EDUSUM

#1 Online Certification Guide

CS0-001

CySA+

A Success Guide to Prepare-
CompTIA Cybersecurity Analyst

edusum.com

Table of Contents

Introduction to CS0-001 Exam on CompTIA Cybersecurity Analyst

Use this quick start guide to collect all the information about CompTIA CySA+ (CS0-001) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the CS0-001 CompTIA Cybersecurity Analyst exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual CompTIA CySA Plus certification exam.

The CompTIA CySA+ certification is mainly targeted to those candidates who want to build their career in IT Security domain. The CompTIA Cybersecurity Analyst (CySA+) exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of CompTIA CySA Plus.

CompTIA CS0-001 Certification Details:

Exam Name	CompTIA Cybersecurity Analyst (CySA+)
Exam Code	CS0-001
Exam Price	$346 (USD)
Duration	165 min
Number of Questions	85
Passing Score	750 / 900
Books / Training	CompTIA CertMaster for CSA+
Schedule Exam	CompTIA Marketplace
Sample Questions	CompTIA CySA+ Sample Questions
Practice Exam	**CompTIA CS0-001 Certification Practice Exam**

CompTIA CS0-001 Exam Syllabus:

Topic	Details
Threat Management 27%	
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes.	1. Procedures/common tasks 1. Topology discovery 2. OS fingerprinting 3. Service discovery 4. Packet capture 5. Log review 6. Router/firewall ACLs review 7. Email harvesting 8. Social media profiling 9. Social engineering 10. DNS harvesting 11. Phishing 2. Variables 1. Wireless vs. wired 2. Virtual vs. physical 3. Internal vs. external 4. On-premises vs. cloud 3. Tools 1. NMAP 2. Host scanning 3. Network mapping 4. NETSTAT 5. Packet analyzer 6. IDS/IPS 7. HIDS/NIDS 8. Firewall rule-based and logs 9. Syslog 10. Vulnerability scanner
Given a scenario, analyze the results of a network reconnaissance.	1. Point-in-time data analysis 1. Packet analysis 2. Protocol analysis 3. Traffic analysis 4. Netflow analysis 5. Wireless analysis 2. Data correlation and analytics

Topic	Details
	1. Anomaly analysis 2. Trend analysis 3. Availability analysis 4. Heuristic analysis 5. Behavioral analysis 3. Data output 1. Firewall logs 2. Packet captures 3. NMAP scan results 4. Event logs 5. Syslogs 6. IDS report 4. Tools 1. SIEM 2. Packet analyzer 3. IDS 4. Resource monitoring tool 5. Netflow analyzer
Given a network-based threat, implement or recommend the appropriate response and countermeasure.	1. Network segmentation 1. System isolation 2. Jump box 2. Honeypot 3. Endpoint security 4. Group policies 5. ACLs 1. Sinkhole 6. Hardening 1. Mandatory Access Control (MAC) 2. Compensating controls 3. Blocking unused ports/services 4. Patching 7. Network Access Control (NAC) 1. Time-based 2. Rule-based

Topic	Details
	3. Role-based 4. Location-based
Explain the purpose of practices used to secure a corporate environment.	1. Penetration testing 1. Rules of engagement 2. Timing 3. Scope 4. Authorization 5. Exploitation 6. Communication 7. Reporting 2. Reverse engineering 1. Isolation/sandboxing 2. Hardware 3. Source authenticity of hardware 4. Trusted foundry 5. OEM documentation 6. Software/malware 7. Fingerprinting/hashing 8. Decomposition 3. Training and exercises 1. Red team 2. Blue team 3. White team 4. Risk evaluation 1. Technical control review 2. Operational control review 3. Technical impact and likelihood 4. High 5. Medium 6. Low
Vulnerability Management 26%	
Given a scenario, implement an information security vulnerability management process.	1. Identification of requirements 1. Regulatory environments 2. Corporate policy 3. Data classification 4. Asset inventory 5. Critical

Topic	Details
	6. Non-critical 2. Establish scanning frequency 1. Risk appetite 2. Regulatory requirements 3. Technical constraints 4. Workflow 3. Configure tools to perform scans according to specification 1. Determine scanning criteria 2. Sensitivity levels 3. Vulnerability feed 4. Scope 5. Credentialed vs. non-credentialed 6. Types of data 7. Server-based vs. agent-based 8. Tool updates/plug-ins 9. SCAP 10. Permissions and access 4. Execute scanning 5. Generate reports 1. Automated vs. manual distribution 6. Remediation 1. Prioritizing 2. Criticality 3. Difficulty of implementation 4. Communication/change control 5. Sandboxing/testing 6. Inhibitors to remediation 7. MOUs 8. SLAs 9. Organizational governance 10. Business process interruption 11. Degrading functionality 7. Ongoing scanning and continuous monitoring
Given a scenario, analyze the output resulting from a vulnerability scan.	1. Analyze reports from a vulnerability scan 1. Review and interpret scan results 2. Identify false positives

