

Exam Questions CAS-004

CompTIA Advanced Security Practitioner (CASP+) Exam

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



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

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

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

Answer: B

Explanation:

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

NEW QUESTION 3

A systems administrator is preparing to run a vulnerability scan on a set of information systems in the organization. The systems administrator wants to ensure that the targeted systems produce accurate information especially regarding configuration settings. Which of the following scan types will provide the systems administrator with the MOST accurate information?

- A. A passive, credentialed scan
- B. A passive, non-credentialed scan
- C. An active, non-credentialed scan
- D. An active, credentialed scan

Answer: D

NEW QUESTION 4

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 5

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

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

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

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

Answer: A

Explanation:

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

- ? SQL injection, which exploits a vulnerability in the application's database query to execute malicious SQL commands.
- ? Cross-site scripting (XSS), which injects malicious JavaScript code into the application's web page to execute on the client-side browser.
- ? Directory traversal, which accesses files or directories outside of the intended scope by manipulating the file path.

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

- ? Prevent the exfiltration of a company report by validating the file parameter in the URL and ensuring that it matches a predefined list of allowed files or formats.
- ? Enhance the security of the web application by filtering out any malicious or invalid input from users or attackers.
- ? Be more effective and efficient than other techniques, such as firewall, WAF (Web Application Firewall), or DLP (Data Loss Prevention), which may not be able to detect or block all types of web application attacks.

NEW QUESTION 6

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

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

Answer: B

NEW QUESTION 7

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

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

Answer: B

Explanation:

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

NEW QUESTION 8

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 9

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 10

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 \$520,000 per day revenue loss for each day the system is delayed going into production.
- 2) The inherent risk is high.
- 3) The residual risk is low.
- 4) There will be a staged deployment to the solution rollout to the contact center. Which of the following risk-handling techniques will BEST meet the organization's requirements?

- A. Apply for a security exemption, as the risk is too high to accept.
- B. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.

- C. Accept the risk, as compensating controls have been implemented to manage the risk.
- D. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.

Answer: D

NEW QUESTION 10

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

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

Answer: D

Explanation:

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

NEW QUESTION 12

Device event logs sources from MDM software as follows:

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 13

A forensic expert working on a fraud investigation for a US-based company collected a few disk images as evidence. Which of the following offers an authoritative decision about whether the evidence was obtained legally?

- A. Lawyers
- B. Court
- C. Upper management team
- D. Police

Answer: A

NEW QUESTION 18

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

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

Answer: A

Explanation:

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

NEW QUESTION 20

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 22

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

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

Answer: C

NEW QUESTION 26

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

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

Answer: B

Explanation:

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

NEW QUESTION 29

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

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

Answer: D

NEW QUESTION 31

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

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

Answer: C

Explanation:

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

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

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

have been denied if running in enforcing mode.

Disabled: SELinux is turned off.

To ensure its custom Android devices are used exclusively for package tracking, the company must configure SELinux to run in enforcing mode. This mode will prevent any unauthorized actions or applications from running on the devices and protect them from potential threats or misuse. References: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/chap-security-enhanced_linux-introduction#sect-Security-Enhanced_Linux-Modes <https://source.android.com/security/selinux>

NEW QUESTION 34

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

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

Answer: B

Explanation:

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

References: [CompTIA CASP+ Study Guide, Second Edition, page 36]

NEW QUESTION 36

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

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

Answer: C

Explanation:

The inability to select AES-256 encryption will most likely be a limiting factor when selecting mobile device managers for the company. AES-256 is a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. It is considered one of the strongest encryption methods available and is widely used for securing sensitive data. Mobile device managers are software applications that allow administrators to remotely manage and secure mobile devices used by employees. However, not all mobile device managers may support AES-256 encryption or allow the company to enforce it as a policy on all mobile devices.

Verified References: <https://www.comptia.org/training/books/casp-cas-004-study-guide>, <https://searchmobilecomputing.techtarget.com/definition/mobile-device-management>

NEW QUESTION 41

An organization's existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day vulnerability on the VPN concentrator. Consequently, the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.

Which of the following designs would be BEST for the CISO to use?

