CompTIA.CAS-005.v2026-11-04.q267

Exam Code:	CAS-005
Exam Name:	CompTIA SecurityX Certification Exam
Certification Provider:	CompTIA
Free Question Number:	267
Version:	v2026-11-04
# of views:	105
# of Questions views:	2670
https://www.freecram.net/torrent/CompTIA.CAS-005.v2026-11-04.q267.html	

NEW QUESTION: 1
After a company discovered a zero-day vulnerability in its VPN solution, the company plans to deploy cloud-hosted resources to replace its current on-premises systems. An engineer must find an appropriate solution to facilitate trusted connectivity. Which of the following capabilities is the most relevant?
A. Container orchestration
B. Microsegmentation
C. Conditional access
D. Secure access service edge
Answer: D (LEAVE A REPLY)
SASE combines network security (e.g., SWG, CASB, ZTNA, FWaaS) with WAN capabilities (SD- WAN) into a single cloud-delivered service. It is designed to provide secure and optimized access to cloud resources, replacing traditional VPNs with Zero Trust principles. This directly addresses the need for trusted connectivity while mitigating risks like VPN vulnerabilities.

NEW QUESTION: 2
During a review of the email security solution, a security analyst collects the following information:

File	Sender	Action	Time stamp
Invoice.rar	(External) jdoe@comptia.org	Quarantine	10:00:00
Cchrome.exe	(Internal) johnd@corp.com	Quarantine	10:15:00
Invoice.docx	(External) jdoe@comptia.org	Allowed	10:20:00

Which of the following is the best way to improve the email security solution on the email gateway?
A. Enabling allow lists
B. Configuring signature-based detection
C. Implementing a HIDS
D. Deploying sandboxing
Answer: (SHOW ANSWER)

NEW QUESTION: 3

A security architect is troubleshooting an issue with an OIDC implementation. The architect reviews the following configuration and errors:

Parameter	Required
client_id	Yes
state	Yes
response_type	Yes
scope	Yes
redirect_uri	No
nonce	Yes
code_challenge	No
code_challenge_type	No

Error: Invalid authentication request code

Which of the following is the most likely cause of the error?

A. The redirect-urlparameter is not in the allowed list of redirect hosts in the configuration.

B. Introspection is not enabled within the OIDC code implementation.

C. The encoding of the URL parameters on the proxy system is failing.

D. The stateparameter is being reused within the authentication challenge.

E. OAuth 2.0 was unable to verify the lack of an interception attack.

Answer: (SHOW ANSWER)

In OIDC, the redirect_uri must exactly match one of the allowed redirect URIs configured in the authorization server. If it is missing or not in the allowed list, the server will return an "invalid authentication request code" error, which fits the scenario shown.

NEW QUESTION: 4

A security engineer must implement controls to limit access between developer endpoints and a cloud provider bucket for data storage. Developers routinely save sensitive files to the bucket as part of their projects. The security engineer must reduce the risk of unintended data exposure.

Which of the following is the most appropriate control to implement?

A. Require server-side encryption using a KMS in the cloud provider.

B. Implement context-aware reauthentication to the local system.

C. Deploy an ACL on the virtual private cloud to avoid public access.

D. Restrict HTTP POST and PUT traffic to specific URLs at the proxy.

Answer: (SHOW ANSWER)

Applying an ACL on the virtual private cloud to restrict bucket access ensures that sensitive files are not exposed publicly. This limits access to only authorized endpoints, reducing the risk of unintended data exposure while still allowing developers to use the storage securely.

NEW QUESTION: 5

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)

A SOAR platform streamlines and automates repetitive detection and response workflows, like alert triage, enrichment, and ticketing, freeing up analysts to focus on high-value tasks. This orchestration capability reduces mean time to acknowledge and respond, directly boosting overall SOC efficiency and performance.

NEW QUESTION: 6
An engineer is designing a solution that addresses the following requirements:
- The security controls must be redundant.
- The security operations cannot be entirely disrupted by a supply chain attack.
- The systems must be resilient and better prepared for zero-day vulnerabilities.
Which of the following is the best way to meet these requirements?
A. Leveraging a managed service provider to support operations
B. Acquiring security solutions from a single vendor for seamless integration
C. Migrating current security solutions to the cloud
D. Deploying heterogeneous security solutions to offer a layered approach
Answer: (SHOW ANSWER)
The requirements emphasize redundancy, resilience, and avoiding a situation where a single supply chain attack could disable security operations. A heterogeneous, layered design reduces common-mode failure risk because different products, vendors, and control layers are less likely to fail in the same way at the same time. This also improves resilience against zero-day vulnerabilities, since one vendor's unknown weakness is less likely to compromise every control simultaneously. CompTIA's SecurityX objectives explicitly include "Security controls: preventive, detective, corrective, compensating, and deterrent" and "Architecture patterns: resilience, scalability, and performance." Those objective themes directly support a diverse, layered-control approach.

NEW QUESTION: 7
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? (Choose two.)
A. Configure firewall rules to block all external traffic.
B. Enable input validation for all fields.
C. Enable automatic updates to be installed on all servers.
D. Configure the security group to enable external traffic.
E. Set up a DLP policy to alert for exfiltration on all application servers.
F. Enable nightly vulnerability scans.
Answer: A,B (LEAVE A REPLY)
Configure firewall rules to block all external traffic: Since the security policy requires that only internal users have access to the application, configuring firewall rules to block all external traffic ensures that the application is not exposed to unauthorized users on the internet. This mitigates unauthorized access risks.
Enable input validation for all fields: Buffer overflows often exploit improper or lack of input validation. Enabling strict input validation ensures that only properly formatted data is accepted, preventing malicious input designed to exploit vulnerabilities in the application.

NEW QUESTION: 8
A mobile administrator is reviewing the following mobile device DHCP logs to ensure the proper mobile settings are applied to managed devices:

```
10,10/18/2021,17:01:05,Assign,192.168.1.10,UserA-MobileDevice,0236FB12CA0B
23,10/19/2021,07:11:19,Assign,192.168.1.23,UserA-MobileDevice,068ADIFAB109
10,10/20/2021,19:22:56,Assign,192.168.1.96,UserA-MobileDevice,0ABC65E81AB0
10,10/21/2021,22:34:15,Assign,192.168.1.33,UserA-MobileDevice,BAC034EF9451
10,10/22/2021,11:55:41,Assign,192.168.1.12,UserA-MobileDevice,0E938663221B
```

Which of the following mobile configuration settings is the mobile administrator verifying?

A. Service set identifier authentication

B. Wireless network auto joining

C. 802.1X with mutual authentication

D. Association MAC address randomization

Answer: (SHOW ANSWER)

The DHCP logs show multiple distinct MAC addresses associated with the same user and device (UserA-MobileDevice). This behavior suggests that the device is using MAC address randomization, a feature designed to enhance privacy by generating a unique, temporary MAC address when connecting to wireless networks. The mobile administrator is verifying this setting to ensure that the mobile devices are properly randomizing their MAC addresses for added security.

NEW QUESTION: 9

As part of a new software development method, a program manager requires that unit tests be written for all code before being promoted to production. The program manager wants to ensure that requirements can be tested and approved. Any security concerns should also be addressed prior to code deployment. Which of the following is an additional benefit of this new requirement?

A. Dynamic analysis

B. Integration testing

C. Software composition analysis

D. Input fuzzing

Answer: B (LEAVE A REPLY)

Requiring unit tests before promotion supports integration testing, as validated units can be reliably combined and tested together. This ensures that requirements are verifiable and that security concerns are addressed earlier in the development cycle.

NEW QUESTION: 10

A global manufacturing company has an internal application that is critical to making products. This application cannot be updated and must be available in the production area. A security architect is implementing security for the application. Which of the following best describes the action the architect should take?

A. Disallow wireless access to the application.

B. Deploy Intrusion detection capabilities using a network tap

C. Create an acceptable use policy for the use of the application

D. Create a separate network for users who need access to the application

Answer: (SHOW ANSWER)

Placing the application and its users on a separate, segmented network limits exposure and reduces the risk of compromise, especially since the application cannot be updated. This approach ensures availability while applying strong network-level security controls.

NEW QUESTION: 11

A company moved its on-premises services to the cloud. Although a recent audit verified that data throughout the cloud service is properly classified and documented, other systems are unable to act or filter based on this information. Which of the following should the company deploy to allow other cloud-based systems to consume this information?

A. Data mapping

B. Data labeling

C. Log scraping

D. Resource tagging

Answer: (SHOW ANSWER)

Data labeling enables metadata tagging for data classification, which allows systems to filter, act, and enforce policies based on the labels.

Data mapping is used for understanding data flows but does not support automation. Log scraping and resource tagging are unrelated to enabling system actions based on data classification.

NEW QUESTION: 12

An organization is implementing advanced security controls associated with the execution of software applications on corporate endpoints. The organization must implement a deny-all, permit-by-exception approach to software authorization for all systems regardless of OS. Which of the following should be implemented to meet these requirements?

A. SELinux

B. MDM

C. XDR

D. Block list

E. Atomic execution

Answer: (SHOW ANSWER)

MDM is correct because it is the only listed solution capable of enforcing cross-platform application allowlisting, which matches the required deny-all, permit-by-exception approach.).

NEW QUESTION: 13

A security analyst received a notification from a cloud service provider regarding an attack detected on a web server. The cloud service provider shared the following information about the attack:

- The attack came from inside the network.
- The attacking source IP was from the internal vulnerability scanners
- The scanner is not configured to target the cloud servers.

Which of the following actions should the security analyst take first?

A. Create an allow list for the vulnerability scanner IPs m order to avoid false positives

B. Configure the scan policy to avoid targeting an out-of-scope host

C. Set network behavior analysis rules

D. Quarantine the scanner sensor to perform a forensic analysis

Answer: (SHOW ANSWER)

Since the attack originated from an internal vulnerability scanner that wasn't supposed to scan the cloud servers, the first action should be to correct the scan policy to ensure it excludes out-of-scope targets. This prevents unintended disruption or alerts in the future.

NEW QUESTION: 14

A security architect for a global organization with a distributed workforce recently received funding lo deploy a CASB solution. Which of the following most likely explains the choice to use a proxy- based CASB?

A. The capability to block unapproved applications and services is possible

B. Privacy compliance obligations are bypassed when using a user-based deployment

C. Protecting and regularly rotating API secret keys requires a significant time commitment

D. Corporate devices cannot receive certificates when not connected to on-premises devices

Answer: (SHOW ANSWER)

A proxy-based CASB (Cloud Access Security Broker) allows the organization to inspect and control cloud traffic in real-time, providing the capability to block unapproved applications and services. This solution is effective for enforcing security policies and ensuring compliance across a distributed workforce by intercepting cloud traffic and applying security controls.

NEW QUESTION: 15

A security architect performs a baseline review on the SIEM. The findings indicate that multiple use cases are missing and coverage is limited for defense evasion techniques. Which of the following processes best describes what the architect should do?

A. Implement a TIP on the internal network to facilitate the creation of a use case.

B. Perform a penetration test on critical devices and document IOCs for use cases.

C. Create a list of use cases based on Snort detection rules.

D. Use Sigma to build the logic of the use cases and testing on the SIEM.

Answer: (SHOW ANSWER)

Sigma is a vendor-agnostic detection rule format that allows building and testing SIEM use cases efficiently. Using Sigma ensures broader coverage, including defense evasion techniques, and provides a standardized approach for detection logic.

NEW QUESTION: 16

A security engineer discovers that some workstations are trying to establish communication with an unknown domain. The engineer compiles the following information:

Domain	IP	TTL
c2callback25.io	189.45.22.9	5 minutes
c2callback25.io	201.100.13.45	3 minutes
c2callback25.io	200.171.140.192	3 minutes
c2callback25.io	188.144.20.10	5 minutes

Which of the following best describes this attack?

A. Fast flux

B. Sinkholing

C. On-path attack

D. DNS poisoning

Answer: (SHOW ANSWER)

The same domain resolves to multiple different IP addresses with very short TTL values. This pattern indicates rapid rotation of IP addresses associated with the domain. Fast flux is commonly used by botnets and command-and-control infrastructures to frequently change DNS records so the malicious service remains reachable while making it difficult for defenders to block or track the infrastructure.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:

https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 17

After a penetration test on the internal network the following report was generated:

Attack	Target	Result
Compromised host	ADMIN01$.CORP.LOCAL	Successful
Hash collected	KRBTGT.CORP.LOCAL	Successful
Hash collected	SQLSV.CORP.LOCAL	Successful
Pass the hash	SQLSV.CORP.LOCAL	Failed
Domain control	CORP.LOCAL	Successful

itexam.net CompTIA

Which of the following should be recommended to remediate the attack?

A. Deleting SQLSV

B. Reimaging ADMIN01$

C. Rotating KRBTGT password

D. Resetting the local domain

Answer: (SHOW ANSWER)

The KRBTGT account is a critical account used by the Kerberos authentication protocol. The fact that the hash for KRBTGT.CORP.LOCAL was successfully collected during the attack indicates that the attacker may have gained access to Kerberos tickets and could potentially impersonate users. Rotating the KRBTGT password helps mitigate the risk of Kerberos ticket forging, which is a common post-exploitation technique in attacks such as Pass-the-Ticket and Golden Ticket attacks. This will prevent attackers from using stolen hashes to impersonate users or gain unauthorized access to the domain.

NEW QUESTION: 18

A threat intelligence company's business objective is to allow customers to integrate data directly to different TIPs through an API. The company would like to address as many of the following objectives as possible:

- Reduce compute spend as much as possible.
- Ensure availability for all users.
- Reduce the potential attack surface.
- Ensure the integrity of the data provided.

Which of the following should the company consider to best meet the objectives?

A. Configuring a unique API secret key for accounts

B. Publishing a list of IOCs on a public directory

C. Implementing rate limiting for each registered user

D. Providing a hash of all data that is made available

Answer: (SHOW ANSWER)

Configuring a unique API secret key for accounts ensures only authenticated users can access the API, reducing the attack surface while maintaining data integrity and availability. It also supports efficient resource use by restricting unauthorized access, aligning with the business objectives.

NEW QUESTION: 19

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

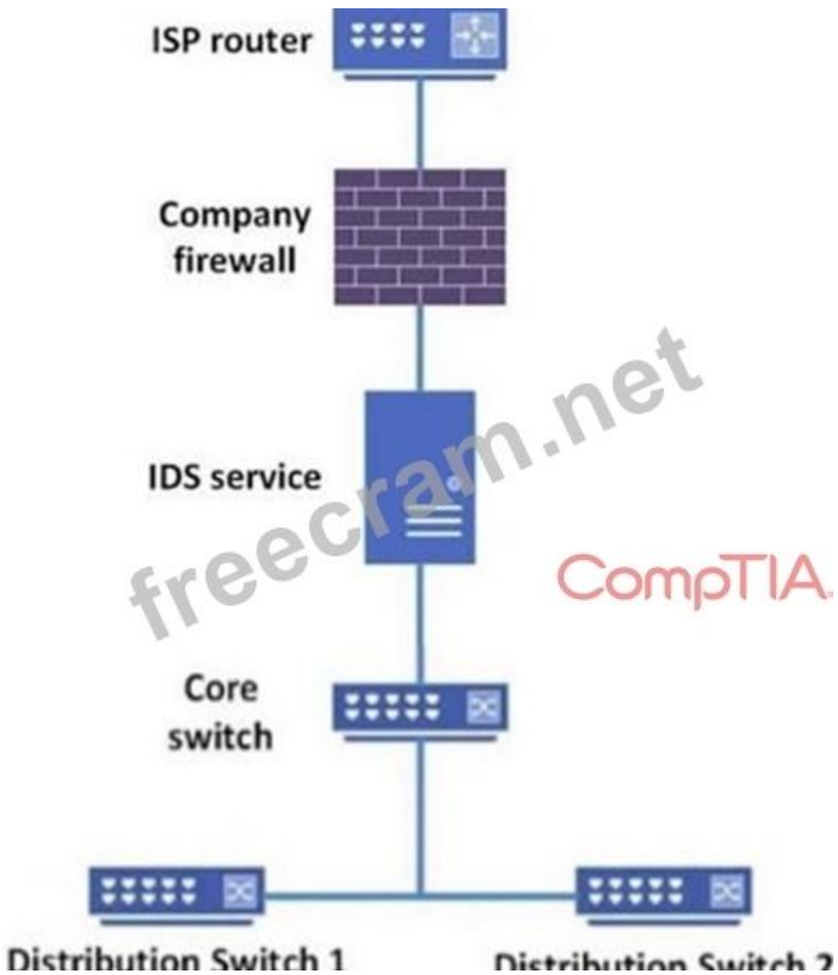
A. BGP

B. SD-WAN

C. PAM
D. NAC
E. MFA
F. Remote access VPN
G. Network segmentation
Answer: C,E,G (LEAVE A REPLY)

NEW QUESTION: 20
A company must meet the following security requirements when implementing controls in order to be compliant with government policy:
- Access to the system document repository must be MFA enabled.
- Ongoing risk monitoring must be displayed on a system dashboard.
- Staff must receive email notifications about periodic tasks.
Which of the following best meets all of these requirements?
Freecram.net
A. Implementing a GRC tool
B. Configuring a privileged access management system
C. Launching a vulnerability management program
D. Creating a risk register
Answer: (SHOW ANSWER)
A Governance, Risk, and Compliance (GRC) tool integrates multifactor authentication for access control, provides dashboards for ongoing risk monitoring, and supports automated email notifications, fulfilling all specified requirements.

