describes the type of malware the solution should protect against?

A. Worm
B. Logic bomb
C. Fileless
D. Rootkit

Correct Answer: C

QUESTION 43
A company publishes several APIs for customers and is required to use keys to segregate customer data sets. Which of the following would be BEST to use to store customer keys?

A. A trusted platform module
B. A hardware security module
C. A localized key store
D. A public key infrastructure

Correct Answer: B

QUESTION 44
An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:

ERR_SSL_VERSION_OR_CIPHER_MISMATCH

Which of the following is MOST likely the root cause?

A. The client application is testing PFS.
B. The client application is configured to use ECDHE.
C. The client application is configured to use RC4.
D. The client application is configured to use AES-256 in GCM.

Correct Answer: C

QUESTION 45
An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment's notice. Which of the following should the organization consider FIRST to address this requirement?

A. Implement a change management plan to ensure systems are using the appropriate versions.
B. Hire additional on-call staff to be deployed if an event occurs.
C. Design an appropriate warm site for business continuity.
D. Identify critical business processes and determine associated software and hardware requirements.

Correct Answer: C

QUESTION 46
A security engineer was auditing an organization's current software development practice and

discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops. Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.
B. Implement the SDLC security guidelines.
C. Track the library versions and monitor the CVE website for related vulnerabilities.
D. Perform unit testing of the open-source libraries.

Correct Answer: D

QUESTION 47
The goal of a Chief information Security Officer (CISO) providing up-to-date metrics to a bank's risk committee is to ensure:

A. Budgeting for cybersecurity increases year over year.
B. The committee knows how much work is being done.
C. Business units are responsible for their own mitigation.
D. The bank is aware of the status of cybersecurity risks

Correct Answer: A

QUESTION 48
Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours. Based on RPO requirements, which of the following recommendations should the management team make?

A. Leave the current backup schedule intact and pay the ransom to decrypt the data.
B. Leave the current backup schedule intact and make the human resources fileshare read-only.
C. Increase the frequency of backups and create SIEM alerts for IOCs.
D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Correct Answer: C

QUESTION 49
A security engineer needs to recommend a solution that will meet the following requirements:

- Identify sensitive data in the provider's network
- Maintain compliance with company and regulatory guidelines
- Detect and respond to insider threats, privileged user threats, and compromised accounts
- Enforce datacentric security, such as encryption, tokenization, and access control

Which of the following solutions should the security engineer recommend to address these requirements?

A. WAF
B. CASB
C. SWG

D. DLP

Correct Answer: B

QUESTION 50
An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue. Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.
B. Change the operating system.
C. Buy a new server and create an active-active cluster.
D. Upgrade the server with a new one.

Correct Answer: A

QUESTION 51
An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items. Which of the following phases establishes the identification and prioritization of critical systems and functions?

A. Review a recent gap analysis.
B. Perform a cost-benefit analysis.
C. Conduct a business impact analysis.
D. Develop an exposure factor matrix.

Correct Answer: C

QUESTION 52
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

A. Key sharing
B. Key distribution
C. Key recovery
D. Key escrow

Correct Answer: D

QUESTION 53
A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:

- The credentials used to publish production software to the container registry should be stored in a secure location.
- Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly.

Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

A. TPM
B. Local secure password file
C. MFA
D. Key vault

Correct Answer: D

QUESTION 54
Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:

A. when it is passed across a local network.
B. in memory during processing
C. when it is written to a system's solid-state drive.
D. by an enterprise hardware security module.

Correct Answer: A

QUESTION 55
A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	55	2	$2000
June	721	596	120	6	$6000

Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	930	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

Which of the following meets the budget needs of the business?

A. Filter ABC
B. Filter XYZ
C. Filter GHI
D. Filter TUV

Correct Answer: C

QUESTION 56
An engineering team is developing and deploying a fleet of mobile devices to be used for specialized inventory management purposes. These devices should:

- Be based on open-source Android for user familiarity and ease.
- Provide a single application for inventory management of physical assets.
- Permit use of the camera be only the inventory application for the purposes of scanning.
- Disallow any and all configuration baseline modifications.

Restrict all access to any device resource other than those requirement?

A. Set an application wrapping policy, wrap the application, distributes the inventory APK via the

MAM tool, and test the application restrictions.
B. Write a MAC sepolicy that defines domains with rules, label the inventory application, build the policy, and set to enforcing mode.
C. Swap out Android Linux kernel version for >2,4,0, but the internet build Android, remove unnecessary functions via MDL, configure to block network access, and perform integration testing
D. Build and install an Android middleware policy with requirements added, copy the file into/ user/init, and then built the inventory application.

Correct Answer: A

QUESTION 57
Which of the following technologies allows CSPs to add encryption across multiple data storages?

A. Symmetric encryption
B. Homomorphic encryption
C. Data dispersion
D. Bit splitting

Correct Answer: D

QUESTION 58
During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee. Which of the following processes would BEST satisfy this requirement?

A. Monitor camera footage corresponding to a valid access request.
B. Require both security and management to open the door.
C. Require department managers to review denied-access requests.
D. Issue new entry badges on a weekly basis.

Correct Answer: B

QUESTION 59
A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/auth.log:

graphic.ssh_auth_log.

Which of the following actions would BEST address the potential risks by the activity in the logs?

A. Alerting the misconfigured service account password
B. Modifying the AllowUsers configuration directive
C. Restricting external port 22 access
D. Implementing host-key preferences