Correct Answer: B

QUESTION 60
A networking team was asked to provide secure remote access to all company employees. The team decided to use client-to-site VPN as a solution. During a discussion, the Chief Information Security Officer raised a security concern and asked the networking team to route the Internet traffic of remote users through the main office infrastructure. Doing this would prevent remote users from accessing the Internet through their local networks while connected to the VPN. Which of the following solutions does this describe?

A. Full tunneling
B. Asymmetric routing
C. SSH tunneling
D. Split tunneling

Correct Answer: B

QUESTION 61
A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation. Which of the following is the BEST solution to meet these objectives?

A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.
B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.
C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.
D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Correct Answer: B

QUESTION 62
Which of the following are risks associated with vendor lock-in? (Choose two.)

A. The client can seamlessly move data.
B. The vendor can change product offerings.
C. The client receives a sufficient level of service.
D. The client experiences decreased quality of service.
E. The client can leverage a multicloud approach.
F. The client experiences increased interoperability.

Correct Answer: BD

QUESTION 63
A company is implementing SSL inspection. During the next six months, multiple web

applications that will be separated out with subdomains will be deployed. Which of the following will allow the inspection of the data without multiple certificate deployments?

A.   Include all available cipher suites.
B.   Create a wildcard certificate.
C.   Use a third-party CA.
D.   Implement certificate pinning.

Correct Answer: B

QUESTION 64
A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA. Which of the following is the BEST solution?

A.   Deploy an RA on each branch office.
B.   Use Delta CRLs at the branches.
C.   Configure clients to use OCSP.
D.   Send the new CRLs by using GPO.

Correct Answer: C

QUESTION 65
While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware. Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

A.   Pay the ransom within 48 hours.
B.   Isolate the servers to prevent the spread.
C.   Notify law enforcement.
D.   Request that the affected servers be restored immediately.

Correct Answer: B

QUESTION 66
Which of the following represents the MOST significant benefit of implementing a passwordless authentication solution?

A.   Biometric authenticators are immutable.
B.   The likelihood of account compromise is reduced.
C.   Zero trust is achieved.
D.   Privacy risks are minimized.

Correct Answer: B

QUESTION 67
A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack. Which of the following is the NEXT step of the incident response plan?

A. Remediation
B. Containment
C. Response
D. Recovery

Correct Answer: B

QUESTION 68
Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs. Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement rate limiting on the API.
B. Implement geoblocking on the WAF.
C. Implement OAuth 2.0 on the API.
D. Implement input validation on the API.

Correct Answer: A

QUESTION 69
A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:

▪ 22
▪ 25
▪ 110
▪ 137
▪ 138
▪ 139
▪ 445

Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process. Which of the following would be the BEST solution to harden the system?

A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.
B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.
C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.
D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.

Correct Answer: A

QUESTION 70
An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted

in the exposure of the customers' information. Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

A. NIST
B. GDPR
C. PCI DSS
D. ISO

Correct Answer: C

QUESTION 71
The Chief information Officer (CIO) wants to establish a non-banding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership. Which of the follow would MOST likely be used?

A. MOU
B. OLA
C. NDA
D. SLA

Correct Answer: A

QUESTION 72
A security architect is given the following requirements to secure a rapidly changing enterprise with an increasingly distributed and remote workforce:

▪ Cloud-delivered services
▪ Full network security stack
▪ SaaS application security management
▪ Minimal latency for an optimal user experience
▪ Integration with the cloud 1AM platform

Which of the following is the BEST solution?

A. Routing and Remote Access Service (RRAS)
B. NGFW
C. Managed Security Service Provider (MSSP)
D. SASE

Correct Answer: D

QUESTION 73
A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization. Which of the following should be the analyst's FIRST action?

A. Create a full inventory of information and data assets.
B. Ascertain the impact of an attack on the availability of crucial resources.
C. Determine which security compliance standards should be followed.
D. Perform a full system penetration test to determine the vulnerabilities.

Correct Answer: A

QUESTION 74
A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements. Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

A.   Designing data protection schemes to mitigate the risk of loss due to multitenancy
B.   Implementing redundant stores and services across diverse CSPs for high availability
C.   Emulating OS and hardware architectures to blur operations from CSP view
D.   Purchasing managed FIM services to alert on detected modifications to covered data

Correct Answer: D

QUESTION 75
A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line. Which of the following commands would be the BEST to run to view only active Internet connections?

A.   sudo netstat -antu | grep "LISTEN" | awk `{print$5}'
B.   sudo netstat -nlt -p | grep "ESTABLISHED"
C.   sudo netstat -plntu | grep -v "Foreign Address"
D.   sudo netstat -pnut -w | column -t -s $'\w'
E.   sudo netstat -pnut | grep -P ^tcp

Correct Answer: E

QUESTION 76
A company is repeatedly being breached by hackers who valid credentials. The company's Chief information Security Officer (CISO) has installed multiple controls for authenticating users, including biometric and token-based factors. Each successive control has increased overhead and complexity but has failed to stop further breaches. An external consultant is evaluating the process currently in place to support the authentication controls. Which of the following recommendation would MOST likely reduce the risk of unauthorized access?

A.   Implement strict three-factor authentication.
B.   Implement least privilege policies
C.   Switch to one-time or all user authorizations.
D.   Strengthen identify-proofing procedures

Correct Answer: A

QUESTION 77
A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

Test email sent from bp_app01 to external client_app01_mailing_list.