NEW QUESTION: 21
A network security architect is working on capturing network traffic to support the following objectives in the pictured network:
- Capture relevant traffic to share with a threat intelligence vendor.
- Collect only traffic that could indicate a potential network intrusion.
- Minimize the budget and resource requirements of the collected traffic.



freecram.net
CompTIA.

Which of the following is the best way for the network security architect to capture network traffic?

A. Placing a network tap on the ISP router

B. Configuring a span port on the core switch

C. Deploying a transparent proxy on the firewall

D. Connecting a network hub to the IDS device

Answer: (SHOW ANSWER)

Configuring a SPAN (port mirroring) session on the core switch allows the architect to mirror selected network traffic to the IDS service for monitoring and analysis. This approach enables capturing only specific traffic flows relevant to potential intrusion activity by filtering VLANs or interfaces, which reduces the volume of collected data. SPAN functionality is built into most switches, making it a cost-effective solution that minimizes additional hardware and operational resources while still providing visibility into traffic that could indicate network attacks.

NEW QUESTION: 22

Previously intercepted communications must remain secure even if a current encryption key is compromised in the future. Which of the following best supports this requirement?

A. Tokenization

B. Key stretching

C. Forward secrecy

D. Simultaneous authentication of equals

Answer: (SHOW ANSWER)

Forward secrecy (FS) ensures that past encrypted data remains secure even if encryption keys are compromised in the future. It generates ephemeral session keys that are not reused.

NEW QUESTION: 23
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 Dockerfiles in a randomized namespace.
Answer: (SHOW ANSWER)
A secrets management tool is the most appropriate solution for securely managing and storing secrets (such as API keys, passwords, or tokens) in the new containerized environment. Secrets management tools, such as HashiCorp Vault, AWS Secrets Manager, or Azure Key Vault, provide secure storage, access control, and audit logs for secrets. They are designed to manage secrets in a way that avoids hardcoding sensitive data in configuration files or Dockerfiles, which could be exposed or compromised.

NEW QUESTION: 24
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. Self-encrypting disks with field-level encryption
C. NX/XN Implementation to minimize data retention
D. Token-based access for application users
E. Address space layout randomization
Answer: (SHOW ANSWER)
trying to connect a remote site to the central
Tokenization through an HSM (Hardware Security Module) is the most appropriate solution for securely storing and using previously saved payment methods for recurring transactions. Tokenization replaces sensitive data (like credit card numbers) with a token, which is a non- sensitive equivalent that cannot be reversed without the corresponding HSM. This ensures that sensitive payment information is never stored in an accessible format and protects customer data from breaches while still enabling the application to perform transactions.

NEW QUESTION: 25
After an increase in adversarial activity, a company wants to implement security measures to mitigate the risk of a threat actor using compromised accounts to mask unauthorized activity. Which of the following is the best way to mitigate the issue?
A. User and entity behavior analytics
B. Reverse engineering
C. Threat intelligence platforms
D. Web application firewall
Answer: A (LEAVE A REPLY)

NEW QUESTION: 26
A security engineer is performing threat modeling for an AI training architecture. The architecture implements a CI/CD pipeline to train a new AI model on a fixed schedule with live data from a back-end storage location. The engineer wants to use a threat modeling activity to focus on the threat as it moves through the CI/CD pipeline to the production environment. Which of the following is the most appropriate action for the engineer to take?

A. Map to OWASP Top 10.
B. Execute automated code reviews.
C. Identify trust boundaries.
D. Document data flows.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
A company needs to quickly assess whether software deployed across the company's global corporate network contains specific software libraries. Which of the following best enables the company's SOC to respond quickly when such an assessment is required?
A. Maintaining SAST/DAST reports on a server with access restricted to SOC staff
B. Contractually requiring all software vendors to attest to third-party risk mitigations
C. Requiring all suppliers and internal developers to implement a thorough SBoM
D. Implementing a GRC tool to maintain a list of all software vendors and internal developers
Answer: (SHOW ANSWER)
A Software Bill of Materials (SBoM) provides an inventory of all libraries and components in deployed software. Maintaining SBoMs allows the SOC to quickly identify affected systems when a vulnerable library is discovered, enabling a rapid and accurate response.

NEW QUESTION: 28
A security architect needs to enable a container orchestrator for DevSecOps and SOAR initiatives. The engineer has discovered that several Ansible YAML files used for the automation of configuration management have the following content:

```
$ hostnamectl
COMPTIA001

$ cat /etc/ansible/ansible.cfg
[inventory]
enable_plugins = kubernetes.core.k8s

$ cat /etc/ansible/projects/roles/k8/default/main.yml
---
- Name: Create a Kubernetes Service Objects
  kubernetes.core.k8s:
    state: present
    definition:
         apiVersion: v2
         kind: Service

$ cat /etc/kubernetes/manifests
insecure-bind-address "localhost"
```

freecram.net
CompTIA

Which of the following should the engineer do to correct the security issues presented within this content?
A. Update the kubernetes.core.k8smodule to kubernetes.core.k8s_servicein the main.ymlfile.

B. Update the COMPTIA001hostname to localhostusing the hostnamectlcommand.
C. Update the state: presentmodule to state: absent in the main.ymlfile.
D. Update or remove the ansible.cfgfile.
E. Update the insecure-bind-addressfrom localhostto the COMPTIA001in the manifests file.
Answer: D (LEAVE A REPLY)
The Ansible configuration file (/etc/ansible/ansible.cfg) contains an enable_plugins directive that allows Kubernetes modules to interact with Kubernetes resources. However, it does not enforce secure practices for managing these interactions, which could potentially expose sensitive data or allow unauthorized changes if not correctly configured or overly permissive.
The insecure configuration in the Ansible YAML file or the ansible.cfgfile should be reviewed or updated to enforce stricter security. Specifically, the configuration might inadvertently expose Kubernetes services to untrusted sources, and enabling plugins like kubernetes.core.k8s without sufficient control could lead to vulnerabilities.
Updating or removing the ansible.cfgfile ensures that secure defaults are applied, or more secure plugin configurations can be explicitly added, addressing the underlying issue.

NEW QUESTION: 29
A security engineer is developing a solution to meet the following requirements:
- All endpoints should be able to establish telemetry with a SIEM.
- All endpoints should be able to be integrated into the XDR platform.
- SOC services should be able to monitor the XDR platform
Which of the following should the security engineer implement to meet the requirements?
A. CDR and central logging
B. HIDS and vTPM
C. WAF and syslog
D. HIPS and host-based firewall
Answer: (SHOW ANSWER)
To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host-based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.

NEW QUESTION: 30
A company updates its cloud-based services by saving infrastructure code in a remote repository. The code is automatically deployed into the development environment every time the code is saved lo the repository. The developers express concern that the deployment often fails, citing minor code issues and occasional security control check failures in the development environment.
Which of the following should a security engineer recommend to reduce the deployment failures? (Select two).
Freecram.net
A. Software composition analysis
B. Pre-commit code linting
C. Repository branch protection
D. Automated regression testing
E. Code submit authorization workflow
F. Pipeline compliance scanning
Answer: (SHOW ANSWER)
Pre-commit code linting: Linting tools analyze code for syntax errors and adherence to coding standards before the code is committed to the repository. This helps catch minor code issues early in the development process, reducing the likelihood of deployment failures.

Automated regression testing: Automated regression tests ensure that new code changes do not introduce bugs or regressions into the existing codebase. By running these tests automatically during the deployment process, developers can catch issues early and ensure the stability of the development environment.

NEW QUESTION: 31
A systems engineer is configuring SSO for a business that will be using SaaS applications for its remote-only workforce. Privileged actions in SaaS applications must be allowed only from corporate mobile devices that meet minimum security requirements, but BYOD must also be permitted for other activity. Which of the following would best meet this objective?
A. Block any connections from outside the business's network security boundary.
B. Install machine certificates on corporate devices and perform checks against the clients.
C. Configure device attestations and continuous authorization controls.
D. Deploy application protection policies using a corporate, cloud-based MDM solution.
Answer: (SHOW ANSWER)
Device attestation ensures that only corporate-approved devices can perform privileged actions in SaaS applications. Continuous authorization monitors ongoing device compliance, dynamically adjusting permissions based on security posture.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 32
A security analyst is assessing a new application written in Java. The security analyst must determine which vulnerabilities exist during runtime. Which of the following would provide the most exhaustive list of vulnerabilities while meeting the objective?
A. Input validation
B. Dynamic analysis
C. Side-channel analysis
D. Fuzz testing
E. Static analysis
Answer: (SHOW ANSWER)
Dynamic analysis is the most appropriate technique for assessing vulnerabilities during runtime.
It involves testing the application while it is running, which allows the security analyst to observe the application's behavior, detect vulnerabilities that emerge during execution, and understand how the application interacts with its environment. This provides a comprehensive view of vulnerabilities that may not be detected through static code analysis, as it accounts for issues like memory corruption, data leaks, and runtime exceptions.

NEW QUESTION: 33
A security engineer wants to stay up-to-date on new detections that are released on a regular basis. The engineer's organization uses multiple tools rather than one specific vendor security stack. Which of the following rule-based languages is the most appropriate to use as a baseline for detection rules with the multiple security tool setup?
A. Sigma
B. YARA
C. Snort
D. Rita

Answer: (SHOW ANSWER)
Sigma is a rule-based detection language that is vendor-agnostic, meaning it can be used across different SIEM (Security Information and Event Management) tools.

NEW QUESTION: 34
A company needs to define a new road map for improving secure coding practices in the software development life cycle and implementing better security standards. Which of the following is the best way for the company to achieve this goal?
A. Performing a Software Assurance Maturity Model assessment and generating a road map as a final result
B. Conducting a threat-modeling exercise for the main applications and developing a road map based on the necessary security implementations
C. Developing a new road map, including secure coding best practices, based on the security area road map and annual goals defined by the Chief Information Security Officer
D. Using the best practices in the OWASP secure coding manual to define a new road map
Answer: (SHOW ANSWER)
Performing a Software Assurance Maturity Model (SAMM) assessment provides a structured way to evaluate current secure software practices and generate a tailored improvement road map. It aligns well with the goal of enhancing secure coding practices and implementing better security standards across the SDLC.

NEW QUESTION: 35
An organization decides to move to a distributed workforce model. Several legacy systems exist on premises and cannot be migrated because of existing compliance requirements. However, all new systems are required to be cloud-based. Which of the following would best ensure network access security?
A. Utilizing a VPN for all users who require legacy system access
B. Shifting all legacy systems to the existing public cloud infrastructure
C. Configuring an SDN to block malicious traffic to on-premises networks
D. Deploying microsegmentation with a firewall acting as the core router
Answer: (SHOW ANSWER)
Using a VPN for users who require access to legacy systems ensures secure, encrypted connectivity to the on-premises environment while maintaining compliance and supporting a distributed workforce. It's the most effective solution given the constraints on migrating legacy systems.

NEW QUESTION: 36
A security engineer is reviewing a security incident in which an employee account was compromised. The engineer notes the following activity after reviewing the logs:

```
Username: employee1
Password: Thi5i5aPa55w0rd
Last logon: 2025-04-08 19:23:56UTC ASN-Unknown Location
Previous logon: 2025-04-08 19:21:56UTC ASN-Location1
Password last modification date: 2025-03-07 09:08:08UTC
MFA status: enabled
```

Which of the following is the best way to reduce the probability of a future compromise?
A. Using a different third-party MFA vendor
B. Configuring password complexity to include special characters
C. Implementing conditional access across the organization
D. Increasing the rotation rate of account credentials
Answer: (SHOW ANSWER)
The logs show two login events within minutes from different network locations or ASNs, which is characteristic of an impossible travel or suspicious location scenario. Even though MFA is enabled, access was still obtained, indicating that additional contextual access controls are needed. Implementing conditional access allows authentication decisions to incorporate factors such

as location, network, device posture, and behavioral anomalies, enabling the system to block or require additional verification for suspicious login attempts and significantly reducing the likelihood of similar compromises.

NEW QUESTION: 37
While investigating an email server that crashed, an analyst reviews the following log files:

Time	Source	Process name	Process user	Action
10:25	ADMIN-PC	backup-mailbox	backup-admin	Network access
10:27	LOCAL	mailbox-store	SYSTEM	Write to disk
10:28	SALES-PC1	user-login	sales-user1	Network access
10:30	LOCAL	acct-switch	SYSTEM	Success
10:35	SALES-PC1	mailbox-erase	SYSTEM	Delete from disk
10:36	LOCAL	mailbox-store	SYSTEM	File not found

freecram.net CompTIA

Which of the following is most likely the root cause?
A. The administrator's account credentials were intercepted and reused.
B. The backup process did not complete and caused cascading failure.
C. A hardware failure in the storage array caused the mailboxes to be inaccessible.
D. A user with low privileges was able to escalate and erase all mailboxes.
Answer: (SHOW ANSWER)
The log shows the backup-admin performing network access followed shortly by the SYSTEM user deleting mailbox data, indicating possible misuse of the administrator's credentials or session.
This suggests the administrator's credentials were likely intercepted and reused, leading to unauthorized deletion and the server crash.

NEW QUESTION: 38
A nation-state actor is exposed for attacking large corporations by establishing persistence in smaller companies that are likely to be acquired by these large corporations. The actor then provisions user accounts in the companies for use post-acquisition. Before an upcoming acquisition, a security officer conducts threat modeling with this attack vector. Which of the following practices is the best way to investigate this threat?
A. Restricting internet traffic originating from countries in which the nation-state actor is known to operate
B. Comparing all existing credentials to personnel and services
C. Auditing vendors to mitigate supply chain risk during the acquisition
D. Placing a hold on all information about corporate interest in acquisitions
Answer: (SHOW ANSWER)
Comparing all existing credentials to personnel and services is the best practice to investigate this threat. By reviewing and comparing the credentials used by employees and services within the company, the security officer can identify any unauthorized or suspicious accounts, including those provisioned by the nation-state actor for post-acquisition persistence.
This step helps identify and mitigate the risk of malicious accounts being established before the acquisition takes place.

NEW QUESTION: 39
A security engineer would like to control configurations on mobile devices while fulfilling the following requirements:
- Support and control Apple and Android devices.
- The device must be corporate-owned.
Which of the following would enable the engineer to meet these requirements? (Choose two.)

A. Create a group policy to lock down mobile devices.
B. Update verbiage in the acceptable use policy for the internet.
C. Implement an MDM solution.
D. Implement a captive portal solution.
E. Update policy to prohibit the use of BYOD devices.
F. Implement a RADIUS solution.
Answer: C,E (LEAVE A REPLY)
Implement an MDM solution (Mobile Device Management): An MDM solution is specifically designed to manage, monitor, and secure mobile devices. It allows organizations to enforce configuration policies, enforce encryption, restrict apps, and control access to corporate resources on both Apple and Android devices. This solution directly meets the requirement to support and control corporate-owned devices.
Update policy to prohibit the use of BYOD devices: By prohibiting the use of Bring Your Own Device (BYOD) devices, the organization ensures that only corporate-owned devices are used, fulfilling the requirement that the devices must be corporate-owned. This policy helps maintain control over the mobile devices within the organization's environment.

