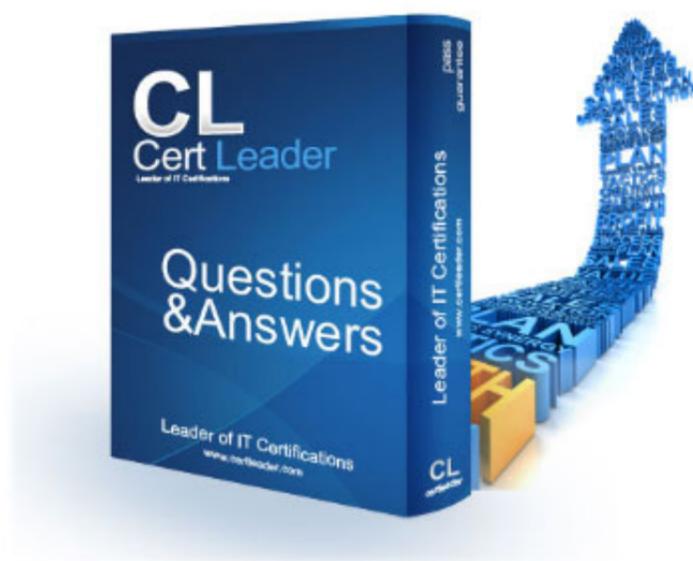


CAS-004 Dumps

CompTIA Advanced Security Practitioner (CASP+) Exam

<https://www.certleader.com/CAS-004-dumps.html>



NEW QUESTION 1

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%20personal%20data.&text=The%20General%20Data%20Protection%20Regulation,collected%2C%20processed%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 2

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vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated OSs.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

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

Answer: B

NEW QUESTION 3

A company requires a task to be carried by more than one person concurrently. This is an example of:

- A. separation of duties.
- B. dual control
- C. least privilege
- D. job rotation

Answer: B

Explanation:

Dual control is a security principle that requires two or more authorized individuals to perform a task concurrently. This reduces the risk of fraud, error, or misuse of sensitive assets or information. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide>, <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/using-dual-control-to-mitigate-risk>

NEW QUESTION 4

An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization's headquarters and only datacenter are located in New York City. The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:

Low latency for all mobile users to improve the users' experience
SSL offloading to improve web server performance

Protection against DoS and DDoS attacks
High availability

Which of the following should the organization implement to BEST ensure all requirements are met?

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

Answer: B

NEW QUESTION 5

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 6

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

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

Answer: A

Explanation:

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

NEW QUESTION 7

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 8

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

Which of the following solutions should the security architect recommend?

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

Answer: A

Explanation:

Replacing the current antivirus with an EDR (endpoint detection and response) solution is the best solution for addressing several service outages on the endpoints due to new malware. An EDR solution is a technology that provides advanced capabilities for detecting, analyzing, and responding to threats or incidents on endpoints, such as computers, laptops, mobile devices, or servers. An EDR solution can use behavioral analysis, machine learning, threat intelligence, or other methods to identify new or unknown malware that may evade traditional antivirus solutions. An EDR solution can also provide automated or manual remediation actions, such as isolating, blocking, or removing malware from endpoints. Removing the web proxy and installing a UTM (unified threat management) appliance is not a good solution for addressing service outages on endpoints due to new malware, as it could expose endpoints to more threats or attacks by removing a layer of protection that filters web traffic, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Implementing a deny list feature on endpoints is not a good solution for addressing service outages on endpoints due to new malware, as it could be ineffective or impractical for blocking new or unknown malware that may not be on the deny list, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Adding a firewall module on the current antivirus solution is not a good solution for addressing service outages on endpoints due to new malware, as it could introduce compatibility or performance issues for endpoints by adding an additional feature that may not be integrated or optimized with the antivirus solution, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Verified References: <https://www.comptia.org/blog/what-is-edr> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 9

The Chief Information Security Officer (CISO) of a small local 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 10

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 10

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 15

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 20

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

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

Answer: A

NEW QUESTION 25

A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.

Which of the following techniques would BEST support this?

- A. Configuring systemd services to run automatically at startup
- B. Creating a backdoor
- C. Exploiting an arbitrary code execution exploit

D. Moving laterally to a more authoritative server/service

Answer: B

NEW QUESTION 27

A security engineer at a company is designing a system to mitigate recent setbacks caused competitors that are beating the company to market with the new products. Several of the products incorporate propriety enhancements developed by the engineer's company. The network already includes a SEIM and a NIPS and requires 2FA for all user access. Which of the following system should the engineer consider NEXT to mitigate the associated risks?

- A. DLP
- B. Mail gateway
- C. Data flow enforcement
- D. UTM

Answer: A

Explanation:

A DLP system is the best option for the company to mitigate the risk of losing its proprietary enhancements to competitors. DLP stands for data loss prevention, which is a set of tools and policies that aim to prevent unauthorized access, disclosure, or exfiltration of sensitive data. DLP can monitor, filter, encrypt, or block data transfers based on predefined rules and criteria, such as content, source, destination, etc. DLP can help protect the company's intellectual property and trade secrets from being compromised by malicious actors or accidental leaks. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.csoonline.com/article/3245746/what-is-dlp-data-loss-prevention-and-how- does-it-work.html>

NEW QUESTION 28

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 31

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 33

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 38

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	82	0	\$0
February	375	314	58	1	\$1000
March	360	289	99	0	\$0
April	281	213	87	1	\$1000
May	331	273	56	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, $ALE = ARO \times SLE$. Filter XYZ has an ARO of 0.1 and an SLE of \$10 million, so $ALE = 0.1 \times \$10 \text{ 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 41

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

- A. The NTP server is set incorrectly for the developers.
- B. The CA has included the certificate in its CRL_
- C. The certificate is set for the wrong key usage.
- D. Each application is missing a SAN or wildcard entry on the certificate.

Answer: C

Explanation:

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

NEW QUESTION 43

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 47

A development team created a mobile application that contacts a company's back-end APIs housed in a PaaS environment. The APIs have been experiencing high processor utilization due to scraping activities. The security engineer needs to recommend a solution that will prevent and remedy the behavior.

