Free Questions for SY0-601 by go4braindumps

Shared by Becker on 05-09-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company recently transitioned to a strictly BYOD culture due to the cost of replacing lost or damaged corporate-owned mobile devices. Which of the following technologies would be BEST to balance the BYOD culture while also protecting the company's data?

Options:

A) Containerization

B) Geofencing

C) Full-disk encryption

D) Remote wipe

Answer:

A

Explanation:

https://www.hexnode.com/blogs/what-is-containerization-and-why-is-it-important-for-your-business/

Question 2

Question Type: **MultipleChoice**

A Chief Security Office's (CSO's) key priorities are to improve preparation, response, and recovery practices to minimize system downtime and enhance organizational resilience to ransomware attacks. Which of the following would BEST meet the CSO's objectives?

Options:

A) Use email-filtering software and centralized account management, patch high-risk systems, and restrict administration privileges on fileshares.

B) Purchase cyber insurance from a reputable provider to reduce expenses during an incident.

C) Invest in end-user awareness training to change the long-term culture and behavior of staff and executives, reducing the organization's susceptibility to phishing attacks.

D) Implement application whitelisting and centralized event-log management, and perform regular testing and validation of full backups.

Answer:

D

Question 3

Question Type: MultipleChoice

A network engineer has been asked to investigate why several wireless barcode scanners and wireless computers in a warehouse have intermittent connectivity to the shipping server. The barcode scanners and computers are all on forklift trucks and move around the warehouse during their regular use. Which of the following should the engineer do to determine the issue? (Choose two.)

Options:

A) Perform a site survey

B) Deploy an FTK Imager

C) Create a heat map

D) Scan for rogue access points

E) Upgrade the security protocols

F) Install a captive portal

Answer:

A, C

Explanation:

heat map and site survey will provide the wifi strength and identify the weakness areas..this will give the opportunity if we need to increase WiFI strength or give suggestion to the forklift drivers about the movement

Question 4

Question Type: **MultipleChoice**

A security administrator suspects an employee has been emailing proprietary information to a competitor. Company policy requires the administrator to capture an exact copy of the employee's hard disk. Which of the following should the administrator use?

Options:

A) dd

B) chmod

C) dnsenum

D) logger

Answer:

A

Question 5

Question Type: **MultipleChoice**

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

Options:

A) SSAE SOC 2

B) PCI DSS

C) GDPR

D) ISO 31000

Answer:

C

Question 6

Question Type: MultipleChoice

A financial organization has adopted a new secure, encrypted document-sharing application to help with its customer loan process. Some important PII needs to be shared across this new platform, but it is getting blocked by the DLP systems. Which of the following actions will BEST allow the PII to be shared with the secure application without compromising the organization's security posture?

Options:

A) Configure the DLP policies to allow all PII

B) Configure the firewall to allow all ports that are used by this application

C) Configure the antivirus software to allow the application

D) Configure the DLP policies to whitelist this application with the specific PII

E) Configure the application to encrypt the PII

Answer:

D

Question 7

Question Type: MultipleChoice

After reading a security bulletin, a network security manager is concerned that a malicious actor may have breached the network using the same software flaw. The exploit code is publicly available and has been reported as being used against other industries in the same vertical. Which of the following should the network security manager consult FIRST to determine a priority list for forensic review?

Options:

A) The vulnerability scan output

B) The IDS logs

C) The full packet capture data

D) The SIEM alerts

Answer:

A

Question 8

Question Type: MultipleChoice

Several employees return to work the day after attending an industry trade show. That same day, the security manager notices several malware alerts coming from each of the employee's workstations. The security manager investigates but finds no signs of an attack on the perimeter firewall or the NIDS. Which of the following is MOST likely causing the malware alerts?

Options:

A) A worm that has propagated itself across the intranet, which was initiated by presentation media

B) A fileless virus that is contained on a vCard that is attempting to execute an attack

C) A Trojan that has passed through and executed malicious code on the hosts

D) A USB flash drive that is trying to run malicious code but is being blocked by the host firewall

Answer:

A

Question 9

Question Type: MultipleChoice

Which of the following would be MOST effective to contain a rapidly attack that is affecting a large number of organizations?

Options:

A) Machine learning

B) DNS sinkhole

C) Blocklist

D) Honeypot

Answer:

D

Question 10

Question Type: **MultipleChoice**

An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?

Options:

A) The system was configured with weak default security settings.

B) The device uses weak encryption ciphers.

C) The vendor has not supplied a patch for the appliance.

D) The appliance requires administrative credentials for the assessment.

Answer:

C

Question 11

Question Type: MultipleChoice

A company's bank has reported that multiple corporate credit cards have been stolen over the past several weeks. The bank has provided the names of the affected cardholders to the company's forensics team to assist in the cyber-incident investigation.

An incident responder learns the following information:

The timeline of stolen card numbers corresponds closely with affected users making Internet-based purchases from diverse websites via enterprise desktop PCs.

All purchase connections were encrypted, and the company uses an SSL inspection proxy for the inspection of encrypted traffic of the hardwired network.

Purchases made with corporate cards over the corporate guest WiFi network, where no SSL inspection occurs, were unaffected.

Which of the following is the MOST likely root cause?

Options:

A) HTTPS sessions are being downgraded to insecure cipher suites

B) The SSL inspection proxy is feeding events to a compromised SIEM

C) The payment providers are insecurely processing credit card charges

D) The adversary has not yet established a presence on the guest WiFi network

Answer:

C

20%
DISCOUNT