NEW QUESTION: 40
A security operations analyst is reviewing network traffic baselines for nightly database backups.
Given the following information:

Date	Time	Bandwidth consumed	SRC server	DST server
12/1	12:01 a.m.	11.24GB	PRDDB01	BACKUP01
12/2	12:01 a.m.	11.57GB	PRDDB01	BACKUP01
12/3	12:01 a.m.	11.70GB	PRDDB01	BACKUP01
12/3	12:46 a.m.	97.00GB	PRDDB01	85.34.17.98
12/4	12:01 a.m.	10.95GB	PRDDB01	BACKUP01

Which of the following should the security analyst do next?
A. Consult with a network engineer to determine the impact of bandwidth usage.
B. Quarantine PRDDB01 and then alert the database engineers.
C. Refer to the incident response playbook for the proper response.
D. Review all the network logs for further data exfiltration.
Answer: C (LEAVE A REPLY)
The unexpected 97GB data transfer to an external IP (85.34.17.98) at an unusual time (12:46 a.m.) is a strong indicator of potential data exfiltration. The appropriate next step is to follow the incident response playbook to ensure a structured and compliant response.

NEW QUESTION: 41
A security administrator has isolated a computer system because it was targeted by a ransomware attack. Which of the following should the security administrator do to recover from this attack in the most secure way?
A. Check if file versioning is enabled and restore the files.
B. Restore the system from a baseline snapshot.
C. Determine if the encryption key can be recovered. If it can, restore the files.
D. Seek approval from senior leadership to pay the ransom and unencrypt the files with the provided key.
Answer: (SHOW ANSWER)
Restoring from a known-good, immutable snapshot ensures you return the system to a clean, pre-infection state without any residual ransomware artifacts or potential backdoors. Snapshots are typically protected from tampering and provide a trusted recovery point, making this the most secure and reliable remediation method.

NEW QUESTION: 42
A pharmaceutical company employs automated control systems to fabricate chemicals. During a recent experiment to attempt to secure these systems, a security engineer finds that the controllers do not appear to be sensitive to additional network latency. Which of the following is the best recommendation for this issue?
A. Performing integrity checks on control system command journals
B. Performing baseline reviews on the system configurations
C. Integrating a proxy to drop improperly formatted commands
D. Implementing in-line encryption between the control systems
E. Deploying and configuring a protocol accelerator
Answer: (SHOW ANSWER)
The test showed that the control systems are not sensitive to additional network latency. This means security controls that introduce latency can be safely deployed without disrupting operations. Implementing in-line encryption between the control systems would protect command and telemetry traffic from interception or manipulation while maintaining system functionality.
Since latency is not a concern, encryption becomes a viable and effective control for securing communications within the industrial control environment.

NEW QUESTION: 43
The Chief Information Security Officer of a large multinational organization has asked the security risk manager to use risk scenarios during a risk analysis. Which of the following is the most likely reason for this approach?
A. To connect risks to business objectives
B. To ensure a consistent approach to risk
C. To present a comprehensive view of risk
D. To provide context to the relevancy of risk
Answer: (SHOW ANSWER)
Using risk scenarios helps to provide context to the relevancy of risk by illustrating how specific risks could affect the organization. This approach helps stakeholders understand the potential impact of risks in real-world terms, making it easier to prioritize actions based on the likelihood and consequences of each scenario. It also helps decision-makers better assess the practical implications of different risks on business operations.

NEW QUESTION: 44
A Chief Information Security Officer receives the following findings from a third-party risk assessment report:
Finding #1: Absence of a risk management process
Finding #2: Absence of a formal information security management system
Finding #3: Absence of formal procedures to review access
Finding #4: Absence of management engagement on monitoring security objectives Which of the following is best for the security team to use when remediating the findings?
A. Incorporate PCI DSS compliance.
B. Implement ISO/IEC 27001 standard recommendation.
C. Use OWASP to implement consistent security testing.
D. Research appropriate CIS benchmarks and apply them.
Answer: (SHOW ANSWER)
ISO/IEC 27001 provides a comprehensive framework for establishing, implementing, maintaining, and continually improving an information security management system. The standard specifically addresses risk management processes, formalized security governance, access control management and periodic reviews, and leadership involvement in monitoring and improving security objectives. Implementing this framework directly remediates the governance and management deficiencies identified in the assessment findings.

NEW QUESTION: 45
An organization has several systems deployed in a public cloud and wants to confirm that when data retention periods are reached, the data is properly disposed of. Which of the following best meets the organization's needs?
A. Double encrypting the data using both asymmetric and symmetric keys managed by the cloud service provider
B. Utilizing a data-wiping software to overwrite the existing data
C. Encrypting the data with customer-managed keys and then deleting both the encryption key and the volume
D. Asking the cloud provider for copies of certificates of destruction
Answer: (SHOW ANSWER)
Encrypting data with customer-managed keys and deleting both the key and the volume ensures that the data becomes cryptographically unrecoverable, even if the physical media still exists. This is the most reliable method for secure data disposal in cloud environments.

NEW QUESTION: 46
A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner. Which of the following is the best way to reduce the number of failed patch deployments?
A. Compliance tracking
B. Situational awareness
C. Change management
D. Quality assurance
Answer: (SHOW ANSWER)
To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 47
An organization's vulnerability management team is reviewing the following output from a scan of a production server:
Finding ID | Summary
Weak cryptographic library | The device allows the use of weak
cryptographic libraries.
End-of-life, third-party library | The running service includes an end- of-life, third-party library.
Remote service detected | The device is running FTP on TCP port 21.
End-of-life operating system | The operating system has reached end-of- life status.
Database detected | This device includes an installed database.
Which of the following should the team do first?
A. Deploy a bastion host in front of the devices.
B. Close the ports to the database service.

C. Upgrade to a manufacturer-supported operating system.
D. Disable the running FTP service.
Answer: (SHOW ANSWER)
The end-of-life operating system is the highest-priority foundational issue because it affects the overall security posture of the host. An unsupported OS no longer receives vendor security updates, which increases exposure across the entire system, including services and libraries running on it. From a SecurityX perspective, vulnerability management and asset lifecycle issues are part of security operations and enterprise resilience. Resolving the unsupported platform first addresses the broadest root problem. CompTIA's SecurityX exam coverage includes security operations, vulnerability management activities, and proper hardware/software asset management as core skills.

NEW QUESTION: 48
A systems engineer is configuring a system baseline for servers that will provide email services.
As part of the architecture design, the engineer needs to improve performance of the systems by using an access vector cache, facilitating mandatory access control and protecting against:
- Unauthorized reading and modification of data and programs
- Bypassing application security mechanisms
- Privilege escalation
- interference with other processes
Which of the following is the most appropriate for the engineer to deploy?
A. SELinux
B. Privileged access management
C. Self-encrypting disks
D. NIPS
Answer: (SHOW ANSWER)
SELinux (Security-Enhanced Linux) is a mandatory access control (MAC) system that enforces strict policies to prevent unauthorized access, privilege escalation, and inter-process interference. It also uses access vector caches to enhance performance, making it the most appropriate choice for this scenario.

NEW QUESTION: 49
A SOC engineer is designing a solution to automate a sequence of tasks in a timely manner with the least amount of effort. The following objectives must be met:
- IOCs must be verified
- Malicious domains must be blocked on all firewalls and email gateways
- An email must be sent confirming the status of the operations
Which of the following is the best way to achieve this goal?
A. Using APIs to perform queries over the IOC
B. Using a TAXII server to share STIX files
C. Running SCAP to configure the baseline
D. Deploying and executing playbooks
Answer: (SHOW ANSWER)
Executing automated playbooks enables a SOAR workflow that orchestrates multiple security tasks with minimal manual effort. A playbook can verify indicators of compromise, automatically push blocking rules to firewalls and email gateways, and send notification emails once the actions are completed. This approach automates the entire response sequence and ensures it is performed quickly and consistently.

NEW QUESTION: 50
A malware analyst must examine the following partial file sample recovered from a Linux workstation:



Attempts to run the code in a sandbox produce no results. Which of the following should the malware analyst do next to further analyze the malware and discover useful IoCs?

A. Convert the hex-encoded sample to binary and attempt to decompile it.

B. Run the encoded sample through an online vulnerability tool and check for any matches.

C. Pad the beginning and end of the sample with binary executables and attempt to execute it.

D. Use a disassembler on the unencoded snippet to convert from binary to ASCII text.

Answer: (SHOW ANSWER)

The sample is presented in hex format, not as a runnable binary. The correct next step is to convert the hex-encoded sample into its binary form and then attempt decompilation or disassembly. This allows the analyst to properly examine the executable structure and extract IoCs.

NEW QUESTION: 51

Which of the following best describes the reason a network architect would enable forward secrecy on all VPN tunnels?

A. This process is a requirement to enable hardware-accelerated cryptography.

B. This process reduces the success of attackers performing cryptanalysis.

C. The business requirements state that confidentiality is a critical success factor.

D. Modern cryptographic protocols list this process as a prerequisite for use.

Answer: (SHOW ANSWER)

Forward secrecy, also known as perfect forward secrecy, is a feature of certain key agreement protocols that ensures session keys will not be compromised even if the server's private key is compromised in the future. By enabling forward secrecy on VPN tunnels, each session uses a unique key, and these keys are not derived from a common master key. This means that even if an attacker obtains the server's private key, they cannot decrypt past sessions, thereby significantly reducing the effectiveness of cryptanalysis attacks.

NEW QUESTION: 52

Which of the following best explains the importance of determining organization risk appetite when operating with a constrained budget?

A. Risk appetite directly impacts acceptance of high-impact low-likelihood events.

B. Organizational risk appetite varies from organization to organization

C. Budgetary pressure drives risk mitigation planning in all companies

D. Risk appetite directly influences which breaches are disclosed publicly

Answer: (SHOW ANSWER)

Risk appetite defines the level of risk an organization is willing to accept. When budgets are constrained, understanding this threshold is essential to prioritize resources and determine whether to accept, mitigate, or transfer high-impact, low-likelihood risks.

NEW QUESTION: 53

An engineering team determines the cost to mitigate certain risks is higher than the asset values.
The team must ensure the risks are prioritized appropriately. Which of the following is the best way to address the issue?
A. Data labeling
B. Branch protection
C. Vulnerability assessments
D. Purchasing insurance
Answer: (SHOW ANSWER)
When the cost to mitigate certain risks is higher than the asset values, the best approach is to purchase insurance. This method allows the company to transfer the risk to an insurance provider, ensuring that financial losses are covered in the event of an incident. This approach is cost-effective and ensures that risks are prioritized appropriately without overspending on mitigation efforts.

NEW QUESTION: 54
A security architect wants to ensure a remote host's identity and decides that pinning the X.509 certificate to the device is the most effective solution. Which of the following must happen first?
A. Use Distinguished Encoding Rules (DER) for the certificate.
B. Extract the private key from the certificate.
C. Use an out-of-band method to obtain the certificate.
D. Compare the retrieved certificate with the embedded certificate.
Answer: (SHOW ANSWER)
When implementing certificate pinning, the first step is to securely obtain the remote host's
X.509 certificate through an out-of-band method. This ensures that the certificate is trusted and verified outside of the regular communication channel (e.g., via a secure channel or pre-distribution), preventing any potential man-in-the-middle attacks. Once the certificate is securely obtained and verified, it can then be pinned to the device so that future connections to that host will only be accepted if the certificate matches the pinned one.

NEW QUESTION: 55
During a recent assessment, a security analyst observed the following:

Hostname	BIOS password	Fully patched	Firewall status
Sales2	welcome!	No	Active
Accounting1	$$m0neY	Yes	Active
Marketing6	HiTHER3	Yes	Inactive
Operations3	welcome!	Yes	Active

CompTIA freeexam.net
Which of the following should the analyst use to address the vulnerabilities in the future?
A. Least privilege
B. System image hardening
C. Defense in depth
D. OS update
Answer: (SHOW ANSWER)

NEW QUESTION: 56
After an incident occurred, a team reported during the lessons-learned review that the team.
- Lost important Information for further analysis.
- Did not utilize the chain of communication
- Did not follow the right steps for a proper response

Which of the following solutions is the best way to address these findinds?
A. Requesting budget for better forensic tools to Improve technical capabilities for Incident response operations
B. Building playbooks for different scenarios and performing regular table-top exercises
C. Requiring professional incident response certifications tor each new team member
D. Publishing the incident response policy and enforcing it as part of the security awareness program
Answer: (SHOW ANSWER)
Building playbooks for different incident scenarios provides a structured, repeatable process for the team to follow, ensuring critical steps are followed, information is not lost, and communication is effectively managed. Regular table-top exercises help familiarize the team with these procedures, allowing them to practice and refine their response capabilities before a real incident occurs. This directly addresses the issues raised in the lessons-learned review.

NEW QUESTION: 57
A security architect discovers the following while reviewing code for a company's website:
selection = "SELECT Item FROM Catalog WHERE ItemID = " &
Request("ItemID")
Which of the following should the security architect recommend?
A. Client-side processing
B. Query parameterization
C. Data normalization
D. Escape character blocking
E. URL encoding
Answer: (SHOW ANSWER)
The code provided constructs an SQL query by directly concatenating user input (Request("ItemID")) with the query string. This approach is vulnerable to SQL injection attacks, where malicious input can be crafted to manipulate or compromise the database.
Query parameterization ensures that user input is treated as a parameter rather than executable code. By using parameterized queries, the database engine automatically escapes and safely handles input, eliminating the risk of SQL injection. This is the recommended best practice to secure database interactions against such vulnerabilities.

NEW QUESTION: 58
Which of the following best describes a common use case for homomorphic encryption?
A. Transmitting confidential data to a CSP for processing on a large number of resources without revealing information
B. Maintaining the confidentiality of data both at rest and in transit to and from a CSP for processing
C. Storing proprietary data across multiple nodes in a private cloud to prevent access by unauthenticated users
D. Processing data on a server after decrypting in order to prevent unauthorized access in transit
Answer: (SHOW ANSWER)

NEW QUESTION: 59
A compliance officer is reviewing the data sovereignty laws in several countries where the organization has no presence. Which of the following is the most likely reason for reviewing these laws?
A. The organization is performing due diligence of potential tax issues
B. The organization has been subject to legal proceedings in countries where it has a presence
C. The organization is concerned with new regulatory enforcement in other countries
D. The organization has suffered brand reputation damage from incorrect media coverage

Answer: (SHOW ANSWER)
Data sovereignty laws govern how data must be handled, stored, and transferred based on the jurisdiction in which the data resides. Even if the organization has no physical presence in certain countries, new regulatory enforcement in these regions may affect its operations, especially if it processes or stores data related to citizens in those countries. Therefore, the compliance officer is likely reviewing these laws to ensure the organization remains compliant with international regulations.

NEW QUESTION: 60
A security analyst is reviewing a SIEM and generates the following report:

Log source	Destination IP	Source IP	Hostname	Event ID	Action	Time
DEV001	192.168.1.2	192.168.2.2	VM001	9928	Deny connection	4:55:28
DEV001	192.168.3.2	192.168.2.2	VM001	1912	IPS Alert	7:21:41
DEV001	10.1.1.1,192.168.2.2,VM001,1822 Malware detection,8:11:12					
DEV001	10.1.1.1	192.168.2.2	VM001	9927	Allow connection	8:15:32

Later, the incident response team notices an attack was executed on the VM001 host. Which of the following should the security analyst do to enhance the alerting process on the SIEM platform?
A. Include the EDR solution on the SIEM as a new log source.
B. Perform a log correlation on the SIEM solution.
C. Improve parsing of data on the SIEM.
D. Create a new rule set to detect malware.
Answer: B (LEAVE A REPLY)
The logs show related events (e.g., malware detection, IPS alert, and eventual connection allowance) from the same source and host. Log correlation connects these related events across time to generate meaningful, actionable alerts. Enhancing correlation would have helped detect the attack pattern earlier.

