D. A complex password policy

Correct Answer: B

QUESTION 340
During an investigation, a security manager receives notification from local authorities mat company proprietary data was found on a former employees home computer. The former employee's corporate workstation has since been repurposed, and the data on the hard drive has been overwritten. Which of the following would BEST provide the security manager with enough details to determine when the data was removed from the company network?

A. Properly congured hosts with security logging
B. Properly congured endpoint security tool with darting
C. Properly congured SIEM with retention policies
D. Properly congured USB blocker with encryption

Correct Answer: D
QUESTION 341
An organization's finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).

A. Corrective
B. Deterrent
C. Preventive
D. Mandatory vacations
E. Job rotation
F. Separation of duties

Correct Answer: DE

QUESTION 342
A recent security audit revealed that a popular website with IP address 172.16.1.5 also has an FTP service that employees were using to store sensitive corporate data. The organization's outbound firewall processes rules top-down. Which of the following would permit HTTP and HTTPS, while denying all other services for this host?

A. access-rule permit tcp destination 172.16.1.5 port 80
   access-rule permit tcp destination 172.16-1-5 port 443
   access-rule deny ip destination 172.16.1.5
B. access-rule permit tcp destination 172.16.1.5 port 22
   access-rule permit tcp destination 172.16.1.5 port 443
   access-rule deny tcp destination 172.16.1.5 port 80
C. access-rule permit tcp destination 172.16.1.5 port 21
   access-rule permit tcp destination 172.16.1.5 port 80
   access-rule deny ip destination 172.16.1.5
D. access-rule permit tcp destination 172.16.1.5 port 80
   access-rule permit tcp destination 172.16.1.5 port 443
   access-rule deny tcp destination 172.16.1.5 port 21

Correct Answer: D

QUESTION 343

Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

A. MSSP
B. Public cloud
C. Hybrid cloud
D. Fog computing

Correct Answer: C

QUESTION 344
After a WiFi scan of a local office was conducted, an unknown wireless signal was identified Upon investigation, an unknown Raspberry Pi device was found connected to an Ethernet port using a single connection. Which of the following BEST describes the purpose of this device?

A. loT sensor
B. Evil twin
C. Rogue access point
D. On-path attack

Correct Answer: C

QUESTION 345
A security analyst needs to find real-time data on the latest malware and loCs. Which of the following best describe the solution the analyst should persue?

A. advisories and bulletins
B. threat feeds
C. security news articles
D. peer-peviewed content

Correct Answer: B

QUESTION 346
A systems administrator reports degraded performance on a virtual server. The administrator increases the virtual memory allocation, which improves conditions, but performance degrades again after a few days The administrator runs an analysis tool and sees the following output:

```
==3214== timeAttend.exe analyzed
==3214== ERROR SUMMARY:
==3214== malloc/free: in use at exit: 4608 bytes in 18 blocks.
==3214== checked 82116 bytes
==3214== definitely lost: 4608 bytes in 18 blocks.
```

The administrator terminates the timeAttend.exe, observes system performance over the next few days and notices that the system performance does not degrade Which of the following issues is MOST likely occurring?

A. DLL injection
B. API attack

C. Buffer overflow
D. Memory leak

Correct Answer: B

QUESTION 347
Which of the following environments utilizes dummy data and is MOST likely to be installed locally on a system that allows code to be assessed directly and modified easily with each build?

A. Production
B. Test
C. Staging
D. Development

Correct Answer: B

QUESTION 348
The board of doctors at a company contracted with an insurance firm to limit the organization's liability. Which of the following risk management practices does the BEST describe?

A. Transference
B. Avoidance
C. Mitigation
D. Acknowledgement

Correct Answer: A

QUESTION 349
Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public. Which of the following security solutions would mitigate the risk of future data disclosures?

A. FDE
B. TPM
C. HIDS
D. VPN

Correct Answer: A

QUESTION 350
A small business office is setting up a wireless infrastructure with primary requirements centered around protecting customer information and preventing unauthorized access to the business network. Which of the following would BEST support the office's business needs? (Select TWO)

A. Installing WAPs with strategic placement
B. Configuring access using WPA3
C. Installing a WIDS
D. Enabling MAC filtering
E. Changing the WiFi password every 30 days
F. Reducing WiFi transmit power throughout the office

Correct Answer: BD

QUESTION 351
A security monitoring company offers a service that alerts ifs customers if their credit cards have been stolen. Which of the following is the MOST likely source of this information?

A. STIX
B. The dark web
C. TAXII
D. Social media
E. PCI

Correct Answer: B

QUESTION 352
A company wants to deploy systems alongside production systems in order to entice threat actors and to learn more about attackers. Which of the following BEST describe these systems?

A. DNS sinkholes
B. Honepots
C. Virtual machines
D. Neural network

Correct Answer: A

QUESTION 353
A security analyst is reviewing the following output from a system:

```
TCP   192.160.10.10:80 192.160.1.2:60101 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60102 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60103 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60104 TIME_WAIT
TCP   192.160.10.10:80 192.160.1.2:60105 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60106 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60107 TIME_WAIT
TCP   192.168.10.10:80 192.168.1.2:60108 TIME_WAIT
TCP   192.160.10.10:80 192.168.1.2:60109 TIME_WAIT
TCP   192.160.10.10:80 192.160.1.2:60110 TIME_WAIT
```

Which of the following is MOST likely being observed?

A. ARP palsoning
B. Man in the middle
C. Denial of service
D. DNS poisoning

Correct Answer: C

QUESTION 354
When implementing automation with loT devices, which of the following should be considered FIRST to keep the network secure?

A. Z-Wave compatibility
B. Network range
C. Zigbee configuration
D. Communication protocols

Correct Answer: D

QUESTION 355
Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?

A. Hashing
B. Salting
C. Integrity
D. Digital signature

Correct Answer: A
Explanation:
https://www.digitalocean.com/community/tutorials/how-to-verify-downloaded-files

Confidentiality = Encryption
Integrity = Hashing
Availability = Redundancy/Resilience

QUESTION 356
A systems analyst is responsible for generating a new digital forensics chain-of-custody form. Which of the following should the analyst include in this documentation? (Choose two.)

A. The order of volatility
B. ACRC32 checksum
C. The provenance of the artifacts
D. The vendor's name
E. The date and time
F. A warning banner

Correct Answer: AE

QUESTION 357
A security forensics analyst is examining a virtual server. The analyst wants to preserve the present state of the virtual server, including memory contents. Which of the following backup types should be used?

A. Snapshot
B. Differential
C. Cloud
D. Full
E. Incremental

Correct Answer: A

QUESTION 358