Which of the following would BEST safeguard the APIs? (Choose two.)

- A. Bot protection
- B. OAuth 2.0
- C. Input validation
- D. Autoscaling endpoints
- E. Rate limiting
- F. CSRF protection

Answer: DE

Explanation:

Reference: <https://stackoverflow.com/questions/3161548/how-do-i-prevent-site-scraping>

NEW QUESTION 48

A cloud security engineer is setting up a cloud-hosted WAF. The engineer needs to implement a solution to protect the multiple websites the organization hosts. The organization websites are:

- * www.mycompany.org
- * www.mycompany.com
- * campus.mycompany.com
- * wiki.mycompany.org

The solution must save costs and be able to protect all websites. Users should be able to notify the cloud security engineer of any on-path attacks. Which of the following is the BEST solution?

- A. Purchase one SAN certificate.
- B. Implement self-signed certificates.
- C. Purchase one certificate for each website.
- D. Purchase one wildcard certificate.

Answer: D

Explanation:

Purchasing one wildcard certificate is the best solution to protect multiple websites hosted by an organization in a cloud-hosted WAF. A wildcard certificate is a type of SSL/TLS certificate that can secure a domain name and any number of its subdomains with a single certificate. For example, a wildcard certificate for *.mycompany.com can secure www.mycompany.com, campus.mycompany.com, and any other subdomain under mycompany.com. A wildcard certificate can save costs and simplify management compared to purchasing individual certificates for each website.

References: [CompTIA CASP+ Study Guide, Second Edition, page 301]

NEW QUESTION 52

An organization is assessing the security posture of a new SaaS CRM system that handles sensitive PII and identity information, such as passport numbers. The SaaS CRM system does not meet the organization's current security standards. The assessment identifies the following:

- 1- There will be a \$20,000 per day revenue loss for each day the system is delayed going into production.
- 2- The inherent risk is high.
- 3- The residual risk is low.
- 4- There will be a staged deployment to the solution rollout to the contact center.

Which of the following risk-handling techniques will BEST meet the organization's requirements?

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

Answer: A

NEW QUESTION 56

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 57

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 58

A company Invested a total of \$10 million for a new storage solution Installed across live on-site datacenters. Fifty 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 62

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://eklitze.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 67

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 69

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

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

Answer: C

NEW QUESTION 71

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-fs1 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-fs1 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-fs1, 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-fs1 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-logout to abc-usa-fs1, 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 76

A security is assisting the marketing department with ensuring the security of the organization's social media platforms. The two main concerns are:

The Chief marketing officer (CMO) email is being used department wide as the username The password has been shared within the department Which of the following controls would be BEST for the analyst to recommend?

- A. Configure MFA for all users to decrease their reliance on other authentication.
- B. Have periodic, scheduled reviews to determine which OAuth configuration are set for each media platform.
- C. Create multiple social media accounts for all marketing user to separate their actions.
- D. Ensure the password being shared is sufficiently and not written down anywhere.

Answer: A

Explanation:

Configuring MFA for all users to decrease their reliance on other authentication is the best option to improve email security at the company. MFA stands for multi-factor authentication, which is a method of verifying a user's identity by requiring two or more factors, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access to email accounts even if the username or password is compromised or shared. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.csoonline.com/article/3239144/what-is-mfa-how-multi-factor-authentication-works.html>

NEW QUESTION 77

A software development company is building a new mobile application for its social media platform. The company wants to gain its users' trust by re reducing the risk of on-path attacks between the mobile client and its servers and by implementing stronger digital trust. To support users' trust, the company has released the following internal guidelines:

- * Mobile clients should verify the identity of all social media servers locally.
- * Social media servers should improve TLS performance of their certificate status.
- + Social media servers should inform the client to only use HTTPS.

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

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

Answer: BF

Explanation:

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

NEW QUESTION 80

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 81

A security analyst is reviewing the following vulnerability assessment report:

```
192.168.1.5, Host = Server1, CVS7.5, Web Server, Remotely Executable = Yes, Exploit = Yes
205.1.3.5, Host = Server2, CVS6.5, Bind Server, Remotely Executable = Yes, Exploit = POC
207.1.5.7, Host = Server3, CVS5.5, Email server, Remotely Executable = Yes, Exploit = Yes
192.168.1.6, Host = Server4, CVS9.8, Domain Controller, Remotely Executable = Yes, Exploit = No
```

Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?

- A. Server1
- B. Server2
- C. Server 3
- D. Servers

Answer: A

NEW QUESTION 82

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 84

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 85

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

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

Answer: AC

Explanation:

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

NEW QUESTION 88

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 93

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
DocumentRoot /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 97

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

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

Answer: A

Explanation:

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

NEW QUESTION 102

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

- Cloud-delivered services
 - Full network security stack
 - SaaS application security management
 - Minimal latency for an optimal user experience
 - Integration with the cloud IAM platform
- Which of the following is the BEST solution?

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

Answer: D

NEW QUESTION 103

A security analyst is trying to identify the source of a recent data loss incident. The analyst has reviewed all the for the time surrounding the identified all the assets on the network at the time of the data loss. The analyst suspects the key to finding the source was obfuscated in an application. Which of the following tools should the analyst use NEXT?

- A. Software Decompiler
- B. Network enurrerator
- C. Log reduction and analysis tool
- D. Static code analysis

Answer: D

NEW QUESTION 106

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 108

An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.

Which of the following processes can be used to identify potential prevention recommendations?

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

Answer: C

Explanation:

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

NEW QUESTION 113

An organization wants to perform a scan of all its systems against best practice security configurations.

Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for fill automation? (Choose two.)

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

Answer: BF

Explanation:

Reference: <https://www.govinfo.gov/content/pkg/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf> (p.12)

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

NEW QUESTION 115

A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack.

Which of the following is the NEXT step of the incident response plan?