NEW QUESTION: 61
A security officer is receiving alerts from a cloud service provider about a new wave of phishing campaigns. To prepare employees, the cloud service provider advises the company to make announcements and develop basic security competence. Which of the following solutions best aligns with the cloud service provider's advice?
A. Enhancing crisis management
B. Developing tabletop exercises
C. Establishing a security awareness program
D. Creating simulated attacks
Answer: (SHOW ANSWER)
A security awareness program educates employees about current threats, safe behaviors, and how to recognize phishing attempts. Announcements and training that build basic security competence align directly with this approach, preparing users to identify and report phishing campaigns and reducing the likelihood of successful attacks.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 62
A company is adopting microservice architecture in order to quickly remediate vulnerabilities and deploy to production. All of the microservices run on the same Linux platform. Significant time was spent updating the base OS before deploying code. Which of the following should the company do to make the process efficient?
A. Use Terraform scripts while creating golden images.
B. Create a cron job to run apt-update every 30 days.
C. Use snapshots to deploy code to existing compute instances.
D. Deploy a centralized update server.
Answer: A (LEAVE A REPLY)
Creating golden images with Terraform enables automated, consistent, and up-to-date deployment of microservices with a pre-patched base OS. This significantly reduces time spent on manual updates and accelerates production deployment in a microservices environment.

NEW QUESTION: 63
In order to follow new regulations, the Chief Information Security Officer plans to use a defense- in-depth approach for a perimeter network. Which of the following protections would best achieve this goal?
A. SAST, DAST, IAST
B. NGFW, IPS, EDR
C. SASE, IDS, SAST
D. CASB, DLP, EDR
Answer: (SHOW ANSWER)
A defense-in-depth approach for a perimeter network is best achieved with layered network and endpoint protections. NGFW provides advanced firewall capabilities, IPS detects and blocks network intrusions, and EDR extends protection to endpoints, creating a comprehensive security posture.

NEW QUESTION: 64
An auditor is reviewing the logs from a web application to determine the source of an incident.
The web application architecture includes an internet-accessible application load balancer, a number of web servers in a private subnet, application servers, and one database server in a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

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

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

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

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

A. Enable the X-Forwarded-For header at the load balancer.

B. Install a software-based HIDS on the application servers.

C. Install a certificate signed by a trusted CA.

D. Use stored procedures on the database server.

E. Store the value of the $_SERVER['REMOTE_ADDR'] received by the web servers.

Answer: (SHOW ANSWER)

In a tiered setup behind a proxy or load balancer, the web servers' REMOTE_ADDR will only ever show the balancer's IP, not the true client's.

By configuring the load balancer to inject the X-Forwarded-For HTTP header with the original client IP, that value can be logged by the web servers (and propagated downstream), ensuring every request can be traced back to the real source address.

NEW QUESTION: 65

A security architect wants to configure a mail server so it maintains an updated list of IOCs and blocks known-malicious incoming emails. Which of the following will the security architect most likely need for this task?

A. Log analyzer

B. Threat feed API

C. Scheduled taskWebhooks

D. Webhooks

E. Inbox deletion code

F. Security runbook

Answer: (SHOW ANSWER)

A threat intelligence feed API provides continuously updated indicators of compromise such as malicious IP addresses, domains, URLs, and email indicators. Integrating the mail server with this feed allows it to automatically retrieve updated threat intelligence and use those indicators to detect and block known malicious incoming emails. This enables the system to maintain a current list of threats without manual updates.

NEW QUESTION: 66

An organization determined its preparedness for a ransomware attack is inadequate. A security administrator is working on ways to improve and monitor the organization's response to ransomware attacks. Which of the following is the best action for the administrator to take?

A. Conduct backup testing.

B. Define the recovery point objective.

C. Perform a business impact analysis.
D. Verify the encryption key length.
Answer: (SHOW ANSWER)
Conducting backup testing is the best action to take in order to improve preparedness for a ransomware attack. Ensuring that backups are regularly tested and can be restored is crucial to recovering from a ransomware attack. Without reliable backups, a successful recovery from an attack could be delayed or impossible.

NEW QUESTION: 67
A company is migrating its data center to the cloud. Some hosts had been previously isolated, but a risk assessment convinced the engineering team to reintegrate the systems. Because the systems were isolated, the risk associated with vulnerabilities was low. Which of the following should the security team recommend be performed before migrating these servers to the cloud?
A. Performing patching and hardening
B. Deploying host and network IDS
C. Implementing least functionality and time-based access
D. Creating a honeypot and adding decoy files
Answer: (SHOW ANSWER)
Before migrating previously isolated systems to the cloud, it is essential to perform patching and hardening. These systems may have been neglected while isolated, so updating them with the latest security patches and applying hardening measures (such as disabling unnecessary services and implementing strict access controls) is crucial to reduce vulnerabilities. This ensures that the systems are secure before they are exposed to the wider cloud environment. CASP+ emphasizes the importance of securing systems through patch management and hardening before integrating them into more exposed environments like the cloud.

NEW QUESTION: 68
An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of the impact. Which of the following should the organization perform next?
A. Assess the residual risk.
B. Update the organization's threat model.
C. Move to the next risk in the register.
D. Recalculate the magnitude of the impact.
Answer: (SHOW ANSWER)
After applying mitigations that reduce the likelihood of a risk's impact, the next step is to assess the residual risk--the risk that remains after controls are implemented. This ensures the organization understands if the mitigation is sufficient or if further action is needed, aligning with risk management best practices.

NEW QUESTION: 69
A manufacturing plant is updating its IT services. During discussions, the senior management team created the following list of considerations:
- Staff turnover is high and seasonal.
- Extreme conditions often damage endpoints.
- Losses from downtime must be minimized.
- Regulatory data retention requirements exist.
Which of the following best addresses the considerations?
A. Establishing further environmental controls to limit equipment damage
B. Using a non-persistent virtual desktop interface with thin clients
C. Deploying redundant file servers and configuring database journaling
D. Maintaining an inventory of spare endpoints for rapid deployment

Answer: (SHOW ANSWER)
Using a non-persistent virtual desktop interface (VDI) with thin clients addresses the concerns effectively. Thin clients are durable and less prone to damage, and VDI allows for easy reconfiguration and deployment of endpoints, especially in environments with high staff turnover.
It also reduces the impact of endpoint failures and minimizes downtime while meeting regulatory data retention requirements, as the data resides centrally.

NEW QUESTION: 70
During a security assessment, a penetration tester executed the following attack:

```
C:\> copy /y "C:\payloads\evil.exe" "C:\Program Files\Data Process\data.exe"
C:\Program Files\Data Process\> sc start data.exe
```

The tester then shared the results with the security analyst. Which of the following should the analyst do to remediate the attack?
A. Implement a security endpoint solution.
B. Enable a PowerShell execution policy on the endpoint.
C. Disable services with unquoted paths on the endpoint.
D. Enable user control access on the endpoint.
Answer: (SHOW ANSWER)

NEW QUESTION: 71
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 checkUserExistsfunction.
Answer: (SHOW ANSWER)
The use of gets() allows an attacker to overflow the 20-byte username buffer by entering more data than it can hold. Enforcing a 20-character limit (for example, by switching to fgets(username, sizeof(username), stdin)) prevents buffer overruns and eliminates this class of vulnerability.

NEW QUESTION: 72
During a gap assessment, an organization notes that BYOD usage is a significant risk. The organization implemented administrative policies prohibiting BYOD usage. However, the organization has not implemented technical controls to prevent the unauthorized use of BYOD assets when accessing the organization's resources. Which of the following solutions should the organization implement to best reduce the risk of BYOD devices? (Choose two.)
A. Cloud IAM to enforce the use of token based MFA
B. Conditional access, to enforce user-to-device binding
C. NAC, to enforce device configuration requirements
D. PAM. to enforce local password policies
E. SD-WAN. to enforce web content filtering through external proxies

F. DLP, to enforce data protection capabilities
Answer: (SHOW ANSWER)
Conditional access allows the organization to restrict access based on device trust, enforcing user-to-device binding and blocking unauthorized BYOD devices.
Network Access Control (NAC) ensures only compliant and authorized devices can connect to the network, enforcing security configurations and reducing BYOD risks.

NEW QUESTION: 73
After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.
- Exfiltration of intellectual property
- Unencrypted files
- Weak user passwords
Which of the following is the best way to mitigate these vulnerabilities? (Select two).
A. Implementing data loss prevention
B. Deploying file integrity monitoring
C. Restricting access to critical file services only
D. Deploying directory-based group policies
E. Enabling modem authentication that supports MFA
F. Implementing a version control system
G. Implementing a CMDB platform
Answer: (SHOW ANSWER)
Implementing data loss prevention (DLP) will help prevent the exfiltration of intellectual property by monitoring and controlling the movement of sensitive data.
Deploying directory-based group policies can help enforce strong password policies, restrict access to sensitive resources, and ensure that security settings (such as encryption) are applied to files and systems across the organization. These actions directly address the identified vulnerabilities.

NEW QUESTION: 74
An organization is developing an in-house software platform to support capital planning and reporting functions. In addition to role-based access controls and auditing/logging capabilities, the product manager must include requirements associated with archiving data and immutable backups. Which of the following organizational considerations are most likely associated with this requirement? (Choose two.)
A. Crypto-export management controls
B. Supply chain weaknesses
C. Device attestation
D. Quality assurance
E. Legal hold compliance
F. Ransomware resilience
Answer: (SHOW ANSWER)
Legal hold compliance requires data archiving and immutability to preserve records for regulatory or legal purposes.
Ransomware resilience is achieved through immutable backups, which protect data integrity by preventing unauthorized alteration or deletion.

NEW QUESTION: 75
A company needs a highly secure method to transfer documents over an insecure network. The documents are highly sensitive, and the documents' encryption must be guaranteed even if the network traffic is intercepted. Which of the following encryption techniques is the best option?
A. Asymmetric

B. One-time pad
C. Symmetric
D. Lightweight
Answer: (SHOW ANSWER)

NEW QUESTION: 76
Which of the following items should be included when crafting a disaster recovery plan?
A. Redundancy
B. Testing exercises
C. Autoscaling
D. Competitor locations
Answer: (SHOW ANSWER)
Testing exercises are a critical component of a disaster recovery (DR) plan because they ensure that the plan works effectively in a real-world scenario. Testing allows organizations to validate their recovery procedures, identify potential gaps, and make improvements before an actual disaster occurs. It helps ensure that all team members are familiar with their roles and that the recovery process can be executed smoothly.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 77
During a vulnerability assessment, a scan reveals the following finding:
Windows Server 2016 Missing hotfix KB87728 - CVSS 3.1 Score: 8.1 [High]
- Affected host 172.16.15.2
Later in the review process, the remediation team marks the finding as a false positive. Which of the following is the best way to avoid this issue on future scans?
A. Getting an up-to-date list of assets from the CMDB
B. Performing an authenticated scan on the servers
C. Configuring the sensor with an advanced policy for fingerprinting servers
D. Coordinating the scan execution with the remediation team early in the process
Answer: (SHOW ANSWER)
Authenticated scans allow the vulnerability scanner to log in to the target system and directly verify installed patches, system configurations, and software versions. This provides accurate information about whether specific hotfixes or updates are present. Without authentication, scanners rely on external fingerprinting and banner analysis, which can misidentify patch status and lead to false positives. Using authenticated scanning significantly improves accuracy and reduces incorrect vulnerability findings.

NEW QUESTION: 78
A security audit of a company's application finds that customer account passwords are manually set and never expire. The company wants to fix the password issue on a minimal budget within 30 days while minimizing the impact to customers. Which of the following should the company do?
A. Implement a self-service credential reset portal.
B. Configure a privilege access management solution.

C. Migrate authentication methods to allow for OAuth 2.

D. Contact each user to reset their password.

Answer: (SHOW ANSWER)

NEW QUESTION: 79

After an incident response exercise, a security administrator reviews the following table:

Service	Risk rating	Criticality rating	Alert severity
Public website	Medium	Low	Low
Email	High	High	High
Human resources systems	High	Medium	Medium
Phone system	High	Critical	Critical
Intranet	Low	Low	Low

freecram.net CompTIA

Which of the following should the administrator do to best support rapid incident response in the future?

A. Automate alerting to IT support for phone system outages.

B. Enable dashboards for service status monitoring

C. Send emails for failed log-In attempts on the public website

D. Configure automated Isolation of human resources systems

Answer: (SHOW ANSWER)

Enabling dashboards for service status monitoring is the best action to support rapid incident response. Dashboards provide real-time visibility into the status of critical systems, enabling quicker identification of issues and a more informed, proactive response during an incident. By having a centralized view of service status, the security administrator can respond more quickly and efficiently to any disruptions.

NEW QUESTION: 80

An organization has a hybrid architecture that requires disparate systems to communicate with one another without a common chain of trust. Which of the following is the best solution?

Freecram.net

A. Deploying a hierarchical access control model

B. Enabling context-based authentication

C. Using microsegmentation between servers

D. Implementing remote attestation services

Answer: (SHOW ANSWER)

Remote attestation allows systems to verify the integrity and trustworthiness of another system by cryptographically validating its hardware, firmware, and software state before allowing communication. In hybrid environments where systems may not share a common certificate chain or centralized trust authority, remote attestation provides a mechanism to establish trust dynamically by proving that each system is running in a known, trusted configuration. This enables secure interaction between otherwise disparate systems.

NEW QUESTION: 81

Which of the following utilizes policies that route packets to ensure only specific types of traffic are being sent to the correct destination based on application usage?

A. SDN

B. pcap

C. vmstat

D. DNSSEC
E. VPC
Answer: A (LEAVE A REPLY)
SDN (Software-Defined Networking) utilizes policies and centralized control to dynamically route packets and ensure that specific types of traffic are sent to the correct destination based on application usage. SDN provides flexibility and programmability to control network traffic and routing at the application level, allowing policies to be applied to direct packets in a way that optimizes the network and meets security or performance requirements.

NEW QUESTION: 82
Company A acquired Company B and needs to determine how the acquisition will impact the attack surface of the organization as a whole. Which of the following is the best way to achieve this goal? (Choose two.)
A. Implementing DLP controls preventing sensitive data from leaving Company B's network
B. Documenting third-party connections used by Company B
C. Reviewing the privacy policies currently adopted by Company B
D. Requiring data sensitivity labeling tor all files shared with Company B
E. Forcing a password reset requiring more stringent passwords for users on Company B's network
F. Performing an architectural review of Company B's network
Answer: (SHOW ANSWER)
To determine how the acquisition of Company B will impact the attack surface, the following steps are crucial:
Documenting third-party connections used by Company B: Understanding all external connections is essential for assessing potential entry points for attackers and ensuring that these connections are secure.
Performing an architectural review of Company B's network: This review will identify vulnerabilities and assess the security posture of the acquired company's network, providing a comprehensive understanding of the new attack surface. These actions will provide a clear picture of the security implications of the acquisition and help in developing a plan to mitigate any identified risks.

NEW QUESTION: 83
A company needs to increase the maturity level for the cybersecurity department's governance structure. To achieve this goal, the company wants to implement a set of controls that can be used as part of the standard operational procedures and policies within the department and the company. Which of the following frameworks best aligns with this goal?
A. COSO
B. CIS
C. COBIT
D. ITIL
Answer: (SHOW ANSWER)

NEW QUESTION: 84
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)

The most appropriate action is to create an organizational risk register for project prioritization. This helps the company document and assess risks, prioritize critical systems, and determine which systems, such as the old 2008 Windows server running a business-critical process, need to be addressed most urgently. A risk register ensures that resources are allocated properly and that mitigation plans are in place for the most critical systems to prevent revenue loss in the event of a failure.

NEW QUESTION: 85
A company needs to create a design that facilitates monitoring and alerting over the identity and access management surface. A primary design consideration should be the existence of multiple independent identity providers with a hybrid, multicloud environment. Which of the following components should be included as part of the design?
A. UBA
B. CASB
C. TIP
D. SASE
Answer: (SHOW ANSWER)
The requirement is to "facilitate monitoring and alerting over the identity and access management surface" across multiple independent identity providers in a hybrid, multicloud environment.
That calls for analytics focused on user and entity behavior, not just network edges or cloud apps.
UBA (User Behavior Analytics) is specifically designed to ingest identity- and access-related events from many sources (IdPs, directories, cloud services, VPNs, etc.) and then correlate and alert on anomalous authentication, access patterns, and account misuse across environments.