- A. Adding a second redundant layer of alternate vendor VPN concentrators
- B. Using Base64 encoding within the existing site-to-site VPN connections
- C. Distributing security resources across VPN sites
- D. Implementing IDS services with each VPN concentrator
- E. Transitioning to a container-based architecture for site-based services

Answer: A

Explanation:

If one VPN concentrator goes down due to a zero-day threat, having a redundant VPN concentrator of a different vendor should keep you going.

NEW QUESTION 42

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

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

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

Answer: A

NEW QUESTION 47

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 49

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

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

Answer: A

NEW QUESTION 53

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

Which of the following techniques would BEST support this?

- A. Configuring systemd services to run automatically at startup
- B. Creating a backdoor
- C. Exploiting an arbitrary code execution exploit
- D. Moving laterally to a more authoritative server/service

Answer: B

NEW QUESTION 58

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

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

Answer: D

Explanation:

Executing the files in the sandbox on the web proxy is the best solution to reduce the risk of employees downloading and opening malicious files from the internet. A sandbox is a secure and isolated environment that can run untrusted or potentially harmful code without affecting the rest of the system. By executing the files in the sandbox, the web proxy can analyze their behavior and detect any malicious activity before allowing them to reach the corporate workstations.

References: [CompTIA CASP+ Study Guide, Second Edition, page 273]

NEW QUESTION 59

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

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

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

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

Answer: D

NEW QUESTION 63

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 64

A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line. Which of the following commands would be the BEST to run to view only active Internet connections?

- A. sudo netstat -antu | grep "LISTEN" | awk '{print\$5}'
- B. sudo netstat -nlt -p | grep "ESTABLISHED"
- C. sudo netstat -plntu | grep -v "Foreign Address"
- D. sudo netstat -pnut -w | column -t -s '\$\w'
- E. sudo netstat -pnut | grep -P ^tcp

Answer: E

Explanation:

Reference: <https://www.codegrepper.com/code-examples/shell/netstat+find+port>
 The netstat command is a tool that displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The command has various options that can modify its output. The options used in the correct answer are:
 p: Show the PID and name of the program to which each socket belongs.
 n: Show numerical addresses instead of trying to determine symbolic host, port or user names.
 u: Show only UDP connections. t: Show only TCP connections.
 The grep command is a tool that searches for a pattern in a file or input. The option used in the correct answer is:
 P: Interpret the pattern as a Perl-compatible regular expression (PCRE).
 The pattern used in the correct answer is ^tcp, which means any line that starts with tcp. This will filter out any UDP connections from the output.
 The sudo command is a tool that allows a user to run programs with the security privileges of another user (usually the superuser or root). This is necessary to run the netstat command with the -p option, which requires root privileges.
 The correct answer will show only active TCP connections with numerical addresses and program names, which can be considered as active Internet connections. The other answers will either show different types of connections (such as listening or local), use different options that are not relevant (such as -a, -l, -w, or -s), or use different commands that are not useful (such as awk or column). References: <https://man7.org/linux/man-pages/man8/netstat.8.html>
<https://man7.org/linux/man-pages/man1/grep.1.html> <https://man7.org/linux/man-pages/man8/sudo.8.html>

NEW QUESTION 67

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 70

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

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

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

Answer: A

NEW QUESTION 73

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

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

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

Answer: DE

Explanation:

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

NEW QUESTION 78

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 81

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

Which of the following solutions does this describe?

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

Answer: A

Explanation:

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

NEW QUESTION 84

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 85

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 88

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 93

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 94

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

* System capacity is optimized.

* Cost is reduced.

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

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

Answer: BD

Explanation:

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

NEW QUESTION 97

An organization's assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API. Given this information, which of the following is a noted risk?

- A. Feature delay due to extended software development cycles
- B. Financial liability from a vendor data breach
- C. Technical impact to the API configuration
- D. The possibility of the vendor's business ceasing operations

Answer: A

Explanation:

Reference: <https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability>

NEW QUESTION 100

A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.

Which of the following should the engineer report as the ARO for successful breaches?

