CompTIA

Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam

NEW QUESTION 1
An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC.
Which of the following is the BEST approach for supply chain assessment when selecting a vendor?

A. Gather information from providers, including datacenter specifications and copies of audit reports.
B. Identify SLA requirements for monitoring and logging.
C. Consult with senior management for recommendations.
D. Perform a proof of concept to identify possible solutions.

Answer: B

NEW QUESTION 2
A cybersecurity analyst is reading a daily intelligence digest of new vulnerabilities The type of vulnerability that should be disseminated FIRST is one that:

A. enables remote code execution that is being exploited in the wild.
B. enables data leakage but is not known to be m the environment
C. enables lateral movement and was reported as a proof of concept
D. affected the organization in the past but was probably contained and eradicated

Answer: C

NEW QUESTION 3
Which of the following should be found within an organization's acceptable use policy?

A. Passwords must be eight characters in length and contain at least one special character.
B. Customer data must be handled properly, stored on company servers, and encrypted when possible
C. Administrator accounts must be audited monthly, and inactive accounts should be removed.
D. Consequences of violating the policy could include discipline up to and including termination.

Answer: D

NEW QUESTION 4
A security administrator needs to create an IDS rule to alert on FTP login attempts by root. Which of the following rules is the BEST solution?

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 5
A security analyst has been alerted to several emails that snow evidence an employee is planning malicious activities that involve employee PII on the network before leaving the organization. The security analysis BEST response would be to coordinate with the legal department and:

A. the public relations department
B. senior leadership
C. law enforcement
D. the human resources department

Answer: D

NEW QUESTION 6
Which of the following BEST articulates the benefit of leveraging SCAP in an organization’s cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes to enterprise security services
B. It enables standard checklist and vulnerability analysis expressions for automation
C. It establishes a continuous integration environment for software development operations
D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 7
A security analyst discovered a specific series of IP addresses that are targeting an organization. None of the attacks have been successful. Which of the following should the security analyst perform NEXT?

A. Begin blocking all IP addresses within that subnet.
B. Determine the attack vector and total attack surface.
C. Begin a kill chain analysis to determine the impact.
D. Conduct threat research on the IP addresses

Answer: D

NEW QUESTION 8
During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.

Which of the following commands should the analyst investigate FIRST?

A. Line 1
B. Line 2
C. Line 3
D. Line 4
E. Line 5
F. Line 6

Answer: B

NEW QUESTION 9
Which of the following software assessment methods would be BEST for gathering data related to an application's availability during peak times?

A. Security regression testing
B. Stress testing
C. Static analysis testing
D. Dynamic analysis testing
E. User acceptance testing

Answer: B

NEW QUESTION 10
An organization developed a comprehensive incident response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

A. A simulated breach scenario involving the incident response team
B. Completion of annual information security awareness training by all employees
C. Tabletop activities involving business continuity team members
D. Completion of lessons-learned documentation by the computer security incident response team
E. External and internal penetration testing by a third party

Answer: A

NEW QUESTION 10
It is important to parameterize queries to prevent:

A. the execution of unauthorized actions against a database.
B. a memory overflow that executes code with elevated privileges.
C. the establishment of a web shell that would allow unauthorized access.
D. the queries from using an outdated library with security vulnerabilities.

Answer: A

NEW QUESTION 11
A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?

A. Motion detection
B. Perimeter fencing
C. Monitored security cameras
D. Badged entry

Answer: A

NEW QUESTION 15
An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:

Which of the following should be the focus of the investigation?

A. webserver.org-dmz.org
B. sftp.org-dmz.org
C. 83hht23.org-int.org
D. ftps.bluemed.net

Answer: A

NEW QUESTION 20
A security analyst is reviewing the following log from an email security service.

Which of the following BEST describes the reason why the email was blocked?

A. The To address is invalid.
B. The email originated from the www.spamfilter.org URL.
C. The IP address and the remote server name are the same.
D. The IP address was blacklisted.
E. The From address is invalid.