NEW QUESTION: 86
An organization wants to create a threat model to identity vulnerabilities in its infrastructure.
Which of the following, should be prioritized first?
A. External-facing Infrastructure with known exploited vulnerabilities
B. Internal infrastructure with high-seventy and Known exploited vulnerabilities
C. External facing Infrastructure with a low risk score and no known exploited vulnerabilities
D. External-facing infrastructure with a high risk score that can only be exploited with local access to the resource
Answer: A (LEAVE A REPLY)
External-facing infrastructure with known exploited vulnerabilities poses the highest immediate risk, as it is directly accessible to attackers and already associated with active threats.
This should be the top priority in any threat modeling effort.

NEW QUESTION: 87
A security operation analyst is reviewing the following log entries for suspicious activity:

```
Mar 23 18:14:23 <192.168.12.4>[564218]:failed password attempt for 'admin' from 104.18.16.28
Mar 23 18:14:43 <192.168.12.4>[564218]:failed password attempt for 'admin' from 104.18.16.29
Mar 23 18:15:13 <192.168.12.4>[564218]:failed password attempt for 'guest' from 104.18.16.29
Mar 23 18:15:35 <192.168.12.4>[564218]:failed password attempt for 'guest' from 104.18.16.28
Mar 23 18:16:21 <192.168.12.4>[564218]:failed password attempt for 'root' from 104.18.16.29
Mar 23 18:16:53 <192.168.12.4>[564218]:failed password attempt for 'root' from 104.18.16.28
Mar 24 18:16:56 <192.168.12.4>[564218]:password auth success for 'root' from 192.168.12.56
Mar 24 18:18:23 <192.168.12.4>[564218]:exit after auth('root'):exited normally
Mar 24 19:18:55 <192.168.12.4>[564218]:password auth success for 'root' from 104.18.16.28
```

Which of the following should the analyst do first?

A. Search OSINT on the external IP 104.18.16.29.
B. Review host 192.168.12.56 for malicious software.
C. Perform a vulnerability scan on server 192.168.12.4.
D. Disable the guest account on the host 192.168.12.4.
Answer: (SHOW ANSWER)

NEW QUESTION: 88
An endpoint security engineer finds that a newly acquired company has a variety of non-standard applications running and no defined ownership for those applications. The engineer needs to find a solution that restricts malicious programs and software from running in that environment, while allowing the non-standard applications to function without interruption. Which of the following application control configurations should the engineer apply?
A. Deny list
B. Allow list
C. Audit mode
D. MAC list
Answer: (SHOW ANSWER)
Audit mode allows monitoring and logging of applications without enforcing restrictions. This is ideal in environments with non-standard applications and undefined ownership because it enables the engineer to observe the environment and gradually implement control without interruption.
Audit mode provides critical visibility into the software landscape, ensuring that necessary applications remain functional.

NEW QUESTION: 89
A company is having issues with its vulnerability management program New devices/IPs are added and dropped regularly, making the vulnerability report inconsistent. Which of the following actions should the company lake to most likely improve the vulnerability management process?
A. Request a weekly report with all new assets deployed and decommissioned
B. Extend the DHCP lease lime to allow the devices to remain with the same address for a longer period.
C. Implement a shadow IT detection process to avoid rogue devices on the network
D. Perform regular discovery scanning throughout the 11 landscape using the vulnerability management tool
Answer: D (LEAVE A REPLY)
To improve the vulnerability management process in an environment where new devices/IPs are added and dropped regularly, the company should perform regular discovery scanning throughout the IT landscape using the vulnerability management tool.
Accurate Asset Inventory: Regular discovery scans help maintain an up-to-date inventory of all assets, ensuring that the vulnerability management process includes all relevant devices and IPs.
Consistency in Reporting: By continuously discovering and scanning new and existing assets, the company can generate consistent and comprehensive vulnerability reports that reflect the current state of the network.
Proactive Management: Regular scans enable the organization to proactively identify and address vulnerabilities on new and existing assets, reducing the window of exposure to potential threats.

NEW QUESTION: 90
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?
Freecram.net
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: (SHOW ANSWER)
To minimize downtime, testing should occur in a virtual lab, not production. The best approach is to test solutions methodically: implement one solution at a time, run an attack simulation, collect metrics, roll back, and repeat. This isolates each solution's effectiveness, ensuring accurate metrics for decision-making without production impact.

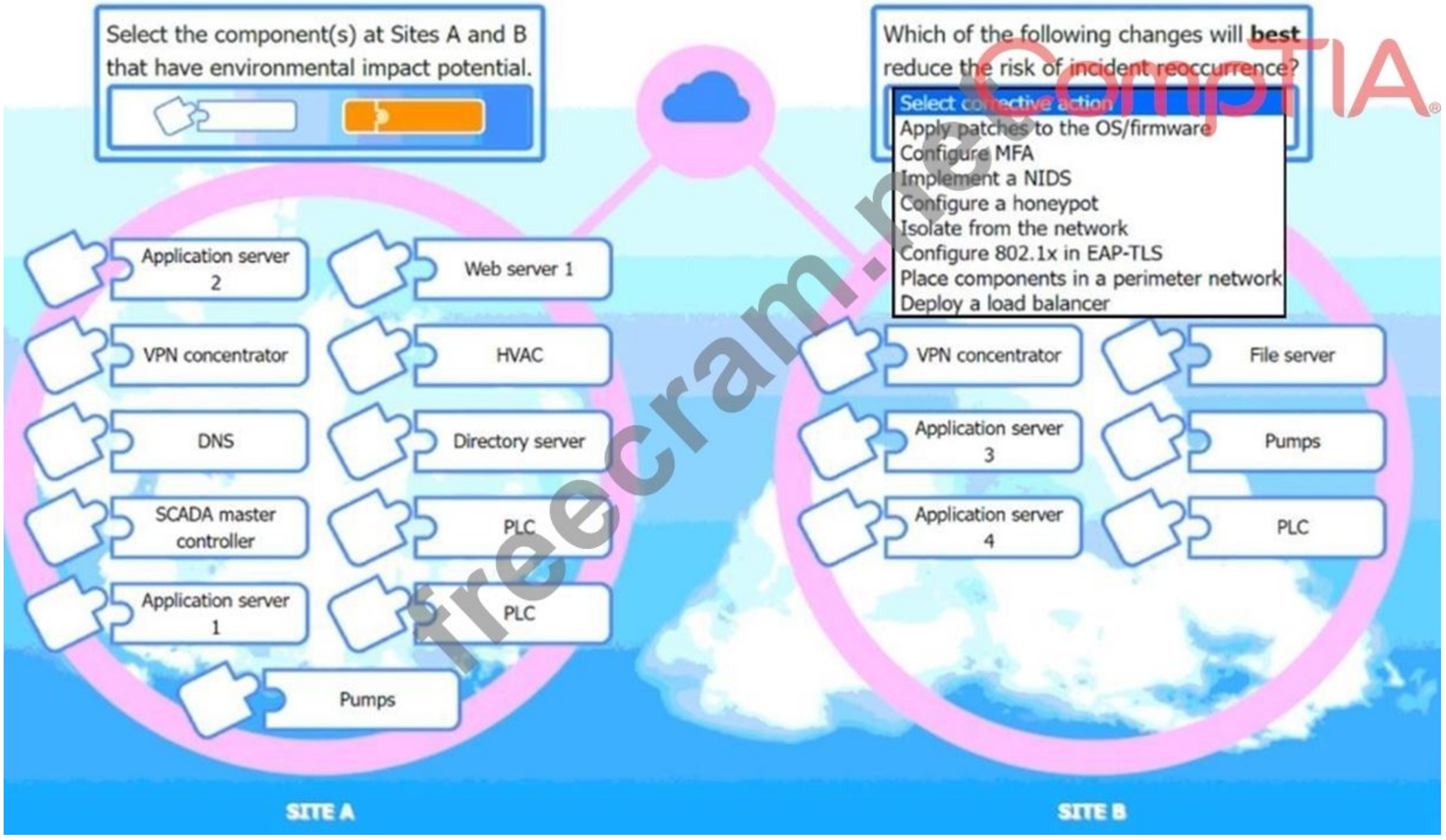
NEW QUESTION: 91
A company discovers intellectual property data on commonly known collaboration web applications that allow the use of slide templates. The systems administrator is reviewing the configurations of each tool to determine how to prevent this issue. The following security solutions are deployed:
- CASB
- SASE
- WAF
- EDR
- Firewall
- IDS
- SIEM
- DLP endpoints
Which of the following should the administrator do to address the issue?
A. Enable blocking for all WAF policies.
B. Enforce a policy to block unauthorized web applications within CASB.
C. Create an alert within the SIEM for outgoing network traffic to the suspected website.
D. Configure DLP endpoints to block sensitive data to the mass media.
Answer: (SHOW ANSWER)
A CASB sits inline between users and cloud services, giving you visibility and control over shadow IT. By configuring your CASB to block or quarantine uploads to any unsanctioned collaboration or file-sharing platforms, you'll prevent sensitive slide decks from being stored in those public web apps. This stops the leakage at the cloud access layer rather than relying on endpoint or network detection alone.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 92
SIMULATION
An incident occurred at Site A when an attacker successfully caused water pressure to increase in the pump room.
The organization is concerned about reoccurrence of this attack and that similar attacks might be successful on other cyber-physical systems within the network.
All devices and components reside on a flat network within the 10.1.0.0/16 space.
INSTRUCTIONS

Take the appropriate actions to reduce the risk of reoccurrence of this and other environmental security vulnerabilities.
Select the component(s) at Sites A and B that have environmental impact potential. Then, select the corrective action that will best reduce the risk of incident reoccurrence.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Answer Area



Answer:

At Site A:

SCADA master controller - Controls and monitors physical processes.

PLC (both) - Programmable Logic Controllers directly interface with pumps/valves.

Pumps - Direct environmental impact (increased water pressure in incident).

- At Site B:
- PLC - As above, interfaces with physical systems.
- Pumps - As above, environmental impact through pressure, flow, etc.
- Corrective Action - Isolate from the network

The devices reside on a flat network, increasing risk. Isolation (e.g., segmentation or VLANs) limits lateral movement and access to critical cyber-physical systems (CPS) like PLCs and pumps.

NEW QUESTION: 93

SIMULATION

During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

INSTRUCTIONS

Review each of the events and select the appropriate analysis and action options for each IoC.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

IoC 1 | IoC 2 | IoC 3

Source Svc	Type	Dest	Data
Apache_httpd	DNSQ	@10.1.1.1:53	update.s.domain
Apache_httpd	DNSQR	@10.1.2.5	CNAME 3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd	DNSQ	@10.1.1.1:53	3a129sk219r0slsmfkzzz000.s.domain
Apache_httpd	DNSQR	@10.1.2.5	IN A 108.158.253.253

Analysis: Select analysis

- Select analysis
- Someone is footprinting a network subnet.
- Service identification and fingerprinting are occurring.
- Canonical name records in a public DNS cache are being updated.
- An employee is attempting to access a blocked website.
- An employee is using P2P services to download files.
- The service is attempting to resolve a malicious domain.
- A host is participating in an IRC-based botnet.
- An application is performing an automatic update.

Action: Select action

- Select action
- Configure the DNS server to perform recursion.
- Block ping requests across the WAN interface.
- Deploy a network-based DLP solution.
- Enforce endpoint controls on third-party software installations.
- Implement a blocklist for known malicious ports.
- Close ticket as resolved.
- Investigate for software supply-chain attacks.

free exam.net
CompTIA

IoC 1 | **IoC 2** | IoC 3

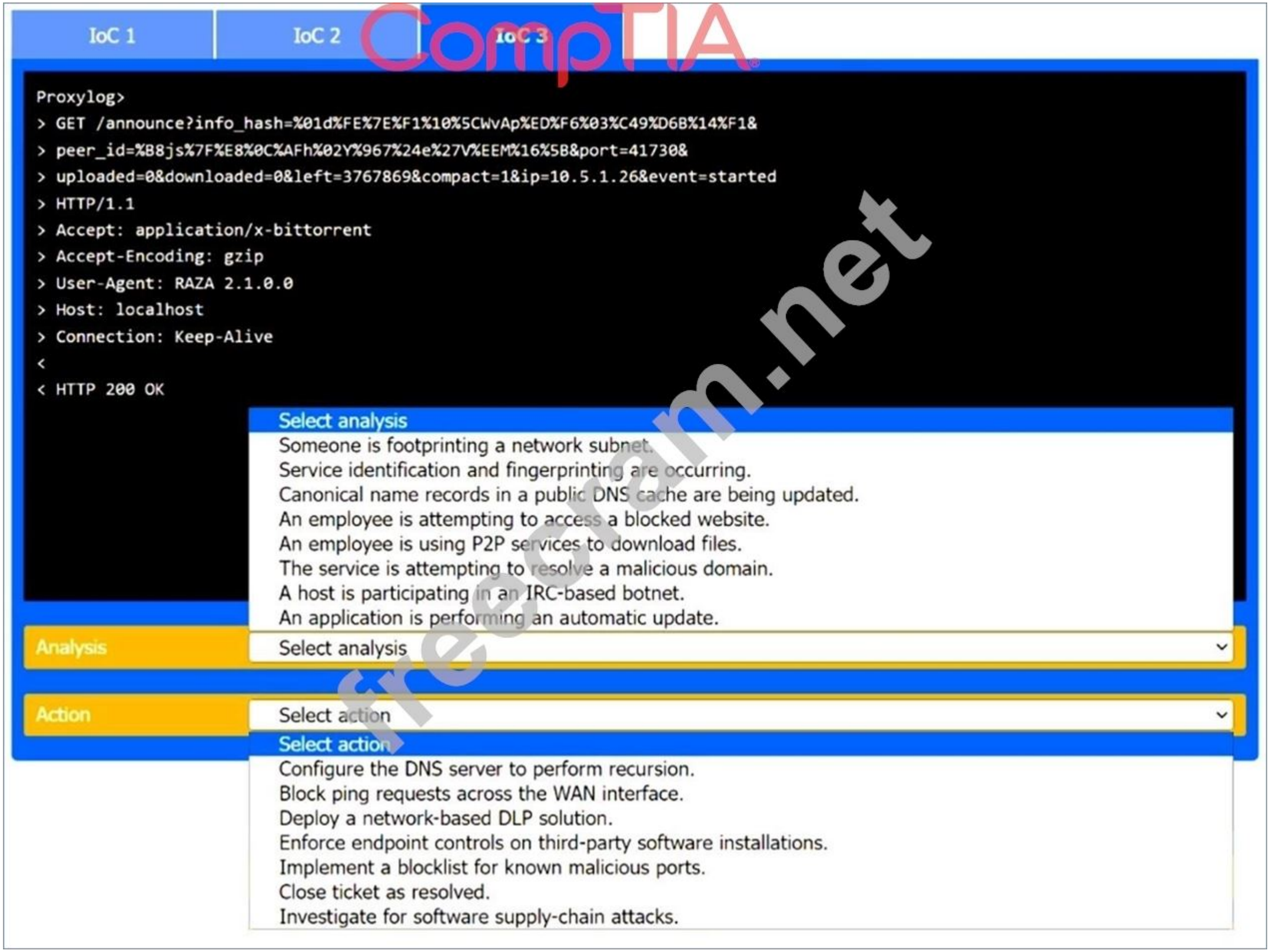
Src	Dst	Proto	Data	Action
10.0.5.5	10.1.2.1	IP_ICMP	ECHO	Drop
10.0.5.5	10.1.2.2	IP_ICMP	ECHO	Drop
10.0.5.5	10.1.2.3	IP_ICMP	ECHO	Drop
10.0.5.5	10.1.2.4	IP_ICMP	ECHO	Drop
10.0.5.5	10.1.2.5	IP_ICMP	ECHO	Drop

Analysis: Select analysis

- Select analysis
- Someone is footprinting a network subnet.
- Service identification and fingerprinting are occurring.
- Canonical name records in a public DNS cache are being updated.
- An employee is attempting to access a blocked website.
- An employee is using P2P services to download files.
- The service is attempting to resolve a malicious domain.
- A host is participating in an IRC-based botnet.
- An application is performing an automatic update.

