DUMPSHQ

Free Questions for SY0-701 by dumpshq

Shared by Lane on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A company is decommissioning its physical servers and replacing them with an architecture that will reduce the number of individual operating systems. Which of the following strategies should the company use to achieve this security requirement?

Options:

A- Microservices

B- Containerization

C- Virtualization

D- Infrastructure as code

Answer:

B

Explanation:

To reduce the number of individual operating systems while decommissioning physical servers, the company should use containerization. Containerization allows multiple applications to run in isolated environments on a single operating system, significantly reducing the overhead compared to running multiple virtual machines, each with its own OS.

Containerization: Uses containers to run multiple isolated applications on a single OS kernel, reducing the need for multiple OS instances and improving resource utilization.

Microservices: An architectural style that structures an application as a collection of loosely coupled services, which does not necessarily reduce the number of operating systems.

Virtualization: Allows multiple virtual machines to run on a single physical server, but each VM requires its own OS, not reducing the number of OS instances.

Infrastructure as code: Manages and provisions computing infrastructure through machine-readable configuration files, but it does not directly impact the number of operating systems.

Question 2

Question Type: MultipleChoice

A company hired a security manager from outside the organization to lead security operations. Which of the following actions should the security manager perform first in this new role?

Options:

A- Establish a security baseline.

B- Review security policies.

C- Adopt security benchmarks.

D- Perform a user ID revalidation.

Answer:

B

Explanation:

When a security manager is hired from outside the organization to lead security operations, the first action should be to review the existing security policies. Understanding the current security policies provides a foundation for identifying strengths, weaknesses, and areas that require improvement, ensuring that the security program aligns with the organization's goals and regulatory requirements.

Review security policies: Provides a comprehensive understanding of the existing security framework, helping the new manager to identify gaps and areas for enhancement.

Establish a security baseline: Important but should be based on a thorough understanding of existing policies and practices.

Adopt security benchmarks: Useful for setting standards, but reviewing current policies is a necessary precursor.

Perform a user ID revalidation: Important for ensuring user access is appropriate but not the first step in understanding overall security operations.

Question 3

Question Type: MultipleChoice

A. Deterrent

Options:

B- Corrective

C- Compensating

D- Preventive

Answer:

C

Explanation:

When a critical legacy server is segmented into a private network, the security control being used is compensating. Compensating controls are alternative measures put in place to satisfy a security requirement when the primary control is not feasible or practical. In this case, segmenting the legacy server into a private network serves as a compensating control to protect it from potential vulnerabilities that cannot be mitigated directly.

Compensating: Provides an alternative method to achieve the desired security outcome when the primary control is not possible.

Deterrent: Aims to discourage potential attackers but does not directly address segmentation.

Corrective: Used to correct or mitigate the impact of an incident after it has occurred.

Preventive: Aims to prevent security incidents but is not specific to the context of segmentation.

Question 4

Question Type: MultipleChoice

A company that is located in an area prone to hurricanes is developing a disaster recovery plan and looking at site considerations that allow the company to immediately continue operations. Which of the following is the best type of site for this company?

Options:

A- Cold

B- Tertiary

C- Warm

D- Hot

Answer:

D

Explanation:

For a company located in an area prone to hurricanes and needing to immediately continue operations, the best type of site is a hot site. A hot site is a fully operational offsite data center that is equipped with hardware, software, and network connectivity and is ready to take over operations with minimal downtime.

Hot site: Fully operational and can take over business operations almost immediately after a disaster.

Cold site: A basic site with infrastructure in place but without hardware or data, requiring significant time to become operational.

Tertiary site: Not a standard term in disaster recovery; it usually refers to an additional backup location but lacks the specifics of readiness.

Warm site: Equipped with hardware and connectivity but requires some time and effort to become fully operational, not as immediate as a hot site.

Question 5

Question Type: **MultipleChoice**

A security administrator identifies an application that is storing data using MD5. Which of the following best identifies the vulnerability likely present in the application?

Options:

A- Cryptographic

B- Malicious update

C- Zero day

D- Side loading

Answer:

A

Explanation:

The vulnerability likely present in the application that is storing data using MD5 is a cryptographic vulnerability. MD5 is considered to be a weak hashing algorithm due to its susceptibility to collision attacks, where two different inputs produce the same hash output, compromising data integrity and security.

Cryptographic: Refers to vulnerabilities in cryptographic algorithms or implementations, such as the weaknesses in MD5.

Malicious update: Refers to the intentional injection of harmful updates, not related to the use of MD5.

Zero day: Refers to previously unknown vulnerabilities for which no patch is available, not specifically related to MD5.

Side loading: Involves installing software from unofficial sources, not directly related to the use of MD5.

Question 6

Question Type: MultipleChoice

A security engineer needs to configure an NGFW to minimize the impact of the increasing number of various traffic types during attacks. Which of the following types of rules is the engineer the most likely to configure?

Options:

A- Signature-based

B- Behavioral-based

C- URL-based

D- Agent-based

Answer:

B

Explanation:

To minimize the impact of the increasing number of various traffic types during attacks, a security engineer is most likely to configure behavioral-based rules on a Next-Generation Firewall (NGFW). Behavioral-based rules analyze the behavior of traffic patterns and can detect and block unusual or malicious activity that deviates from normal behavior.