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

Answer: A

Explanation:

Reference: <https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/>

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

NEW QUESTION 102

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

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

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

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

Answer: BF

Explanation:

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

NEW QUESTION 106

A software house is developing a new application. The application has the following requirements:

- Reduce the number of credential requests as much as possible
- Integrate with social networks
- Authenticate users

Which of the following is the BEST federation method to use for the application?

- A. WS-Federation
- B. OpenID
- C. OAuth
- D. SAML

Answer: D

Explanation:

Reference: <https://auth0.com/blog/how-saml-authentication-works/>

NEW QUESTION 110

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

- A. Execute never
- B. Noexecute
- C. Total memory encryption
- D. Virtual memory protection

Answer: A

Explanation:

Execute never is a technology that can be enabled on the ARM architecture to prevent malware from inserting itself in another process' memory location. Execute never (also known as XN or NX) is a feature that marks certain memory regions as non-executable, meaning that they cannot be used to run code. This prevents malware from exploiting buffer overflows or other memory corruption vulnerabilities to inject malicious code into another process' memory space.

References: [CompTIA CASP+ Study Guide, Second Edition, page 295]

NEW QUESTION 113

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 117

A health company has reached the physical and computing capabilities in its datacenter, but the computing demand continues to increase. The infrastructure is fully virtualized and runs custom and commercial healthcare application that process sensitive health and payment information. Which of the following should the company implement to ensure it can meet the computing demand while complying with healthcare standard for virtualization and cloud computing?

- A. Hybrid IaaS solution in a single-tenancy cloud
- B. PaaS solution in a multi-tenancy cloud
- C. SaaS solution in a community cloud
- D. Private SaaS solution in a single-tenancy cloud.

Answer: A

Explanation:

A hybrid IaaS solution in a single-tenancy cloud is the best option for the company to meet the computing demand while complying with healthcare standards for virtualization and cloud computing. A hybrid IaaS solution allows the company to use both on-premises and cloud-based resources to scale up its capacity and performance. A single-tenancy cloud ensures that the company's data and applications are isolated from other customers and have dedicated resources and security controls. Verified References:

<https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html>

NEW QUESTION 122

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

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

Answer: C

Explanation:

A single-tenancy SaaS solution is the best solution for this company. SaaS stands for software as a service, which is a cloud-based model that allows customers to access applications hosted by a provider over the internet. A single-tenancy SaaS solution means that the company has its own dedicated instance of the application and its underlying infrastructure, which offers more control, customization, and security than a multi-tenancy SaaS solution where multiple customers share the same resources. A single-tenancy SaaS solution also eliminates the need for managing a private cloud or an on-premises infrastructure. Verified

References: <https://www.comptia.org/training/books/casp-cas-004-study-guide> , <https://www.ibm.com/cloud/learn/saas>

NEW QUESTION 126

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

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

Answer: B

Explanation:

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

NEW QUESTION 130

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 131

A new, online file hosting service is being offered. The service has the following security requirements:

- Threats to customer data integrity and availability should be remediated first.
- The environment should be dynamic to match increasing customer demands.
- The solution should not interfere with customers' ability to access their data at anytime.
- Security analysts should focus on high-risk items.

Which of the following would BEST satisfy the requirements?

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

Answer: C

Explanation:

A SOAR (Security Orchestration, Automation, and Response) solution is a software platform that can automate the detection and response of known threats, such as ransomware, phishing, or denial-of-service attacks. A SOAR solution can also integrate with other security tools, such as IPS, NGFW, SIEM, and threat feeds, to provide a comprehensive and dynamic security posture. A SOAR solution would best satisfy the requirements of the online file hosting service, because it would:

? Remediate threats to customer data integrity and availability first, by automatically applying predefined actions or workflows based on the severity and type of the threat.

? Allow the environment to be dynamic to match increasing customer demands, by scaling up or down the security resources and processes as needed.

? Not interfere with customers' ability to access their data at anytime, by minimizing the human intervention and downtime required for threat response.

? Enable security analysts to focus on high-risk items, by reducing the manual tasks and alert fatigue associated with threat detection and response.

