process - Incident response plan update - Incident summary report - IoC generation - Monitoring
Given an incident, analyze potential indicators of compromise.	1. 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 2. 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 3. Application-related - Anomalous activity - Introduction of new accounts - Unexpected output - Unexpected outbound communication - Service interruption - Application log

Topic	Details
Given a scenario, utilize basic digital forensics techniques.	1. Network • Wireshark • tcpdump 2. Endpoint • Disk • Memory 3. Mobile 4. Cloud 5. Virtualization 6. Legal hold 7. Procedures 8. Hashing • Changes to binaries 9. Carving 10. Data acquisition
Compliance and Assessment - 13%	
Understand the importance of data privacy and protection.	1. Privacy vs. security 2. Non-technical controls • Classification • Ownership • Retention • Data types • Retention standards Confidentiality • Legal requirements • Data sovereignty • Data minimization • Purpose limitation • Non-disclosure agreement (NDA) 3. Technical controls • Encryption • Data loss prevention (DLP) • Data masking • Deidentification

Topic	Details
	- Tokenization - Digital rights management (DRM) Watermarking - Geographic access requirements - Access controls
Given a scenario, apply security concepts in support of organizational risk mitigation.	1. Business impact analysis 2. Risk identification process 3. Risk calculation - Probability - Magnitude 4. Communication of risk factors 5. Risk prioritization - Security controls - Engineering tradeoffs 6. Systems assessment 7. Documented compensating controls 8. Training and exercises - Red team - Blue team - White team - Tabletop exercise 9. Supply chain assessment - Vendor due diligence - Hardware source authenticity
Explain the importance of frameworks, policies, procedures, and controls.	1. Frameworks - Risk-based - Prescriptive 2. Policies and procedures - Code of conduct/ethics - Acceptable use policy (AUP) - Password policy - Data ownership - Data retention

Topic	Details
	• Account management • Continuous monitoring • Work product retention 3. Category • Managerial • Operational • Technical 4. Control type • Preventative • Detective • Corrective • Deterrent • Compensating • Physical 5. Audits and assessments • Regulatory • Compliance

CompTIA CS0-002 Sample Questions:

Question: 1

A cybersecurity analyst receives a phone call from an unknown person with the number blocked on the caller ID. After starting conversation, the caller begins to request sensitive information.

Which of the following techniques is being applied?

a) Social engineering
b) Phishing
c) Impersonation
d) War dialing

Answer: a

Question: 2

Given the following logs:

```
Aug 18 11:00:57 comptia sshd[5657]: Failed password for root from 10.10.10.192 port 38980 ssh2
Aug 18 23:08:26 comptia sshd[5768]: Failed password for root from 18.70.0.160 port 38156 ssh2
Aug 18 23:08:30 comptia sshd[5770]: Failed password for admin from 18.70.0.160 port 38556 ssh2
Aug 18 23:08:34 comptia sshd[5772]: Failed password for invalid user asterisk from 18.70.0.160 port 38864 ssh2
Aug 18 23:08:38 comptia sshd[5774]: Failed password for invalid user sjobeck from 10.10.1.16 port 39157 ssh2
Aug 18 23:08:42 comptia sshd[5776]: Failed password for root from 18.70.0.160 port 39467 ssh2
```

Which of the following can be suspected?

a) An unauthorized user is trying to gain access from 10.10.10.192.
b) An authorized user is trying to gain access from 10.10.10.192.
c) An authorized user is trying to gain access from 18.70.0.160.
d) An unauthorized user is trying to gain access from 18.70.0.160.

Answer: d

Question: 3

The security analyst determined that an email containing a malicious attachment was sent to several employees within the company, and it was not stopped by any of the email filtering devices.

An incident was declared. During the investigation, it was determined that most users deleted the email, but one specific user executed the attachment.

Based on the details gathered, which of the following actions should the security analyst perform NEXT?

a) Obtain a copy of the email with the malicious attachment. Execute the file on another user's machine and observe the behavior. Document all findings.
b) Acquire a full backup of the affected machine. Reimage the machine and then restore from the full backup.
c) Take the affected machine off the network. Review local event logs looking for activity and processes related to unknown or unauthorized software.
d) Take possession of the machine. Apply the latest OS updates and firmware. Discuss the problem with the user and return the machine.

Answer: c

Question: 4

Which of the following is the main benefit of sharing incident details with partner organizations or external trusted parties during the incident response process?

a) It facilitates releasing incident results, findings and resolution to the media and all appropriate government agencies
b) It shortens the incident life cycle by allowing others to document incident details and prepare reports.
c) It enhances the response process, as others may be able to recognize the observed behavior and provide valuable insight.
d) It allows the security analyst to defer incident-handling activities until all parties agree on how to proceed with analysis.

Answer: c

Question: 5

A security analyst has been asked to review permissions on accounts within Active Directory to determine if they are appropriate to the user's role.
During this process, the analyst notices that a user from building maintenance is part of the Domain Admin group.
Which of the following does this indicate?

a) Cross-site scripting
b) Session hijack
c) Privilege escalation
d) Rootkit

Answer: c

Question: 6

In the last six months, a company is seeing an increase in credential-harvesting attacks. The latest victim was the chief executive officer (CEO).

Which of the following countermeasures will render the attack ineffective?

a) Use a complex password according to the company policy.
b) Implement an intrusion-prevention system.
c) Isolate the CEO's computer in a higher security zone.
d) Implement multifactor authentication.

Answer: d

Question: 7

A security analyst wants to capture data flowing in and out of a network. Which of the following would MOST likely assist in achieving this goal?

a) Taking a screenshot.
b) Analyzing network traffic and logs.
c) Analyzing big data metadata.
d) Capturing system image.

Answer: b

Question: 8

After a security breach, it was discovered that the attacker had gained access to the network by using a brute-force attack against a service account with a password that was set to not expire, even though the account had a long, complex password.

Which of the following could be used to prevent similar attacks from being successful in the future?

a) Complex password policies
b) Account lockout
c) Self-service password reset portal
d) Scheduled vulnerability scans

Answer: b

Question: 9

Which of the following tools should a cybersecurity analyst use to verify the integrity of a forensic image before and after an investigation?

a) strings
b) sha1sum
c) file
d) dd
e) gzip

Answer: b

Question: 10

There are reports that hackers are using home thermostats to ping a national service provider without the provider's knowledge.

Which of the following attacks is occurring from these devices?

a) IoT
b) DDoS
c) MITM
d) MIMO

Answer: b

Study Guide to Crack CompTIA CySA Plus CS0-002 Exam:

- Getting details of the CS0-002 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CS0-002 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the CompTIA provided training for CS0-002 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CS0-002 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CS0-002 practice tests is must. Continuous practice will make you an expert in all syllabus areas.