CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

NEW QUESTION 1
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.

Answer: C

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.

NEW QUESTION 2
Ann, a CIRT member, is conducting incident response activities on a network that consists
of several hundred virtual servers and thousands of endpoints and users. The network generates more than 10,000 log messages per second. The enterprise belong to a large, web-based cryptocurrency startup, Ann has distilled the relevant information into an easily digestible report for executive management . However, she still needs to collect evidence of the intrusion that caused the incident. Which of the following should Ann use to gather the required information?

A. Traffic interceptor log analysis
B. Log reduction and visualization tools
C. Proof of work analysis
D. Ledger analysis software

Answer: B

NEW QUESTION 3
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

Answer: B

Explanation:
Reference: https://gdpr.eu/right-to-be- forgotten/#:~:text=Also%20known%20as%20the%20right,to%20delete%20their%20person al%20data.&text=The%20General%20Data%20Protection%20Regulation,collected%2C%2 0processed%2C%20and%20erased
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 References: https://www.comptia.org/blog/what-is-gdpr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 4
A mobile application developer is creating a global, highly scalable, secure chat application. The developer would like to ensure the application is not susceptible to on-path attacks while the user is traveling in potentially hostile regions. Which of the following would BEST achieve that goal?

A. Utilize the SAN certificate to enable a single certificate for all regions.
B. Deploy client certificates to all devices in the network.
C. Configure certificate pinning inside the application.
D. Enable HSTS on the application's server side for all communication.

Answer: C

Explanation:
Certificate pinning is a technique that embeds one or more trusted certificates or public keys inside an application, and verifies that any certificate presented by a server matches one of those certificates or public keys. Certificate pinning can prevent on-path attacks, such as man-in-the-middle (MITM) attacks, which intercept and modify the communication between a client and a server.
Configuring certificate pinning inside the application would allow the mobile application developer to create a global, highly scalable, secure chat application that is not susceptible to on-path attacks while the user is traveling in potentially hostile regions, because it would:
? Ensure that only trusted servers can communicate with the application, by
rejecting any server certificate that does not match one of the pinned certificates or public keys.
? Protect the confidentiality, integrity, and authenticity of the chat messages, by
preventing any attacker from intercepting, modifying, or impersonating them.
? Enhance the security of the application by reducing its reliance on external factors, such as certificate authorities (CAs), certificate revocation lists (CRLs), or online certificate status protocol (OCSP).

NEW QUESTION 5
Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

A. Remote provider BCDR
B. Cloud provider BCDR
C. Alternative provider BCDR
D. Primary provider BCDR

Answer: B

NEW QUESTION 6
An organization is assessing the security posture of a new SaaS CRM system that handles sensitive PI I 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 520,000 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.

Answer: D

NEW QUESTION 7
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.

Answer: D

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.

NEW QUESTION 8
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.

Answer: C

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 References: https://www.comptia.org/blog/what-is-impossible- travel https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 9
A new requirement for legislators has forced a government security team to develop a validation process to verify the integrity of a downloaded file and the sender of the file Which of the following is the BEST way for the security team to comply with this requirement?

A. Digital signature
B. Message hash
C. Message digest
D. Message authentication code

Answer: A

Explanation:

A digital signature is a cryptographic technique that allows the sender of a file to sign it with their private key and the receiver to verify it with the sender's public key. This ensures the integrity and authenticity of the file, as well as the non-repudiation of the sender. A message hash or a message digest is a one-way function that produces a fixed- length output from an input, but it does not provide any information about the sender. A message authentication code (MAC) is a symmetric-key technique that allows both the sender and the receiver to generate and verify a code using a shared secret key, but it does not provide non-repudiation. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.1: Apply cryptographic techniques

NEW QUESTION 10
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.

Answer: A

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 References: https://www.comptia.org/blog/what-is-rate-limiting https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 10
The Chief information Security Officer (CISO) of a small locate bank has a compliance requirement that a third-party penetration test of the core banking application must be conducted annually. Which of the following services would fulfill the compliance requirement with the LOWEST resource usage?

A. Black-box testing
B. Gray-box testing
C. Red-team hunting
D. White-box testing
E. Blue-learn exercises

Answer: C

NEW QUESTION 12
A security engineer needs to recommend a solution that will meet the following requirements:
Identify sensitive data in the provider's network
Maintain compliance with company and regulatory guidelines
Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control
Which of the following solutions should the security engineer recommend to address these requirements?

A. WAF
B. CASB
C. SWG
D. DLP

Answer: D

Explanation:
DLP (data loss prevention) is a solution that can meet the following requirements: identify sensitive data in the provider's network, maintain compliance with company and regulatory guidelines, detect and respond to insider threats, privileged user threats, and compromised accounts, and enforce data-centric security, such as encryption, tokenization, and access control. DLP can monitor, classify, and protect data in motion, at rest, or in use, and prevent unauthorized disclosure or exfiltration. WAF (web application firewall) is a solution that can protect web applications from common attacks, such as SQL injection or cross-site scripting, but it does not address the requirements listed. CASB (cloud access security broker) is a solution that can enforce policies and controls for accessing cloud services and applications, but it does not address the requirements listed. SWG (secure web gateway) is a solution that can monitor and filter web traffic to prevent malicious or unauthorized access, but it does not address the requirements listed. Verified References: https://www.comptia.org/blog/what-is-data-loss-prevention https://partners.comptia.org/docs/default-source/resources/casp-content-guid

NEW QUESTION 14
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

Answer: D

NEW QUESTION 17
A security compliance requirement states that specific environments that handle sensitive data must be protected by need-to-know restrictions and can only connect to authorized endpoints. The requirement also states that a DLP solution within the environment must be used to control the data from leaving the environment.
Which of the following should be implemented for privileged users so they can support the environment from their workstations while remaining compliant?

A. NAC to control authorized endpoints
B. FIM on the servers storing the data
C. A jump box in the screened subnet
D. A general VPN solution to the primary network

Answer: A

Explanation:
Network Access Control (NAC) is used to bolster the network security by
restricting the availability of network resources to managed endpoints that don't satisfy the compliance requirements of the Organization.

NEW QUESTION 21
An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:
• Some developers can directly publish code to the production environment.
• Static code reviews are performed adequately.
• Vulnerability scanning occurs on a regularly scheduled basis per policy.
Which of the following should be noted as a recommendation within the audit report?

A. Implement short maintenance windows.
B. Perform periodic account reviews.
C. Implement job rotation.
D. Improve separation of duties.

Answer: D

NEW QUESTION 26
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

Answer: C

Explanation:
Reference: https://source.android.com/security/selinux/customize
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. References:
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

NEW QUESTION 31
An organization established an agreement with a partner company for specialized help desk services. A senior security officer within the organization Is tasked with providing documentation required to set up a dedicated VPN between the two entities. Which of the following should be required?

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

Answer: B

Explanation:
An ISA, or interconnection security agreement, is a document that should be required to set up a dedicated VPN between two entities that provide specialized help desk services. An ISA defines the technical and security requirements for establishing, operating, and maintaining a secure connection between two or more organizations. An ISA also specifies the roles and responsibilities of each party, the security controls and policies to be implemented, the data types and classifications to be exchanged, and the incident response procedures to be followed.
References: [CompTIA CASP+ Study Guide, Second Edition, page 36]

NEW QUESTION 32
A company that all mobile devices be encrypted, commensurate with the full disk encryption scheme of assets, such as workstation, servers, and laptops. Which of the following will MOST likely be a limiting factor when selecting mobile device managers for the company?

A. Increased network latency

B. Unavailable of key escrow
C. Inability to selected AES-256 encryption
D. Removal of user authentication requirements

Answer: C

Explanation:
The inability to select AES-256 encryption will most likely be a limiting factor when selecting mobile device managers for the company. AES-256 is a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. It is considered one of the strongest encryption methods available and is widely used for securing sensitive data. Mobile device managers are software applications that allow administrators to remotely manage and secure mobile devices used by employees. However, not all mobile device managers may support AES-256 encryption or allow the company to enforce it as a policy on all mobile devices. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://searchmobilecomputing.techtarget.com/definition/mobile-device-management

NEW QUESTION 35
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.

Answer: D

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. References: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 10, Investigating Intrusions and Suspicious Activity.

NEW QUESTION 37
The Chief information Officer (CIO) wants to establish a non-banding agreement with a third party that outlines the objectives of the mutual arrangement dealing with data transfers between both organizations before establishing a format partnership. Which of the follow would MOST likely be used?

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

Answer: A

NEW QUESTION 40
A system administrator at a medical imaging company discovers protected health information (PHI) on a general-purpose file server. Which of the following steps should the administrator take NEXT?

A. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2.
B. Take an MD5 hash of the server.
C. Delete all PHI from the network until the legal department is consulted.
D. Consult the legal department to determine the legal requirements.

Answer: A

NEW QUESTION 43
A security architect is reviewing the following proposed corporate firewall architecture and configuration:

```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:
Web servers must receive all updates via HTTP/S from the corporate network. Web servers should not initiate communication with the Internet.
Web servers should only connect to preapproved corporate database servers.
Employees' computing devices should only connect to web services over ports 80 and 443. Which of the following should the architect recommend to ensure all requirements are met

in the MOST secure manner? (Choose two.)

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443
B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP80,443
C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535
E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0- 65535
F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Answer: AD

NEW QUESTION 44
The Chief Information Security Officer is concerned about the possibility of employees downloading 'malicious files from the internet and 'opening them on corporate workstations. Which of the following solutions would be BEST to reduce this risk?

A. Integrate the web proxy with threat intelligence feeds.
B. Scan all downloads using an antivirus engine on the web proxy.
C. Block known malware sites on the web proxy.
D. Execute the files in the sandbox on the web proxy.

Answer: D

Explanation:
Executing the files in the sandbox on the web proxy is the best solution to reduce the risk of employees downloading and opening malicious files from the internet. A sandbox is a secure and isolated environment that can run untrusted or potentially harmful code without affecting the rest of the system. By executing the files in the sandbox, the web proxy can analyze their behavior and detect any malicious activity before allowing them to reach the corporate workstations.
References: [CompTIA CASP+ Study Guide, Second Edition, page 273]

NEW QUESTION 45
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.

Answer: D

NEW QUESTION 48
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

Answer: B

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.

NEW QUESTION 52
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.

Answer: C

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 References: https://www.comptia.org/blog/what-is-rpo https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 54
A cybersecurity analyst created the following tables to help determine the maximum budget amount the business can justify spending on an improved email filtering system:

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	55	2	$2000
June	721	598	120	6	$6000

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

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

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

Answer: B

Explanation:
Filter XYZ is the best option that meets the budget needs of the business. Filter XYZ has an ALE of $1 million per year, which is lower than any other filter option. ALE stands for annualized loss expectancy, which is a measure of how much money a business can expect to lose due to a risk over a year. ALE is calculated by multiplying the annualized rate of occurrence (ARO) of an event by the single loss expectancy (SLE) of an event. ARO is how often an event is expected to occur in a year. SLE is how much money an event will cost each time it occurs. Therefore, ALE = ARO x SLE. Filter XYZ has an ARO of 0.1 and an SLE of $10 million, so ALE = 0.1 x $10 million = $1 million. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.techopedia.com/definition/24771/annualized-loss-expectancy-ale

NEW QUESTION 58
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

Answer: E

Explanation:
Reference: https://www.codegrepper.com/code-examples/shell/netstat+find+port
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). References: 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

NEW QUESTION 59

Which of the following testing plans is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions?

A. Disaster recovery checklist
B. Tabletop exercise
C. Full interruption test
D. Parallel test

Answer: B

Explanation:
A tabletop exercise is a type of testing plan that is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions. A tabletop exercise is a simulation of a potential disaster or incident that involves a verbal or written discussion of how each department would respond to it. The purpose of a tabletop exercise is to identify gaps, weaknesses, or conflicts in the disaster recovery plan, and to improve communication and coordination among the team members.
References: [CompTIA CASP+ Study Guide, Second Edition, page 455]

NEW QUESTION 60
A company just released a new video card. Due to limited supply and nigh demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's Intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems. Which of the following now describes the level of risk?

A. Inherent Low
B. Mitigated
C. Residual
D. Transferred

Answer: A

NEW QUESTION 61
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 3.10 seconds
```

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

Answer: A

NEW QUESTION 64
A networking team was asked to provide secure remote access to all company employees. The team decided to use client-to-site VPN as a solution. During a discussion, the Chief Information Security Officer raised a security concern and asked the networking team to route the Internet traffic of remote users through the main office infrastructure. Doing this would prevent remote users from accessing the Internet through their local networks while connected to the VPN.
Which of the following solutions does this describe?

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

Answer: A

Explanation:
The concern is users operating in a spit tunnel config which is what is being described. Using a Full Tunnel would route traffic from all applications through a single tunnel. https://cybernews.com/what-is-vpn/split-tunneling/

NEW QUESTION 65
A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.
The technician will define this threat as:

A. a decrypting RSA using obsolete and weakened encryption attack.
B. a zero-day attack.

C. an advanced persistent threat.
D. an on-path attack.

Answer: C

Explanation:
Reference: https://www.internetsociety.org/deploy360/tls/basics/
An advanced persistent threat (APT) is a type of cyberattack that involves a stealthy and continuous process of compromising and exploiting a target system or network. An APT typically has a specific goal or objective, such as stealing sensitive data, disrupting operations, or sabotaging infrastructure. An APT can use various techniques to evade detection and maintain persistence, such as encryption, proxy servers, malware, etc. The scenario described in the question matches the characteristics of an APT. References: https://www.cisco.com/c/en/us/products/security/what-is-apt.html https://www.imperva.com/learn/application-security/advanced-persistent-threat-apt/

NEW QUESTION 66
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

Answer: C

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.”

NEW QUESTION 67
A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability.
Which of the following would BEST resolve and mitigate the issue? (Select TWO).

A. Deploying a WAF signature
B. Fixing the PHP code
C. Changing the web server from HTTPS to HTTP
D. UsingSSLv3
E. Changing the code from PHP to ColdFusion
F. Updating the OpenSSL library

Answer: AF

Explanation:
Deploying a web application firewall (WAF) signature is a way to detect and block attempts to exploit the Heartbleed vulnerability on the web server. A WAF signature is a pattern that matches a known attack vector, such as a malicious heartbeat request. By deploying a WAF signature, the company can protect its web application from Heartbleed attacks until the underlying vulnerability is fixed.
Updating the OpenSSL library is the ultimate way to fix and mitigate the Heartbleed vulnerability. The OpenSSL project released version 1.0.1g on April 7, 2014, which patched the bug by adding a bounds check to the heartbeat function. By updating the OpenSSL library on the web server, the company can eliminate the vulnerability and prevent any future exploitation.
* B. Fixing the PHP code is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not in the PHP code, but in the OpenSSL library that handles the SSL/TLS encryption for the web server.
* C. Changing the web server from HTTPS to HTTP is not a way to resolve or mitigate the Heartbleed vulnerability, because it would expose all the web traffic to eavesdropping and tampering by attackers. HTTPS provides confidentiality, integrity, and authentication for web communications, and should not be disabled for security reasons.
* D. Using SSLv3 is not a way to resolve or mitigate the Heartbleed vulnerability, because SSLv3 is an outdated and insecure protocol that has been deprecated and replaced by TLS. SSLv3 does not support modern cipher suites, encryption algorithms, or security features, and is vulnerable to various attacks, such as POODLE.
* E. Changing the code from PHP to ColdFusion is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not related to the programming language of the web application, but to the OpenSSL library that handles the SSL/TLS encryption for the web server.
https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug https://heartbleed.com/

NEW QUESTION 72
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.

Answer: A

NEW QUESTION 73
A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization. The legal department provided the security team with a list of search terms to investigate.
This is an example of:

A. due intelligence
B. e-discovery.
C. due care.
D. legal hold.

Answer: A

Explanation:
Reference: https://www.ansarada.com/due-diligence/hr

NEW QUESTION 76
A small business would like to provide guests who are using mobile devices encrypted WPA3 access without first distributing PSKs or other credentials. Which of the following features will enable the business to meet this objective?

A. Simultaneous Authentication of Equals
B. Enhanced open
C. Perfect forward secrecy
D. Extensible Authentication Protocol

Answer: A

NEW QUESTION 78
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

Answer: C

NEW QUESTION 80
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

Answer: B

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 References: https://www.comptia.org/blog/what-is-aslr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 84
An organization is running its e-commerce site in the cloud. The capacity is sufficient to meet the organization's needs throughout most of the year, except during the holidays when the organization plans to introduce a new line of products and expects an increase in traffic. The organization is not sure how well its products will be received. To address this issue, the organization needs to ensure that:
* System capacity is optimized.
* Cost is reduced.
Which of the following should be implemented to address these requirements? (Select
TWO).