Reference: CASP+ (Plus) CompTIA Advanced Security Practitioner Certification ...

NEW QUESTION 134

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

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

Answer: AC

Explanation:

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

NEW QUESTION 139

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

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

Answer: C

Explanation:

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

Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide: Chapter 5:

Security Testing, Section 5.4: Defining Scope and Objective.

NEW QUESTION 142

A company wants to refactor a monolithic application to take advantage of cloud native services and service microsegmentation to secure sensitive application components. Which of the following should the company implement to ensure the architecture is portable?

- A. Virtualized emulators
- B. Type 2 hypervisors
- C. Orchestration
- D. Containerization

Answer: D

Explanation:

Containerization is a technology that allows applications to run in isolated and portable environments called containers. Containers are lightweight and self-contained units that include all the dependencies, libraries, and configuration files needed for an application to run. Containers can be deployed on any platform that supports the container runtime engine, such as Docker or Kubernetes. Containerization would allow the company to refactor a monolithic application to take advantage of cloud native services and service microsegmentation to secure sensitive application components, because containerization would:

- ? Enable the application to be split into smaller and independent components (microservices) that can communicate with each other through APIs or message queues.
- ? Allow the application to leverage cloud native services, such as load balancers, databases, or serverless functions, that can be integrated with containers through configuration files or environment variables.
- ? Enhance the security of the application by isolating each container from other containers and the host system, and applying fine-grained access control policies and network rules to each container or group of containers.
- ? Ensure the portability of the application by enabling it to run on any cloud provider or platform that supports containers, without requiring any changes to the application code or configuration.

NEW QUESTION 147

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

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

Answer: D

Explanation:

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

NEW QUESTION 150

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 155

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 157

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 162

A company's Chief Information Officer wants to implement IDS software onto the current system's architecture to provide an additional layer of security. The software must be able to monitor system activity, provide information on attempted attacks, and provide analysis of malicious activities to determine the processes or users involved. Which of the following would provide this information?

- A. HIPS
- B. UEBA
- C. HIDS
- D. NIDS

Answer: B

NEW QUESTION 166

A security architect for a large, multinational manufacturer needs to design and implement a security solution to monitor traffic. When designing the solution, which of the following threats should the security architect focus on to prevent attacks against the network?

- A. Packets that are the wrong size or length
- B. Use of any non-DNP3 communication on a DNP3 port
- C. Multiple solicited responses over time
- D. Application of an unsupported encryption algorithm

Answer: C

NEW QUESTION 167

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

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

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

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

Answer: BF

Explanation:

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

NEW QUESTION 172

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 177

A company plans to build an entirely remote workforce that utilizes a cloud-based infrastructure. The Chief Information Security Officer asks the security engineer to design connectivity to meet the following requirements:

Only users with corporate-owned devices can directly access servers hosted by the cloud provider.

The company can control what SaaS applications each individual user can access. User browser activity can be monitored.

Which of the following solutions would BEST meet these requirements?

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

Answer: B

Explanation:

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

NEW QUESTION 180

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 181

A company suspects a web server may have been infiltrated by a rival corporation. The security engineer reviews the web server logs and finds the following:

```
ls -l -a /usr/heimz/public; cat ./config/db.yml
```

The security engineer looks at the code with a developer, and they determine the log entry is created when the following line is run:

```
system ("ls -l -a ${path}")
```

Which of the following is an appropriate security control the company should implement?

- A. Restrict directory permission to read-only access.
- B. Use server-side processing to avoid XSS vulnerabilities in path input.
- C. Separate the items in the system call to prevent command injection.
- D. Parameterize a query in the path variable to prevent SQL injection.

Answer: C

Explanation:

The company using the wrong port is the most likely root cause of why secure LDAP is not working. Secure LDAP is a protocol that provides secure communication between clients and servers using LDAP (Lightweight Directory Access Protocol), which is a protocol that allows querying and modifying directory services over TCP/IP. Secure LDAP uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt LDAP traffic and prevent unauthorized disclosure or interception.

NEW QUESTION 183

During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee.

Which of the following processes would BEST satisfy this requirement?