Behavioral-based: Detects anomalies by comparing current traffic behavior to known good behavior, making it effective against various traffic types during attacks.

Signature-based: Relies on known patterns of known threats, which might not be as effective against new or varied attack types.

URL-based: Controls access to websites based on URL categories but is not specifically aimed at handling diverse traffic types during attacks.

Agent-based: Typically involves software agents on endpoints to monitor and enforce policies, not directly related to NGFW rules.

Question 7

Question Type: MultipleChoice

A network administrator is working on a project to deploy a load balancer in the company's cloud environment. Which of the following fundamental security requirements does this project fulfill?

Options:

A- Privacy

B- Integrity

C- Confidentiality

D- Availability

Answer:

D

Explanation:

Deploying a load balancer in the company's cloud environment primarily fulfills the fundamental security requirement of availability. A load balancer distributes incoming network traffic across multiple servers, ensuring that no single server becomes overwhelmed and that the service remains available even if some servers fail.

Availability: Ensures that services and resources are accessible when needed, which is directly supported by load balancing.

Privacy: Protects personal and sensitive information from unauthorized access but is not directly related to load balancing.

Integrity: Ensures that data is accurate and has not been tampered with, but load balancing is not primarily focused on data integrity.

Confidentiality: Ensures that information is accessible only to authorized individuals, which is not the primary concern of load balancing.

Question 8

Question Type: MultipleChoice

The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

Options:

A- Shadow IT

B- Insider threat

C- Data exfiltration

D- Service disruption

Answer:

A

Explanation:

The marketing department setting up its own project management software without informing the appropriate departments is an example of Shadow IT. Shadow IT refers to the use of IT systems, devices, software, applications, and services without explicit approval from the IT department.

Shadow IT: Involves the use of unauthorized systems and applications within an organization, which can lead to security risks and compliance issues.

Insider threat: Refers to threats from individuals within the organization who may intentionally cause harm or misuse their access, but this scenario is more about unauthorized use rather than malicious intent.

Data exfiltration: Involves unauthorized transfer of data out of the organization, which is not the main issue in this scenario.

Service disruption: Refers to interruptions in service availability, which is not directly related to the marketing department's actions.

Question 9

Question Type: **MultipleChoice**

During a recent breach, employee credentials were compromised when a service desk employee issued an MFA bypass code to an attacker who called and posed as an employee. Which of the following should be used to prevent this type of incident in the future?

Options:

A- Hardware token MFA

B- Biometrics

C- Identity proofing

D- Least privilege

Answer:

C

Explanation:

To prevent the issuance of an MFA bypass code to an attacker posing as an employee, implementing identity proofing would be most effective. Identity proofing involves verifying the identity of individuals before granting access or providing sensitive information.

Identity proofing: Ensures that the person requesting the MFA bypass is who they claim to be, thereby preventing social engineering attacks where attackers pose as legitimate employees.

Hardware token MFA: Provides an additional factor for authentication but does not address verifying the requester's identity.

Biometrics: Offers strong authentication based on physical characteristics but is not related to the process of issuing MFA bypass codes.

Least privilege: Limits access rights for users to the bare minimum necessary to perform their work but does not prevent social engineering attacks targeting the service desk.

Question 10

Question Type: **MultipleChoice**

To improve the security at a data center, a security administrator implements a CCTV system and posts several signs about the possibility of being filmed. Which of the following best describe these types of controls? (Select two).

Options:

A- Preventive

B- Deterrent

C- Corrective

D- Directive

E- Compensating

F- Detective

Answer:

B, F

Explanation:

The CCTV system and signs about the possibility of being filmed serve as both deterrent and detective controls.

Deterrent controls: Aim to discourage potential attackers from attempting unauthorized actions. Posting signs about CCTV serves as a deterrent by warning individuals that their actions are being monitored.

Detective controls: Identify and record unauthorized or suspicious activity. The CCTV system itself functions as a detective control by capturing and recording footage that can be reviewed later.

Preventive controls: Aim to prevent security incidents but are not directly addressed by the CCTV and signs in this context.

Corrective controls: Aim to correct or mitigate the impact of a security incident.

Directive controls: Provide guidelines or instructions but are not directly addressed by the CCTV and signs.

Compensating controls: Provide alternative measures to compensate for the absence or failure of primary controls.

Question 11

Question Type: **MultipleChoice**

A manager receives an email that contains a link to receive a refund. After hovering over the link, the manager notices that the domain's URL points to a suspicious link. Which of the following security practices helped the manager to identify the attack?

Options:

A- End user training

B- Policy review

C- URL scanning

D- Plain text email

Answer:

A

Explanation:

The security practice that helped the manager identify the suspicious link is end-user training. Training users to recognize phishing attempts and other social engineering attacks, such as hovering over links to check the actual URL, is a critical component of an organization's security awareness program.

End user training: Educates employees on how to identify and respond to security threats, including suspicious emails and phishing attempts.

Policy review: Ensures that policies are understood and followed but does not directly help in identifying specific attacks.

URL scanning: Automatically checks URLs for threats, but the manager identified the issue manually.

Plain text email: Ensures email content is readable without executing scripts, but the identification in this case was due to user awareness.