

# CompTIA

## Exam Questions CS0-002

CompTIA Cybersecurity Analyst (CySA+) Certification Exam



#### NEW QUESTION 1

Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?

- A. Human resources
- B. Public relations
- C. Marketing
- D. Internal network operations center

**Answer: B**

#### NEW QUESTION 2

A cybersecurity analyst is supposing an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?

- A. Requirements analysis and collection planning
- B. Containment and eradication
- C. Recovery and post-incident review
- D. Indicator enrichment and research pivoting

**Answer: D**

#### NEW QUESTION 3

A security analyst needs to reduce the overall attack surface. Which of the following infrastructure changes should the analyst recommend?

- A. Implement a honeypot.
- B. Air gap sensitive systems.
- C. Increase the network segmentation.
- D. Implement a cloud-based architecture.

**Answer: C**

#### NEW QUESTION 4

A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentiality protection. Which of the following is the BEST technical security control to mitigate this risk?

- A. Switch to RADIUS technology
- B. Switch to TACACS+ technology.
- C. Switch to 802.1X technology
- D. Switch to the WPA2 protocol.

**Answer: B**

#### NEW QUESTION 5

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 6

During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and.

- A. DST 138.10.2.5.
- B. DST 138.10.25.5.
- C. DST 172.10.3.5.
- D. DST 172.10.45.5.
- E. DST 175.35.20.5.

**Answer: A**

#### NEW QUESTION 7

Which of the following BEST describes the process by which code is developed, tested, and deployed in small batches?

- A. Agile
- B. Waterfall
- C. SDLC
- D. Dynamic code analysis

**Answer:**

A

**NEW QUESTION 8**

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: B**

**NEW QUESTION 9**

An organization developed a comprehensive modern 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 evolving 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**

A security analyst has been alerted to several emails that show 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 10**

A security manager has asked an analyst to provide feedback on the results of a penetration test. After reviewing the results the manager requests information regarding the possible exploitation of vulnerabilities Much of the following information data points would be MOST useful for the analyst to provide to the security manager who would then communicate the risk factors to senior management? (Select TWO)

- A. Probability
- B. Adversary capability
- C. Attack vector
- D. Impact
- E. Classification
- F. Indicators of compromise

**Answer: AD**

**NEW QUESTION 15**

Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?

- A. Secure email
- B. Encrypted USB drives
- C. Cloud containers
- D. Network folders

**Answer: B**

**NEW QUESTION 19**

A web developer wants to create a new web part within the company website that aggregates sales from individual team sites. A cybersecurity analyst wants to ensure security measurements are implemented during this process. Which of the following remediation actions should the analyst take to implement a vulnerability management process?

- A. Personnel training
- B. Vulnerability scan
- C. Change management
- D. Sandboxing

**Answer: C**

**NEW QUESTION 23**

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 28**

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 32**

Which of the following MOST accurately describes an HSM?

- A. An HSM is a low-cost solution for encryption.
- B. An HSM can be networked based or a removable USB
- C. An HSM is slower at encrypting than software
- D. An HSM is explicitly used for MFA

**Answer: A**

#### **NEW QUESTION 35**

A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT. Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?

- A. Attack vectors
- B. Adversary capability
- C. Diamond Model of Intrusion Analysis
- D. Kill chain
- E. Total attack surface

**Answer: B**

#### **NEW QUESTION 39**

A development team uses open-source software and follows an Agile methodology with two-week sprints. Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server. Which of the following should be done to correct the cause of the vulnerability?

- A. Deploy a WAF in front of the application.
- B. Implement a software repository management tool.
- C. Install a HIPS on the server.
- D. Instruct the developers to use input validation in the code.

**Answer: B**

#### **NEW QUESTION 43**

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 45**

A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server. Which of the following is the FIRST step the analyst should take?

- A. Create a full disk image of the server's hard drive to look for the file containing the malware.
- B. Run a manual antivirus scan on the machine to look for known malicious software.
- C. Take a memory snapshot of the machine to capture volatile information stored in memory.
- D. Start packet capturing to look for traffic that could be indicative of command and control from the miner.