A. Containerization
B. Load balancer
C. Microsegmentation
D. Autoscaling
E. CDN
F. WAF

Answer: BD

Explanation:
Load balancer and autoscaling are the solutions that should be implemented to address the requirements of optimizing system capacity and reducing cost for an e-

commerce site in the cloud. A load balancer is a device or service that distributes incoming network traffic across multiple servers or instances based on various criteria, such as availability, performance, or location. A load balancer can improve system capacity by balancing the workload and preventing overloading or underutilization of resources. Autoscaling is a feature that allows cloud services to automatically adjust the number of servers or instances based on the demand or predefined rules. Autoscaling can reduce cost by scaling up or down the resources as needed, avoiding unnecessary expenses or wastage. References: [CompTIA CASP+ Study Guide, Second Edition, pages 406-407 and 410]

NEW QUESTION 89
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.

Answer: D

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 References: https://www.comptia.org/blog/what-is-deception-technology https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 92
A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.
Which of the following should the engineer report as the ARO for successful breaches?

A. 0.5
B. 8
C. 50
D. 36,500

Answer: A

Explanation:
Reference: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative- risk-analysis/
The ARO (annualized rate of occurrence) for successful breaches is the number of times an event is expected to occur in a year. To calculate the ARO for successful breaches, the engineer can divide the number of breaches by the number of years. In this case, the company's data has been breached two times in four years, so the ARO is 2 / 4 = 0.5. The other options are incorrect calculations. Verified References: https://www.comptia.org/blog/what-is-risk-management https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 94
A company recently deployed a SIEM and began importing logs from a firewall, a file server, a domain controller a web server, and a laptop. A security analyst receives a series of SIEM alerts and prepares to respond. The following is the alert information:

Severity	Source device	Event info	Time (UTC)
Medium	abc-usa-fw01	RDP (3389) traffic from abc-admin-lp01 to abc-usa-fs1	1020:08
Low	abc-ger-dc1	Successful logon event for user jdoe on abc-usa-fs1	1020:34
Medium	abc-ger-fw01	RDP (3389) traffic from abc-usa-fs1 to abc-ger-fs1	1021:02
Low	abc-usa-fw01	SMB (445) traffic from abc-usa-fs1 to abc-web01	1020:51
Low	abc-usa-dc1	Successful logon event for user jdoe on abc-ger-fs1	1024:55
High	abc-usa-fw01	FTP (21) traffic from abc-ger-fs1 to abc-web01	1025:16
High	abc-web01	Successful logon event for user Administrator	1126:40

Which of the following should the security analyst do FIRST?

A. Disable Administrator on abc-uaa-fsl, the local account is compromised
B. Shut down the abc-usa-fsl server, a plaintext credential is being used
C. Disable the jdoe account, it is likely compromised
D. Shut down abc-usa-fw01; the remote access VPN vulnerability is exploited

Answer: C

Explanation:

Based on the SIEM alerts, the security analyst should first disable the jdoe account, as it is likely compromised by an attacker. The alerts show that the jdoe account successfully logged on to the abc-usa-fsl server, which is a file server, and then initiated SMB (445) traffic to the abc-web01 server, which is a web server. This indicates that the attacker may be trying to exfiltrate data from the file server to the web server. Disabling the jdoe account would help stop this unauthorized activity and prevent further damage.
Disabling Administrator on abc-usa-fsl, the local account is compromised, is not the first action to take, as it is not clear from the alerts if the local account is compromised or not. The alert shows that there was a successful logon event for Administrator on abc-usa-fsl, but it does not specify if it was a local or domain account, or if it was authorized or not. Moreover, disabling the local account would not stop the SMB traffic from jdoe to abc- web01.
Shutting down the abc-usa-fsl server, a plaintext credential is being used, is not the first action to take, as it is not clear from the alerts if a plaintext credential is being used or not. The alert shows that there was RDP (3389) traffic from abc-admin1-logon to abc-usa-fsl, but it does not specify if the credential was encrypted or not. Moreover, shutting down the file server would disrupt its normal operations and affect other users.
Shutting down abc-usa-fw01; the remote access VPN vulnerability is exploited, is not the first action to take, as it is not clear from the alerts if the remote access VPN vulnerability is exploited or not. The alert shows that there was FTP (21) traffic from abc-usa-dcl to abc- web01, but it does not specify if it was related to the VPN or not. Moreover, shutting down the firewall would expose the network to other threats and affect other
services. References: What is SIEM? | Microsoft Security, What is a SIEM Alert? | Cofense

NEW QUESTION 99
A company security engineer arrives at work to face the following scenario:
1) Website defacement
2) Calls from the company president indicating the website needs to be fixed Immediately because It Is damaging the brand
3) A Job offer from the company's competitor
4) A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data
Which of the following threat actors Is MOST likely involved?

A. Organized crime
B. Script kiddie
C. APT/nation-state
D. Competitor

Answer: C

Explanation:
An Advanced Persistent Threat (APT) is an attack that is targeted, well-planned, and conducted over a long period of time by a nation-state actor. The evidence provided in the scenario indicates that the security analyst has identified a foreign adversary, which is strong evidence that an APT/nation-state actor is responsible for the attack. Resources: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 5: “Advanced Persistent Threats,” Wiley, 2018.
https://www.wiley.com/en- us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition
-p-9781119396582

NEW QUESTION 102
Company A is establishing a contractual with Company B. The terms of the agreement are formalized in a document covering the payment terms, limitation of liability, and intellectual property rights. Which of the following documents will MOST likely contain these elements

A. Company A-B SLA v2.docx
B. Company A OLA v1b.docx
C. Company A MSA v3.docx
D. Company A MOU v1.docx
E. Company A-B NDA v03.docx

Answer: C

Explanation:
A MSA stands for master service agreement, which is a document that covers the general terms and conditions of a contractual relationship between two parties. It usually includes payment terms, limitation of liability, intellectual property rights, dispute resolution, and other clauses that apply to all services provided by one party to another. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://www.upcounsel.com/master-service-agreement

NEW QUESTION 106
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

Answer: D

Explanation:
Reference: https://searchsecurity.techtarget.com/definition/cryptanalysis
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. References: https://www.ibm.com/security/homomorphic-encryption
https://www.synopsys.com/blogs/software-security/homomorphic-encryption/

NEW QUESTION 109
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. Noexecute

C. Total memory encryption
D. Virtual memory protection

Answer: A

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. Execute never (also known as XN or NX) is a feature that marks certain memory regions as non-executable, meaning that they cannot be used to run code. This prevents malware from exploiting buffer overflows or other memory corruption vulnerabilities to inject malicious code into another process' memory space.
References: [CompTIA CASP+ Study Guide, Second Edition, page 295]

NEW QUESTION 114
A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.
Which of the following BEST describes the type of malware the solution should protect against?

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

Answer: C

Explanation:
Reference: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital- threats/tracking-detecting-and-thwarting-powershell-based-malware-and-attacks

NEW QUESTION 117
A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?

A. Community cloud service model
B. Multinency SaaS
C. Single-tenancy SaaS
D. On-premises cloud service model

Answer: C

Explanation:
A single-tenancy SaaS solution is the best solution for this company. SaaS stands for software as a service, which is a cloud-based model that allows customers to access applications hosted by a provider over the internet. A single-tenancy SaaS solution means that the company has its own dedicated instance of the application and its underlying infrastructure, which offers more control, customization, and security than a multi-tenancy SaaS solution where multiple customers share the same resources. A single- tenancy SaaS solution also eliminates the need for managing a private cloud or an on- premises infrastructure. Verified
References: https://www.comptia.org/training/books/casp- cas-004-study-guide , https://www.ibm.com/cloud/learn/saas

NEW QUESTION 121
A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.
Which of the following should the security administrator do to mitigate the risk?

A. Explain to the networking team the reason Flash is no longer available and insist the team move up the timetable for replacement.
B. Air gap the legacy system from the network and dedicate a laptop with an end-of-life OS on it to connect to the system via crossover cable for management.
C. Suggest that the networking team contact the original embedded system's vendor to get an update to the system that does not require Flash.
D. Isolate the management interface to a private VLAN where a legacy browser in a VM can be used as needed to manage the system.

Answer: D

NEW QUESTION 126
Which of the following represents the MOST significant benefit of implementing a passwordless authentication solution?

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

Answer: B

Explanation:
Reference: https://cloudworks.no/en/5-benefits-of-passwordless-authentication/

NEW QUESTION 131
As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents.
Which of the following BEST describes this kind of risk response?

A. Risk rejection
B. Risk mitigation
C. Risk transference
D. Risk avoidance

Answer: C

NEW QUESTION 136
A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:
22
25
110
137
138
139
445
Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.
Which of the following would be the BEST solution to harden the system?

