Free Questions for CS0-002 by dumpssheet

Shared by Copeland on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company needs to expand Its development group due to an influx of new feature requirements (rom Its customers. To do so quickly, the company is using Junior-level developers to fill in as needed. The company has found a number of vulnerabilities that have a direct correlation to the code contributed by the junior-level developers. Which of the following controls would best help to reduce the number of software vulnerabilities Introduced by this situation?

Options:

A- Requiring senior-level developers to review code written by junior-level developers

B- Hiring senior-level developers only

C- Allowing only senior-level developers to write code for new features

D- Using authorized source code repositories only

Answer:

A

Explanation:

This control would best help to reduce the number of software vulnerabilities introduced by this situation because it ensures that code quality and security standards are met before deploying to production. Senior-level developers can provide feedback, guidance, and corrections to junior-level developers and catch any errors or flaws in their code.

Question 2

Question Type: **MultipleChoice**

An analyst needs to provide recommendations based on a recent vulnerability scan:

Plug-in name	Family
SMB use domain SID to enumerate users	Windows : User management
SYN scanner	Port scanners
SSL certificate cannot be trusted	General
Scan not performed with admin privileges	Settings

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?

Options:

A- SMB use domain SID to enumerate users

B- SYN scanner

C- SSL certificate cannot be trusted

D- Scan not performed with admin privileges

Answer:

D

Explanation:

This should be addressed to ensure potential vulnerabilities are identified because it indicates that the vulnerability scan was not able to access some resources or perform some actions that require higher privileges on the target system. This could result in missing or inaccurate findings, as some vulnerabilities may not be detected or verified.

Question 3

Question Type: MultipleChoice

After running the cat file01.bin | hexdump -c command, a security analyst reviews the following output snippet:

00000000 ff d8 ft e0 00 10 4a 46 49 46 00 01 01 00 00 01 |.....JFIF.....|

Which of the following digital-forensics techniques is the analyst using?

Options:

A- Reviewing the file hash

B- Debugging the binary file

C- Implementing file carving

D- Verifying the file type

E- Utilizing reverse engineering

Answer:

D

Explanation:

This is the digital-forensics technique that the analyst is using by running the cat file01.bin | hexdump -c command. This command displays the contents of the binary file in hexadecimal and ASCII format, which can help identify the file type based on its header or signature. In this case, the output snippet shows that the file type is JPEG, as indicated by the ff d8 ff e0 bytes at the beginning and the JFIF string in ASCII.

Question 4

Question Type: MultipleChoice

A threat intelligence group issued a warning to its members regarding an observed increase in attacks performed by a specific threat actor and the related loCs. Which is of the following is (he best method to operationalize these loCs to detect future attacks?

Options:

A- Analyzing samples of associated malware

B- Publishing an internal executive threat report

C- Executing an adversary emulation exercise

D- Integrating the company's SIEM platform

Answer:

D

Explanation:

This is the best method to operationalize these loCs to detect future attacks because it allows the company to collect, correlate, analyze, and alert on the indicators of compromise (loCs) from various sources and systems. A SIEM stands for security information and event management, which is a software or service that provides centralized visibility and management of security events and data.

Question 5

Question Type: MultipleChoice

A company notices unknown devices connecting to the internal network and would like to implement a solution to block all non-corporate managed machines. Which of the following solutions would be best to accomplish this goal?

Options:

A- WPA2 for W1F1 networks

B- NAC with 802.1X implementation

C- Extensible Authentication Protocol

D- RADIUS with challenge/response

Answer:

B

Explanation:

This solution is the best to accomplish the goal of blocking all non-corporate managed machines from connecting to the internal network. NAC stands for network access control, which is a method of enforcing policies and rules on network devices based on their identity, role, location, and other attributes. 802.1X is a standard for port-based network access control, which authenticates devices before granting them access to a network port or wireless access point.

Question 6

Question Type: MultipleChoice

An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the first steps to confirm and respond to the incident? (Select two).

Options:

A- Pause the virtual machine.

B- Shut down the virtual machine.

C- Take a snapshot of the virtual machine.

D- Remove the NIC from the virtual machine.

E- Review host hypervisor log of the virtual machine.

F- Execute a migration of the virtual machine.

Answer:

A, C

Explanation:

These steps are the best to confirm and respond to the incident because they preserve the state of the compromised server for further analysis and evidence collection. Pausing the virtual machine prevents any further changes or damage by the attacker, while taking a snapshot creates a copy of the virtual machine's memory and disk contents.

Question 7

Question Type: **MultipleChoice**

An organization has the following vulnerability remediation policies:

* For production environment servers:

* Vulnerabilities with a CVSS score of 9.0 or greater must be remediated within 48 hours.

* Vulnerabilities with a CVSS score of 5.0 to 8.9 must be remediated within 96 hours.

* Vulnerabilities in lower environments may be left unremediated for up to two weeks.

* All vulnerability remediations must be validated in a testing environment before they are applied in the production environment.