**Answer: D**

#### NEW QUESTION 50

A compliance officer of a large organization has reviewed the firm's vendor management program but has discovered there are no controls defined to evaluate third-party risk or hardware source authenticity. The compliance officer wants to gain some level of assurance on a recurring basis regarding the implementation of controls by third parties.

Which of the following would BEST satisfy the objectives defined by the compliance officer? (Choose two.)

- A. Executing vendor compliance assessments against the organization's security controls
- B. Executing NDAs prior to sharing critical data with third parties
- C. Soliciting third-party audit reports on an annual basis
- D. Maintaining and reviewing the organizational risk assessment on a quarterly basis
- E. Completing a business impact assessment for all critical service providers
- F. Utilizing DLP capabilities at both the endpoint and perimeter levels

**Answer:** AC

#### NEW QUESTION 51

A security analyst is attempting to utilize the blowing threat intelligence for developing detection capabilities:

In which of the following phases is this APT MOST likely to leave discoverable artifacts?

- A. Data collection/exfiltration
- B. Defensive evasion
- C. Lateral movement
- D. Reconnaissance

**Answer:** A

#### NEW QUESTION 53

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 in 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 54

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer data. Developers use personal workstations, giving the company little to no visibility into the development activities.

Which of the following would be BEST to implement to alleviate the CISO's concern?

- A. DLP
- B. Encryption
- C. Test data
- D. NDA

**Answer:** D

#### NEW QUESTION 55

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 58

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 60

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 65

An organization that handles sensitive financial information wants to perform tokenization of data to enable the execution of recurring transactions. The organization is most interested in a secure, built-in device to support its solution. Which of the following would MOST likely be required to perform the desired function?

- A. TPM
- B. eFuse
- C. FPGA
- D. HSM
- E. UEFI

**Answer: D**

#### NEW QUESTION 67

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 72

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 76**

As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?

- A. Critical asset list
- B. Threat vector
- C. Attack profile
- D. Hypothesis

**Answer: A**

**NEW QUESTION 79**

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 81**

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 of data classifications
- C. Reporting on data retention and purging activities
- D. Formal identification of data ownership
- E. Execution of NDAs

**Answer: A**

**NEW QUESTION 82**

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 84**

For machine learning to be applied effectively toward security analysis automation, it requires.

- A. relevant training data.
- B. a threat feed API.
- C. a multicore, multiprocessor system.
- D. anomalous traffic signatures.

**Answer: A**

**NEW QUESTION 89**

A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com. Below is the existing SPF record:

Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?

- A)
- B)
- C)
- D)

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

**Answer:** B

**NEW QUESTION 90**

Which of the following are components of the intelligence cycle? (Select TWO.)

- A. Collection
- B. Normalization
- C. Response
- D. Analysis
- E. Correction
- F. Dissension

**Answer:** BE

**NEW QUESTION 95**

A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization \$1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised. Which of the following is the value of this risk?

- A. \$75,000
- B. \$300,000
- C. \$1.425 million
- D. \$1.5 million

**Answer:** A

**NEW QUESTION 99**

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic. Which of the following would BEST accomplish this goal?

- A. Continuous integration and deployment
- B. Automation and orchestration
- C. Static and dynamic analysis
- D. Information sharing and analysis

**Answer:** B

**NEW QUESTION 104**

The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?

- A. Post of the company blog
- B. Corporate-hosted encrypted email
- C. VoIP phone call
- D. Summary sent by certified mail
- E. Externally hosted instant message

**Answer:** C

**NEW QUESTION 108**

An organization wants to move non-essential services into a cloud computing environment. Management has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work BEST to attain the desired outcome?

- A. Duplicate all services in another instance and load balance between the instances.
- B. Establish a hot site with active replication to another region within the same cloud provider.
- C. Set up a warm disaster recovery site with the same cloud provider in a different region
- D. Configure the systems with a cold site at another cloud provider that can be used for failover.

**Answer:** C

**NEW QUESTION 110**

An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment. One of the primary concerns is exfiltration of data by malicious insiders. Which of the following controls is the MOST appropriate to mitigate risks?

- A. Data deduplication
- B. OS fingerprinting
- C. Digital watermarking
- D. Data loss prevention

**Answer:** D

### NEW QUESTION 112

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

The analyst runs the following command next:

Which of the following would explain the difference in results?