Action: Select action

- Select action
- Configure the DNS server to perform recursion.
- Block ping requests across the WAN interface.
- Deploy a network-based DLP solution.
- Enforce endpoint controls on third-party software installations.
- Implement a blocklist for known malicious ports.
- Close ticket as resolved.
- Investigate for software supply-chain attacks.


IoC 1
IoC 2
IoC 3
Proxylog>
> GET /announce?info_hash=%01d%FE%7E%F1%10%5CWvAp%ED%F6%03%C49%D6B%14%F1&
> peer_id=%B8js%7F%E8%0C%AFh%02Y%967%24e%27V%EEM%16%5B&port=41730&
> uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started
> HTTP/1.1
> Accept: application/x-bittorrent
> Accept-Encoding: gzip
> User-Agent: RAZA 2.1.0.0
> Host: localhost
> Connection: Keep-Alive
<
< HTTP 200 OK
Select analysis
Someone is footprinting a network subnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An employee is attempting to access a blocked website.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.
A host is participating in an IRC-based botnet.
An application is performing an automatic update.
Analysis
Select analysis
Action
Select action
Select action
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Enforce endpoint controls on third-party software installations.
Implement a blocklist for known malicious ports.
Close ticket as resolved.
Investigate for software supply-chain attacks.

Answer:

IoC 1

Indicators:

DNS queries for a suspicious subdomain (update.s.domain, *.s.domain)

Responses include odd CNAME and A records

Activity resembles contacting a malicious domain

Correct Selections:

Analysis: The service is attempting to resolve a malicious domain

Action: Implement a blocklist for known malicious ports

IoC 2

Indicators:

ICMP Echo (ping) requests from 10.0.5.5 to multiple hosts

All packets are dropped

Suggests a device is probing the network

Correct Selections:

Analysis: Someone is footprinting a network subnet

Action: Block ping requests across the WAN interface

IoC 3

Indicators:

BitTorrent traffic (/announce?info_hash, peer_id, application/x-bittorrent)

Indicates P2P protocol activity

Correct Selections:

Analysis: An employee is using P2P services to download files

Action: Enforce endpoint controls on third-party software installations

NEW QUESTION: 94

A retail organization wants to properly test and verify its capabilities to detect and/or prevent specific TTPs as mapped to the MITRE ATTACK framework specific to APTs. Which of the following should be used by the organization to accomplish this goal?

A. Tabletop exercise

B. Penetration test

C. Sandbox detonation

D. Honeypot

Answer: (SHOW ANSWER)

A penetration test is the most appropriate method to test and verify an organization's capabilities to detect and prevent specific Tactics, Techniques, and Procedures (TTPs) as mapped to the MITRE ATT&CK framework. During a penetration test, ethical hackers simulate real-world attacks, attempting to exploit vulnerabilities and execute the TTPs associated with advanced persistent threats (APTs). This allows the organization to evaluate its detection mechanisms, security controls, and response capabilities in a controlled environment.

NEW QUESTION: 95

A government agency implements a configuration that disables cellular network access on government-issued devices while roaming internationally. The agency issues mobile hotspots and requires employees to use them for internet access. Which of the following best describes the agency's rationale?

A. To protect against SIM hijack vulnerabilities

B. To defend from carrier OTA attack vectors

C. To block malicious radio connections

D. To prevent attempts to downgrade the protocol to legacy 3G

E. To filter directed electromagnetic interference

Answer: (SHOW ANSWER)

By disabling direct cellular roaming and requiring mobile hotspots, the agency reduces exposure to foreign carriers' over-the-air (OTA) update mechanisms. This defends against carrier-based OTA attack vectors that could compromise devices when connected to international networks.

NEW QUESTION: 96

A user reports application access issues to the help desk. The help desk reviews the logs for the user:

Time	Internal IP	Public IP	IP Geolocation	Application	Action
8:47 PM	192.168.1.5	104.18.16.29	Toronto	VPN	Allow
8:48 PM	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:48 PM	10.10.2.21	95.67.137.12	Los Angeles	HR System	Allow
8:49 PM	10.10.2.21	95.67.137.12	Los Angeles	Email	Allow
8:52 PM	192.168.1.5	104.18.16.29	Toronto	HR System	Deny

CompTIA freecram.net

Which of the following is most likely the reason for the issue?

A. The user inadvertently tripped the geoblock rule in NGFW.

B. A threat actor has compromised the user's account and attempted to log in.

C. The user is not allowed to access the human resources system outside of business hours.

D. The user did not attempt to connect from an approved subnet.

Answer: (SHOW ANSWER)

The logs show that the user connected from Toronto (104.18.16.29) and Los Angeles (95.67.137.12) within minutes. The sudden location change is a typical trigger for geoblocking in a Next-Generation Firewall (NGFW), leading to the HR System being denied.

NEW QUESTION: 97

A security engineer is creating a single CSR for the following web server hostnames:

wwwint.internal

www.company.com

home.internal

www.internal

Which of the following would meet the requirement?

A. SAN

B. CN

C. CA

D. CRL

E. Issuer

Answer: (SHOW ANSWER)
A single CSR (Certificate Signing Request) can include multiple DNS names by populating the Subject Alternative Name (SAN) extension with each hostname. This ensures the issued certificate will be valid for all listed names: wwwint.internal, www.company.com, home.internal, and www.internal. The Common Name (CN) alone only supports one name, whereas SAN supports multiple.

NEW QUESTION: 98
A systems administrator works with engineers to process and address vulnerabilities as a result of continuous scanning activities. The primary challenge faced by the administrator is differentiating between valid and invalid findings. Which of the following would the systems administrator most likely verify is properly configured?
A. Report retention time
B. Scanning credentials
C. Exploit definitions
D. Testing cadence
Answer: (SHOW ANSWER)
When differentiating between valid and invalid findings from vulnerability scans, the systems administrator should verify that the scanning credentials are properly configured. Valid credentials ensure that the scanner can authenticate and access the systems being evaluated, providing accurate and comprehensive results. Without proper credentials, scans may miss vulnerabilities or generate false positives, making it difficult to prioritize and address the findings effectively.

NEW QUESTION: 99
A security administrator is performing a gap assessment against a specific OS benchmark. The benchmark requires the following configurations be applied to endpoints:
- Full disk encryption
- Host-based firewall
- Time synchronization
- Password policies
- Application allow listing
- Zero Trust application access
Which of the following solutions best addresses the requirements? (Choose two.)
A. CASB
B. SBoM
C. SCAP
D. SASE
E. HIDS
F. MDM
Answer: (SHOW ANSWER)
SCAP (Security Content Automation Protocol) supports automated compliance checking against security benchmarks (like OS hardening guides), helping to identify and remediate configuration gaps.
MDM (Mobile Device Management) allows centralized enforcement of full disk encryption, firewall settings, password policies, and application allow listing on endpoints.

NEW QUESTION: 100
A company purchased Burp Suite licenses this year for each application security engineer. The engineers have used Burp Suite to identify several issues with the company's SaaS application. In the upcoming year, the Chief Information Security Officer would like to purchase additional tools to protect the SaaS product. Which of the following is the best option?

Freecram.net

A. DAST
B. SAST
C. IAST
D. ZAP
Answer: (SHOW ANSWER)
IAST (Interactive Application Security Testing): Combines both dynamic and static testing techniques and is highly suited for securing SaaS applications by providing insights into runtime and code-level issues.
DAST (Dynamic Application Security Testing): Focuses on runtime vulnerabilities but lacks code- level analysis.
SAST (Static Application Security Testing): Analyzes source code but does not address runtime vulnerabilities.
ZAP (OWASP ZAP) is a DAST tool similar to Burp Suite, providing redundant functionality rather than new protections.

NEW QUESTION: 101
A company is concerned about the security of customer data. The IT department has configured all web applications with appropriate access controls to restrict to only authorized users. Which of the following solutions addresses this concern?
A. SIEM
B. Vulnerability scanner
C. DLP
D. Threat intelligence platform
Answer: (SHOW ANSWER)
Data Loss Prevention (DLP) solutions are specifically designed to prevent unauthorized access, sharing, or exfiltration of sensitive data such as customer information. It complements access controls by monitoring and enforcing data protection policies.

NEW QUESTION: 102
A hospital's requirements for remote third-party monitoring of the HVAC system include the following:
- The vendor must be able to continuously monitor system health and
respond accordingly.
- The vendor must only have network access to the HVAC system.
- The vendor must be the only entity with access to the HVAC system.
Which of the following best meets the hospital's requirements?
A. Deploying a RDP jump box to allow remote system monitoring
B. Implementing a reverse web proxy and allowing access from the internet
C. Installing the vendor's monitoring appliance on the internal network and allowing outbound SSL connectivity
D. Creating a site-to-site VPN tunnel and allowing restricted access to the system
Answer: (SHOW ANSWER)

NEW QUESTION: 103
A systems administrator wants to introduce a newly released feature for an internal application.
The administrate docs not want to test the feature in the production environment. Which of the following locations is the best place to test the new feature?
A. Staging environment
B. Testing environment
C. CI/CO pipeline

D. Development environment

Answer: (SHOW ANSWER)

The best location to test a newly released feature for an internal application, without affecting the production environment, is the staging environment.

Staging Environment: This environment closely mirrors the production environment in terms of hardware, software, configurations, and settings. It serves as a final testing ground before deploying changes to production. Testing in the staging environment ensures that the new feature will behave as expected in the actual production setup.

Isolation from Production: The staging environment is isolated from production, which means any issues arising from the new feature will not impact the live users or the integrity of the production data. This aligns with best practices in change management and risk mitigation.

Realistic Testing: Since the staging environment replicates the production environment, it provides realistic testing conditions. This helps in identifying potential issues that might not be apparent in a development or testing environment, which often have different configurations and workloads.

NEW QUESTION: 104

To bring digital evidence in a court of law, the evidence must be:

A. material.

B. tangible.

C. consistent.

D. conserved.

Answer: (SHOW ANSWER)

For any evidence, digital or otherwise, to be admissible in court, it must be both relevant to the issues at hand (i.e., material) and authentic. "Material" evidence has a legitimate and effective influence on proving a fact in dispute. In practice, this means the digital artifacts you collect must directly relate to the elements of the case and help establish or refute a key point.

NEW QUESTION: 105

An organization receives intelligence information about a foreign adversary targeting instances of a web server application that the organization uses. The information includes:

- The originating IP addresses of the attack
- The common commands run on the affected device
- The indicators that a device has been affected
- The actions that can be taken on the device to stop the attack

Which of the following should the organization do first?

A. Draft an incident response playbook

B. Build tactics, techniques, and procedures

C. Create Snort and YARA rules

D. Configure user behavior analytics

Answer: (SHOW ANSWER)

The intelligence already provides actionable indicators such as attacker IP addresses, commands used, signs of compromise, and remediation steps. The first step is to operationalize this intelligence for detection by creating IDS and malware detection signatures. Snort rules can detect network activity from the known attacker infrastructure and command patterns, while YARA rules can identify malicious artifacts or behaviors on affected systems. This enables immediate detection and monitoring for the described attack.

NEW QUESTION: 106

An organization recently implemented a purchasing freeze that has impacted endpoint life-cycle management efforts. Which of the following should a security manager do to reduce risk without replacing the endpoints?

A. Dispose of end-of-support devices

B. Reimage the system

C. Remove unneeded services
D. Deploy EDR
Answer: (SHOW ANSWER)

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 107
A security engineer needs 10 secure the OT environment based on me following requirements:
- Isolate the OT network segment
- Restrict Internet access.
- Apply security updates two workstations
- Provide remote access to third-party vendors
Which of the following design strategies should the engineer implement to best meet these requirements?
A. Deploy a jump box on the third party network to access the OT environment and provide updates using a physical delivery method on the workstations
B. Implement a bastion host in the OT network with security tools in place to monitor access and use a dedicated update server for the workstations.
C. Enable outbound internet access on the OT firewall to any destination IP address and use the centralized update server for the workstations
D. Create a staging environment on the OT network for the third-party vendor to access and enable automatic updates on the workstations.
Answer: (SHOW ANSWER)
To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network. The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.

NEW QUESTION: 108
A security team determines that the most significant risks within the pipeline are:
- Unauthorized code changes
- The current inability to perform independent verification of software modules Which of the following best addresses these concerns?
A. Digital signatures
B. Non-repudiation
C. Lightweight cryptography
D. Code signing
Answer: (SHOW ANSWER)

NEW QUESTION: 109
A security operations engineer needs to prevent inadvertent data disclosure when encrypted SSDs are reused within an enterprise. Which of the following is the most secure way to achieve this goal?
A. Executing a script that deletes and overwrites all data on the SSD three times
B. Wiping the SSD through degaussing

C. Securely deleting the encryption keys used by the SSD
D. Writing non-zero, random data to all cells of the SSD
Answer: (SHOW ANSWER)
The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively unreadable, rendering any residual data useless.
This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.

NEW QUESTION: 110
To prevent data breaches, security leaders at a company decide to expand user education to:
- Create a healthy security culture.
- Comply with regulatory requirements
- Improve incident reporting
Which of the following would best meet their objective?
Freecram.net
A. Performing a DoS attack
B. Scheduling regular penetration tests
C. Simulating a phishing campaign
D. Deploying fake ransomware
Answer: (SHOW ANSWER)
Simulating a phishing campaign helps users recognize phishing attempts and enhances overall security awareness. It is a practical way to improve incident reporting and ensure that users understand common attack vectors. This directly supports creating a healthy security culture, complying with regulatory requirements related to security training, and improving the response to security incidents.

NEW QUESTION: 111
A systems administrator wants to use existing resources to automate reporting from disparate security appliances that do not currently communicate. Which of the following is the best way to meet this objective?
A. Configuring an API Integration to aggregate the different data sets
B. Combining back-end application storage into a single, relational database
C. Purchasing and deploying commercial off the shelf aggregation software
D. Migrating application usage logs to on-premises storage
Answer: (SHOW ANSWER)
Configuring an API integration is the best way to automate reporting from disparate security appliances. APIs allow for the integration of data from different sources, enabling automated aggregation and reporting without the need to invest in new tools or migrate data manually. This solution leverages existing resources and allows the systems to communicate effectively.

NEW QUESTION: 112
During an incident response activity, the response team collected some artifacts from a compromised server, but the following information is missing:
- Source of the malicious files
- Initial attack vector
- Lateral movement activities
The next step in the playbook is to reconstruct a timeline. Which of the following best supports this effort?
A. Executing decompilation of binary files
B. Analyzing all network routes and connections
C. Performing primary memory analysis

D. Collecting operational system logs and storage disk data
Answer: (SHOW ANSWER)
Collecting operating system logs and storage disk data provides historical records of file creation, modifications, user activity, and system events. These artifacts are essential for reconstructing a detailed timeline of the attack, including the source of malicious files, initial entry, and lateral movement.

NEW QUESTION: 113
A cybersecurity architect is reviewing the detection and monitoring capabilities for a global company that recently made multiple acquisitions. The architect discovers that the acquired companies use different vendors for detection and monitoring. The architect's goal is to:
- Create a collection of use cases to help detect known threats
- Include those use cases in a centralized library for use across all
of the companies
Which of the following is the best way to achieve this goal?
A. Sigma rules
B. Ariel Query Language
C. UBA rules and use cases
D. TAXII/STIX library
Answer: (SHOW ANSWER)
To create a collection of use cases for detecting known threats and include them in a centralized library for use across multiple companies with different vendors, Sigma rules are the best option.
Vendor-Agnostic Format: Sigma rules are a generic and open standard for writing SIEM (Security Information and Event Management) rules. They can be translated to specific query languages of different SIEM systems, making them highly versatile and applicable across various platforms.
Centralized Rule Management: By using Sigma rules, the cybersecurity architect can create a centralized library of detection rules that can be easily shared and implemented across different detection and monitoring systems used by the acquired companies. This ensures consistency in threat detection capabilities.
Ease of Use and Flexibility: Sigma provides a structured and straightforward format for defining detection logic. It allows for the easy creation, modification, and sharing of rules, facilitating collaboration and standardization across the organization.