Answer: D

NEW QUESTION 25
A web-based front end for a business intelligence application uses pass-through authentication to authenticate users The application then uses a service account, to perform queries and look up data m a database A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

A. Change the security model to force the users to access the database as themselves
B. Parameterize queries to prevent unauthorized SQL queries against the database
C. Configure database security logging using syslog or a SIEM
D. Enforce unique session IDs so users do not get a reused session ID

Answer: B

NEW QUESTION 28
Which of the following technologies can be used to house the entropy keys for disk encryption on desktops and laptops?

A. Self-encrypting drive
B. Bus encryption
C. TPM
D. HSM

Answer: A

NEW QUESTION 30
A company's Chief Information Security Officer (CISO) is concerned about the integrity of some highly confidential files. Any changes to these files must be tied back to a specific authorized user's activity session. Which of the following is the BEST technique to address the CISO's concerns?

A. Configure DLP to reject all changes to the files without pre-authorizatio
B. Monitor the files for unauthorized changes.
C. Regularly use SHA-256 to hash the directory containing the sensitive informatio
D. Monitor the files for unauthorized changes.
E. Place a legal hold on the file
F. Require authorized users to abide by a strict time context access policy.Monitor the files for unauthorized changes.
G. Use Wireshark to scan all traffic to and from the director
H. Monitor the files for unauthorized changes.

Answer: A

NEW QUESTION 31
A security team wants to make SaaS solutions accessible from only the corporate campus.
Which of the following would BEST accomplish this goal?

A. Geofencing
B. IP restrictions
C. Reverse proxy
D. Single sign-on

Answer: A

NEW QUESTION 34
A hybrid control is one that:

A. is implemented differently on individual systems
B. is implemented at the enterprise and system levels
C. has operational and technical components
D. authenticates using passwords and hardware tokens

Answer: B

NEW QUESTION 35
Ransomware is identified on a company's network that affects both Windows and MAC hosts. The command and control channel for encryption for this variant uses TCP ports from 11000 to 65000. The channel goes to good1. Iholdbadkeys.com, which resolves to IP address 72.172.16.2.
Which of the following is the MOST effective way to prevent any newly infected systems from actually encrypting the data on connected network drives while causing the least disruption to normal Internet traffic?

A. Block all outbound traffic to web host good1 iholdbadkeys.com at the border gateway.
B. Block all outbound TCP connections to IP host address 172.172.16.2 at the border gateway.
C. Block all outbound traffic on TCP ports 11000 to 65000 at the border gateway.
D. Block all outbound traffic on TCP ports 11000 to 65000 to IP host address 172.172.16.2 at the border gateway.

Answer: A

NEW QUESTION 39
A security analyst is reviewing the following log entries to identify anomalous activity:
Which of the following attack types is occurring?

A. Directory traversal
B. SQL injection
C. Buffer overflow
D. Cross-site scripting

Answer: A

NEW QUESTION 40
A security analyst at a technology solutions firm has uncovered the same vulnerabilities on a vulnerability scan for a long period of time. The vulnerabilities are on systems that are dedicated to the firm's largest client. Which of the following is MOST likely inhibiting the remediation efforts?

A. The parties have an MOU between them that could prevent shutting down the systems
B. There is a potential disruption of the vendor-client relationship
C. Patches for the vulnerabilities have not been fully tested by the software vendor
D. There is an SLA with the client that allows very little downtime

Answer: D

NEW QUESTION 43
An information security analyst observes anomalous behavior on the SCADA devices in a power plant. This behavior results in the industrial generators overheating and destabilizing the power supply.
Which of the following would BEST identify potential indicators of compromise?

A. Use Burp Suite to capture packets to the SCADA device's IP.
B. Use tcpdump to capture packets from the SCADA device IP.
C. Use Wireshark to capture packets between SCADA devices and the management system.
D. Use Nmap to capture packets from the management system to the SCADA devices.