- A. ICMP is being blocked by a firewall.
- B. The routing tables for ping and hping3 were different.
- C. The original ping command needed root permission to execute.
- D. hping3 is returning a false positive.

**Answer: A**

### NEW QUESTION 113

Because some clients have reported unauthorized activity on their accounts, a security analyst is reviewing network packet captures from the company's API server. A portion of a capture file is shown below:

```
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="http://schemas.s/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.somesite.org"+xmlns:i="http://www.w3.org/2001/XMLSchema-instance"></s:Body></s:Envelope> 192.168.1.22 - -
api.somesite.com 200 0 1006 1001 0 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap
<<a:Password>Password123</a:Password><a:ResetPasswordToken+i:nil="true"/>
<a:ShouldImpersonatedAuthenticationBePopulated+i:nil="true"/><a:Username>somebody@companyname.com 192.168.5.66 - - api.somesite.com 200 0 11558
1712 2024 192.168.4.89
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetIPLocation+xmlns="http://tempuri.org/">
<a:IPAddress>516.7.446.605</a:IPAddress><a:ZipCode+i:nil="true"/></request></GetIPLocation></s:Body>< 192.168.1.22 - - api.somesite.com 200 0 1003 1011
307 192.168.1.22
POST /services/v1_0/Public/Members.svc/soap <s:Envelope+xmlns:s="
http://schemas.xmlsoap.org/soap/envelope/"><s:Body><IsLoggedIn+xmlns="http://tempuri.org/">
<request+xmlns:a="http://schemas.datacontract.org/2004/07/somesite.web+xmlns:i="
http://www.w3.org/2001/XMLSchema-instance"><a:Authentication>
<a:ApiToken>kmL4krG2CwwWBan5BRv5Djb7syxXTNKcWfUjSjd</a:ApiToken><a:ImpersonateUserId>0
<a:NetworkId>4</a:NetworkId><a:ProviderId>"1=1</a:ProviderId><a:UserId>13026046</a:UserId></a:Authe 192.168.5.66 - - api.somesite.com 200 0 1378 1209
48 192.168.4.89
```

Which of the following MOST likely explains how the clients' accounts were compromised?

- A. The clients' authentication tokens were impersonated and replayed.
- B. The clients' usernames and passwords were transmitted in cleartext.
- C. An XSS scripting attack was carried out on the server.
- D. A SQL injection attack was carried out on the server.

**Answer: A**

### NEW QUESTION 117

Which of the following attacks can be prevented by using output encoding?

- A. Server-side request forgery
- B. Cross-site scripting

- C. SQL injection
- D. Command injection
- E. Cross-site request forgery
- F. Directory traversal

**Answer:** B

#### NEW QUESTION 119

A team of security analysis has been alerted to potential malware activity. The initial examination indicates one of the affected workstations on 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 critically 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 Identify potentially affected systems by creating a correlation
- D. Identify potentially affected system by creating a correlation search in the SIEM based on the network traffic.

**Answer:** D

#### NEW QUESTION 122

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 127

A threat feed notes malicious actors have been infiltrating companies and exfiltration data to a specific set of domains Management at an organization wants to know if it is a victim Which of the following should the security analyst recommend to identity this behavior without alerting any potential malicious actors?

- A. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested
- B. Add the domains to a DNS sinkhole and create an alert m the SIEM toot when the domains are queried
- C. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443
- D. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information

**Answer:** D

#### NEW QUESTION 131

A storage area network (SAN) was inadvertently powered off while power maintenance was being performed in a datacenter. None of the systems should have lost all power during the maintenance. Upon review, it is discovered that a SAN administrator moved a power plug when testing the SAN's fault notification features.

Which of the following should be done to prevent this issue from reoccurring?

- A. Ensure both power supplies on the SAN are serviced by separate circuits, so that if one circuit goes down, the other remains powered.
- B. Install additional batteries in the SAN power supplies with enough capacity to keep the system powered on during maintenance operations.
- C. Ensure power configuration is covered in the datacenter change management policy and have the SAN administrator review this policy.
- D. Install a third power supply in the SAN so loss of any power intuit does not result in the SAN completely powering off.

