Free Questions for CAS-004 by ebraindumps

Shared by Cooke on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Law enforcement officials informed an organization that an investigation has begun. Which of the following is the FIRST step the organization should take?

Options:

A- Initiate a legal hold.

B- Refer to the retention policy

C- Perform e-discovery.

D- Review the subpoena

Answer:

A

Explanation:

A legal hold is a process by which an organization instructs its employees or other relevant parties to preserve specific data for potential litigation. A legal hold is triggered when litigation is reasonably anticipated, such as when law enforcement officials inform an organization that an investigation has begun. The first step the organization should take is to initiate a legal hold to ensure that relevant evidence is not deleted, destroyed, or altered. A legal hold also demonstrates the organization's good faith and compliance with its duty to preserve evidence. Verified Reference:

https://percipient.co/litigation-hold-triggers-and-the-duty-to-preserve-evidence/

https://www.everlaw.com/blog/ediscovery-best-practices/guide-to-legal-holds/

Question 2

Question Type: MultipleChoice

A company with multiple locations has taken a cloud-only approach to its infrastructure The company does not have standard vendors or systems resulting in a mix of various solutions put in place by each location The Chief Information Security Officer wants to ensure that the internal security team has visibility into all platforms Which of the following best meets this objective?

Options:

A- Security information and event management

B- Cloud security posture management

C- SNMFV2 monitoring and log aggregation

D- Managed detection and response services from a third party

Answer:

A

Explanation:

Security Information and Event Management (SIEM) systems provide real-time analysis of security alerts generated by applications and network hardware. SIEMs are beneficial in environments where there is a mix of various solutions, as they can collect and aggregate logs from multiple sources, providing the internal security team with a centralized view and visibility into all platforms. This would best meet the objective of ensuring visibility into all platforms, regardless of the differing solutions across the company's locations.

Question 3

Question Type: MultipleChoice

An IoT device implements an encryption module built within its SoC where the asymmetric private key has been defined in a write-once read-many portion of the SoC hardware Which of the following should the IoT manufacture do if the private key is compromised?

Options:

A- Use over-the-air updates to replace the private key

B- Manufacture a new IoT device with a redesigned SoC

C- Replace the public portion of the IoT key on its servers

D- Release a patch for the SoC software

Answer:

B

Explanation:

If the asymmetric private key defined in the write-once read-many (WORM) portion of the System on Chip (SoC) is compromised, the IoT device manufacturer cannot simply replace or update the key through software changes due to the nature of WORM memory. The compromised key would necessitate the production of a new IoT device with a redesigned SoC that includes a new, secure private key. This is because the integrity of the encryption module is fundamental to the device's security, and a compromised key cannot be allowed to persist in the hardware.

Question 4

Question Type: MultipleChoice

Company A is merging with Company B Company A is a small, local company Company B has a large, global presence The two companies have a lot of duplication in their IT systems processes, and procedures On the new Chief Information Officer's (ClO's) first day a fire breaks out at Company B's mam data center Which of the following actions should the CIO take first?

Options:

A- Determine whether the incident response plan has been tested at both companies, and use it to respond

B- Review the incident response plans, and engage the disaster recovery plan while relying on the IT leaders from both companies.

C- Ensure hot. warm, and mobile disaster recovery sites are available, and give an update to the companies' leadership teams

D- Initiate Company A's IT systems processes and procedures, assess the damage, and perform a BIA

Answer:

B

Explanation:

In the event of a fire at the main data center, the immediate action should be to review and engage the disaster recovery plan. This is to ensure the continuity of business operations. The CIO should coordinate with IT leaders from both companies to ensure a unified response. Assessing the damage and planning for recovery are crucial, and leveraging the expertise from both companies can help streamline the process.

Question 5

Question Type: **MultipleChoice**

A security administrator needs to recommend an encryption protocol after a legacy stream cipher was deprecated when a security flaw was discovered. The legacy cipher excelled at maintaining strong cryptographic security and provided great performance for a streaming video service. Which of the following AES modes should the security administrator recommend given these requirements?