The organization has two environments: production and testing. The accountingProd server is the only server that contains highly sensitive information.

A recent vulnerability scan provided the following report:

Hostname	Environment	Vulnerability	CVSS score
timecardProd	Production	OS missing patch KB035	8.2
timecardTest	Testing	OS missing patch KB035	8.2
expenseProd	Production	OS missing patch KB022	7.1
expenseTest	Testing	OS missing patch KB022	7.1
accountingProd	Production	OS missing patch KB022	7.1
accountingTest	Testing	OS missing patch KB022	7.1
stagingTest	Testing	OS missing patch KB044	9.8

Which of the following identifies the server that should be patched first? (Choose Two)

Options:

A- timecardProd

B- timecardTesl

C- expense Prod

D- expenseTest

E- accountingProd

F- accountingTest

G- stagingTest

Answer:

C, E

Explanation:

These servers should be patched first because they have vulnerabilities with CVSS scores of 9.0 and 8.9 respectively, which fall under the policy of remediating within 48 hours and 96 hours for production environment servers. The other servers either have lower CVSS scores, are in lower environments, or do not contain highly sensitive information.

Question 8

Question Type: MultipleChoice

A security analyst is concerned about sensitive data living on company file servers following a zero-day attack that nearly resulted in a breach of millions of customer records. The after action report indicates a lack of controls around the file servers that contain sensitive dat

a. Which of the following DLP considerations would best help the analyst to classify and address the sensitive data on the file servers?

Options:

A- Implement a CASB device and connect the SaaS applications.

B- Deploy network DLP appliances pointed to all file servers.

C- Use data-at-rest scans to locate and identify sensitive data.

D- Install endpoint DLP agents on all computing resources.

Answer:

C

Explanation:

Use data-at-rest scans to locate and identify sensitive data. This option is the best DLP consideration for addressing the sensitive data on the file servers. Data-at-rest scans are performed on data that is stored on a device or a network, such as file servers, and can help identify and classify sensitive data based on predefined policies or rules. The other options are not relevant for this scenario, as they either deal with data in transit (network DLP appliances), data in use (endpoint DLP agents), or cloud-based data (CASB device).

Question 9

Question Type: MultipleChoice

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 ClSO's concerns?

Options:

A- Configure DLP to reject all changes to the files without pre-authorization. Monitor the files for unauthorized changes.

B- Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes.

C- Place a legal hold on the files Require authorized users to abide by a strict time context access policy. Monitor the files for

unauthorized changes.

D- Use Wireshark to scan all traffic to and from the directory. Monitor the files for unauthorized changes.

Answer:

B

Explanation:

Regularly use SHA-256 to hash the directory containing the sensitive information. Monitor the files for unauthorized changes. This option is the best technique to ensure the integrity of the files and tie any changes to a specific user session. Hashing is a process that generates a unique value for a given input, and any modification to the input will result in a different hash value. By using SHA-256, which is a secure hashing algorithm, the analyst can compare the hash values of the files before and after each user session and detect any unauthorized changes.

Question 10

Question Type: MultipleChoice

A security analyst is reviewing a new Internet portal that will be used for corporate employees to obtain their pay statements. Corporate policy classifies pay statement information as confidential, and it must be protected by MF

Options:

A- Which of the following would best fulfill the MFA requirement while keeping the portal accessible from the internet?

A- Obtaining home public IP addresses of corporate employees to implement source IP restrictions and requiring a username and password

B- Requiring the internet portal to be accessible from only the corporate SSO internet endpoint and requiring a smart card and PIN

C- Moving the internet portal server to a DMZ that is only accessible from the corporate VPN and requiring a username and password

D- Distributing a shared password that must be provided before the internet portal loads and requiring a username and password

Answer:

B

Explanation:

Requiring the internet portal to be accessible from only the corporate SSO internet endpoint and requiring a smart card and PIN. This option provides the best MFA requirement because it uses two factors of authentication: something you have (smart card) and something you know (PIN). It also restricts access to the portal from a trusted source (corporate SSO internet endpoint).

Question 11

Question Type: MultipleChoice

Which of the following is a reason for correctly identifying APTs that might be targeting an organization?

Options:

A- APTs' passion for social justice will make them ongoing and motivated attackers.

B- APTs utilize methods and technologies differently than other threats

C- APTs are primarily focused on financial gam and are widely available over the internet.

D- APTs lack sophisticated methods, but their dedication makes them persistent.

Answer:

B

Explanation:

APTs utilize methods and technologies differently than other threats. APTs stand for Advanced Persistent Threats, and they are sophisticated and stealthy attacks that target specific organizations or networks over a long period of time, often with political or financial motives. APTs utilize methods and technologies differently than other threats, such as using custom-made malware, exploiting zero-day vulnerabilities, leveraging social engineering techniques, or employing multiple vectors of attack. APTs can also evade detection by

existing security tools or controls, by using encryption, obfuscation, proxy servers, or other techniques to hide their activities or communications.