C. Production
D. Test

Correct Answer: B

QUESTION 453
An application developer accidentally uploaded a company's code-signing certificate private key to a public web server. The company is concerned about malicious use of its certificate. Which of the following should the company do FIRST?

A. Delete the private key from the repository-.
B. Verify the public key is not exposed as well.
C. Update the DLP solution to check for private keys.
D. Revoke the code-signing certificate.

Correct Answer: D

QUESTION 454
The chief compliance officer from a bank has approved a background check policy for all new hires. Which of the following is the policy MOST likely protecting against?

A. Preventing any current employees' siblings from working at the bank to prevent nepotism
B. Hiring an employee who has been convicted of theft to adhere to industry compliance
C. Filtering applicants who have added false information to resumes so they appear better qualified
D. Ensuring no new hires have worked at other banks that may be trying to steal customer information

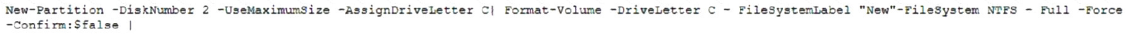
Correct Answer: B

QUESTION 455
As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again. Which of the following would allow the security analyst to alert the SOC if an event is reoccurring?

A. Creating a playbook within the SOAR
B. Implementing rules in the NGFW
C. Updating the DLP hash database
D. Publishing a new CRL with revoked certificates

Correct Answer: A

QUESTION 456
A user downloaded an extension for a browser, and the uses device later became infected. The analyst who is investigating the incident saw various logs where the attacker was hiding activity by deleting data The following was observed running:



```
New-Partition -DiskNumber 2 -UseMaximumSize -AssignDriveLetter C| Format-Volume -DriveLetter C - FileSystemLabel "New"-FileSystem NTFS - Full -Force
-Confirm:$false |
```

Which of the following is the malware using to execute the attack?

A. PowerShell
B. Python
C. Bash
D. Macros

Correct Answer: D

QUESTION 457
A security engineer needs to create a network segment that can be used for servers that require connections from untrusted networks. When of the following should the engineer implement?

A. An air gap
B. A hot site
C. A VLAN
D. A screened subnet

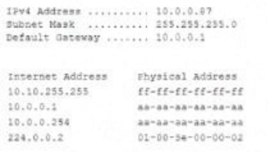
Correct Answer: C

QUESTION 458
Which of the following is the MOST likely reason for securing an air-gapped laboratory HVAC system?

A. To avoid data leakage
B. To protect surveillance logs
C. To ensure availability
D. To restrict remote access

Correct Answer: A

QUESTION 459
A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:



```
IPv4 Address .......... 10.0.0.87
Subnet Mask  .......... 255.255.255.0
Default Gateway ....... 10.0.0.1

Internet Address     Physical Address
10.10.255.255        ff-ff-ff-ff-ff-ff
10.0.0.1             aa-aa-aa-aa-aa-aa
10.0.0.254           aa-aa-aa-aa-aa-aa
224.0.0.2            01-00-5e-00-00-02
```

Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?

A. Denial of service
B. ARP poisoning
C. Command injection
D. MAC flooding

Correct Answer: D

QUESTION 460
Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?

A. Risk matrix
B. Risk tolerance
C. Risk register
D. Risk appetite

Correct Answer: B

QUESTION 461
Several employees have noticed other bystanders can clearly observe a terminal where passcodes are being entered. Which of the following can be eliminated with the use of a privacy screen?

A. Shoulder surfing
B. Spear phishing
C. Impersonation attack
D. Card cloning

Correct Answer: A

QUESTION 462
Multiple business accounts were compromised a few days after a public website had its credentials database leaked on the Internet. No business emails were identified in the breach, but the security team thinks that the list of passwords exposed was later used to compromise business accounts. Which of the following would mitigate the issue?

A. Complexity requirements
B. Password history
C. Acceptable use policy
D. Shared accounts

Correct Answer: B

QUESTION 463
A software company is analyzing a process that detects software vulnerabilities at the earliest stage possible. The goal is to scan the source looking for unsecure practices and weaknesses before the application is deployed in a runtime environment. Which of the following would BEST assist the company with this objective?

A. Use fuzzing testing
B. Use a web vulnerability scanner
C. Use static code analysis
D. Use a penetration-testing OS

Correct Answer: C
Explanation:

Fuzzing
Fuzzing or fuzz testing is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program. The program is then monitored for exceptions such as crashes, failing built-in code assertions, or potential memory leaks.

Static program analysis
Static program analysis is the analysis of computer software performed without executing any programs, in contrast with dynamic analysis, which is performed on programs during their execution. What is static code analysis?
Static code analysis is a method of debugging by examining source code before a program is run . It's done by analyzing a set of code against a set (or multiple sets) of coding rules... This type of analysis addresses weaknesses in source code that might lead to vulnerabilities.

Penetration test
A penetration test, colloquially known as a pen test or ethical hacking, is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system; this is not to be confused with a vulnerability assessment.

QUESTION 464
Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?

A. Whaling
B. Spam
C. Invoice scam
D. Pharming

Correct Answer: D

QUESTION 465
A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?

A. Implementation of preventive controls
B. Implementation of detective controls
C. Implementation of deterrent controls
D. Implementation of corrective controls

Correct Answer: B

QUESTION 466
A security administrator has noticed unusual activity occurring between different global instances and workloads and needs to identify the source of the unusual traffic. Which of the following log sources would be BEST to show the source of the unusual traffic?

A. HIDS
B. UEBA
C. CASB
D. VPC

Correct Answer: C

QUESTION 467
Which biometric error would allow an unauthorized user to access a system?

A. False acceptance
B. False entrance
C. False rejection
D. False denial

Correct Answer: A

QUESTION 468
During an asset inventory, several assets, supplies, and miscellaneous items were noted as missing. The security manager has been asked to find an automated solution to detect any future theft of equipment. Which of the following would be BEST to implement?

A. Badges
B. Fencing
C. Access control vestibule
D. Lighting
E. Cameras

Correct Answer: C

QUESTION 469
A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?

A. BYOD
B. VDI
C. COPE
D. CYOD

Correct Answer: D

QUESTION 470
A systems administrator is troubleshooting a server's connection to an internal web server. The administrator needs to determine the correct ports to use. Which of the following tools BEST shows which ports on the web server are in a listening state?

A. Ipconfig
B. ssh
C. Ping
D. Netstat

Correct Answer: D
Explanation:
https://www.sciencedirect.com/topics/computer-science/listening-port