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

Answer: B

Explanation:

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

NEW QUESTION 118

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

Which of the following techniques would be BEST suited for this requirement?

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

Answer: A

Explanation:

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

NEW QUESTION 121

A pharmaceutical company recently experienced a security breach within its customer-facing web portal. The attackers performed a SQL injection attack and exported tables from the company's managed database, exposing customer information.

The company hosts the application with a CSP utilizing the IaaS model. Which of the following parties is ultimately responsible for the breach?

- A. The pharmaceutical company
- B. The cloud software provider
- C. The web portal software vendor
- D. The database software vendor

Answer: A

NEW QUESTION 122

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 SIDe 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 125

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

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

Answer: D

NEW QUESTION 130

Given the following log snippet from a web server:

```
84.55.41.60 - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810 FROM (SELECT COUNT(*), CONCAT(0x7171787671, (SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60 - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=(SELECT 7505 FROM (SELECT COUNT(*), CONCAT(0x7171787671, (SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60 - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=(SELECT CONCAT(0x7171787671, (SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60 - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

Which of the following BEST describes this type of attack?

- A. SQL injection
- B. Cross-site scripting
- C. Brute-force
- D. Cross-site request forgery

Answer: A

NEW QUESTION 133

During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked

using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee.

Which of the following processes would BEST satisfy this requirement?

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

Answer: B

Explanation:

Reference: <https://www.getkisi.com/access-control>

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

NEW QUESTION 138

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

- A. `grep -v '^4[0-9]{12}(:[0-9]{3})?$' file`
- B. `grep '^4[0-9]{12}(:[0-9]{3})?$' file`
- C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file`
- D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file`

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

Answer: C

NEW QUESTION 140

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

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

Answer: E

NEW QUESTION 143

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

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

Answer: B

NEW QUESTION 147

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 151

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

implement?

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

Answer: B

Explanation:

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

Verified References:

? <https://attack.mitre.org/>

? <https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-attck-framework/>

? <https://www.ibm.com/topics/threat-management>

NEW QUESTION 155

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. IaaS
- B. SaaS
- C. FaaS
- D. PaaS

Answer: D

NEW QUESTION 160

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

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

Answer: B

Explanation:

Data exposure is a security concern that will most likely need to be addressed during migration of all company data to the cloud, as it could involve sensitive or confidential data being accessed or disclosed by unauthorized parties. Data exposure could occur due to misconfigured cloud services, insecure data transfers, insider threats, or malicious attacks. Data exposure could also result in compliance violations, reputational damage, or legal liabilities. Latency is not a security concern, but a performance concern that could affect the speed or quality of data access or transmission. Data loss is not a security concern, but an availability concern that could affect the integrity or recovery of data. Data dispersion is not a security concern, but a management concern that could affect the visibility or control of data. Verified References: <https://www.comptia.org/blog/what-is-data-exposure>

<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 165

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 167

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 171

A global organization's Chief Information Security Officer (CISO) has been asked to analyze the risks involved in a plan to move the organization's current MPLS-based WAN network to use commodity Internet and SD-WAN hardware. The SD-WAN provider is currently highly regarded but is a regional provider. Which of the following is MOST likely identified as a potential risk by the CISO?

- A. The SD-WAN provider would not be able to handle the organization's bandwidth requirements.
- B. The operating costs of the MPLS network are too high for the organization.
- C. The SD-WAN provider uses a third party for support.
- D. Internal IT staff will not be able to properly support remote offices after the migration.

Answer: C

Explanation:

SD-WAN (Software-Defined Wide Area Network) is a technology that allows organizations to use multiple, low-cost Internet connections to create a secure and dynamic WAN. SD-WAN can provide benefits such as lower costs, higher performance, and easier management compared to traditional WAN technologies, such as MPLS (Multiprotocol Label Switching).

However, SD-WAN also introduces some potential risks, such as:

- ? The reliability and security of the Internet connections, which may vary depending on the location, provider, and traffic conditions.
- ? The compatibility and interoperability of the SD-WAN hardware and software, which may come from different vendors or use different standards.
- ? The availability and quality of the SD-WAN provider's support, which may depend on the provider's size, reputation, and outsourcing practices.

In this case, the CISO would most likely identify the risk that the SD-WAN provider uses a third party for support, because this could:

- ? Affect the organization's ability to resolve issues or request changes in a timely and effective manner.
- ? Expose the organization's network data and configuration to unauthorized or malicious parties.
- ? Increase the complexity and uncertainty of the SD-WAN service level agreement (SLA) and contract terms.

NEW QUESTION 172

A financial institution has several that currently employ the following controls:

- * The servers follow a monthly patching cycle.
- * All changes must go through a change management process.
- * Developers and systems administrators must log into a jumpbox to access the servers hosting the data using two-factor authentication.
- * The servers are on an isolated VLAN and cannot be directly accessed from the internal production network.

An outage recently occurred and lasted several days due to an upgrade that circumvented the approval process. Once the security team discovered an unauthorized patch was installed, they were able to resume operations within an hour. Which of the following should the security administrator recommend to reduce the time to resolution if a similar incident occurs in the future?

- A. Require more than one approver for all change management requests.
- B. Implement file integrity monitoring with automated alerts on the servers.
- C. Disable automatic patch update capabilities on the servers
- D. Enhanced audit logging on the jump servers and ship the logs to the SIEM.

Answer: B

NEW QUESTION 176

A security analyst is reading the results of a successful exploit that was recently conducted by third-party penetration testers. The testers reverse engineered a privileged executable. In the report, the planning and execution of the exploit is detailed using logs and outputs from the test. However, the attack vector of the exploit is missing, making it harder to recommend remediation's. Given the following output:

```

0x014435a5 <+7>: mov 0x8(%ebp),%eax
0x014435a8 <+10>: movl $0xffffffff,-0x1c(%ebp) //Tester note, Start
0x014435af <+17>: mov %eax,%edx
0x014435b1 <+19>: mov $0x0,%eax
0x014435b6 <+24>: mov -0x1c(%ebp),%ecx
0x014435b9 <+27>: mov %edx,%edi
0x014435bb <+29>: repnz scas %es:(%edi),%al
0x014435bd <+31>: mov %ecx,%eax
0x014435bf <+33>: not %eax
0x014435c1 <+35>: sub $0x1,%eax //Tester note, end
0x014435c4 <+38>: mov %al,-0x9(%ebp)
0x014435c7 <+41>: cmpb $0x3,-0x9(%ebp) //Tester note <=4
0x014435cb <+45>: jbe 0x1448500 <validate_passwd+98>
0x014435cd <+47>: cmpl $0x8,-0x9(%ebp) //Tester note >=8
0x014435d1 <+51>: ja 0x1448500 <validate_passwd+98>
0x014435d3 <+53>: movl $0x1448660,(%esp)
0x014435de <+60>: call 0x14483a0 <puts@plt>
0x014435df <+65>: mov 0x144a020,%eax
0x014435e4 <+70>: mov %eax,(%esp)
0x014435e7 <+73>: call 0x1448380 <fflush@plt>
0x014435ec <+78>: mov 0x8(%ebp),%eax
0x014435ef <+81>: mov %eax,0x4(%esp)
0x014435f3 <+85>: lea -0x14(%ebp),%eax
0x014435f6 <+88>: mov %eax,(%esp)
0x014435f9 <+91>: call 0x1448390 <strcpy@plt> //Tester note, breakpoint
0x014435fe <+96>: jmp 0x1448519 <validate_passwd+123>
0x01448500 <+98>: movl $0x144866f,(%esp)

```

The penetration testers MOST likely took advantage of:

- A. A TOC/TOU vulnerability
- B. A plain-text password disclosure
- C. An integer overflow vulnerability
- D. A buffer overflow vulnerability

Answer: A

NEW QUESTION 181

The Chief information Officer (CIO) of a large bank, which uses multiple third-party organizations to deliver a service, is concerned about the handling and security of customer data by the parties. Which of the following should be implemented to BEST manage the risk?

- A. Establish a review committee that assesses the importance of suppliers and ranks them according to contract renewal
- B. At the time of contract renewal, incorporate designs and operational controls into the contracts and a right-to-audit clause
- C. Regularly assess the supplier's post-contract renewal with a dedicated risk management team.
- D. Establish a team using members from first line risk, the business unit, and vendor management to assess only design security controls of all supplier
- E. Store findings from the reviews in a database for all other business units and risk teams to reference.
- F. Establish an audit program that regularly reviews all suppliers regardless of the data they access, how they access the data, and the type of data, Review all design and operational controls based on best practice standard and report the finding back to upper management.
- G. Establish a governance program that rates suppliers based on their access to data, the type of data, and how they access the data Assign key controls that are reviewed and managed based on the supplier's rating
- H. Report finding units that rely on the suppliers and the various risk teams.

Answer: D

Explanation:

A governance program that rates suppliers based on their access to data, the type of data, and how they access the data is the best way to manage the risk of handling and security of customer data by third parties. This allows the company to assign key controls that are reviewed and managed based on the supplier's rating and report findings to the relevant units and risk teams. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/third-party-risk-management>

NEW QUESTION 185

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

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

Answer: D

Explanation:

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

NEW QUESTION 188

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 191

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

```
database server logs
14/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size' unassigned value 0 adjusted to 2048
14/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 at 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 195

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:

```
(&(objectClass=*)(objectClass=*))(&(objectClass=void)(type=admin))
```

Which of the following would BEST mitigate this vulnerability?

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

Answer: C

NEW QUESTION 199

A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open-

source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away. Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

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

Answer: C

Explanation:

Reference: <https://www.microfocus.com/en-us/what-is/sast>

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

NEW QUESTION 200

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 205

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

- A. Log collection
- B. Reverse proxy
- C. AWAFF
- D. API mode

Answer: A

NEW QUESTION 208

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

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

Answer: B

NEW QUESTION 210

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

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

Answer: B

Explanation:

Isolating the servers is the best immediate action to take after reporting the incident to the management team, as it can limit the damage and contain the ransomware infection. Paying the ransom is not advisable, as it does not guarantee the recovery of the data and may encourage further attacks. Notifying law enforcement is a possible step, but not the next one after reporting. Requesting that the affected servers be restored immediately may not be feasible or effective, as it depends on the availability and integrity of backups, and it does not address the root cause of the attack. Verified References:

<https://www.comptia.org/blog/what-is-ransomware-and-how-to-protect-yourself> <https://www.comptia.org/certifications/comptia-advanced-security-practitioner>

NEW QUESTION 212

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 216

Which of the following is the MOST important cloud-specific risk from the CSP's viewpoint?

- A. Isolation control failure
- B. Management plane breach
- C. Insecure data deletion
- D. Resource exhaustion

Answer: B

NEW QUESTION 217

A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.

Which of the following would be BEST to proceed with the transformation?

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

Answer: C

Explanation:

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

NEW QUESTION 222

A developer implement the following code snippet.

```
catch (Exception e)
{
    if(log.isDebugEnabled())
    {
        log.debug("Caught InvalidSQLException Exception --"
            + e.toString());
    }
}
```

Which of the following vulnerabilities does the code snippet resolve?

- A. SQL inject
- B. Buffer overflow
- C. Missing session limit
- D. Information leakage

Answer: A

Explanation:

SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL commands on a database by inserting them into an input field. The code snippet resolves this vulnerability by using parameterized queries, which prevent the input from being interpreted as part of the SQL command. Verified References:

<https://www.comptia.org/training/books/casp-cas-004-study-guide> , https://owasp.org/www-community/attacks/SQL_Injection

NEW QUESTION 226

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 227

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 232

A Chief information Security Officer (CISO) is developing corrective-action plans based on the following from a vulnerability scan of internal hosts:

```
High CVEs: 10-01
CVT: 100 "jpg_stream_overflow()" Buffer Overflow Vulnerability (Windows) (CVE: 1.3.4.1.4.1.25423.1.0.00017)
Product Detection result: open/argp/argp/1.3.4 by SSG Version Detection (Remote) (CVE: 1.3.4.1.4.1.25423.1.0.000109)

Summary
This host is running IIS and is prone to buffer overflow vulnerability.
Vulnerability Detection Result: Installed version: 1.3.4
Fixed version: 1.3.12/1.4.2

Impact
Successful exploitation could allow attackers to execute arbitrary code and failed attempts will likely result in denial-of-service conditions. Impact Level: System/Application
```

Which of the following MOST appropriate corrective action to document for this finding?