Topic	Details
	3. Identify exceptions 4. Prioritize response actions 2. Validate results and correlate other data points 1. Compare to best practices or compliance 2. Reconcile results 3. Review related logs and/ or other data sources 4. Determine trends
Compare and contrast common vulnerabilities found in the following targets within an organization.	1. Servers 2. Endpoints 3. Network infrastructure 4. Network appliances 5. Virtual infrastructure 1. Virtual hosts 2. Virtual networks 3. Management interface 6. Mobile devices 7. Interconnected networks 8. Virtual Private Networks (VPNs) 9. Industrial Control Systems (ICSs) 10. SCADA devices
Cyber Incident Response 23%	
Given a scenario, distinguish threat data or behavior to determine the impact of an incident.	1. Threat classification 1. Known threats vs. unknown threats 2. Zero day 3. Advanced persistent threat 2. Factors contributing to incident severity and prioritization 1. Scope of impact 2. Downtime 3. Recovery time 4. Data integrity 5. Economic 6. System process criticality 7. Types of data 8. Personally Identifiable 9. Information (PII) 10. Personal Health Information (PHI) 11. Payment card information 12. Intellectual property 13. Corporate confidential

Topic	Details
	14. Accounting data 15. Mergers and acquisitions
Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation.	1. Forensics kit 1. Digital forensics workstation 2. Write blockers 3. Cables 4. Drive adapters 5. Wiped removable media 6. Cameras 7. Crime tape 8. Tamper-proof seals 9. Documentation/forms 10. Chain of custody form 11. Incident response plan 12. Incident form 13. Call list/escalation list 2. Forensic investigation suite 1. Imaging utilities 2. Analysis utilities 3. Chain of custody 4. Hashing utilities 5. OS and process analysis 6. Mobile device forensics 7. Password crackers 8. Cryptography tools 9. Log viewers
Explain the importance of communication during the incident response process.	1. Stakeholders 1. HR 2. Legal 3. Marketing 4. Management 2. Purpose of communication processes 1. Limit communication to trusted parties 2. Disclosure based on regulatory/ legislative requirements 3. Prevent inadvertent release of information 4. Secure method of communication 3. Role-based responsibilities

Topic	Details
	1. Technical 2. Management 3. Law enforcement 4. Retain incident response provider
Given a scenario, analyze common symptoms to select the best course of action to support incident response.	1. Common network-related symptoms 1. Bandwidth consumption 2. Beaconing 3. Irregular peer-to-peer communication 4. Rogue devices on the network 5. Scan sweeps 6. Unusual traffic spikes 2. Common host-related symptoms 1. Processor consumption 2. Memory consumption 3. Drive capacity consumption 4. Unauthorized software 5. Malicious processes 6. Unauthorized changes 7. Unauthorized privileges 8. Data exfiltration 3. Common application-related symptoms 1. Anomalous activity 2. Introduction of new accounts 3. Unexpected output 4. Unexpected outbound communication 5. Service interruption 6. Memory overflows
Summarize the incident recovery and post-incident response process.	1. Containment techniques 1. Segmentation 2. Isolation 3. Removal 4. Reverse engineering 2. Eradication techniques 1. Sanitization 2. Reconstruction/reimage

Topic	Details
	3. Secure disposal 3. Validation 1. Patching 2. Permissions 3. Scanning 4. Verify logging/communication to security monitoring 4. Corrective actions 1. Lessons learned report 2. Change control process 3. Update incident response plan 5. Incident summary report
Security Architecture and Tool Sets 24%	
Explain the relationship between frameworks, common policies, controls, and procedures.	1. Regulatory compliance 2. Frameworks 1. NIST 2. ISO 3. COBIT 4. SABSA 5. TOGAF 6. ITIL 3. Policies 1. Password policy 2. Acceptable use policy 3. Data ownership policy 4. Data retention policy 5. Account management policy 6. Data classification policy 4. Controls 1. Control selection based on criteria 2. Organizationally defined parameters 3. Physical controls 4. Logical controls 5. Administrative controls 5. Procedures

Topic	Details
	1. Continuous monitoring 2. Evidence production 3. Patching 4. Compensating control development 5. Control testing procedures 6. Manage exceptions 7. Remediation plans 6. Verifications and quality control 1. Audits 2. Evaluations 3. Assessments 4. Maturity model 5. Certification
Given a scenario, use data to recommend remediation of security issues related to identity and access management.	1. Security issues associated with context-based authentication 1. Time 2. Location 3. Frequency 4. Behavioral 2. Security issues associated with identities 1. Personnel 2. Endpoints 3. Servers 4. Services 5. Roles 6. Applications 3. Security issues associated with identity repositories 1. Directory services 2. TACACS+ 3. RADIUS 4. Security issues associated with federation and single sign-on 1. Manual vs. automatic provisioning/deprovisioning 2. Self-service password reset