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

Answer: B

Explanation:

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

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

NEW QUESTION 188

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

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

Answer: E

NEW QUESTION 192

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

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

Answer: B

Explanation:

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

Verified References:

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

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

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

NEW QUESTION 195

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

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

Answer: C

Explanation:

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

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

? The reliability and security of the Internet connections, which may vary depending on the location, provider, and traffic conditions.

? The compatibility and interoperability of the SD-WAN hardware and software, which may come from different vendors or use different standards.

? The availability and quality of the SD-WAN provider's support, which may depend on the provider's size, reputation, and outsourcing practices.

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

? Affect the organization's ability to resolve issues or request changes in a timely and effective manner.

? Expose the organization's network data and configuration to unauthorized or malicious parties.

? Increase the complexity and uncertainty of the SD-WAN service level agreement (SLA) and contract terms.

NEW QUESTION 196

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 200

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 204

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

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

Answer: D

Explanation:

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

NEW QUESTION 206

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

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 208

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 213

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 217

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

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

Answer: A

NEW QUESTION 220

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 221

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 224

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 229

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

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

Answer: B

Explanation:

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

NEW QUESTION 233

A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise. The company would like to find a way to use this information to protect the environment while still gaining valuable attack information.

Which of the following would be BEST for the company to implement?

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

Answer: D

Explanation:

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

NEW QUESTION 236

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. Containenzation

Answer: CDF

Explanation:

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

NEW QUESTION 238

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 240

A developer implement the following code snippet.

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

Which of the following vulnerabilities does the code snippet resolve?

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

Answer: A

Explanation:

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

NEW QUESTION 244

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

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

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

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

Answer: D

Explanation:

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

NEW QUESTION 245

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

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

Answer: C

Explanation:

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

NEW QUESTION 247

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

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

Answer: C

Explanation:

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

NEW QUESTION 249

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 253

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

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

Answer: D

Explanation:

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

NEW QUESTION 257

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

```
High CVEs: 30-01
CVE: CVE-2017-1351: Buffer Overflow Vulnerability (Windows) (IDB: 1.3.4.1.4.1.25423.1.0.000017)
Product Detection result: open/activex/1.3.4 by IIS Version Detection (Source: IDB: 1.3.4.1.4.1.25423.1.0.000109)

Summary
This host is running IIS and is prone to buffer overflow vulnerability.
Vulnerability Detection Result: installed version: 1.3.4
Fixed version: 1.3.15/1.4.5

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

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

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

Answer: A

NEW QUESTION 261

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

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

Which of the following techniques should be used?

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

Answer: A

NEW QUESTION 265

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

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

Answer: C

NEW QUESTION 268

A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens' personal, private, and confidential data?

- A. The principle of lawful, fair, and transparent processing
- B. The right to be forgotten principle of personal data erasure requests
- C. The non-repudiation and deniability principle
- D. The principle of encryption, obfuscation, and data masking

Answer: A

NEW QUESTION 273

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

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

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

Answer: D

Explanation:

SD-WAN (software-defined wide area network) vertical heterogeneity is a technique that can help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility. SD-WAN vertical heterogeneity involves using different types of network links (such as broadband,

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

NEW QUESTION 278

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

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

Answer: D

NEW QUESTION 279

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

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

Answer: A

NEW QUESTION 280

A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year. Which of the following will MOST likely secure the data on the lost device?

- A. Require a VPN to be active to access company data.
- B. Set up different profiles based on the person's risk.
- C. Remotely wipe the device.
- D. Require MFA to access company applications.

Answer: C

Explanation:

Remotely wiping the device is the best way to secure the data on the lost device, as it would erase all the data and prevent unauthorized access. Requiring a VPN to be active to access company data may not protect the data on the device itself, as it could be stored locally or cached. Setting up different profiles based on the person's risk may not prevent data loss or theft, as it depends on the level of access and encryption. Requiring MFA to access company applications may not protect the data on the device itself, as it could be stored locally or cached. Verified References: <https://www.comptia.org/blog/what-is-byod> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 283

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 287

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 289

A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.

Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

- A. Perform additional SAST/DAST on the open-source libraries.
- B. Implement the SDLC security guidelines.
- C. Track the library versions and monitor the CVE website for related vulnerabilities.
- D. Perform unit testing of the open-source libraries.

Answer: C

Explanation:

Reference: <https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/>

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

NEW QUESTION 291

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

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

Answer: C

Explanation:

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

NEW QUESTION 296

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

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

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

- A. Quarantine 10.0.5.52 and run a malware scan against the host.
- B. Access 10.0.5.52 via EDR and identify processes that have network connections.
- C. Isolate 10.0.50.6 via security groups.
- D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Answer: D

NEW QUESTION 297

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

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

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

Answer: D

NEW QUESTION 299

An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key.

Which of the following would BEST secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

- A. Implement a VPN for all APIs.
- B. Sign the key with DSA.
- C. Deploy MFA for the service accounts.
- D. Utilize HMAC for the keys.

Answer: D

Explanation:

Utilizing HMAC (hash-based message authentication code) for the keys is the best option for securing the REST API connection to the database while preventing the use of a hard-coded string in the request string. HMAC is a technique that uses a secret key and a hash function to generate a code that can verify the authenticity and integrity of a message, preventing unauthorized modifications or tampering. Utilizing HMAC for the keys can prevent the use of a hard-coded string in the request string, as it can dynamically generate a unique code for each request based on the secret key and the message content, making it difficult to forge or replay. Implementing a VPN (virtual private network)

for all APIs is not a good option for securing the REST API connection to the database, as it could introduce latency or performance issues for API requests, as well as not prevent the use of a hard-coded string in the request string. Signing the key with DSA (Digital Signature Algorithm) is not a good option for securing the REST API connection to the database, as it could be vulnerable to attacks or forgery if the key is compromised or weak, as well as not prevent the use of a hard-coded string in the request string. Deploying MFA (multi-factor authentication) for the service accounts is not a good option for securing the REST API connection to the database, as it could affect the usability or functionality of API requests, as well as not prevent the use of a hard-coded string in the request string. Verified References: <https://www.comptia.org/blog/what-is-hmac> <https://partners.comptia.org/docs/default-source/resources/casp-content-guide>

NEW QUESTION 303

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 306

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