- A. The product owner should perform a business impact assessment regarding the ability to implement a WAF.
- B. The application developer should use a static code analysis tool to ensure any application code is not vulnerable to buffer overflows.
- C. The system administrator should evaluate dependencies and perform upgrade as necessary.
- D. The security operations center should develop a custom IDS rule to prevent attacks buffer overflows against this server.

Answer: A

NEW QUESTION 236

A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:

- ? Be efficient at protecting the production environment
- ? Not require any change to the application
- ? Act at the presentation layer

Which of the following techniques should be used?

- A. Masking
- B. Tokenization
- C. Algorithmic
- D. Random substitution

Answer: A

NEW QUESTION 241

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 and 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 246

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

Which of the following would be the BEST option to implement?

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

Answer: D

Explanation:

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

NEW QUESTION 247

A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:

- * 1. The network supports core applications that have 99.99% uptime.
- * 2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
- * 3. Documents downloaded from websites must be scanned for malware.

Which of the following solutions should the network architect implement to meet the requirements?

- A. Reverse proxy, stateful firewalls, and VPNs at the local sites
- B. IDSs, WAFs, and forward proxy IDS
- C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy
- D. IPSs at the hub, Layer 4 firewalls, and DLP

Answer: C

NEW QUESTION 250

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

Which of the following should the security team recommend FIRST?

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

Answer: D

Explanation:

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

NEW QUESTION 252

A host on a company's network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis.

Which of the following steps would be best to perform FIRST?

- A. Turn off the infected host immediately.
- B. Run a full anti-malware scan on the infected host.
- C. Modify the smb.conf file of the host to prevent outgoing SMB connections.
- D. Isolate the infected host from the network by removing all network connections.

Answer: D

NEW QUESTION 253

A security analyst observes the following while looking through network traffic in a company's cloud log:

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

Which of the following steps should the security analyst take FIRST?

- A. Quarantine 10.0.5.52 and run a malware scan against the host.

- B. Access 10.0.5.52 via EDR and identify processes that have network connections.
- C. Isolate 10.0.50.6 via security groups.
- D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Answer: D

NEW QUESTION 257

An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.

Which of the following side-channel attacks did the team use?

- A. Differential power analysis
- B. Differential fault analysis
- C. Differential temperature analysis
- D. Differential timing analysis

Answer: B

Explanation:

"Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults—unexpected environmental conditions—into cryptographic operations, to reveal their internal states."

NEW QUESTION 260

A company that uses AD is migrating services from LDAP to secure LDAP. During the pilot phase, services are not connecting properly to secure LDAP. Block is an excerpt of output from the troubleshooting session:

```
openssl s_client -host ldap1.comptia.com -port 636

CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/.CN=*.comptia.com
Issuer=/.DC=com/DC=danville/CN=chicago
```

Which of the following BEST explains why secure LDAP is not working? (Select TWO.)

- A. The clients may not trust idapt by default.
- B. The secure LDAP service is not started, so no connections can be made.
- C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
- D. Secure LDAP should be running on UDP rather than TCP.
- E. The company is using the wrong por
- F. It should be using port 389 for secure LDAP.
- G. Secure LDAP does not support wildcard certificates.
- H. The clients may not trust Chicago by default.

Answer: AF

Explanation:

The clients may not trust idapt by default because it is a self-signed certificate authority that is not in the trusted root store of the clients. Secure LDAP does not support wildcard certificates because they do not match the fully qualified domain name of the server. Verified References: <https://www.professormesser.com/security-plus/sy0-401/ldap-and-secure-ldap/> , <https://www.comptia.org/training/books/casp-cas-004-study-guide>

NEW QUESTION 265

A major broadcasting company that requires continuous availability to streaming content needs to be resilient against DDoS attacks Which of the following is the MOST important infrastructure security design element to prevent an outage?

- A. Supporting heterogeneous architecture
- B. Leveraging content delivery network across multiple regions
- C. Ensuring cloud autoscaling is in place
- D. Scaling horizontally to handle increases in traffic

Answer: B

Explanation:

A content delivery network (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 availability and performance of web applications 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 application availability. Supporting heterogeneous architecture means using different types of hardware, software, or platforms in an IT environment. This can help improve resilience by reducing single points of failure and increasing compatibility, but it does not directly prevent DDoS attacks. Ensuring cloud autoscaling is in place means using cloud services that automatically adjust the amount of resources allocated to an application based on the demand or load. This can help improve scalability and performance by providing more resources when needed, but it does not directly prevent DDoS attacks. Scaling horizontally means adding more servers or nodes to an IT environment to increase its capacity or throughput. This can help improve scalability and performance by distributing the load across multiple servers, but it does not directly prevent DDoS attacks. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.4: Select controls based on systems security evaluation models

NEW QUESTION 267

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

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

Answer: A

NEW QUESTION 272

A security architect is analyzing an old application that is not covered for maintenance anymore because the software company is no longer in business. Which of the following techniques should have been implemented to prevent these types of risks?

- A. Code reviews
- B. Supply chain visibility
- C. Software audits
- D. Source code escrows

Answer: D

Explanation:

A source code escrow is a legal agreement that involves a third party holding the source code of a software application on behalf of the software vendor and the software licensee. The source code escrow ensures that the licensee can access the source code in case the vendor goes out of business, fails to provide maintenance or support, or breaches the contract terms.