**Answer:** A

#### NEW QUESTION 136

A security analyst receives an alert that highly sensitive information has left the company's network Upon investigation, the analyst discovers an outside IP range

has had connections from three servers more than 100 times in the past month. The affected servers are virtual machines. Which of the following is the BEST course of action?

- A. Shut down the servers as soon as possible, move them to a clean environment, restart, run a vulnerability scanner to find weaknesses, determine the root cause, remediate, and report.
- B. Report the data exfiltration to management, take the affected servers offline, conduct an antivirus scan, remediate all threats found, and return the servers to service.
- C. Disconnect the affected servers from the network, use the virtual machine console to access the systems, determine which information has left the network, find the security weakness, and remediate.
- D. Determine if any other servers have been affected, snapshot any servers found, determine the vector that was used to allow the data exfiltration, and report.
- E. Fix any vulnerabilities, remediate, and report.

**Answer: A**

#### NEW QUESTION 141

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 145

A small organization has proprietary software that is used internally. The system has not been well maintained and cannot be updated with the rest of the environment. Which of the following is the BEST solution?

- A. Virtualize the system and decommission the physical machine.
- B. Remove it from the network and require air gapping.
- C. Only allow access to the system via a jumpbox.
- D. Implement MFA on the specific system.

**Answer: A**

#### NEW QUESTION 148

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 153

A security analyst was alerted to a file integrity monitoring event based on a change to the `vhost-payments.conf` file. The output of the `diff` command against the known-good backup reads as follows:

Which of the following MOST likely occurred?

- A. The file was altered to accept payments without charging the cards.
- B. The file was altered to avoid logging credit card information.
- C. The file was altered to verify the card numbers are valid.
- D. The file was altered to harvest credit card numbers.

**Answer: A**

#### NEW QUESTION 155

A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?

- A. Review the firewall logs.
- B. Review syslogs from critical servers.
- C. Perform fuzzing.
- D. Install a WAF in front of the application server.

**Answer: C**

#### NEW QUESTION 158

Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?

- A. Data custodian
- B. Data owner
- C. Data processor

D. Senior management

**Answer: B**

**NEW QUESTION 160**

Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.

**INSTRUCTIONS**

Review the information provided and determine the following:

- \* 1. How many employees clicked on the link in the phishing email?
- \* 2. On how many workstations was the malware installed?
- \* 3. What is the executable file name of the malware?

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Select the following answer as per diagram below:

**NEW QUESTION 163**

A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application.

Which of the following is a security concern when using a PaaS solution?

- A. The use of infrastructure-as-code capabilities leads to an increased attack surface.
- B. Patching the underlying application server becomes the responsibility of the client.
- C. The application is unable to use encryption at the database level.
- D. Insecure application programming interfaces can lead to data compromise.

**Answer: D**

**NEW QUESTION 166**

A security analyst has discovered that developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?

- A. Create a security rule that blocks Internet access in the development VPC
- B. Place a jumpbox in between the developers' workstations and the development VPC
- C. Remove the administrator profile from the developer user group in identity and access management
- D. Create an alert that is triggered when a developer installs an application on a server

**Answer: A**

**NEW QUESTION 168**

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 171**

The help desk provided a security analyst with a screenshot of a user's desktop:

For which of the following is aircrack-ng being used?

- A. Wireless access point discovery
- B. Rainbow attack
- C. Brute-force attack
- D. PCAP data collection

**Answer: B**

**NEW QUESTION 172**

A security analyst, who is working for a company that utilizes Linux servers, receives the following results from a vulnerability scan:

Which of the following is MOST likely a false positive?

- A. ICMP timestamp request remote date disclosure
- B. Windows SMB service enumeration via \srvsvc
- C. Anonymous FTP enabled
- D. Unsupported web server detection

**Answer: B**

**NEW QUESTION 175**

A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in the situation?

- A. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
- B. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs
- C. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
- D. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains

**Answer: C**

**NEW QUESTION 180**

As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.

Which of the following BEST describes this test?

