Free Questions for CS0-002

Shared by Cleveland on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A social media company is planning an acquisition. Prior to the purchase, the Chief Security Officer (CSO) would like a full report to gain a better understanding of the prospective company's cybersecurity posture and to identify risks in the supply chain. Which of the following will best support the CSO's objective?

Options:

A- Third-party assessment

B- Memorandum of understanding

C- Non-disclosure agreement

D- Software source authenticity

Answer:

A

Explanation:

Third-party assessment. A third-party assessment is a process that explores the risk posed to your organization by third-party vendors along the supply chain.This process evaluates the likelihood that your business is exposed to different third-party risks such as compliance risk, operational risk, financial risk, security risk and cybersecurity risk1.

A third-party assessment can help the CSO gain a better understanding of the prospective company's cybersecurity posture by:

Providing an independent and objective evaluation of the vendor's security policies, controls, and practices.

Identifying any gaps or weaknesses in the vendor's security posture that could compromise your organization's data, systems, or reputation.

Recommending actions or improvements to mitigate or reduce the identified risks and enhance the vendor's security performance.

A third-party assessment can also help the CSO identify risks in the supply chain by:

Mapping and tracing the data flow and dependencies among the vendor and its subcontractors or suppliers.

Assessing how the vendor and its subcontractors or suppliers safeguard data and comply with relevant regulations and standards.

Detecting any signs of malicious or negligent behavior by the vendor or its subcontractors or suppliers that could harm your organization or its customers.

Question 2

Question Type: MultipleChoice

An analyst is reviewing email headers to determine if an email has been sent from a legitimate sender. The organization uses SPF to validate email origination. Which of the following most likely indicates an invalid originator?

Options:

A- Received-SPF: neutral

B- Received-SPF: none

C- Received-SPF softfail

D- Received-SPF: error

Answer:

C

Explanation:

Received-SPF: softfail. SPF stands for Sender Policy Framework, and it is a method of validating email origin by checking the sender's IP address against a list of authorized IP addresses published by the domain owner in a DNS record.SPF can help to prevent email spoofing and phishing by verifying the authenticity of the sender1.

Received-SPF is a header field that indicates the result of the SPF check performed by the recipient's mail server. There are several possible values for this field, but the most common ones are:

pass: The sender's IP address matches one of the authorized IP addresses for the domain. This indicates a valid originator.

fail: The sender's IP address does not match any of the authorized IP addresses for the domain, and the domain owner has explicitly stated that such emails should be rejected. This indicates an invalid originator.

neutral: The sender's IP address does not match any of the authorized IP addresses for the domain, but the domain owner has not stated how to handle such emails. This indicates an unknown originator.

none: The domain does not have an SPF record, or the SPF record is invalid or malformed. This indicates a missing or invalid SPF policy.

softfail: The sender's IP address does not match any of the authorized IP addresses for the domain, but the domain owner has stated that such emails should be accepted with caution.This indicates a suspicious originator2.

Therefore, out of the four options, Received-SPF: softfail most likely indicates an invalid originator, as it suggests that the sender is not authorized by the domain owner and may be trying to impersonate or spoof the domain.

1:What Is SPF?2:SPF Record Check

Question 3

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 CISO'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 4

Question Type: MultipleChoice

During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?

Options:

A- strings
B- head
C- fsstat
D- dd

Answer:

A

Explanation:

The strings command is a Linux utility that can extract human-readable content from any file or partition3.It can be used to analyze a Linux swap partition by finding text strings that may indicate malicious activity or compromise4. The head command (B) can only display the first few lines of a file or partition, which may not contain any useful information. The fsstat command can only display file system statistics such as size, type, and layout, which may not reveal any human-readable content. The dd command (D) can only copy or convert a file or partition, which may not extract any human-readable content.

Question 5

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 6

Question Type: MultipleChoice

Which of the following is the best method to ensure secure boot UEFI features are enabled to prevent boot malware?

Options:

A- Enable secure boot in the hardware and reload the operating system.

B- Reconfigure the system's MBR and enable NTFS.

C- Set I-JEFI to legacy mode and enable security features.

D- Convert the legacy partition table to UEFI and repair the operating system.

B) Reconfigure the system's MBR and enable NTFS is not correct. MBR stands for Master Boot Record, and it is a legacy partitioning scheme that stores information about the partitions and the boot loader on a disk. NTFS stands for New Technology File System, and it is a file system that supports features such as encryption, compression, and access control. Reconfiguring the system's MBR and enabling NTFS would not enable secure boot UEFI features, as they are not related to UEFI or secure boot.Moreover, MBR is incompatible with UEFI, as UEFI requires a different partitioning scheme called GPT (GUID Partition Table)3.

C) Set UEFI to legacy mode and enable security features is not correct. Legacy mode is a compatibility mode that allows UEFI systems to boot using legacy BIOS methods. Legacy mode disables some of the features and benefits of UEFI, such as secure boot, faster boot time, or larger disk support. Setting UEFI to legacy mode would not enable secure boot UEFI features, but rather disable them.

D) Convert the legacy partition table to UEFI and repair the operating system is not correct. Converting the legacy partition table to UEFI means changing the partitioning scheme from MBR to GPT, which is required for UEFI systems to boot. However, this alone would not enable secure boot UEFI features, as it also depends on the firmware settings and the operating system support. Repairing the operating system may or may not fix any issues caused by converting the partition table, but it would not necessarily enable secure boot either.

1:What Is Secure Boot?2:How to Enable Secure Boot3:MBR vs GPT: Which One Is Better for You?: [UEFI vs Legacy BIOS -- The Ultimate Comparison Guide]

Answer:

A

Explanation:

The correct answer is A. Enable secure boot in the hardware and reload the operating system. Secure boot is a feature of UEFI that ensures that only trusted and authorized code can execute during the boot process.Secure boot can prevent boot malware, such as rootkits or bootkits, from compromising the system before the operating system loads1. To enable secure boot, the hardware must support UEFI and have a firmware that implements the secure boot protocol. The operating system must also support UEFI and have a digital signature that matches the keys stored in the firmware. If the operating system was installed in legacy mode or does not have a valid signature, it may not boot with secure boot enabled.Therefore, it may be necessary to reload the operating system after enabling secure boot in the hardware2.

Question 7

Question Type: MultipleChoice

A small business does not have enough staff in the accounting department to segregate duties. The controller writes the checks for the business and reconciles them against the ledger. To ensure there is no fraud occurring, the business conducts quarterly reviews in which a different officer in the business compares all the cleared checks against the ledger. Which of the following BEST describes this type of control?

Options:

A- Deterrent

B- Preventive

C- Compensating

D- Detective

Answer:

C

Explanation:

A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.

'Compensating controls are additional security measures that you take to address a vulnerability without remediating the underlying issue.'

A compensating control is a control that reduces the risk of an existing or potential control weakness2In this case, the lack of segregation of duties in the accounting department is a control weakness that increases the risk of fraud or error. The quarterly reviews by a different officer are a compensating control that reduces this risk by providing an independent verification of the transactions recorded by the controller.