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

Answer: A

NEW QUESTION 140
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

Answer: D

NEW QUESTION 141
A new, online file hosting service is being offered. The service has the following security requirements:
• Threats to customer data integrity and availability should be remediated first.
• The environment should be dynamic to match increasing customer demands.
• The solution should not interfere with customers" ability to access their data at anytime.
• Security analysts should focus on high-risk items.
Which of the following would BEST satisfy the requirements?

A. Expanding the use of IPS and NGFW devices throughout the environment
B. Increasing the number of analysts to Identify risks that need remediation
C. Implementing a SOAR solution to address known threats
D. Integrating enterprise threat feeds in the existing SIEM

Answer: C

Explanation:
A SOAR (Security Orchestration, Automation, and Response) solution is a software platform that can automate the detection and response of known threats, such as ransomware, phishing, or denial-of-service attacks. A SOAR solution can also integrate with other security tools, such as IPS, NGFW, SIEM, and threat feeds, to provide a comprehensive and dynamic security posture. A SOAR solution would best satisfy the requirements of the online file hosting service, because it would:
? Remediate threats to customer data integrity and availability first, by automatically
applying predefined actions or workflows based on the severity and type of the threat.
? Allow the environment to be dynamic to match increasing customer demands, by
scaling up or down the security resources and processes as needed.
? Not interfere with customers' ability to access their data at anytime, by minimizing the human intervention and downtime required for threat response.
? Enable security analysts to focus on high-risk items, by reducing the manual tasks and alert fatigue associated with threat detection and response.
Reference: CASP+ (Plus) CompTIA Advanced Security Practitioner Certification …

NEW QUESTION 144
A company provides guest WiFi access to the internet and physically separates the guest network from the company's internal WIFI. Due to a recent incident in which an attacker gained access to the compay's intend WIFI, the company plans to configure WPA2 Enterprise in an EAP- TLS configuration. Which of the following must be installed on authorized hosts for this new configuration to work properly?

A. Active Directory OPOs
B. PKI certificates
C. Host-based firewall
D. NAC persistent agent

Answer: B

NEW QUESTION 145
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

Answer: B

Explanation:
Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe

NEW QUESTION 149
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

Answer: C

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.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 5:
Security Testing, Section 5.4: Defining Scope and Objective.

NEW QUESTION 150
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.

Answer: A

Explanation:
Reference: https://docs.rapid7.com/insightvm/elevating-permissions/
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 References: https://www.comptia.org/blog/what-is-post-exploitation
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 155
A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility.
Which of the following systems should the consultant review before making a recommendation?

A. CAN
B. ASIC
C. FPGA
D. SCADA

Answer: D

Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/protective-relay

NEW QUESTION 157
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.

Answer: A

Explanation:
Reference: https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa- ecdsa-are-there-easy-answers-for-which-to-choose-when

NEW QUESTION 161
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.

Answer: A

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.

NEW QUESTION 162
A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack.
Which of the following is t he NEXT step of the incident response plan?

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

Answer: B

Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/containment-strategy

NEW QUESTION 164
A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form? (Select TWO.)

A. Text editor
B. OOXML editor
C. Event Viewer
D. XML style sheet
E. SCAP tool
F. Debugging utility

Answer: BD

NEW QUESTION 166
A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and

do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

Which of the following should the security analyst perform?

A. Contact the security department at the business partner and alert them to the email event.
B. Block the IP address for the business partner at the perimeter firewall.
C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
D. Configure the email gateway to automatically quarantine all messages originating from the business partner.

Answer: A

Explanation:
The best option for the security analyst to perform is to contact the security department at the business partner and alert them to the email event. The email appears to be a phishing attempt that tries to trick the employees into revealing their login credentials by impersonating a legitimate sender. The security department at the business partner should be notified so they can investigate the source and scope of the attack and take appropriate actions to protect their systems and users. Verified References: https://www.comptia.org/training/books/casp-cas-004-study-guide , https://us-cert.cisa.gov/ncas/tips/ST04-014

NEW QUESTION 168
An analyst execute a vulnerability scan against an internet-facing DNS server and receives the following report:

```
* Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege
* SSL Medium Strength Cipher Suites Supported
* Vulnerability in DNS Resolution Could Allow Remote Code Execution
* SMB Host SIDs allows Local User Enumeration
```

Which of the following tools should the analyst use FIRST to validate the most critical vulnerability?

A. Password cracker
B. Port scanner
C. Account enumerator
D. Exploitation framework

Answer: A

NEW QUESTION 169
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

Answer: D

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 References: https://www.comptia.org/blog/what-is-integrity
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 170
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

Answer: A

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 References: https://www.comptia.org/blog/what- is-a-tpm-trusted-platform-module https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 175
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

Answer: B

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 decoys 13.
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.

NEW QUESTION 179
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

Answer: D

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. References: https://www.techopedia.com/definition/1772/key-escrow
https://searchsecurity.techtarget.com/definition/key-escrow

NEW QUESTION 182
A mobile administrator is reviewing the following mobile device DHCP logs to ensure the proper mobile settings are applied to managed devices:

```
10,10/18/2021,17:01:05,Assign,192.168.1.10,UserA-MobileDevice,0236FB12CA0B
23,10/19/2021,07:11:19,Assign,192.168.1.23,UserA-MobileDevice,068ADIFAB109
10,10/20/2021,19:22:56,Assign,192.168.1.96,UserA-MobileDevice,0ABC65E81AB0
0,10/21/2021,22:34:15,Assign,192.168.1.33,UserA-MobileDevice,BAC034EF9451
10,10/22/2021,11:55:41,Assign,192.168.1.12,UserA-MobileDevice,0E938663221B
```

Which of the following mobile configuration settings is the mobile administrator verifying?

A. Service set identifier authentication
B. Wireless network auto joining
C. 802.1X with mutual authentication
D. Association MAC address randomization

Answer: B

Explanation:
Wireless network auto joining is the mobile configuration setting that the mobile administrator is verifying by reviewing the mobile device DHCP logs. Wireless network auto joining is a feature that allows mobile devices to automatically connect to a predefined wireless network without requiring user intervention or authentication. This can be useful for corporate or trusted networks that need frequent access by mobile devices. The DHCP logs show that the mobile devices are assigned IP addresses from the wireless network with SSID "CorpWiFi", which indicates that they are auto joining this network. References: [CompTIA CASP+ Study Guide, Second Edition, page 420]

NEW QUESTION 186
A cloud security architect has been tasked with selecting the appropriate solution given the following:
* The solution must allow the lowest RTO possible.
* The solution must have the least shared responsibility possible.
« Patching should be a responsibility of the CSP.
Which of the following solutions can BEST fulfill the requirements?

A. Paas
B. laas
C. Private

D. Saas

Answer: D

Explanation:
SaaS, or software as a service, is the solution that can best fulfill the requirements of having the lowest RTO possible, the least shared responsibility possible, and patching as a responsibility of the CSP. SaaS is a cloud service model that provides users with access to software applications hosted and managed by the CSP over the internet. SaaS has the lowest RTO (recovery time objective), which is the maximum acceptable time for restoring a system or service after a disruption, because it does not require any installation, configuration, or maintenance by the users. SaaS also has the least shared responsibility possible because most of the security aspects are handled by the CSP, such as patching, updating, backup, encryption, authentication, etc.
References: [CompTIA CASP+ Study Guide, Second Edition, pages 403-404]

NEW QUESTION 190
Which of the following agreements includes no penalties and can be signed by two entities that are working together toward the same goal?

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

Answer: A

NEW QUESTION 194
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.

Answer: C

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.

NEW QUESTION 195
Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts partial 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. laaS
B. SaaS
C. FaaS
D. PaaS

Answer: D

NEW QUESTION 200
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

Answer: C

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 References:
? https://www.manageengine.com/data-security/what-is/byod.html
? https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate

NEW QUESTION 201
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.