NEW QUESTION: 114
John Doe's email account was compromised. The attacker's access to John Doe's account was removed and MFA was implemented. The attacker convinced Joe Roe in the accounting department to pay a fraudulent invoice through email exchanges. A security analyst is reviewing the headers from the initial email that Joe Roe received:

```
Received: from 221.15.11.103 (221.15.11.103.mta.com [221.15.11.103])
by mx-01-us-west with esmtps (TLS1.2)
Received-SPF: pass receiver=mx7sgwt-35; client-ip=18.132.124.10;
Received: from 18.132.124.10 (18.132.124.10-internal.com [18.132.124.10])
by mx7sgwt-35 (Postfix) with ESMTPS id zRhQ22fmNnQCdys
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=example.com;
s=default; t=1672873468; i=@exampl.com;
bh=c0YCm8Ivmmc6Jsk7FZNLJpnsp3uLFGRfpJjfdQzs5uQ=;
h=To:Message-ID:Date:Content-Type:Subject:From:From:To:Cc:Subject;
b=RTt/LClrEaCaRriLkhf4ntueKUIa9uU55UOCmYQQR/wys0dyWM+OTXwTb/hs+j+N1=
To: jroe@example.com
Message-ID: <T3.Y5.192564.FR2893JFV@mta.prd>
Date: Mon, 07 Apr 2025 12:04:23 +0000
Content-Type: multipart/alternative; boundary="_----F506BlU672zJ6b3FauAZA===_73/A4-32616-C36L8ZbYC4p"
MIME-Version: 1.0
Reply-To: jdoe@exampl.com
Subject: FW: Invoice
From: jdoe@exampl.com
X-SpamProbability: 0.095349
```

Which of the following best explains how the attacker was able to get the invoice paid?

A. The attacker guessed John Doe's password.

B. The attacker registered a new domain.

C. The attacker's emails did not use domain keys for verification.

D. The email failed the sender policy framework check.

Answer: (SHOW ANSWER)

The email headers show that the message originated from an external mail server associated with a different domain while the visible sender address appears to be from the legitimate company domain. At the same time, the SPF check passed for the sending infrastructure, indicating the sending domain authorized that mail server. This pattern is consistent with a look- alike or newly registered domain used to impersonate a trusted sender, enabling the attacker to send convincing invoice emails that appear legitimate to the recipient.

NEW QUESTION: 115

An organization wants to implement a secure cloud architecture across all instances. Given the following requirements:

- Establish a standard network template
- Deployments must be consistent
- Security policies must be able to be changed at scale

Which of the following technologies meets these requirements?

A. Serverless deployment model

B. Container orchestration

C. Infrastructure as code

D. CLI cloud administration

E. API gateway

Answer: (SHOW ANSWER)

Infrastructure as code defines cloud infrastructure, network configurations, and security policies in version-controlled configuration files that can be deployed automatically. This approach allows organizations to create standardized templates for networks, ensure consistent deployments across environments, and update security policies centrally so changes can be applied at scale to all instances.

NEW QUESTION: 116

A software company deployed a new application based on its internal code repository. Several customers are reporting anti-malware alerts on workstations used to test the application. Which of the following is the most likely cause of the alerts?

A. Misconfigured code commit

B. Unsecure bundled libraries

C. Invalid code signing certificate

D. Data leakage

Answer: (SHOW ANSWER)

Unsecure bundled libraries are the most likely cause of anti-malware alerts. If the application includes third-party components with known vulnerabilities or malicious behavior, endpoint security tools may flag it during testing.

NEW QUESTION: 117

A software development company wants to ensure that users can confirm the software is legitimate when installing it. Which of the following is the best way for the company to achieve this security objective?

A. Code signing

B. Non-repudiation

C. Key escrow

D. Private keys

Answer: (SHOW ANSWER)

Code signing is the process of digitally signing software or executables using a cryptographic certificate. This ensures that users can verify the authenticity of the software and confirm it has not been altered or tampered with since it was signed. It provides assurance that the software is legitimate and originates from the claimed source, addressing the company's security objective.

NEW QUESTION: 118

All organization is concerned about insider threats from employees who have individual access to encrypted material. Which of the following techniques best addresses this issue?

A. SSO with MFA

B. Sating and hashing

C. Account federation with hardware tokens

D. SAE

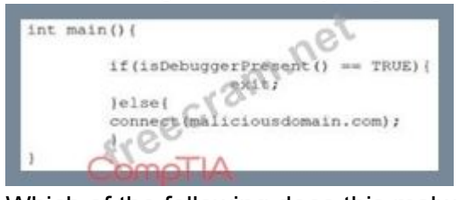
E. Key splitting

Answer: E (LEAVE A REPLY)

Key splitting involves dividing the encryption key into multiple parts, where no single individual holds the entire key. This technique prevents any one person from being able to decrypt the encrypted material by themselves, thus reducing the risk of insider threats.

NEW QUESTION: 119

A reverse engineer is analyzing a malware sample from a recent security incident. When debugging and disassembling the code, the engineer finds the following section of the code:



Which of the following does this malware try to evade?

A. IOC extraction

B. Code similarity
C. Dynamic analysis
D. Malware attribution
Answer: (SHOW ANSWER)
The code checks whether a debugger is present using a debugger detection function and exits if one is detected. Malware commonly includes this type of anti-debugging logic to prevent analysts or automated sandbox systems from observing its behavior during execution. By terminating when debugging is detected, the malware attempts to evade dynamic analysis environments that rely on monitoring runtime behavior.

NEW QUESTION: 120
A 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?
Freecram.net
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)
Harden the camera configuration by changing default usernames and passwords, disabling unnecessary open ports, and ensuring that secure protocols (such as HTTPS, SSH, or others) are used instead of insecure ones (like HTTP or Telnet). This is a critical step in securing IoT devices and protecting them from being exploited. Since the camera is part of the IoT subnet and has been identified with vulnerabilities such as default credentials and open ports, hardening the configuration is the most direct and effective solution to secure its operation.

NEW QUESTION: 121
A company detects suspicious activity associated with inbound connections. Security detection tools are unable to categorize this activity. Which of the following is the best solution to help the company overcome this challenge?
A. Implement an interactive honeypot.
B. Map network traffic to known IoCs.
C. Monitor the dark web.
D. Implement UEBA.
Answer: (SHOW ANSWER)
An interactive honeypot can actively engage with suspicious inbound connections, capturing detailed attacker behavior and tactics, which helps identify and categorize unknown or ambiguous threats more effectively.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 122
An administrator needs to craft a single certificate-signing request for a web-server certificate.

The server should be able to use the following identities to mutually authenticate other resources over TLS:
www.int.comptia.org
webserver01 .int.comptia.org
10.5.100.10
Which of the following certificate fields must be set properly to support this objective?
A. Subject alternative name
B. Organizational unit
C. Extended key usage
D. Certificate extension
Answer: (SHOW ANSWER)
The Subject Alternative Name (SAN) field must be properly set to include all the required identities - FQDNs and IP addresses - so the certificate can be used for mutual TLS authentication with those specific identifiers.

NEW QUESTION: 123
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. A multicloud provider solution
B. A load balancer with a round-robin configuration
C. An on-premises solution as a backup
D. An active-active solution within the same tenant
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
A programmer is reviewing the following proprietary piece of code that was identified as a vulnerability due to users being authenticated when they provide incorrect credentials:

```
GET USERID
GET PASS
JUMP TO :ALLOWUSER:
  IF USERID == GETDBUSER(USERID) AND HASH(PASS) == GETDBPASS(USERID)
EXIT
:ALLOWUSER:
SET USERACL(USERID)
...
...
...
```

CompTIA freecram.net
Which of the following should the programmer implement to remediate the code vulnerability?
A. Salted hashing via the proprietary SHASHfunction
B. Input validation in the first two lines of code
C. Atomic execution of subroutines
D. TOCTOU remediation in SETUSERACL
E. Database connection over encrypted channels

Answer: (SHOW ANSWER)
The code vulnerability stems from improper handling of user input in the authentication process.
In the first two lines, the code retrieves the USERID and PASS inputs, but there is no validation or sanitation of these inputs before they are processed.
By implementing input validation in these initial lines of code, the programmer can ensure that only properly formatted and expected data is passed into the authentication logic. This prevents malicious input, such as SQL injection or other forms of manipulation, which could allow incorrect credentials to be accepted and cause authentication issues. Input validation ensures that the inputs meet specific criteria (e.g., expected length, character set), which mitigates the risk of such vulnerabilities.

NEW QUESTION: 125
A security architect must implement security controls in a software development life cycle for an internally developed application. The architect must identify the components that were used to create the application. Which of the following should the security architect use to meet this requirement?
A. A/B test
B. SAST
C. IAST
D. SBoM
Answer: D (LEAVE A REPLY)
A Software Bill of Materials (SBoM) provides a detailed inventory of all components, libraries, and dependencies used in an application. This allows the security architect to track and manage risks associated with the software supply chain throughout the development life cycle.

NEW QUESTION: 126
Engineers are unable to control pumps at Site A from Site B when the SCADA controller at Site A experiences an outage. A security analyst must provide a secure solution that ensures Site A pumps can be controlled by a SCADA controller at Site B if a similar outage occurs again. Which of the following represents the most cost-effective solution?
A. Procure direct fiber connectivity between Site A and Site B and limit its use to the critical SCADA controller traffic only.
B. Install backup SCADA controllers at each site, isolate them from the OT network, and assign these backup controllers as high-availability pairs.
C. Isolate the OT environment by providing an air-gapped network segment. Place the SCADA controller for each site in this network segment to minimize outages.
D. Configure VPN concentrators inside the OT network segments at Site A and Site B and allow the controllers to act as secondary devices for the other site's pumps across this encrypted tunnel.
Answer: (SHOW ANSWER)
Configuring VPN concentrators inside the OT network segments allows secure, encrypted communication between Site A and Site B. This setup enables each SCADA controller to act as a backup for the other site's pumps during outages, while being cost-effective compared to dedicated fiber or deploying redundant controllers.

NEW QUESTION: 127
A global organization is reviewing potential vendors to outsource a critical payroll function. Each vendor's plan includes using local resources in multiple regions to ensure compliance with all regulations. The organization's Chief Information Security Officer is conducting a risk assessment on the potential outsourcing vendors' subprocessors. Which of the following best explains the need for this risk assessment?
A. Risk mitigations must be more comprehensive than the existing payroll provider.
B. Due care must be exercised during all procurement activities.
C. The responsibility of protecting PII remains with the organization.
D. Specific regulatory requirements must be met in each jurisdiction.
Answer: C (LEAVE A REPLY)
The responsibility for protecting PII remains with the organization, even when outsourcing to third- party vendors or subprocessors. Conducting a risk assessment ensures that these subprocessors maintain adequate security controls to protect sensitive data and meet compliance obligations.

NEW QUESTION: 128
An architect is securing an external infrastructure to support external services. The following components are in use:
- One Kubernetes cluster with multiple pods and nodes for back-end
services
- Two VM Linux instances as the web tier
- One SQL-based database
The company only has funding for two controls and must prioritize resilience. Which of the following are the most effective controls for the company to implement to meet this goal? (Choose two.)
A. An IAM policies enforced
B. A RASP to the workload services
C. A content delivery network
D. A database firewall on the SQL instance
E. An IPS at the web tier
F. An application load balancer
Answer: (SHOW ANSWER)
A content delivery network improves resilience by distributing incoming traffic across globally distributed edge nodes, absorbing traffic spikes and helping mitigate denial-of-service conditions before requests reach the infrastructure. This protects the web tier and backend services from overload and improves availability for external users.
An application load balancer distributes incoming requests across the two web-tier virtual machines and backend services, preventing a single instance from becoming a point of failure.
Load balancing enables high availability and fault tolerance by automatically directing traffic to healthy instances if one becomes unavailable.

NEW QUESTION: 129
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 penetration tester 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)
Most cloud providers require explicit authorization before any penetration testing is performed against their infrastructure. Even though the application is yours, the underlying network, hypervisor, and shared services belong to the CSP. Securing written approval (or verifying that the provider's policy allows the planned tests without advance notice) ensures you won't violate the provider's terms of service or trigger automated abuse defenses that could disrupt service.

NEW QUESTION: 130
After discovering that an employee is using a personal laptop to access highly confidential data, a systems administrator must secure the company's data. Which of the following capabilities best addresses this situation?
Freecram.net
A. OCSP stapling
B. CASB
C. SOAR

D. Conditional access
E. Package monitoring
Answer: (SHOW ANSWER)
Conditional access enforces policies that control device and user access to sensitive data, ensuring only compliant and authorized devices can connect, thereby securing company data when personal laptops attempt access.

NEW QUESTION: 131
After a leak of important documents, a company decides to implement a data protection program to avoid similar incidents in the future. Which of the following should the company do first?
A. Implement data encryption.
B. Perform data storage hardening.
C. Deploy a data loss prevention policy.
D. Develop data labeling standards.
Answer: (SHOW ANSWER)
Developing data labeling standards is the first step in a data protection program. It ensures that data is classified according to sensitivity, which then informs the appropriate encryption, storage hardening, and DLP policies to apply.

NEW QUESTION: 132
An organization recently migrated data to a new file management system. The architect decides to use a discretionary authorization model on the new system. Which of the following best explains the architect's choice?
A. The responsibility of migrating data to the new file management system was outsourced to the vendor providing the platform.
B. The permissions were not able to be migrated to the new system, and several stakeholders were made responsible for granting appropriate access.
C. The legacy file management system did not support modern authentication techniques despite the business requirements.
D. The data custodians were selected by business stakeholders to ensure backups of the file management system are maintained off site.
Answer: (SHOW ANSWER)
A discretionary access control (DAC) model allows data owners or stakeholders to grant access at their discretion. If permissions couldn't be migrated, assigning stakeholders responsibility to manage access aligns with DAC and explains the architect's choice.

NEW QUESTION: 133
Protected company data was recently exfiltrated. The SOC did not find any indication of a network or outside physical intrusion, and the DLP systems reported no unusual activity. The incident response team determined a text file was encrypted and reviews the following:

```
Delivered-To: janedoe@email.net
MessageID: <sdflkh038-kdhen7-23hd7s-afdzx.xt.local>
Created at: Sat, Jan 20, 2024 at 10:50 PM (Delivered after 10 seconds)
From: Jane Doe <janedoe@company.com>
To: janedoe@email.net
Subject: Grocery List for Next Week's Meal Prep
SPF: PASS with IP 12.34.56.78
DKIM: 'PASS' with domain email.company.com
DMARC: 'PASS'

Body:
Make sure not to forget any of the items.
Regards,
Jane Doe Engineer @ Company

Attachments: groceryitem.txt
Attachment Virus Scan: 'PASS'
```

freecram.net
CompTIA

Which of the following is the most appropriate action for the team to take?
A. Review the email security settings for proper configurations.
B. Investigate whether the employee had access to the data that was leaked.
C. Scan attachments with a third-party virus scan to independently confirm the results.
D. Analyze the hardware for undetected supply chain vulnerabilities that may have been exploited.
Answer: B (LEAVE A REPLY)
Since the exfiltration occurred via an encrypted text file sent by an internal account and no external intrusion or DLP alerts were found, the most appropriate next step is to investigate whether the employee legitimately had access to the leaked data. This helps determine if it was an insider threat or misuse of authorized access.

NEW QUESTION: 134
A company developed a new solution that needs to track any changes to the data, and the changes need to be quickly identified. If any changes are attempted without prior approval, multiple events must be triggered, such as:
Raising alerts
Blocking the unapproved changes
Quickly removing access to the data
Which of the following solutions best meets these requirements?
A. Implementing a file integrity monitoring tool and integrating it via orchestration and automation with other security tools
B. Configuring CASB rules, making access to the data available only to authorized personnel
C. Introducing more granular access controls and allowing read-only access for non-privileged users
D. Tracking all application logs, integrating them to the existing SIEM, flagging any changes, and making them visible on security dashboards
Answer: (SHOW ANSWER)

NEW QUESTION: 135
A company sells a security appliance assembled from globally sourced hardware and software components. Installing the security appliance requires enabling administrative permissions for the service accounts on the appliance. Which of the following allows the company to reassure new and existing customers that the risk introduced by the appliance is minimal?
A. The results of a qualitative risk analysis performed on the appliance
B. A business impact analysis and risk prioritization process
C. Results of internal risk reduction studies conducted by a third-party assessor
D. A transparent supply chain risk management and testing program
Answer: (SHOW ANSWER)
A transparent supply chain risk management and testing program gives customers visibility into how the company evaluates, tests, and secures globally sourced components. This directly reassures customers that risks from the appliance are minimized through rigorous, verifiable controls and supply chain oversight.