Options:

A- CTR

B- ECB

C- OF8

D- GCM

Answer:

D

Explanation:

Galois/Counter Mode (GCM) is an AES mode of operation that provides both confidentiality and data integrity. It is well-suited for processing streams of data, making it ideal for streaming video services. GCM is known for its strong cryptographic security and good performance, which aligns with the legacy cipher's characteristics and the streaming service's requirements.

Question 6

Question Type: MultipleChoice

A SOC analyst received an alert about a potential compromise and is reviewing the following SIEM logs:

```
1:15:02PM JDoe successful login on laptop314
1:15:45PM JDoe launched outlook.exe on laptop314
1:17:03PM Process outlook.exe launched cmd.exe on laptop314
1:17:04PM Process cmd.exe launched rdp.exe on laptop314
1:17:04PM Process cmd.exe launched rdp.exe on laptop314
1:17:05PM JDoe successful login on server112
1:17:05PM JDoe successful login on server113
1:17:07PM JDoe launched cmd.exe on server112
```

Which of the following is the most appropriate action for the SOC analyst to recommend?

Options:

A- Disabling account JDoe to prevent further lateral movement

B- Isolating laptop314 from the network

C- Alerting JDoe about the potential account compromise

D- Creating HIPS and NIPS rules to prevent logins

Answer:

B

Explanation:

The SIEM logs indicate suspicious behavior that could be a sign of a compromise, such as the launching of cmd.exe after Outlook.exe, which is atypical user behavior and could indicate that a machine has been compromised to perform lateral movement within the network. Isolating laptop314 from the network would contain the threat and prevent any potential spread to other systems while further investigation takes place.

Question 7

Question Type: MultipleChoice

A forensics investigator is analyzing an executable file extracted from storage media that was submitted (or evidence The investigator must use a tool that can identify whether the executable has indicators, which may point to the creator of the file Which of the following should the investigator use while preserving evidence integrity?

Options:

A- idd

B- bcrypt

C- SHA-3

D- ssdeep

E- dcfldd

Answer:

D

Explanation:

ssdeep is a tool that computes and matches Context Triggered Piecewise Hashing (CTPH), also known as fuzzy hashing. It can be used to identify similar files or slight variations of the same file, which may point to the creator of the file if certain patterns or markers are consistently present. This method allows for integrity checking without altering the evidence, which is critical in forensic investigation.

Question 8

Question Type: MultipleChoice

A company with only U S -based customers wants to allow developers from another country to work on the company's website However, the company plans to block normal internet traffic from the other country Which of the following strategies should the company use to accomplish this objective? (Select two).

Options:

A- Block foreign IP addresses from accessing the website

B- Have the developers use the company's VPN

C- Implement a WAP for the website

D- Give the developers access to a jump box on the network

E- Employ a reverse proxy for the developers

F- Use NAT to enable access for the developers

Answer:

B, D

Explanation:

Having developers use the company's VPN can provide them with secure access to the network while still allowing the company to block normal internet traffic from the other country. A jump box serves as a secure entry point for administrators or in this case, developers, to connect before launching any administrative tasks or accessing further areas of the network. This setup maintains security while still providing necessary access.

Question 9

Question Type: MultipleChoice

A security engineer is assessing the security controls of loT systems that are no longer supported for updates and patching. Which of the following is the best mitigation for defending these loT systems?

Options:

A- Disable administrator accounts

B- Enable SELinux

C- Enforce network segmentation

D- Assign static IP addresses

Answer:

C

Explanation:

Network segmentation is a method to isolate environments from one another, thus limiting the scope of a potential attack. For IoT systems that cannot be updated or patched, network segmentation is the best mitigation technique. It would contain any compromise to the segmented network and prevent it from affecting the rest of the network infrastructure.