Free Questions for SY0-701

Shared by Carney on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An important patch for a critical application has just been released, and a systems administrator is identifying all of the systems requiring the patch. Which of the following must be maintained in order to ensure that all systems requiring the patch are updated?

Options:

A- Asset inventory

B- Network enumeration

C- Data certification

D- Procurement process

Answer:

A

Explanation:

To ensure that all systems requiring the patch are updated, the systems administrator must maintain an accurate asset inventory. This inventory lists all hardware and software assets within the organization, allowing the administrator to identify which systems are affected by the patch and ensuring that none are missed during the update process.

Network enumeration is used to discover devices on a network but doesn't track software that requires patching.

Data certification and procurement process are unrelated to tracking systems for patching purposes.

Question 2

Question Type: **MultipleChoice**

An IT manager is increasing the security capabilities of an organization after a data classification initiative determined that sensitive data could be exfiltrated from the environment. Which of the following solutions would mitigate the risk?

Options:

A- XDR

B- SPF

C- DLP

D- DMARC

Answer:

C

Explanation:

To mitigate the risk of sensitive data being exfiltrated from the environment, the IT manager should implement a Data Loss Prevention (DLP) solution. DLP monitors and controls the movement of sensitive data, ensuring that unauthorized transfers are blocked and potential data breaches are prevented.

XDR (Extended Detection and Response) is useful for threat detection across multiple environments but doesn't specifically address data exfiltration.

SPF (Sender Policy Framework) helps prevent email spoofing, not data exfiltration.

DMARC (Domain-based Message Authentication, Reporting & Conformance) also addresses email security and spoofing, not data exfiltration.

Question 3

Question Type: **MultipleChoice**

A new employee logs in to the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company. Which of the following attack vectors is most likely being used?

Options:

A- Business email

B- Social engineering

C- Unsecured network

D- Default credentials

Answer:

B

Explanation:

The employee notices that the links in the email do not correspond to the company's official URLs, indicating that this is likely a social engineering attack. Social engineering involves manipulating individuals into divulging confidential information or performing actions that may compromise security. Phishing emails, like the one described, often contain fraudulent links to trick the recipient into providing sensitive information or downloading malware.

Business email refers to business email compromise (BEC), which typically involves impersonating a high-level executive to defraud the company.

Unsecured network is unrelated to the email content.

Default credentials do not apply here, as the issue is with suspicious links, not login credentials.

Question 4

Question Type: MultipleChoice

Which of the following threat vectors is most commonly utilized by insider threat actors attempting data exfiltration?

Options:

A- Unidentified removable devices

B- Default network device credentials

C- Spear phishing emails

D- Impersonation of business units through typosquatting

Answer:

A

Explanation:

Unidentified removable devices, such as USB drives, are a common threat vector for insider threat actors attempting data exfiltration. Insiders can easily use these devices to transfer sensitive data out of the organization undetected, making it one of the most commonly utilized methods for data theft.

Default network device credentials are a security vulnerability but not typically used for data exfiltration.

Spear phishing emails are used for external attacks, not insider data exfiltration.

Impersonation through typosquatting is typically used by external actors for phishing or fraud.

Question 5

Question Type: MultipleChoice

Which of the following would best explain why a security analyst is running daily vulnerability scans on all corporate endpoints?

Options:

A- To track the status of patching installations

B- To find shadow IT cloud deployments

C- To continuously the monitor hardware inventory

D- To hunt for active attackers in the network

Answer:

A

Explanation:

Running daily vulnerability scans on all corporate endpoints is primarily done to track the status of patching installations. These scans help identify any missing security patches or vulnerabilities that could be exploited by attackers. Keeping the endpoints up-to-date with the latest patches is critical for maintaining security.

Finding shadow IT cloud deployments and monitoring hardware inventory are better achieved through other tools.

Hunting for active attackers would typically involve more real-time threat detection methods than daily vulnerability scans.

Question 6

Question Type: **MultipleChoice**

An organization is adopting cloud services at a rapid pace and now has multiple SaaS applications in use. Each application has a separate log-in. so the security team wants to reduce the number of credentials each employee must maintain. Which of the following is the first step the security team should take?

Options:

A- Enable SAML

B- Create OAuth tokens.

C- Use password vaulting.

D- Select an IdP

Answer:

D

Explanation:

The first step in reducing the number of credentials each employee must maintain when using multiple SaaS applications is to select an Identity Provider (IdP). An IdP provides a centralized authentication service that supports Single Sign-On (SSO), enabling users to access multiple applications with a single set of credentials.

Enabling SAML would be part of the technical implementation but comes after selecting an IdP.

OAuth tokens are used for authorization, but selecting an IdP is the first step in managing authentication.

Password vaulting stores multiple passwords securely but doesn't reduce the need for separate logins.