Free Questions for SY0-601 by certsinside

Shared by Fuentes on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A large industrial system's smart generator monitors the system status and sends alerts to third-party maintenance personnel when critical failures occur. While reviewing the network logs, the company's security manager notices the generator's IP is sending packets to an internal file server's IP. Which of the following mitigations would be best for the security manager to implement while maintaining alerting capabilities?

Options:

A- Segmentation

B- Firewall allow list

C- Containment

D- Isolation

Answer:

A

Explanation:

Segmentation is a security technique that divides a network into smaller subnetworks or segments based on criteria such as function, role, location, etc. Segmentation can help mitigate the risk of unauthorized access or data leakage by isolating different segments from each other and applying different security policies and controls to each segment. Segmentation can help the security manager to implement a mitigation while maintaining alerting capabilities by separating the smart generator from the internal file server and allowing only necessary communication between them.

Question 2

Question Type: **MultipleChoice**

An organization's Chief Security Officer (CSO) wants to validate the business's involvement in the incident response plan to ensure its validity and thoroughness. Which of the following will the CSO most likely use?

Options:

A- An external security assessment

B- A bug bounty program

C- A tabletop exercise

D- A red-team engagement

Answer:

C

Explanation:

A tabletop exercise is a type of simulation exercise that involves discussing hypothetical scenarios and testing the incident response plan in a low-stress environment. A tabletop exercise can help the CSO to validate the business's involvement in the incident response plan by involving key stakeholders, such as senior management, business units, legal department, etc., in the discussion and evaluation of the plan.

Question 3

Question Type: MultipleChoice

A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?

Options:

A- A non-disclosure agreement

B- Least privilege

C- An acceptable use policy

D- Off boarding

Answer:

D

Explanation:

Off boarding is a security practice that involves revoking access rights and privileges from employees who leave an organization or change their roles. Off boarding can help address the issue of successful logon attempts to access the departed executive's accounts by disabling or deleting their accounts, changing passwords, collecting devices, etc., as soon as they leave the organization.

Question 4

Question Type: MultipleChoice

A worldwide manufacturing company has been experiencing email account compromises. In one incident, a user logged in from the corporate office in France, but then seconds later, the same user account attempted a login from Brazil. Which of the following account

policies would best prevent this type of attack?

Options:

A- Network location

B- Impossible travel time

C- Geolocation

D- Geofencing

Answer:

B

Explanation:

Impossible travel time is a security metric that detects anomalous login attempts based on the time and distance between two locations. Impossible travel time can help prevent email account compromises by flagging login attempts that occur within a short time span from locations that are far apart, such as France and Brazil. Impossible travel time can indicate that an attacker has stolen or guessed the user's credentials and is trying to access their email account from another location.

Question 5

Question Type: MultipleChoice

A company's legal department drafted sensitive documents in a SaaS application and wants to ensure the documents cannot be accessed by individuals in high-risk countries. Which of the following is the most effective way to limit this access?

Options:

A- Data masking

B- Encryption

C- Geolocation policy

D- Data sovereignty regulation

Answer:

C

Explanation:

A geolocation policy is a policy that restricts access to data or resources based on the physical location of the user or device. A geolocation policy can be implemented using technologies such as IP address filtering, GPS tracking, VPN blocking, etc. A geolocation policy can help the company's legal department to ensure the documents cannot be accessed by individuals in high-risk countries by

denying access requests from those countries.

Question 6

Question Type: MultipleChoice

Which of the following exercises should an organization use to improve its incident response process?

Options:

A- Tabletop

B- Replication

C- Failover

D- Recovery

Answer:

A

Explanation:

A tabletop exercise is a type of simulation exercise that involves discussing hypothetical scenarios and testing the incident response plan in a low-stress environment. A tabletop exercise can help an organization to improve its incident response process by identifying gaps, weaknesses, roles, responsibilities, communication channels, etc., and by evaluating the effectiveness and efficiency of the plan.

Question 7

Question Type: MultipleChoice

A host was infected with malware. During the incident response. Joe, a user, reported that he did not receive any emails with links, but he had been browsing the internet all day. Which of the following would most likely show where the malware originated?

Options:

A- The DNS logs

B- The web server logs

C- The SIP traffic logs

D- The SNMP logs

Answer:

A

Explanation:

The web server logs are records of the requests and responses that occur between a web server and a web client, such as a browser. The web server logs can show where the malware originated by indicating the source IP address, the destination URL, the date and time, the HTTP status code, the user agent, etc., of each request and response. The web server logs can help the incident response team to trace back the malicious website that infected the host with malware.

Question 8

Question Type: MultipleChoice

An organization suffered numerous multiday power outages at its current location. The Chief Executive Officer wants to create a disaster recovery strategy to resolve this issue. Which of the following options offer low-cost solutions? (Select two).

Options:

A- Warm site

B- Generator

C- Hot site

D- Cold site

E- Cloud backups

F- UPS

Answer:

B, F

Explanation:

A generator and a UPS (uninterruptible power supply) are low-cost solutions that can provide backup power to an organization in case of a power outage. A generator is a device that converts mechanical energy into electrical energy, while a UPS is a device that provides battery power to a system when the main power source fails. A generator and a UPS can help the organization to maintain its operations and prevent data loss during a power outage.