A source code escrow would have prevented the risk of having an old application that is not covered for maintenance anymore because the software company is no longer in business, because it would:

- ? Allow the licensee to obtain the source code and continue to update, fix, or modify the application according to their needs.
- ? Protect the vendor's intellectual property rights and prevent unauthorized disclosure or use of the source code.
- ? Provide a legal framework and a trusted mediator for resolving any disputes or issues between the vendor and the licensee.

NEW QUESTION 275

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

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

Answer: D

Explanation:

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

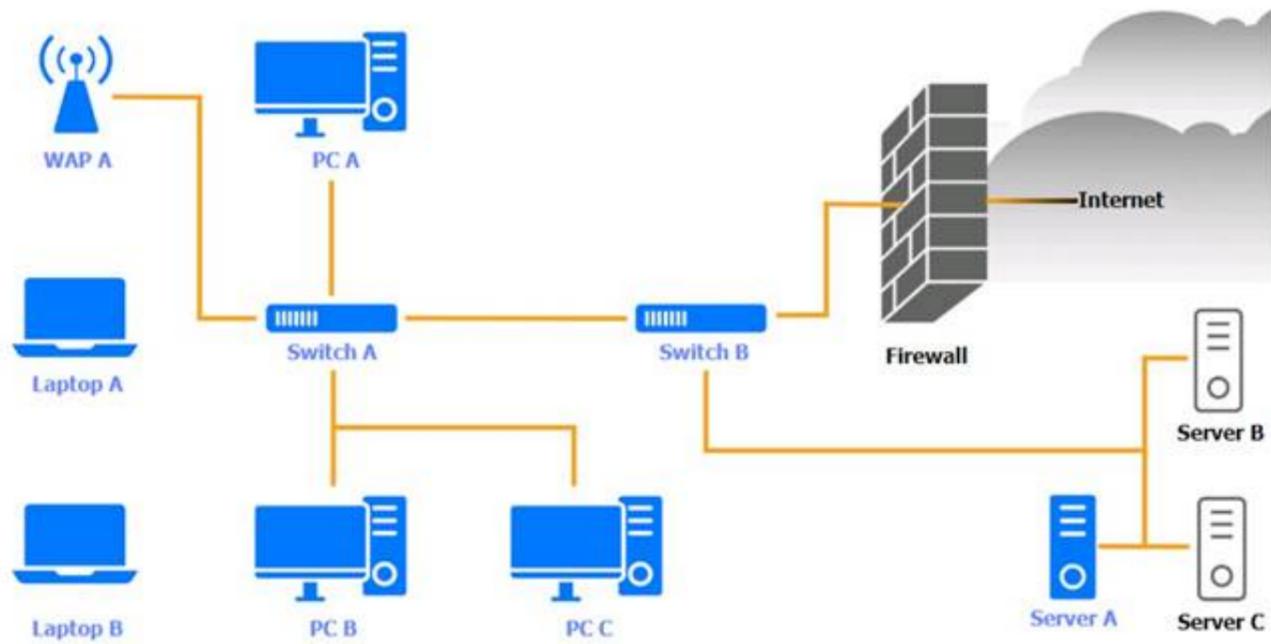
NEW QUESTION 280**SIMULATION**

A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

- The PostgreSQL server must only allow connectivity in the 10.1.2.0/24 subnet.
- The SSH daemon on the database server must be configured to listen to port 4022.
- The SSH daemon must only accept connections from a single workstation.
- All host-based firewalls must be disabled on all workstations.
- All devices must have the latest updates from within the past eight days.
- All HDDs must be configured to secure data at rest.
- Cleartext services are not allowed.
- All devices must be hardened when possible.

Instructions:

Click on the various workstations and network devices to review the posture assessment results. Remediate any possible issues or indicate that no issue is found. Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the PostgreSQL DATABASE VIA ssh



WAP A

WAP A		
Finding	Status	Remediation
Firmware	Updated 5 days ago	<input checked="" type="checkbox"/> No issue
Top 5 used ports	22, 80, 443, 123, 53	<input type="checkbox"/> Patch management
SSID broadcast	Disabled	<input type="checkbox"/> Update endpoint protection
Default admin account	Default password has been changed	<input type="checkbox"/> Enabled disk encryption
HTTP server	Disabled	<input type="checkbox"/> Enable port security on network device
		<input type="checkbox"/> Enable password complexity
		<input type="checkbox"/> Enable host-based firewall to block all traffic
		<input type="checkbox"/> Antivirus scan
		<input type="checkbox"/> Change default administrative password
		<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

PC A

PC A		
OS updates	Updated 2 days ago, last checked 5:08 a.m.	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked 6:11 a.m.	<input type="checkbox"/> Patch management
Browser version	91.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	Normal	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	<input type="checkbox"/> Change default administrative password
Wireless	Disabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Laptop A

Laptop A		
OS updates	Updated 3 days ago, last checked 6:08 a.m.	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked in 6:13 a.m.	<input type="checkbox"/> Patch management
Browser version	91.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	Medium	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	<input type="checkbox"/> Change default administrative password
Wireless	Enabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Switch A

Switch A ✕

Firmware	Updated 7 days ago	<input checked="" type="checkbox"/> No issue
Top 5 used ports	22, 80, 443, 123, 53	<input type="checkbox"/> Patch management
Interfaces disabled (out of 12)	4	<input type="checkbox"/> Update endpoint protection
Default admin account	Default password has not been changed	<input type="checkbox"/> Enabled disk encryption
HTTP server	Disabled	<input type="checkbox"/> Enable port security on network device
		<input type="checkbox"/> Enable password complexity
		<input type="checkbox"/> Enable host-based firewall to block all traffic
		<input type="checkbox"/> Antivirus scan
		<input type="checkbox"/> Change default administrative password
		<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Switch B:

Switch B ✕

Firmware	Updated 7 days ago	<input checked="" type="checkbox"/> No issue
Top 5 used ports	22, 80, 443, 123, 53	<input type="checkbox"/> Patch management
Interfaces disabled (out of 6)	1	<input type="checkbox"/> Update endpoint protection
Default admin account	Default password has been changed	<input type="checkbox"/> Enabled disk encryption
HTTP server	Disabled	<input type="checkbox"/> Enable port security on network device
		<input type="checkbox"/> Enable password complexity
		<input type="checkbox"/> Enable host-based firewall to block all traffic
		<input type="checkbox"/> Antivirus scan
		<input type="checkbox"/> Change default administrative password
		<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Laptop B

Laptop B ✕

OS updates	Updated 3 days ago, last checked 8:08 a.m.	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked in 8:11 a.m.	<input type="checkbox"/> Patch management
Browser version	81.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Disabled	<input type="checkbox"/> Enabled disk encryption
Password Complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	Normal	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 8080, 53	<input type="checkbox"/> Change default administrative password
Wireless	Enabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

PC B

PC B ✕

OS updates	Updated 2 days ago, last checked 5:10 a.m.	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked in 6:13 a.m.	<input type="checkbox"/> Patch management
Browser version	91.2.5 (7/31/2023)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	Medium	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	<input type="checkbox"/> Change default administrative password
Wireless	Disabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

PC C

PC C		
OS updates	Updated 22 days ago	<input checked="" type="checkbox"/> No issue
Endpoint protection	Last checked 6:19 a.m.	<input type="checkbox"/> Patch management
Browser version	91.2.5 (7/18/2022)	<input type="checkbox"/> Update endpoint protection
Disk encryption	Enabled	<input type="checkbox"/> Enabled disk encryption
Password complexity	Enabled	<input type="checkbox"/> Enable port security on network device
Host-based firewall	Disabled	<input type="checkbox"/> Enable password complexity
CPU & memory usage	High	<input type="checkbox"/> Enable host-based firewall to block all traffic
Screensaver	Enabled	<input type="checkbox"/> Antivirus scan
Top 5 used ports	22, 80, 443, 23, 53	<input type="checkbox"/> Change default administrative password
Wireless	Disabled	<input type="checkbox"/> Disable unneeded services
		<input type="checkbox"/> Enable all connectivity settings

Server A

Server A

Nmap | IP Tables

```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.4
80/tcp    closed http
443/tcp   closed ssl/http
1433/tcp  closed mssql
5432/tcp  closed postgresql
...
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R OUTPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -F OUTPUT
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

1 2 3 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --dport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
#iptables --list --verbose
Chain INPUT (policy DROP 5 packets, 341 bytes)

pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- any any anywhere anywhere tcp spts:login:65535 dpt:ssh state NEW,ESTABLISHED
1 28 DROP all -- any any anywhere anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WAP A: No issue found. The WAP A is configured correctly and meets the requirements. PC A = Enable host-based firewall to block all traffic
This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.

Laptop A: Patch management

This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.

Switch A: No issue found. The Switch A is configured correctly and meets the requirements.

Switch B: No issue found. The Switch B is configured correctly and meets the requirements.

Laptop B: Disable unneeded services

This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore, it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.

PC B: Enable disk encryption

This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B's data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.

PC C: Disable unneeded services

This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is the default and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:

sudo nano /etc/ssh/sshd_config

Server A. Need to select the following:

```
1 iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
2 iptables -D OUTPUT 2
3 iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
4 iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

A black and white screen with white text
Description automatically generated

NEW QUESTION 281

A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources.

Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

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

Answer: B

Explanation:

Cgroups (control groups) is a core Linux concept that reflects the ability to limit resource allocation to containers, such as CPU, memory, disk I/O, or network bandwidth. Cgroups can help prevent resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources, as it can enforce quotas or priorities for each container or group of containers. Union filesystem overlay is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a technique that allows multiple filesystems to be mounted on the same mount point, creating a layered representation of files and directories. Linux namespaces is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a feature that isolates and

virtualizes system resources for each process or group of processes, creating independent instances of global resources. Device mapper is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a framework that provides logical volume management, encryption, or snapshotting capabilities for block devices. Verified References: <https://www.comptia.org/blog/what-is-cgroups> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 285

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

- A. `grep -v '^4[0-9]{12}(:[0-9]{3})?$', file`
- B. `grep '^4[0-9]{12}(:[0-9]{3})?$', file`
- C. `grep '^6(?:011|5[0-9]{2})[0-9]{12}?', file`
- D. `grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?', file`

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

Answer: C

NEW QUESTION 289

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

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

Answer: C

Explanation:

Reference: <https://www.sciencedirect.com/topics/computer-science/revoke-certificate>
OCSP (Online Certificate Status Protocol) is a protocol that allows clients to check the revocation status of certificates in real time by querying an OCSP responder server. This would enable the organization to determine whether it is vulnerable to the active campaign utilizing a specific vulnerability, as it would show if any certificates have been compromised or revoked. Deploying an RA (registration authority) on each branch office may not help with checking the revocation status of certificates, as an RA is responsible for verifying the identity of certificate applicants, not issuing or revoking certificates. Using Delta CRLs (certificate revocation lists) at the branches may not provide timely or accurate information on certificate revocation status, as CRLs are updated periodically and may not reflect the latest changes. Implementing an inbound BGP (Border Gateway Protocol) prefix list may not help with checking the revocation status of certificates, as BGP is a protocol for routing network traffic between autonomous systems, not verifying certificates. Verified References: <https://www.comptia.org/blog/what-is-ocsp> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 291

A security consultant has been asked to recommend a secure network design that would:

- Permit an existing OPC server to communicate with a new Modbus server that is controlling electrical relays.
- Limit operational disruptions.

Due to the limitations within the Modbus protocol, which of the following configurations should the security engineer recommend as part of the solution?

- A. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 135.
- B. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 102.
- C. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port 5000.
- D. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502.

Answer: D

Explanation:

OPC (Open Platform Communications) and Modbus are two common protocols used for industrial control systems (ICS). OPC is a standard that allows different devices and applications to exchange data in a vendor-neutral way. Modbus is a serial communication protocol that enables devices to send and receive commands and data over a network. Modbus has two variants: Modbus TCP/IP, which uses TCP port 502 for communication, and Modbus RTU/ASCII, which uses serial ports.