Answer: A

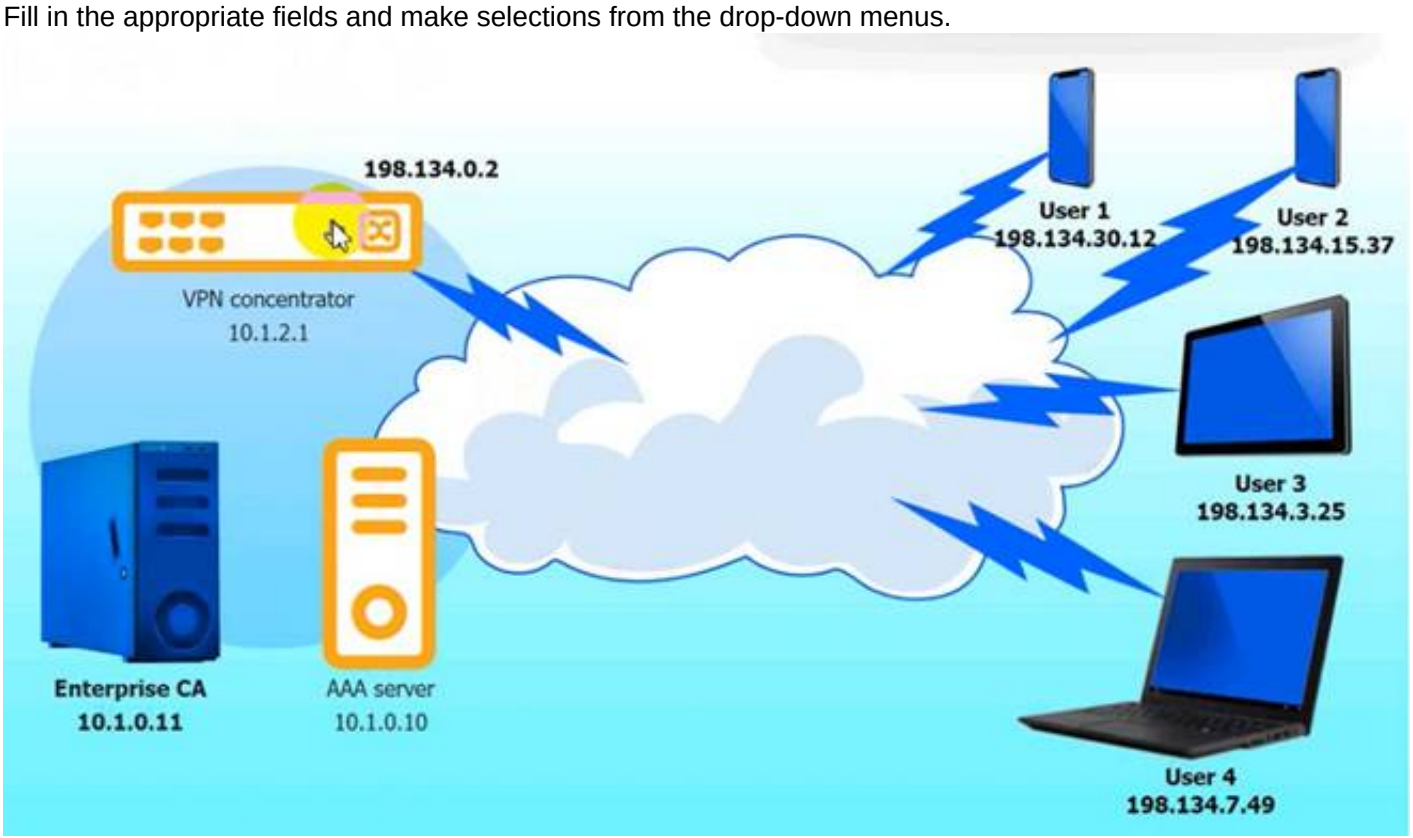
NEW QUESTION 203
A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.
Which of the following should be modified to prevent the issue from reoccurring?

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

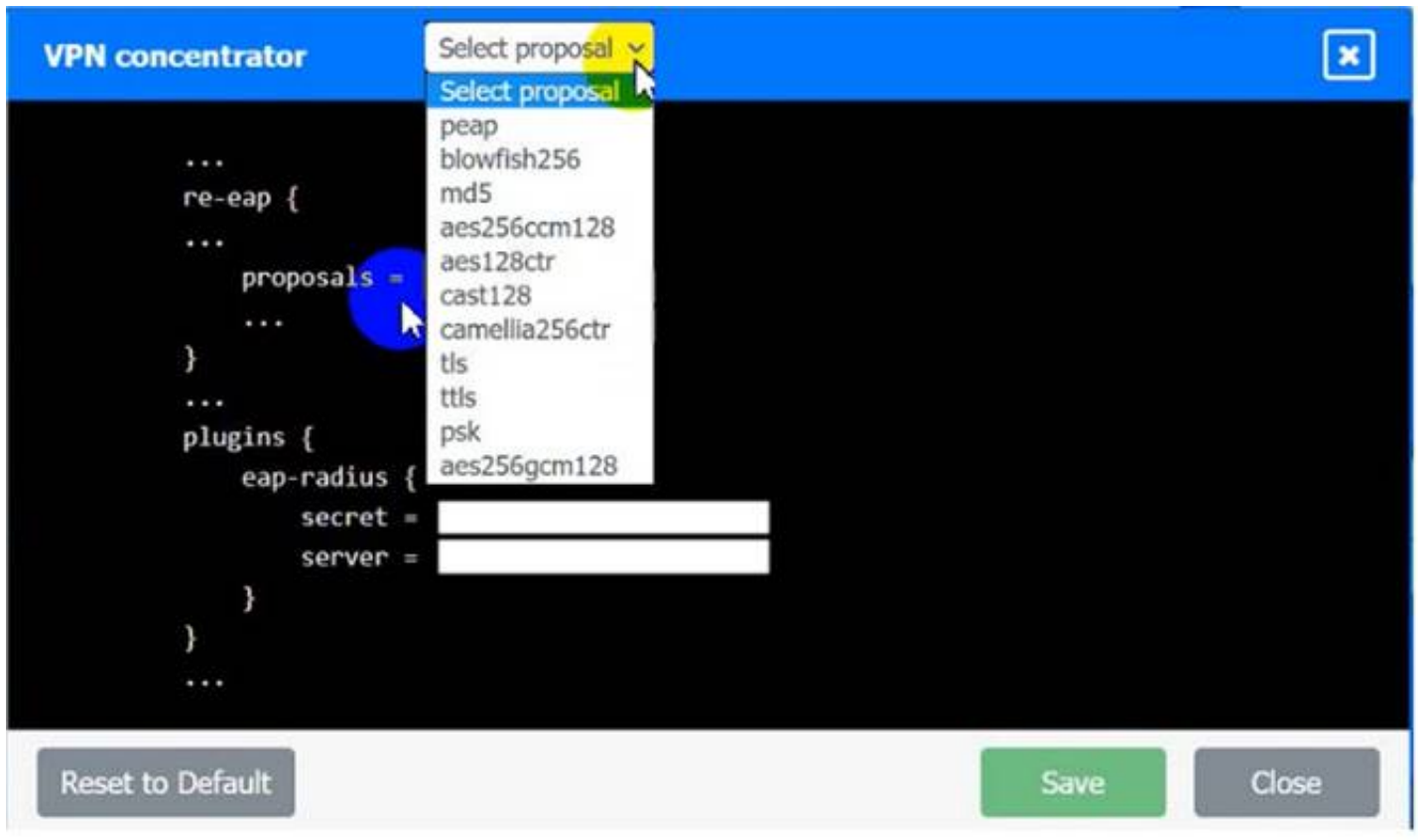
Answer: D

Explanation:
Reference: https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/
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. References: 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