Answer: C

NEW QUESTION 45
A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions. The team plans to use the names and mailing addresses that users have provided.
Which of the following data privacy standards does this violate?

A. Purpose limitation
B. Sovereignty
C. Data minimization
D. Retention

Answer: A

NEW QUESTION 50
An analyst identifies multiple instances of node-to-node communication between several endpoints within the 10.200.2.0/24 network and a user machine at the IP address 10.200.2.5. This user machine at the IP address 10.200.2.5 is also identified as initiating outbound communication during atypical business hours with several IP addresses that have recently appeared on threat feeds.
Which of the following can be inferred from this activity?

A. 10.200.2.0/24 is infected with ransomware.
B. 10.200.2.0/24 is not routable address space.
C. 10.200.2.5 is a rogue endpoint.
D. 10.200.2.5 is exfiltrating data.

Answer: D

NEW QUESTION 52
A large software company wants to move «s source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

A. Establish an alternate site with active replication to other regions
B. Configure a duplicate environment in the same region and load balance between both instances
C. Set up every cloud component with duplicated copies and auto scaling turned on
D. Create a duplicate copy on premises that can be used for failover in a disaster situation

Answer: A

NEW QUESTION 56
A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization.
Which of the following BEST describes the security analyst's goal?

A. To create a system baseline
B. To reduce the attack surface
C. To optimize system performance
D. To improve malware detection

Answer: B

NEW QUESTION 61
An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?

A. Tokenization of sensitive data
B. Establishment o' data classifications
C. Reporting on data retention and purging activities
D. Formal identification of data ownership
E. Execution of NDAs

Answer: A

NEW QUESTION 62
A security analyst is reviewing the following web server log:

Which of the following BEST describes the issue?

A. Directory traversal exploit
B. Cross-site scripting
C. SQL injection

D. Cross-site request forgery

Answer: A

NEW QUESTION 63
The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:

A. web servers on private networks
B. HVAC control systems
C. smartphones
D. firewalls and UTM devices

Answer: D

NEW QUESTION 64
An organization needs to limit its exposure to accidental disclosure when employees send emails that contain personal information to recipients outside the company Which of the following technical controls would BEST accomplish this goal?

A. DLP
B. Encryption
C. Data masking
D. SPF

Answer: A

NEW QUESTION 68
As part of a review of modern response plans, which of the following is MOST important for an organization lo understand when establishing the breach notification period?

A. Organizational policies
B. Vendor requirements and contracts
C. Service-level agreements
D. Legal requirements

Answer: D

NEW QUESTION 72
An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?

A. Root-cause analysis
B. Active response
C. Advanced antivirus
D. Information-sharing community
E. Threat hunting

Answer: E

NEW QUESTION 76
A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integration intelligence into hunt operations?

A. It enables the team to prioritize the focus area and tactics within the company's environment.
B. It provide critically analyses for key enterprise servers and services.
C. It allow analysis to receive updates on newly discovered software vulnerabilities.
D. It supports rapid response and recovery during and followed an incident.

Answer: A

NEW QUESTION 77
A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet.
Which of the following solutions would meet this requirement?

A. Establish a hosted SSO.
B. Implement a CASB.
C. Virtualize the server.
D. Air gap the server.

Answer: D

NEW QUESTION 81
A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security To BEST complete this task, the analyst should place the:

A. firewall behind the VPN server

B. VPN server parallel to the firewall
C. VPN server behind the firewall
D. VPN on the firewall

Answer: B

NEW QUESTION 82
While preparing of an audit of information security controls in the environment an analyst outlines a framework control that has the following requirements:
• All sensitive data must be classified
• All sensitive data must be purged on a quarterly basis
• Certificates of disposal must remain on file for at least three years
This framework control is MOST likely classified as:

A. prescriptive
B. risk-based
C. preventive
D. corrective

Answer: A

NEW QUESTION 83
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue. INSTRUCTIONS
Click on me ticket to see the ticket details Additional content is available on tabs within the ticket
First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 86
A security analyst is investigating a system compromise. The analyst verities the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely expiated?