```
openssl s_client -host ldap1.comptia.com -port 636
CONNECTED(00000003)
...
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
Subject=/CN=*.comptia.com
Issuer=/DC=com/DC=danville/CN=chicago
```

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

- A. The clients may not trust idapt by default.
- B. The secure LDAP service is not started, so no connections can be made.

- C. Danvills.com is under a DDoS-inator attack and cannot respond to OCSP requests.
- D. Secure LDAP should be running on UDP rather than TCP.
- E. The company is using the wrong por
- F. It should be using port 389 for secure LDAP.
- G. Secure LDAP does not support wildcard certificates.
- H. The clients may not trust Chicago by default.

Answer: AF

Explanation:

The clients may not trust idapt by default because it is a self-signed certificate authority that is not in the trusted root store of the clients. Secure LDAP does not support wildcard certificates because they do not match the fully qualified domain name of the server. Verified References:

<https://www.professormesser.com/security-plus/sy0-401/ldap-and-secure-ldap/> , <https://www.comptia.org/training/books/casp-cas-004-study-guide>

NEW QUESTION 309

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 311

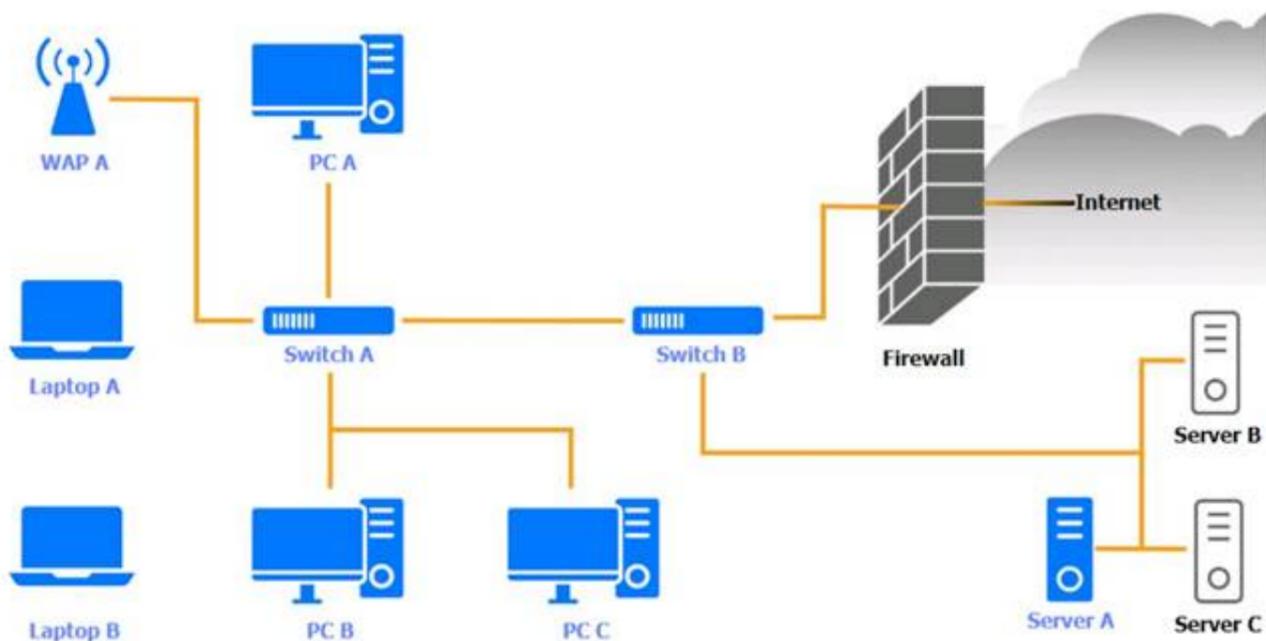
SIMULATION

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

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

Instructions:

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



WAP A

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

PC A

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

Laptop A

Laptop A

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

Switch A

Switch A

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

Switch B:

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

Laptop B

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

PC B

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

PC C

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

Server A

Server A ✕

Nmap IP Tables

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

1 2 3 4

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

1 2 3 4

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

1 2 3 4

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

1 2 3 4

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

Nmap IP Tables