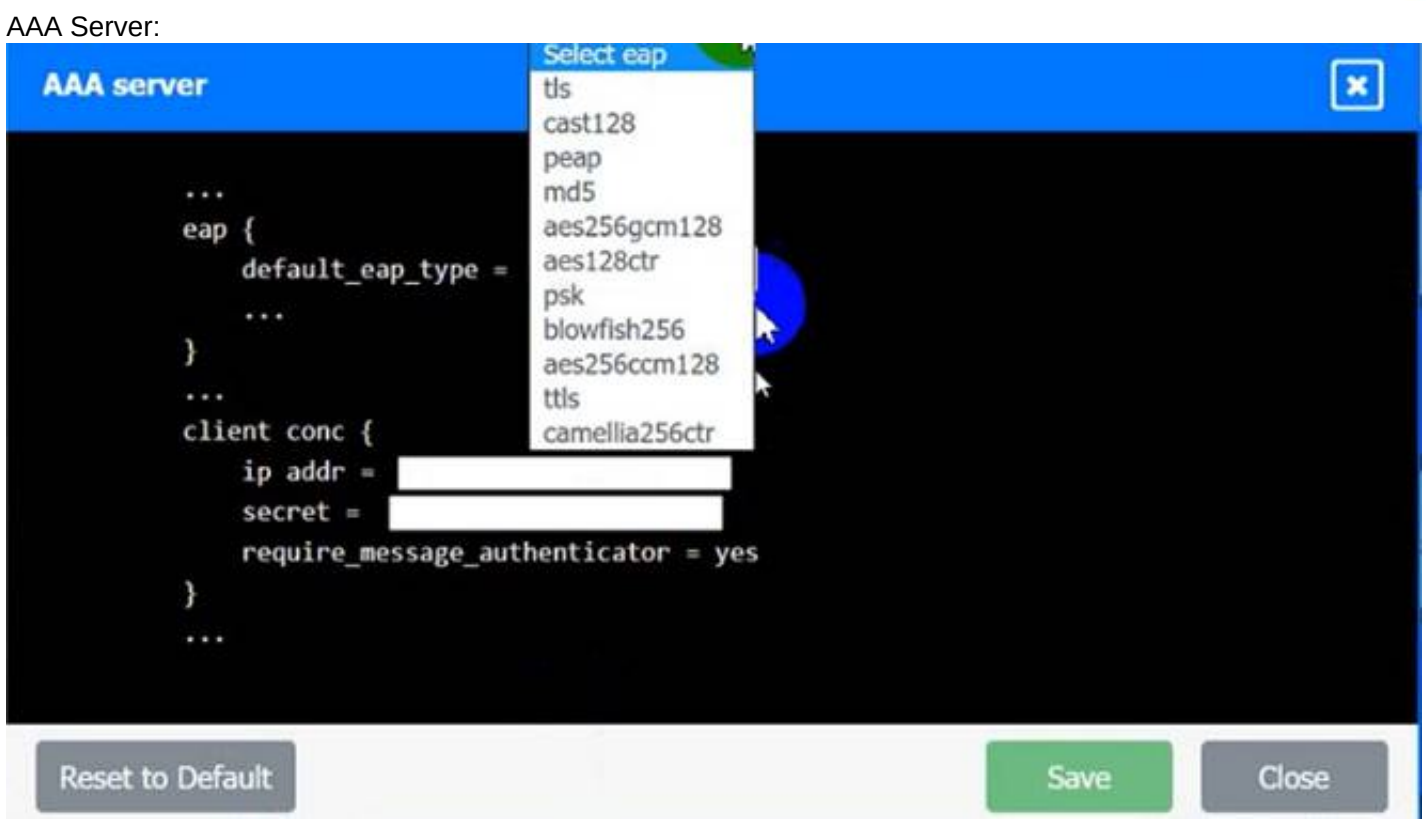
NEW QUESTION 204
SIMULATION
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.
Complete the configuration files to meet the following requirements:
• The EAP method must use mutual certificate-based authentication (With issued client certificates).
• The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
• The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,
INSTRUCTIONS
Click on the AAA server and VPN concentrator to complete the configuration.
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



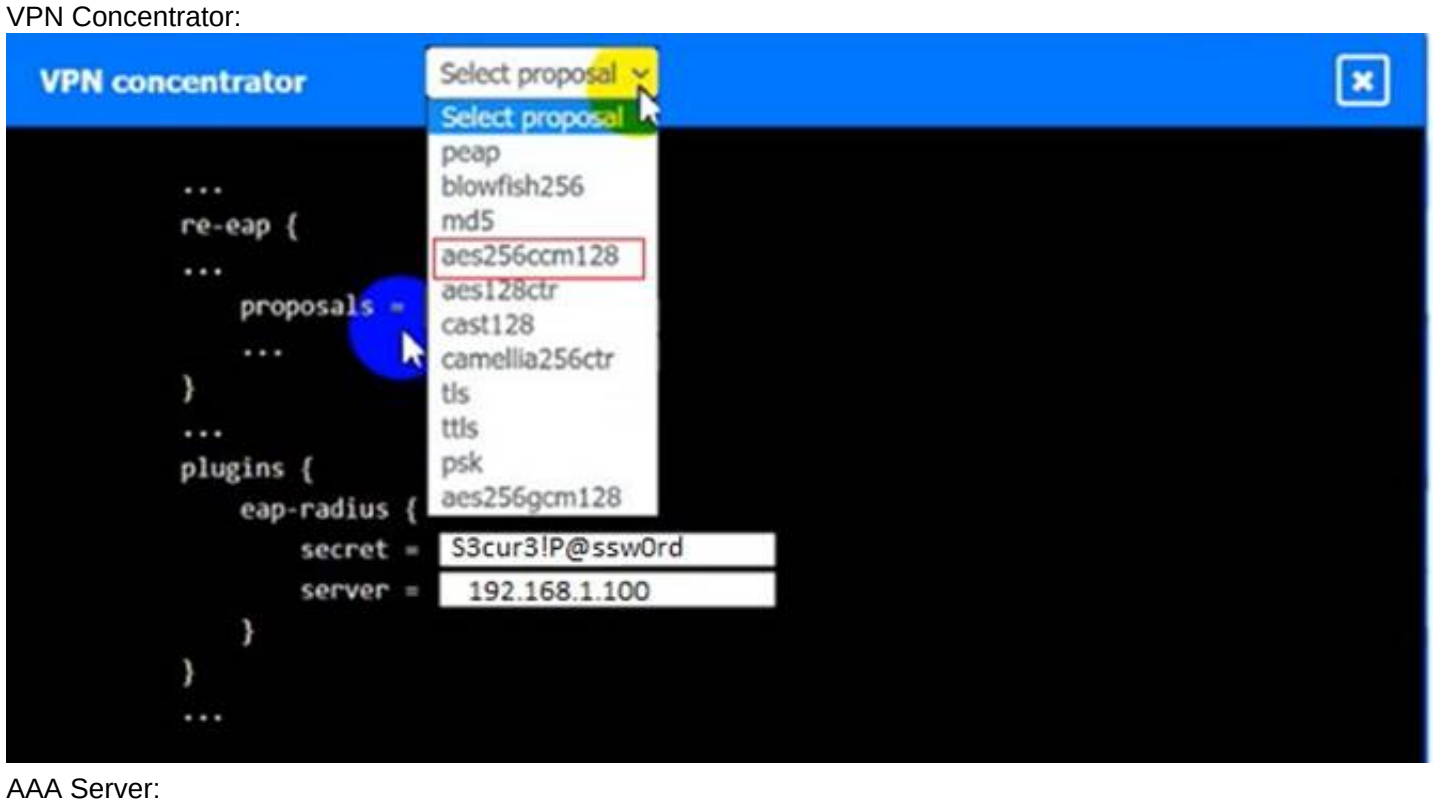
AAA Server:



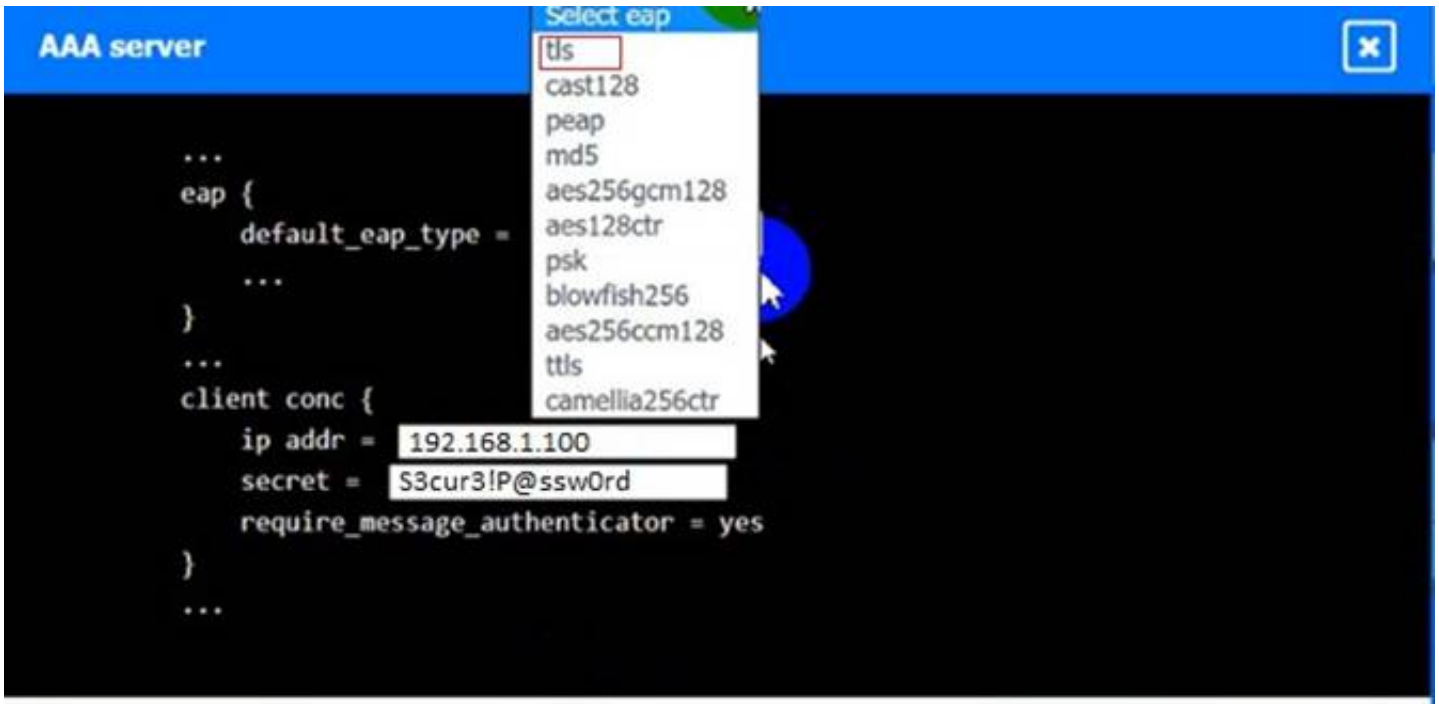
A. Mastered
B. Not Mastered

Answer: A

Explanation:
VPN Concentrator:



