EDUSUM

#1 Online Certification Guide

COMPTIA CS0-003

CompTIA CySA+ Certification Questions & Answers

Exam Summary – Syllabus –Questions

CS0-003

CompTIA Cybersecurity Analyst (CySA+)

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

Table of Contents:

Know Your CS0-003 Certification Well:.....2

CompTIA CS0-003 CySA+ Certification Details:.....2

CS0-003 Syllabus:.....3

Security Operations - 33% 3

Vulnerability Management - 30% 8

Incident Response and Management - 20%.....13

Reporting and Communication - 17% 14

CompTIA CS0-003 Sample Questions:.....16

Study Guide to Crack CompTIA CySA+ CS0-003 Exam: 20

Know Your CS0-003 Certification Well:

The CS0-003 is best suitable for candidates who want to gain knowledge in the CompTIA Cybersecurity. Before you start your CS0-003 preparation you may struggle to get all the crucial CySA+ materials like CS0-003 syllabus, sample questions, study guide.

But don't worry the CS0-003 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 CS0-003 syllabus?
- How many questions are there in the CS0-003 exam?
- Which Practice test would help me to pass the CS0-003 exam at the first attempt?

Passing the CS0-003 exam makes you CompTIA Cybersecurity Analyst (CySA+). Having the CySA+ 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 CS0-003 CySA+ Certification Details:

Exam Name	CompTIA Cybersecurity Analyst (CySA+)
Exam Code	CS0-003
Exam Price	$392 (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	**Pearson VUE**
Sample Questions	**CompTIA CySA+ Sample Questions**
Practice Exam	**CompTIA CS0-003 Certification Practice Exam**

CS0-003 Syllabus:

Topic	Details
Security Operations - 33%	
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

Topic	Details
	• 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)
Given a scenario, analyze indicators of potentially malicious activity.	- Network-related • Bandwidth consumption • Beaconing • 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 • Unauthorized software • Malicious processes • Unauthorized changes • Unauthorized privileges • Data exfiltration • Abnormal OS process behavior • File system changes or anomalies

Topic	Details
	• Registry changes or anomalies • Unauthorized scheduled tasks - Application-related • Anomalous activity • Introduction of new accounts • Unexpected output • Unexpected outbound communication • Service interruption • Application logs - Other • Social engineering attacks • Obfuscated links
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

Topic	Details
	- 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) - Sender Policy Framework (SPF) - Embedded links • File analysis - Hashing • User behavior analysis - Abnormal account activity - Impossible travel - Programming languages/scripting • JavaScript Object Notation (JSON) • Extensible Markup Language (XML) • Python • PowerShell • Shell script • Regular expressions
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

Topic	Details
	• 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

Topic	Details
	• Active defense • Honeypot
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
Vulnerability Management - 30%	
Given a scenario, implement vulnerability scanning methods and concepts.	- Asset discovery • Map scans • Device fingerprinting - Special considerations • Scheduling • Operations • Performance • Sensitivity levels

Topic	Details
	• 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
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

Topic	Details
	- OpenVAS • Debuggers - Immunity debugger - GNU debugger (GDB) • Multipurpose - Nmap - Metasploit framework (MSF) - Recon-ng • Cloud infrastructure assessment tools - Scout Suite - Prowler - Pacu
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

Topic	Details
	- Zero-day
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)
Explain concepts related to vulnerability response, handling, and management.	- Compensating control - Control types • Managerial • Operational • Technical • Preventative • Detective • Responsive • Corrective

Topic	Details
	- 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)

Topic	Details
	- Threat modeling
Incident Response and Management - 20%	
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
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 - Scope - Impact - Isolation - Remediation - Re-imaging - Compensating controls - Containment, eradication, and recovery
Explain the preparation and post-incident activity phases of the incident management life cycle.	- Preparation • Incident response plan • Tools • Playbooks • Tabletop • Training • Business continuity (BC)/disaster recovery (DR) - Post-incident activity

Topic	Details
	• Forensic analysis • Root cause analysis • Lessons learned
Reporting and Communication - 17%	
Explain the importance of vulnerability management reporting and communication.	- Vulnerability management reporting • Vulnerabilities • Affected hosts • Risk score • Mitigation • Recurrence • Prioritization - Compliance 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

Topic	Details
	• Critical vulnerabilities and zero-days • SLOs - Stakeholder identification and communication
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 CS0-003 Sample Questions:

Question: 1

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: 2

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: 3

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

Answer: a

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

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

Question: 6

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: 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

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: 9

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: 10

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) Rootkit
d) Privilege escalation

Answer: d

Study Guide to Crack CompTIA CySA+ CS0-003 Exam:

- Getting details of the CS0-003 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 CS0-003 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 CS0-003 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 CS0-003 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 CS0-003 practice tests is must. Continuous practice will make you an expert in all syllabus areas.