```
#iptables --list --verbose

Chain INPUT (policy DROP 5 packets, 341 bytes)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

WAP A: No issue found. The WAP A is configured correctly and meets the requirements. PC A = Enable host-based firewall to block all traffic
 This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.
 Laptop A: Patch management
 This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.
 Switch A: No issue found. The Switch A is configured correctly and meets the requirements.
 Switch B: No issue found. The Switch B is configured correctly and meets the requirements.
 Laptop B: Disable unneeded services

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

PC B: Enable disk encryption

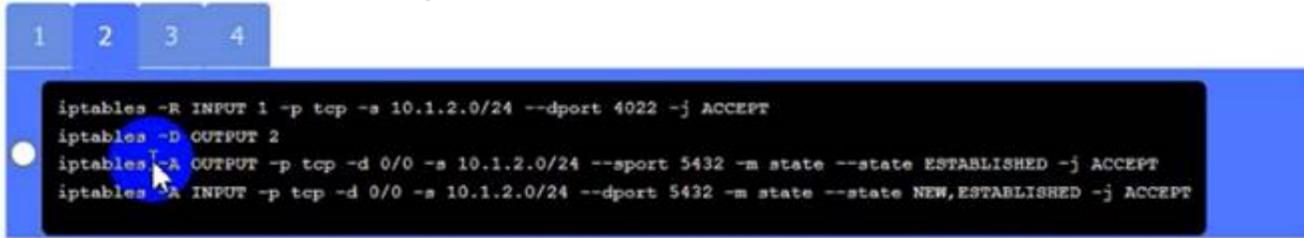
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement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

PC C: Disable unneeded services

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

```
sudo nano /etc/ssh/sshd_config
```

Server A. Need to select the following:



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

A black and white screen with white text
Description automatically generated

NEW QUESTION 313

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

CAS-004 Practice Exam Features:

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