A. Insider threat
B. Buffer overflow
C. Advanced persistent threat
D. Zero day

Answer: D

NEW QUESTION 91
A finance department employee has received a message that appears to have been sent from the Chief Financial Officer (CFO) asking the employee to perform a wife transfer Analysis of the email shows the message came from an external source and is fraudulent. Which of the following would work BEST to improve the likelihood of employees quickly recognizing fraudulent emails?

A. Implementing a sandboxing solution for viewing emails and attachments
B. Limiting email from the finance department to recipients on a pre-approved whitelist
C. Configuring email client settings to display all messages in plaintext when read
D. Adding a banner to incoming messages that identifies the messages as external

Answer: D

NEW QUESTION 95
An analyst is performing penetration testing and vulnerability assessment activities against a new vehicle automation platform.
Which of the following is MOST likely an attack vector that is being utilized as part of the testing and assessment?

A. FaaS
B. RTOS
C. SoC
D. GPS
E. CAN bus

Answer: E

NEW QUESTION 98
After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:

Which of the following IP addresses does the analyst need to investigate further?

A. 192.168.1.1
B. 192.168.1.10
C. 192.168.1.12
D. 192.168.1.193

Answer: C

NEW QUESTION 100
A cybersecurity analyst is responding to an incident. The company's leadership team wants to attribute the incident to an attack group. Which of the following models would BEST apply to the situation?

A. Intelligence cycle
B. Diamond Model of Intrusion Analysis
C. Kill chain
D. MITRE ATT&CK

Answer: B

NEW QUESTION 101
An organization has not had an incident for several month. The Chief information Security Officer (CISO) wants to move to proactive stance for security investigations. Which of the following would BEST meet that goal?

A. Root-cause analysis
B. Active response
C. Advanced antivirus
D. Information-sharing community
E. Threat hunting

Answer: E

NEW QUESTION 105
Which of me following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes lo enterprise security services
B. It enables standard checklist and vulnerability analysis expressions for automaton
C. It establishes a continuous integration environment for software development operations
D. It provides validation of suspected system vulnerabilities through workflow orchestration

Answer: B

NEW QUESTION 107
A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the

attachment to a Linux sandbox for review.
Which of the following commands would MOST likely indicate if the email is malicious?

A. sha256sum ~/Desktop/file.pdf
B. file ~/Desktop/file.pdf
C. strings ~/Desktop/file.pdf | grep "<script"
D. cat < ~/Desktop/file.pdf | grep -i .exe

Answer: A

NEW QUESTION 112
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage The security analyst is trying to determine which user caused the malware to get onto the system Which of the following registry keys would MOST likely have this information?
A)

B)

C)

D)

A. Option A
B. Option B
C. Option C
D. Option D

Answer: C

NEW QUESTION 115
Which of the following policies would slate an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

A. Code of conduct policy
B. Account management policy
C. Password policy
D. Acceptable use policy

Answer: D

NEW QUESTION 118
While analyzing logs from a WAF, a cybersecurity analyst finds the following:

Which of the following BEST describes what the analyst has found?

A. This is an encrypted GET HTTP request
B. A packet is being used to bypass the WAF
C. This is an encrypted packet
D. This is an encoded WAF bypass

Answer: D

NEW QUESTION 122
Risk management wants IT to implement a solution that will permit an analyst to intercept, execute, and analyze potentially malicious files that are downloaded from the Internet.

Which of the following would BEST provide this solution?

A. File fingerprinting
B. Decomposition of malware
C. Risk evaluation
D. Sandboxing

Answer: D

NEW QUESTION 127
A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?

A. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
B. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
C. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
D. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.

Answer: D

NEW QUESTION 130
A new on-premises application server was recently installed on the network. Remote access to the server was enabled for vendor support on required ports, but recent security reports show large amounts of data are being sent to various unauthorized networks through those ports. Which of the following configuration changes must be implemented to resolve this security issue while still allowing remote vendor access?