To allow an OPC server to communicate with a Modbus server that is controlling electrical relays, the security engineer should recommend restricting inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502. This configuration would:

- ? Permit the OPC server to send commands and data to the Modbus server using Modbus TCP/IP protocol over port 502.
- ? Limit operational disruptions, by preventing unauthorized or malicious access to the Modbus server from other sources.
- ? Due to the limitations within the Modbus protocol, such as lack of encryption and authentication, restricting inbound traffic is a necessary security measure to protect the integrity and availability of the ICS.

Reference: CASP+ (Plus) Certification Training | CompTIA IT Certifications

NEW QUESTION 293

A large number of emails have been reported, and a security analyst is reviewing the following information from the emails:

```
Received: From postfix.com [102.8.14.10]
Received: From prod.protection.email.comptia.com [99.5.143.140]
SPF: Pass
From: <carl.b@comptia1.com>
Subject: Subject Matter Experts
X-IncomingHeaderCount: 4
Return-Path: carl.b@comptia.com
Date: Sat, 4 Oct 2020 22:01:59
```

As part of the image process, which of the following is the FIRST step the analyst should take?

- A. Block the email address carl.b@comptia1.com, as it is sending spam to subject matter experts
- B. Validate the final "Received" header against the DNS entry of the domain.
- C. Compare the "Return-Path" and "Received" fields.
- D. Ignore the emails, as SPF validation is successful, and it is a false positive

Answer: C

NEW QUESTION 294

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

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

Answer: BC

NEW QUESTION 299

The Chief Information Officer (CIO) wants to implement enterprise mobility throughout the organization. The goal is to allow employees access to company resources. However the CIO wants the ability to enforce configuration settings, manage data, and manage both company-owned and personal devices. Which of the following should the CIO implement to achieve this goal?

- A. BYOO
- B. CYOD
- C. COPE
- D. MDM

Answer: A

NEW QUESTION 304

A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log aggregator and allows remote access to MSSP analyst. Critical devices send logs to the log aggregator, where data is stored for 12 months locally before being archived to a

multitenant cloud. The data is then sent from the log aggregator to a public IP address in the MSSP datacenter for analysis.

A security engineer is concerned about the security of the solution and notes the following.

- * The critical devices send cleartext logs to the aggregator.
- * The log aggregator utilizes full disk encryption.
- * The log aggregator sends to the analysis server via port 80.
- * MSSP analysis utilizes an SSL VPN with MFA to access the log aggregator remotely.
- * The data is compressed and encrypted prior to being archived in the cloud. Which of the following should be the engineer's GREATEST concern?

- A. Hardware vulnerabilities introduced by the log aggregator server
- B. Network bridging from a remote access VPN
- C. Encryption of data in transit
- D. Multitenancy and data remnants in the cloud

Answer: C

Explanation:

Encryption of data in transit should be the engineer's greatest concern regarding the security of the solution. Data in transit refers to data that is being transferred over a network or between devices. If data in transit is not encrypted, it can be intercepted, modified, or stolen by attackers who can exploit vulnerabilities in the network protocols or devices. The solution in the question sends logs from the critical devices to the aggregator in cleartext and from the aggregator to the analysis server via port 80, which are both insecure methods that expose the data to potential attacks. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide>, <https://us-cert.cisa.gov/ncas/tips/ST04-019>

NEW QUESTION 308

An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment's notice.

Which of the following should the organization consider FIRST to address this requirement?

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

Answer: D

Explanation:

Reference: <https://searchdisasterrecovery.techtarget.com/definition/warm-site>

NEW QUESTION 310

Based on PCI DSS v3.4, One Particular database field can store data, but the data must be unreadable. which of the following data objects meets this requirement?

- A. PAN
- B. CVV2
- C. Cardholder name
- D. expiration date

Answer: A

NEW QUESTION 312

SIMULATION

A product development team has submitted code snippets for review prior to release. INSTRUCTIONS

Analyze the code snippets, and then select one vulnerability, and one fix for each code snippet.

Code Snippet 1

Code Snippet 1	Code Snippet 2
<pre> Web browser: URL: https://comptia.org/profiles/userdetails?userid=103 Web server code: -- String accountQuery = "SELECT * from users WHERE userid = ?"; PreparedStatement stmt = connection.prepareStatement(accountQuery); stmt.setString(1, request.getParameter("userid")); ResultSet queryResponse = stmt.executeQuery(); -- </pre>	

Code Snippet 2

```

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

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

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

    ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                  -h loginserver.comptia.org
                  -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
    accountLookup = subprocess.Popen(ldapLookup)

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

Vulnerability 1:

- ? SQL injection
- ? Cross-site request forgery
- ? Server-side request forgery
- ? Indirect object reference
- ? Cross-site scripting

Fix 1:

- ? Perform input sanitization of the userid field.
- ? Perform output encoding of queryResponse,
- ? Ensure usex:ia belongs to logged-in user.
- ? Inspect URLs and disallow arbitrary requests.
- ? Implement anti-forgery tokens.

Vulnerability 2

- 1) Denial of service
- 2) Command injection
- 3) SQL injection
- 4) Authorization bypass
- 5) Credentials passed via GET

Fix 2

- A) Implement prepared statements and bind variables.
- B) Remove the serve_forever instruction.
- C) Prevent the "authenticated" value from being overridden by a GET parameter.
- D) HTTP POST should be used for sensitive parameters.
- E) Perform input sanitization of the userid field.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Code Snippet 1

Vulnerability 1: SQL injection

SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.

Fix 1: Perform input sanitization of the userid field.

Input sanitization is a technique that prevents SQL injection by validating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.

Code Snippet 2

Vulnerability 2: Cross-site request forgery

Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.

Fix 2: Implement anti-forgery tokens.

Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti-forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

NEW QUESTION 315

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CAS-004 Exam with Our Prep Materials Via below:

<https://www.certleader.com/CAS-004-dumps.html>