AAA Server:



NEW QUESTION 208
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

Answer: DE

NEW QUESTION 210
A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented in order to meet contractual requirements, the company must achieve the following thresholds
• 99 99% uptime
• Load time in 3 seconds
• Response time = <1 0 seconds
Starting with the computing environment, which of the following should a security engineer recommend to BEST meet the requirements? (Select THREE)

A. Installing a firewall at corporate headquarters
B. Deploying a content delivery network
C. Implementing server clusters
D. Employing bare-metal loading of applications
E. Lowering storage input/output
F. Implementing RAID on the backup servers
G. Utilizing redundant power for all developer workstations
H. Ensuring technological diversity on critical servers

Answer: BCE

Explanation:
To meet the contractual requirements of the web service provider, a security engineer should recommend the following actions:
? Deploying a content delivery network (CDN): A CDN is a distributed system of
servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the uptime, load time, and response time of web services by caching content closer to the users, reducing latency and bandwidth consumption. A CDN can also help mitigate distributed denial-of-service (DDoS) attacks by absorbing or filtering malicious traffic before it reaches the origin servers, reducing the impact on the web service availability12.
? Implementing server clusters: A server cluster is a group of servers that work
together to provide high availability, scalability, and load balancing for web services. A server cluster can help improve the uptime, load time, and response time of web services by distributing the workload across multiple servers, reducing the risk of single points of failure and performance bottlenecks. A server cluster can also help recover from failures by automatically switching to another server in case of a malfunction34.
? Lowering storage input/output (I/O): Storage I/O is the amount of data that can be
read from or written to a storage device in a given time. Storage I/O can affect the performance of web services by limiting the speed of data transfer between the servers and the storage devices. Lowering storage I/O can help improve the load time and response time of web services by reducing the latency and congestion of data access. Lowering storage I/O can be achieved by using faster storage devices, such as solid-state drives (SSDs), optimizing the storage layout and configuration, such as using RAID or striping, and caching frequently accessed data in memory5 .
Installing a firewall at corporate headquarters is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can help improve the security of web services by preventing unauthorized access and attacks, but it may also introduce additional latency and complexity to the network.
Employing bare-metal loading of applications is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Bare-metal loading is a technique that allows applications to run directly on hardware without an operating system or a hypervisor. Bare-metal loading can help improve the performance and efficiency of applications by eliminating the overhead and interference of other software layers, but it may also increase the difficulty and cost of deployment and maintenance.
Implementing RAID on the backup servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. RAID (redundant array of independent disks) is a technique that combines multiple disks into a logical unit that provides improved performance, reliability, or both. RAID can help improve the availability and security of backup data by protecting it from disk failures or corruption, but it

may also introduce additional complexity and overhead to the backup process.
Utilizing redundant power for all developer workstations is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Redundant power is a technique that provides multiple sources of power for an IT system in case one fails. Redundant power can help improve the availability and reliability of developer workstations by preventing them from losing power due to outages or surges, but it may also increase the cost and energy consumption of the system.
Ensuring technological diversity on critical servers is not a recommended action to meet the contractual requirements, as it does not directly affect the uptime, load time, or response time of web services. Technological diversity is a technique that uses different types of hardware, software, or platforms in an IT environment. Technological diversity can help improve resilience by reducing single points of failure and increasing compatibility, but it may also introduce additional complexity and inconsistency to the
environment. References: What Is CDN? How Does CDN Work? | Imperva, What Is Server Clustering? | IBM, What Is Server Clustering? | IBM, Server Clustering: What It Is & How It Works | Liquid Web, Storage I/O Performance - an overview | ScienceDirect Topics, [How
to Improve Storage I/O Performance | StarWind Blog], [What Is Firewall Security? | Cisco], [What is Bare Metal? | IBM], [What is RAID? | Dell Technologies US], [What Is Redundant Power Supply? | Dell Technologies US], [Technological Diversity - an overview | ScienceDirect Topics]

NEW QUESTION 213
A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:
Unauthorized insertions into application development environments
Authorized insiders making unauthorized changes to environment configurations
Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

A. Perform static code analysis of committed code and generate summary reports.
B. Implement an XML gateway and monitor for policy violations.
C. Monitor dependency management tools and report on susceptible third-party libraries.
D. Install an IDS on the development subnet and passively monitor for vulnerable services.
E. Model user behavior and monitor for deviations from normal.
F. Continuously monitor code commits to repositories and generate summary logs.

Answer: EF

Explanation:
Modeling user behavior and monitoring for deviations from normal and continuously monitoring code commits to repositories and generating summary logs are actions that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations. Modeling user behavior and monitoring for deviations from normal is a technique that uses baselines, analytics, machine learning, or other methods to establish normal patterns of user activity and identify anomalies or outliers that could indicate malicious or suspicious behavior. Modeling user behavior and monitoring for deviations from normal can help detect unauthorized insertions into application development environments, as it can alert on unusual or unauthorized access attempts, commands, actions, or transactions by users. Continuously monitoring code commits to repositories and generating summary logs is a technique that uses tools, scripts, automation, or other methods to track and record changes made to code repositories by developers, testers, reviewers, or other parties involved in the software development process. Continuously monitoring code commits to repositories and generating summary logs can help detect authorized insiders making unauthorized changes to environment configurations, as it can audit and verify the source, time, reason, and impact of code changes made by authorized users. Performing static code analysis of committed code and generate summary reports is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to detect vulnerabilities, errors, bugs, or quality issues in committed code. Implementing an XML gateway and monitor for policy violations is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to protect XML-based web services from threats or attacks by validating XML messages against predefined policies. Monitoring dependency management tools and report on susceptible third-party libraries is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes to environment configurations, but an action that will enable the data feeds needed to identify outdated or vulnerable third-party libraries used in software development projects. Installing an IDS (intrusion detection system) on the development subnet and passively monitor for vulnerable services is not an action that will enable the data feeds needed to detect unauthorized insertions into application development environments and authorized insiders making unauthorized changes

NEW QUESTION 217
An auditor Is reviewing the logs from a web application to determine the source of an Incident. The web application architecture Includes an Internet-accessible application load balancer, a number of web servers In a private subnet, application servers, and one database server In a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

```
Web server logs
192.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET /../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/ HTTP/1.1" 200 453 Safari/536.36

Application server logs
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not match a known local user. Querying DB
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin processing

Database server logs
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size' unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is self signed.
```

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

A. Enable the x-Forwarded-For header al the load balancer.
B. Install a software-based HIDS on the application servers.
C. Install a certificate signed by a trusted CA.
D. Use stored procedures on the database server.
E. Store the value of the $_server (‘ REMOTE_ADDR '] received by the web servers.

Answer: C

NEW QUESTION 218
An organization requires a legacy system to incorporate reference data into a new system. The organization anticipates the legacy system will remain in operation for the next 18 to 24 months. Additionally, the legacy system has multiple critical vulnerabilities with no patches available to resolve them. Which of the following is the BEST design option to optimize security?

A. Limit access to the system using a jump box.
B. Place the new system and legacy system on separate VLANs
C. Deploy the legacy application on an air-gapped system.
D. Implement MFA to access the legacy system.

Answer: C

NEW QUESTION 222
A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

Which of the following ciphers should the security analyst remove to support the business requirements?

A. TLS_AES_128_CCM_8_SHA256
B. TLS_DHE_DSS_WITH_RC4_128_SHA
C. TLS_CHACHA20_POLY1305_SHA256
D. TLS_AES_128_GCM_SHA256

Answer: B

Explanation:
The security analyst should remove the cipher TLS_DHE_DSS_WITH_RC4_128_SHA to support the business requirements, as it is considered weak and vulnerable to on-path attacks. RC4 is an outdated stream cipher that has been deprecated by major browsers and protocols due to its flaws and weaknesses. The other ciphers are more secure and compliant with secure-by-design principles and PCI DSS. Verified References: https://www.comptia.org/blog/what-is-a-cipher https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 226
A forensic investigator would use the foremost command for:

A. cloning disks.
B. analyzing network-captured packets.
C. recovering lost files.
D. extracting features such as email addresses

Answer: C

NEW QUESTION 229
A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?