Topic	Details
	5. Exploits 1. Impersonation 2. Man-in-the-middle 3. Session hijack 4. Cross-site scripting 5. Privilege escalation 6. Rootkit
Given a scenario, review security architecture and make recommendations to implement compensating controls.	1. Security data analytics 1. Data aggregation and correlation 2. Trend analysis 3. Historical analysis 2. Manual review 1. Firewall log 2. Syslogs 3. Authentication logs 4. Event logs 3. Defense in depth 1. Personnel 2. Training 3. Dual control 4. Separation of duties 5. Third party/consultants 6. Cross training 7. Mandatory vacation 8. Succession planning 9. Processes 10. Continual improvement 11. Scheduled reviews 12. Retirement of processes 13. Technologies 14. Automated reporting 15. Security appliances 16. Security suites 17. Outsourcing 18. Security as a Service 19. Cryptography 20. Other security concepts 21. Network design 22. Network segmentation

Topic	Details
Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC).	1. Best practices during software development 1. Security requirements definition 2. Security testing phases 3. Static code analysis 4. Web app vulnerability scanning 5. Fuzzing 6. Use interception proxy to crawl application 7. Manual peer reviews 8. User acceptance testing 9. Stress test application 10. Security regression testing 11. Input validation 2. Secure coding best practices 1. OWASP 2. SANS 3. Center for Internet Security 4. System design recommendations 5. Benchmarks
Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.	1. Preventative 1. IPS 2. Sourcefire 3. Snort 4. Bro 5. HIPS 6. Firewall 7. Cisco 8. Palo Alto 9. Check Point 10. Antivirus 11. Anti-malware 12. EMET 13. Web proxy 14. Web Application Firewall (WAF) 15. ModSecurity 16. NAXSI 17. Imperva 2. Collective 1. SIEM 2. ArcSight 3. QRadar 4. Splunk

Topic	Details
	5. AlienVault 6. OSSIM 7. Kiwi Syslog 8. Network scanning 9. NMAP 10. Vulnerability scanning 11. Qualys 12. Nessus 13. OpenVAS 14. Nexpose 15. Nikto 16. Microsoft Baseline Security Analyzer 17. Packet capture 18. Wireshark 19. tcpdump 20. Network General 21. Aircrack-ng 22. Command line/IP utilities 23. netstat 24. ping 25. tracert/traceroute 26. ipconfig/ifconfig 27. nslookup/dig 28. Sysinternals 29. OpenSSL 30. IDS/HIDS 31. Bro 3. Analytical 1. Vulnerability scanning 2. Qualys 3. Nessus 4. OpenVAS 5. Nexpose 6. Nikto 7. Microsoft Baseline Security Analyzer 8. Monitoring tools 9. MRTG 10. Nagios 11. SolarWinds 12. Cacti 13. NetFlow Analyzer 14. Interception proxy 15. Burp Suite 16. Zap 17. Vega

Topic	Details
	4. Exploit 1. Interception proxy 2. Burp Suite 3. Zap 4. Vega 5. Exploit framework 6. Metasploit 7. Nexpose 8. Fuzzers 9. Untidy 10. Peach Fuzzer 11. Microsoft SDL File/Regex Fuzzer 5. Forensics 1. Forensic suites 2. EnCase 3. FTK 4. Helix 5. Sysinternals 6. Cellebrite 7. Hashing 8. MD5sum 9. SHAsum 10. Password cracking 11. John the Ripper 12. Cain & Abel 13. Imaging 14. DD

CS0-001 Sample Questions:

01. During a Fagan code inspection, which process can redirect to the planning stage?
a) Overview
b) Preparation
c) Meeting
d) Rework

02. Who is the best facilitator for a post-incident lessons-learned session?
a) CEO
b) CSIRT leader
c) Independent facilitator
d) First responder

03. A cross-site scripting attack is an example of what type of threat vector?
a) Impersonation
b) Email
c) Attrition
d) Web

04. Which of the following is a switch attack?
a) MAC overflow
b) XSS
c) CSRF
d) Inference

05. Susan has been asked to identify the applications that start when a Windows system does. Where should she look first?
a) INDX files
b) Volume shadow copies
c) The Registry
d) The MFT

06. What organization manages the global IP address space?
a) NASA
b) ARIN
c) WorldNIC
d) IANA

07. How many phases does the Spiral model cycle through?
a) Three
b) Four
c) Five
d) Six

08. Which one of the following is an example of a computer security incident?
a) User accesses a secure file
b) Administrator changes a file's permission settings
c) Intruder breaks into a building
d) Former employee crashes a server

09. Using the Agile sprint process, what step will occur at step 2 in the previous graphic?
a) Development
b) Design
c) Testing
d) Gathering user stories

10. The Dirty COW attack is an example of what type of vulnerability?
a) Malicious code
b) Privilege escalation
c) Buffer overflow
d) LDAP injection

Answers to CS0-001 Exam Questions:

Question: 01 Answer: d	Question: 02 Answer: c	Question: 03 Answer: d	Question: 04 Answer: a	Question: 05 Answer: c
Question: 06 Answer: d	Question: 07 Answer: b	Question: 08 Answer: d	Question: 09 Answer: a	Question: 10 Answer: b

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@edusum.com