A. Apply a firewall application server rule.
B. Whitelist the application server.
C. Sandbox the application server.
D. Enable port security.
E. Block the unauthorized networks.

Answer: B

NEW QUESTION 133
An information security analyst is compiling data from a recent penetration test and reviews the following output:

The analyst wants to obtain more information about the web-based services that are running on the target. Which of the following commands would MOST likely provide the needed information?

A. ping -t 10.79.95.173.rdns.datacenters.com
B. telnet 10.79.95.173 443
C. ftpd 10.79.95.173.rdns.datacenters.com 443
D. tracert 10.79.95.173

Answer: B

NEW QUESTION 138
When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

A. nmap –sA –O <system> -noping
B. nmap –sT –O <system> -P0
C. nmap –sS –O <system> -P0
D. nmap –sQ –O <system> -P0

Answer: C

NEW QUESTION 141
An analyst performs a routine scan of a host using Nmap and receives the following output:

Which of the following should the analyst investigate FIRST?

A. Port 21
B. Port 22
C. Port 23
D. Port 80

Answer: C

NEW QUESTION 146
A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?

A. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
B. Incorporate prioritization levels into the remediation process and address critical findings first.
C. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.

D. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities found.

Answer: B

NEW QUESTION 150
A large amount of confidential data was leaked during a recent security breach. As part of a forensic investigation, the security team needs to identify the various types of traffic that were captured between two
compromised devices.
Which of the following should be used to identify the traffic?

A. Carving
B. Disk imaging
C. Packet analysis
D. Memory dump
E. Hashing

Answer: C

NEW QUESTION 154
Which of the following would a security engineer recommend to BEST protect sensitive system data from being accessed on mobile devices?

A. Use a UEFl boot password.
B. Implement a self-encrypted disk.
C. Configure filesystem encryption
D. Enable Secure Boot using TPM

Answer: A

NEW QUESTION 159
A security architect is reviewing the options for performing input validation on incoming web form submissions. Which of the following should the architect as the MOST secure and manageable option?

A. Client-side whitelisting
B. Server-side whitelisting
C. Server-side blacklisting
D. Client-side blacklisting

Answer: B

NEW QUESTION 164
A security analyst is evaluating two vulnerability management tools for possible use in an organization. The analyst set up each of the tools according to the respective vendor's instructions and generated a report of vulnerabilities that ran against the same target server.
Tool A reported the following:

Tool B reported the following:

Which of the following BEST describes the method used by each tool? (Choose two.)

A. Tool A is agent based.
B. Tool A used fuzzing logic to test vulnerabilities.
C. Tool A is unauthenticated.
D. Tool B utilized machine learning technology.
E. Tool B is agent based.
F. Tool B is unauthenticated.

Answer: CE

NEW QUESTION 166
A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame.
Which of the following is the MOST likely cause of this issue?

A. A password-spraying attack was performed against the organization.
B. A DDoS attack was performed against the organization.
C. This was normal shift work activity; the SIEM's AI is learning.
D. A credentialed external vulnerability scan was performed.

Answer: A

NEW QUESTION 170
A security analyst implemented a solution that would analyze the attacks that the organization’s firewalls failed to prevent. The analyst used the existing systems to enact the solution and executed the following command.
S sudo nc -1 -v -c maildemon . py 25 caplog, txt
Which of the following solutions did the analyst implement?

A. Log collector

B. Crontab mail script
C. Snikhole
D. Honeypot

Answer: A

NEW QUESTION 171
While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security.
To provide the MOST secure access model in this scenario, the jumpbox should be.

A. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.
B. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
C. bridged between the IT and operational technology networks to allow authenticated access.
D. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.

Answer: D

NEW QUESTION 172
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CS0-002 Practice Exam Features:

* CS0-002 Questions and Answers Updated Frequently

* CS0-002 Practice Questions Verified by Expert Senior Certified Staff

* CS0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CS0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year