A. HSTS
B. CRL
C. CSRs
D. OCSP

Answer: C

Explanation:
Reference: https://www.ssl.com/faqs/compromised-private-keys/

NEW QUESTION 232
A security engineer needs 10 implement a CASB to secure employee user web traffic. A Key requirement is mat relevant event data must be collected from existing on-premises infrastructure components and consumed by me CASB to expand traffic visibility. The solution must be nighty resilient to network outages.
Which of the following architectural components would BEST meet these requirements?

A. Log collection
B. Reverse proxy
C. AWAF
D. API mode

Answer: A

NEW QUESTION 234
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

Answer: C

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 References: https://www.comptia.org/blog/what-is-pci-dss https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 239
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.

Answer: C

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.

NEW QUESTION 242
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.

Answer: A

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.

NEW QUESTION 244
A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client's systems?

A. The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.
B. The change control board must review and approve a submission.
C. The information system security officer provides the systems engineer with the system updates.
D. The security engineer asks the project manager to review the updates for the client's system.

Answer: B

Explanation:

The change control board (CCB) is a committee that consists of subject matter experts and managers who decide whether to implement proposed changes to a project. The change control board is part of the change management plan, which defines the roles and processes for managing change within a team or organization. The change control board must review and approve a submission for any change request that affects the scope, schedule, budget, quality, or risks of the project. The change control board evaluates the impact and benefits of the change request and decides whether to accept, reject, or defer it.
* A. The implementation engineer requesting direct approval from the systems engineer and the Chief Information Security Officer is not a correct process for requesting updates or corrections to the client's systems, because it bypasses the change control board and the project manager. This could lead to unauthorized changes that could compromise the project's objectives and deliverables.
* C. The information system security officer providing the systems engineer with the system updates is not a correct process for requesting updates or corrections to the client's systems, because it does not involve the change control board or the project manager. This could lead to unauthorized changes that could introduce security vulnerabilities or conflicts with other system components.
* D. The security engineer asking the project manager to review the updates for the client's system is not a correct process for requesting updates or corrections to the client's systems, because it does not involve the change control board. The project manager is
responsible for facilitating the change management process, but not for approving or rejecting change requests.
https://www.projectmanager.com/blog/change-control-board-roles-responsibilities- processes

NEW QUESTION 246
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

Answer: B

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. References: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 8, Working with Third Parties.

NEW QUESTION 247
A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise. The company would like to find a way to use this information to protect the environment while still gaining valuable attack information.
Which of the following would be BEST for the company to implement?

A. A WAF
B. An IDS
C. A SIEM
D. A honeypot

Answer: D

Explanation:
Reference: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

NEW QUESTION 252
An organization requires a contractual document that includes
• An overview of what is covered
• Goals and objectives
• Performance metrics for each party
• A review of how the agreement is managed by all parties
Which of the following BEST describes this type of contractual document?

A. SLA
B. BAA
C. NDA
D. ISA

Answer: A

Explanation:
A Service Level Agreement is a contract between a service provider and a customer that outlines the level of services to be provided, the metrics by which those services will be measured, and how the agreement will be managed by both parties. SLAs also include provisions for dispute resolution and for the termination of the agreement.
Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 5:
Security Testing, Section 5.7: Service Level Agreements.

NEW QUESTION 254
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.

Answer: BD

Explanation:
Reference: https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%2 0the%20data
Vendor lock-in is a situation where a client becomes dependent on a vendor for products or services and cannot easily switch to another vendor without substantial costs or inconvenience. Some of the risks associated with vendor lock-in are that the vendor can change product offerings, such as by discontinuing or modifying features, increasing prices, or reducing support, and that the client experiences decreased quality of service, such as by having poor performance, reliability, or security. These risks could affect the client's business operations, satisfaction, or competitiveness. The client can seamlessly move data, the client receives a sufficient level of service, and the client can leverage a multicloud approach are not risks associated with vendor lock-in, but potential benefits of avoiding vendor lock-in. Verified References: https://www.comptia.org/blog/what-is-vendor- lock-in https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION 258
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

Answer: CDF

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.

NEW QUESTION 259
A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?

A. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.
B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
C. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
D. The DHCP server is unavailable, so no IP address is being sent back to the PC.

Answer: A

NEW QUESTION 262
An auditor needs to scan documents at rest for sensitive text. These documents contain both text and Images. Which of the following software functionalities must be enabled in the DLP solution for the auditor to be able to fully read these documents? (Select TWO).

A. Document interpolation
B. Regular expression pattern matching
C. Optical character recognition functionality
D. Baseline image matching
E. Advanced rasterization
F. Watermarking

Answer: AC

NEW QUESTION 265
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.

Answer: C

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.

NEW QUESTION 267
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

Answer: D

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 References: https://www.comptia.org/blog/what-is-owasp https://partners.comptia.org/docs/default- source/resources/casp-content-guide

NEW QUESTION 271
Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage.
Which of the following should be created to prevent this type of issue in the future?

A. SLA
B. BIA
C. BCM
D. BCP
E. RTO

Answer: D

Explanation:
A Business Continuity Plan (BCP) is a set of policies and procedures that outline how an organization should respond to and recover from disruptions [1]. It is designed to ensure that critical operations and services can be quickly restored and maintained, and should include steps to identify risks, develop plans to mitigate those risks, and detail the procedures to be followed in the event of a disruption. Resources:
CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 4: “Business Continuity Planning,” Wiley, 2018. https://www.wiley.com/en-us/CompTIA+Advanced+Security+Practitioner+CASP%2B+Study+Guide%2C+2nd+Edition
-p-9781119396582

NEW QUESTION 274
A local government that is investigating a data exfiltration claim was asked to review the fingerprint of the malicious user's actions. An investigator took a forensic image of the VM an downloaded the image to a secured USB drive to share with the government. Which of the following should be taken into consideration during the process of releasing the drive to the government?

A. Encryption in transit
B. Legal issues
C. Chain of custody
D. Order of volatility
E. Key exchange

Answer: C

NEW QUESTION 277
Company A acquired Company . During an audit, a security engineer found Company B’s environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A’s security program.
Which of the following risk-handling techniques was used?

A. Accept
B. Avoid
C. Transfer
D. Mitigate

Answer: D

Explanation:
Reference: https://www.pivotpointsecurity.com/blog/risk-tolerance-in-business/

NEW QUESTION 279
A vulnerability assessment endpoint generated a report of the latest findings. A security analyst needs to review the report and create a priority list of items that must be addressed. Which of the following should the analyst use to create the list quickly?

A. Business impact rating

B. CVE dates
C. CVSS scores
D. OVAL

Answer: A

NEW QUESTION 280
A company's Chief Information Security Officer is concerned that the company's proposed move to the cloud could lead to a lack of visibility into network traffic flow logs within the VPC.
Which of the following compensating controls would be BEST to implement in this situation?

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

Answer: B

Explanation:
Reference: https://runpanther.io/cyber-explained/cloud-based-siem-explained/

NEW QUESTION 282
A CSP, which wants to compete in the market, has been approaching companies in an attempt to gain business. The CSP is able to provide the same uptime as other CSPs at a markedly reduced cost. Which of the following would be the MOST significant business risk to a company that signs a contract with this CSP?

A. Resource exhaustion
B. Geographic location
C. Control plane breach
D. Vendor lock-in

Answer: A

Explanation:
Resource exhaustion is a condition that occurs when a system or service runs out of resources, such as memory, CPU, disk space, or bandwidth, and becomes unable to function properly or respond to requests. Resource exhaustion can be caused by high demand, poor design, misconfiguration, or malicious attacks, such as denial-of-service (DoS).
Resource exhaustion would be the most significant business risk to a company that signs a contract with a cloud service provider (CSP) that is able to provide the same uptime as other CSPs at a markedly reduced cost, because this could:
? Indicate that the CSP is oversubscribing or underprovisioning its resources, which
could result in performance degradation, service disruption, or data loss for the company.
? Affect the company's availability, reliability, and scalability requirements, which
could impact its operations, reputation, and customer satisfaction.
? Expose the company to potential security breaches or compliance violations, if the CSP does not implement adequate security controls or measures to prevent or mitigate resource exhaustion.

NEW QUESTION 287
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CAS-004 Practice Exam Features:

* CAS-004 Questions and Answers Updated Frequently

* CAS-004 Practice Questions Verified by Expert Senior Certified Staff

* CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year