- A. Walk through
- B. Full interruption
- C. Simulation
- D. Parallel

**Answer: C**

#### NEW QUESTION 181

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

- A. strace /proc/1301
- B. rpm -V openash-server
- C. /bin/ls -l /proc/1301/exe
- D. kill -9 1301

**Answer: A**

#### NEW QUESTION 182

Which of the following software security best practices would prevent an attacker from being able to run arbitrary SQL commands within a web application? (Choose two.)

- A. Parameterized queries
- B. Session management
- C. Input validation
- D. Output encoding
- E. Data protection
- F. Authentication

**Answer: AC**

#### NEW QUESTION 186

During a cyber incident, which of the following is the BEST course of action?

- A. Switch to using a pre-approved, secure, third-party communication system.
- B. Keep the entire company informed to ensure transparency and integrity during the incident.
- C. Restrict customer communication until the severity of the breach is confirmed.
- D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

**Answer: D**

#### NEW QUESTION 190

An incident responder successfully acquired application binaries off a mobile device for later forensic analysis. Which of the following should the analyst do NEXT?

- A. Decompile each binary to derive the source code.
- B. Perform a factory reset on the affected mobile device.
- C. Compute SHA-256 hashes for each binary.
- D. Encrypt the binaries using an authenticated AES-256 mode of operation.
- E. Inspect the permissions manifests within each application.

**Answer: C**

#### NEW QUESTION 193

An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets. Which of the following should be considered FIRST prior to disposing of the electronic data?

- A. Sanitization policy
- B. Data sovereignty
- C. Encryption policy
- D. Retention standards

**Answer: D**

#### **NEW QUESTION 196**

A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

- A. Run `crontab -r; rm -rf /tmp/.t` to remove and disable the malware on the system.
- B. Examine the server logs for further indicators of compromise of a web application.
- C. Run `kill -9 1325` to bring the load average down so the server is usable again.
- D. Perform a binary analysis on the `/tmp/.t` file, as it is likely to be a rogue SSHD server.

**Answer: B**

#### **NEW QUESTION 197**

A system's authority to operate (ATO) is set to expire in four days. Because of other activities and limited staffing, the organization has neglected to start reauthentication activities until now. The cybersecurity group just performed a vulnerability scan with the partial set of results shown below:

Based on the scenario and the output from the vulnerability scan, which of the following should the security team do with this finding?

- A. Remediate by going to the web config file, searching for the enforce HTTP validation setting, and manually updating to the correct setting.
- B. Accept this risk for now because this is a "high" severity, but testing will require more than the four days available, and the system ATO needs to be completed.
- C. Ignore it
- D. This is false positive, and the organization needs to focus its efforts on other findings.
- E. Ensure HTTP validation is enabled by rebooting the server.

**Answer: A**

#### **NEW QUESTION 200**

A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-in-the-middle attack. The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices. Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?

- A. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network.
- B. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router.
- C. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network.
- D. Conduct a wireless survey to determine if the wireless strength needs to be reduced.

**Answer: A**

#### **NEW QUESTION 202**

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 206**

A SIEM solution alerts a security analyst of a high number of login attempts against the company's webmail portal. The analyst determines the login attempts used credentials from a past data breach. Which of the following is the BEST mitigation to prevent unauthorized access?

- A. Single sign-on
- B. Mandatory access control
- C. Multifactor authentication
- D. Federation
- E. Privileged access management

**Answer: E**

**NEW QUESTION 207**

An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:

The source of the breach is linked to an IP located in a foreign country.  
The breach is isolated to the research and development servers.  
The hash values of the data before and after the breach are unchanged.  
The affected servers were regularly patched, and a recent scan showed no vulnerabilities.  
Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)

- A. The confidentiality of the data is unaffected.
- B. The threat is an APT.
- C. The source IP of the threat has been spoofed.
- D. The integrity of the data is unaffected.
- E. The threat is an insider.

**Answer: BD**

**NEW QUESTION 210**

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 212**

An organization has several systems that require specific logons. Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?

- A. Use SSO across all applications
- B. Perform a manual privilege review
- C. Adjust the current monitoring and logging rules
- D. Implement multifactor authentication

**Answer: B**

**NEW QUESTION 215**

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

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

2nd - Questions 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CS0-002 Practice Test Here](#)**