NEW QUESTION: 136
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) tools inventory and continuously monitor all third-party and open-source components in your codebase, flagging known vulnerabilities and license issues before they make it into production. This directly addresses supply-chain risk by ensuring you know exactly which external libraries you're using and whether they contain any security flaws.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 137
Which of the following most likely explains the reason a security engineer replaced ECC with a lattice-based cryptographic technique?
A. It is computationally efficient and provides perfect forward secrecy.
B. It is more resilient to brute-force attacks than ECC.
C. It supports ephemeral key exchange and digital signatures.
D. It is currently considered a robust PQC technique.
E. It enables processing on data while remaining in an encrypted state.
Answer: (SHOW ANSWER)
Lattice-based schemes, such as Learning With Errors (LWE) or Ring-LWE, are among the leading candidates in NIST's post-quantum cryptography standardization process because their underlying hard problems resist known quantum-algorithm speedups. Replacing ECC with a lattice-based algorithm directly addresses the threat posed by future quantum computers, making it the preferred choice for long-term cryptographic agility.

NEW QUESTION: 138
A company is preparing to move a new version of a web application to production. No major issues were reported during security scanning or quality assurance in the CI/CD pipeline. Which of the following actions should the company take next?
A. Merge the test branch to the main branch.
B. Perform threat modeling on the production application.
C. Conduct unit testing on the submitted code.
D. Perform a peer review on the test branch.
Answer: (SHOW ANSWER)
A peer review is the essential next step once automated scans and QA pass but before merging or deploying code. It brings human insight to catch logic flaws, security oversights, or architectural issues that tools may miss. Conducting the review on the test branch ensures feedback can be addressed without impacting the main branch or production timeline.

NEW QUESTION: 139
An organization has been using self-managed encryption keys rather than the free keys managed by the cloud provider. The Chief Information Security Officer (CISO) reviews the monthly bill and realizes the self-managed keys are more costly than anticipated. Which of the following should the CISO recommend to reduce costs while maintaining a strong security posture?
A. Utilize an on-premises HSM to locally manage keys.
B. Adjust the configuration for cloud provider keys on data that is classified as public.
C. Begin using cloud-managed keys on all new resources deployed in the cloud.
D. Extend the key rotation period to one year so that the cloud provider can use cached keys.
Answer: (SHOW ANSWER)
Risk-Based Approach: Using cloud-provider-managed keys for public data is a reasonable risk- based decision. Public data, by definition, is not confidential.

Cost Optimization: This directly addresses the CISO's concern about cost, as cloud-provider- managed keys are often free or significantly cheaper.
Security Balance: It maintains a strong security posture for sensitive data by continuing to use customer-managed keys where appropriate, while optimizing costs for less sensitive data.

NEW QUESTION: 140

A security officer performs due diligence activities before implementing a third-party solution into the enterprise environment. The security officer needs evidence from the third party that a data subject access request handling process is in place. Which of the following is the security officer most likely seeking to maintain compliance?

Freecram.net

A. Information security standards
B. E-discovery requirements
C. Privacy regulations
D. Certification requirements
E. Reporting frameworks
Answer: (SHOW ANSWER)
Privacy regulations, such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), require companies to provide data subject access request (DSAR) handling processes. A DSAR allows individuals to request details about their personal data stored by a company and request modifications or deletions.

NEW QUESTION: 141
A SOC analyst must perform threat-modeling activities for a large media organization that has the following characteristics:
- The organization maintains operations around the world in support of
multiple entertainment networks.
- Development activities for the organization's web-based platforms
occur overseas.
- Previous information security failures within the organization have
been publicly disclosed.
Which of the following actions is the best for the analyst to consider in the early phases of threat modeling?
A. Implementing STIX and TAXII
B. Conducting an OSINT assessment
C. Reviewing user behavior analytics and identity logs
D. Performing a supply chain analysis
Answer: B (LEAVE A REPLY)
In the early phases of threat modeling, the analyst wants to understand the organization's exposed attack surface, public footprint, prior breaches, reputational visibility, externally visible infrastructure, and information that threat actors can readily gather. Because the scenario explicitly says prior security failures were publicly disclosed and the organization operates globally, OSINT is the most practical first step to inform the threat model. CompTIA's official SecurityX objectives include "Given a scenario, perform threat-modeling activities" as part of the GRC domain, and that early work centers on understanding attacker perspective, exposure, and context before applying more specialized controls.

NEW QUESTION: 142
In a recent audit, several critical legacy systems, which are externally exposed so that a specific vendor can manage them remotely, were identified. These systems must remain available to the vendor for the next six months. A security team segmented the network so these systems can only communicate with internal resources. Which of the following actions would be most appropriate to restore the vendor's access to manage these systems?
A. Disable all connections to the systems, and implement a backup solution to capture the needed data to send to the vendor on a weekly basis.

B. Create a VPN connection and set up firewall rules so only specific connections are allowed to those systems.
C. Disable external connections to those systems for the next six months.
D. Isolate the critical systems so they can only be remotely managed from the internet.
Answer: (SHOW ANSWER)
Creating a VPN connection with firewall rules restricts vendor access to only authorized connections, maintaining security while restoring necessary remote management capability.

NEW QUESTION: 143
An engineer has had scaling issues with a web application hosted on premises and would like to move to a serverless architecture. Which of the following cloud benefits would be best to utilize for this project?
A. Cost savings for hosting
B. Automation of resource provisioning
C. Providing geo-redundant hosting
D. Eliminating need to patch
Answer: B (LEAVE A REPLY)
The best cloud benefit for moving to a serverless architecture in this case is Automation of resource provisioning. Serverless computing automatically scales resources based on demand without requiring manual intervention. This helps to address the scaling issues the engineer is facing by dynamically adjusting resource allocation as needed, improving performance and efficiency without manual effort.

NEW QUESTION: 144
Which of the following enables the meaningful manipulation of encrypted data when the processor does not know the encryption key?
A. Simultaneous authentication of equals
B. Envelope encryption
C. Authenticated encryption with associated data
D. Homomorphic encryption
Answer: (SHOW ANSWER)
Homomorphic encryption allows for the manipulation and computation of encrypted data without needing to decrypt it, meaning the processor does not require access to the encryption key. This enables meaningful operations on encrypted data while maintaining confidentiality.

NEW QUESTION: 145
An organization found a significant vulnerability associated with a commonly used package in a variety of operating systems. The organization develops a registry of software dependencies to facilitate incident response activities. As part of the registry, the organization creates hashes of packages that have been formally vetted. Which of the following attack vectors does this registry address?
A. Supply chain attack
B. Cipher substitution attack
C. On-path attack
D. Pass- the-hash attack
E. Side-channel analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146

An organization has deployed a cloud-based application that provides virtual event services globally to clients. During a typical event, thousands of users access various entry pages within a short period of time. The entry pages include sponsor-related content that is relatively static and is pulled from a database. When the first major event occurs, users report poor response time on the entry pages. Which of the following features is the most appropriate for the company to implement?

A. Horizontal scalability
B. Vertical scalability
C. Containerization
D. Static code analysis
E. Caching

Answer: (SHOW ANSWER)

Since the entry pages contain sponsor-related content that is relatively static and pulled from a database, implementing caching would be the most appropriate solution. Caching stores frequently accessed data in a location that is faster to access than querying the database repeatedly. This reduces the load on the database and improves response times for users, especially during high-traffic events. By caching the static content (like sponsor information), the application can serve those pages faster and handle large numbers of users more efficiently.

NEW QUESTION: 147

A threat hunter is identifying potentially malicious activity associated with an APT. When the threat hunter runs queries against the SIEM platform with a date range of 60 to 90 days ago, the involved account seems to be typically most active in the evenings. When the threat hunter reruns the same query with a date range of 5 to 30 days ago, the account appears to be most active in the early morning. Which of the following techniques is the threat hunter using to better understand the data?

A. TTP-based inquiries
B. User behavior analytics
C. Adversary emulation
D. OSINT analysis activities

Answer: (SHOW ANSWER)

User behavior analytics (UBA) detects anomalous activity by analyzing historical patterns and comparing them to recent behavior. The time shift in account activity suggests potential compromise or misuse.

NEW QUESTION: 148

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 149

Which of the following best describes the advantage of homomorphic encryption when compared to other encryption methodologies?

A. The need for a pre-shared key is removed.
B. Resource utilization is lower.
C. Support for field-specific tokenization is added.

D. Data integrity is protected by advanced hashing routines.
Answer: (SHOW ANSWER)

NEW QUESTION: 150
A CRM company leverages a CSP PaaS service to host and publish its SaaS product. Recently, a large customer requested that all infrastructure components must meet strict regulatory requirements, including configuration management, patch management, and life-cycle management. Which of the following organizations is responsible for ensuring those regulatory requirements are met?
Freecram.net
A. The CRM company
B. The CRM company's customer
C. The CSP
D. The regulatory body
Answer: A (LEAVE A REPLY)
In a PaaS (Platform as a Service) model, the Cloud Service Provider (CSP) is responsible for managing the platform infrastructure, including servers, storage, and the platform software. However, the CRM company, as the customer of the PaaS provider, is responsible for managing and securing their own application, data, and any configurations or compliance requirements for their hosted SaaS product.
Since the CRM company provides the SaaS product to their customers and regulatory compliance is a business requirement for their service, they bear the responsibility to ensure that their application and infrastructure configurations meet regulatory requirements, even if hosted on the CSP's platform.

NEW QUESTION: 151
A pharmaceutical company uses a cloud provider to host thousands of independent resources in object storage. The company needs a practical and effective means of discovering data, monitoring changes, and identifying suspicious activity. Which of the following would best meet these requirements?
A. A machine-learning-based data security service
B. A file integrity monitoring service
C. A cloud configuration assessment and compliance service
D. An automated data classification system
Answer: (SHOW ANSWER)
A machine-learning-based data security service would be the best solution for discovering data, monitoring changes, and identifying suspicious activity in the context of a cloud-based object storage environment. Such a service can analyze patterns in data access and usage to identify anomalies, suspicious behavior, and potential security incidents. Machine learning models can continuously learn and adapt to new behaviors, making it effective at detecting emerging threats in real time.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 152
A security analyst is performing a review of a web application. During testing as a standard user, the following error log appears:
Error Message in Database Connection
Connection to host USA-WebApp-Database failed

Database "Prod-DB01" not found
Table "CustomerInfo" not found
Please retry your request later
Which of the following best describes the analyst's findings and a potential mitigation technique?
A. The findings indicate unsecure references. All potential user input needs to be properly sanitized.
B. The findings indicate unsecure protocols. All cookies should be marked as HttpOnly.
C. The findings indicate information disclosure. The displayed error message should be modified.
D. The findings indicate a SQL injection. The database needs to be upgraded.
Answer: (SHOW ANSWER)
Revealing internal hostnames, database names, and table names in user-facing error messages leaks sensitive implementation details that aid attackers. To mitigate this, the application should catch such exceptions and return a generic, user-friendly error (e.g. "An internal error occurred, please try again later") while logging the full details only on the server side.

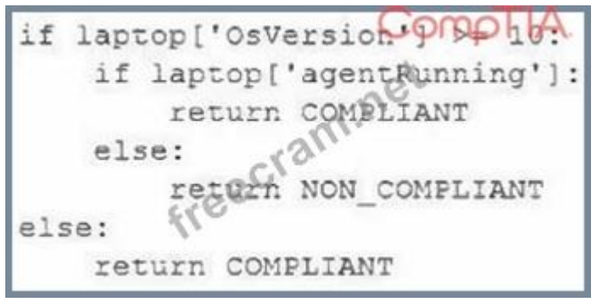
NEW QUESTION: 153
A security engineer receives an alert from the SIEM platform indicating a possible malicious action on the internal network. The engineer generates a report that outputs the logs associated with the incident:

Date	Time	Action	Details
01/23/2024	08:02:41	Login success	JohnS login attempt into VM001
01/24/2024	08:03:32	Login success	JohnS login attempt into SV002
01/25/2024	08:02:12	Login success	JohnS login attempt into VM001
01/26/2024	08:03:21	Login success	JohnS login attempt into VM001
01/26/2024	23:52:41	Login success	JohnS login attempt into SV002
01/27/2024	08:02:54	Login success	JohnS login attempt into SV002

freecram.net CompTIA

Which of the following actions best enables the engineer to investigate further?
A. Consulting logs from the enterprise password manager
B. Searching dark web monitoring resources for exposure
C. Reviewing audit logs from privileged actions
D. Querying user behavior analytics data
Answer: (SHOW ANSWER)
The logs show that JohnS has been logging into different virtual machines (VM001 and SV002), which could indicate suspicious activity, especially if these are sensitive systems. Reviewing audit logs from privileged actions would help the engineer determine whether the logins are associated with unauthorized actions, changes to critical systems, or other suspicious behavior that might indicate a potential malicious action.

NEW QUESTION: 154
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:



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 was running a Windows version below 10 and triggered a false negative.

D. The OS version was higher than 11, and the MDM agent was running, triggering a true negative.

Answer: (SHOW ANSWER)

The provided logic checks for compliance based on the OsVersionand whether the agentRunningis true. Here's how the logic works:

1. If OsVersion >= 10:

- If agentRunningis true, the device is compliant.
- If agentRunningis false, the device is non-compliant.

2. Else (if OsVersion < 10):

- The device is marked as compliant.

This logic means that laptops with an OS version below 10 are mistakenly considered compliant, which is a false negative because they do not meet the policy requirement. This is likely how the employee's laptop, running a version of Windows below 10, was able to connect to the network against policy.

NEW QUESTION: 155

During a penetration test, several users report that certain fileshares on the network could not be accessed. An analyst reviews the network traffic and detects a high number of packets associated with LLMNR and SMB that are being redirected to the penetration tester's computer.

Which of the following attacks is causing the issue?

A. SMB brute-force

B. Directory fuzzing

C. NTLM relay

D. Network poisoning

Answer: (SHOW ANSWER)

The presence of a large number of LLMNR responses redirecting SMB traffic to the penetration tester indicates name resolution poisoning. In this attack, the attacker responds to LLMNR queries before legitimate hosts, convincing systems that the attacker's machine is the requested resource. As a result, SMB connections and authentication attempts are redirected to the attacker's system, disrupting normal access to fileshares and enabling credential capture.

NEW QUESTION: 156

Which of the following key management practices ensures that an encryption key is maintained within the organization?

A. Encrypting using a key stored in an on-premises hardware security module

B. Encrypting using server-side encryption capabilities provided by the cloud provider

C. Encrypting using encryption and key storage systems provided by the cloud provider

D. Encrypting using a key escrow process for storage of the encryption key

Answer: (SHOW ANSWER)
Control: On-premises HSMs provide the highest level of control over encryption keys. The organization has physical and logical control over the HSM and the keys stored within it.
Security: HSMs are designed to be tamper-resistant and protect keys from unauthorized access, even if the surrounding systems are compromised.
Compliance: In some industries, regulatory requirements may mandate that organizations maintain direct control over their encryption keys. On-premises HSMs can help meet these requirements.

NEW QUESTION: 157
An organization currently has IDS, firewall, and DLP systems in place. The systems administrator needs to integrate the tools in the environment to reduce response time. Which of the following should the administrator use?
A. SOAR
B. CWPP
C. XCCDF
D. CMDB
Answer: A (LEAVE A REPLY)
SOAR (Security Orchestration, Automation, and Response): SOAR integrates security tools, automates workflows, and speeds up incident response.

NEW QUESTION: 158
A company receives several complaints from customers regarding its website. An engineer implements a parser for the web server logs that generates the following output:

Browser	User location	Load time	HTTP response
Mozilla 5.0	United States	190ms	302
Chrome 110	France	1.2s	302
Microsoft Edge	India	3.7s	307
Microsoft Edge	Australia	6.4s	200

freecram.net CompTIA

Which of the following should the company implement to best resolve the issue?
A. IDS
B. CDN
C. WAF
D. NAC
Answer: (SHOW ANSWER)
To improve global response times (e.g. India/Australia seeing multi-second load times) and offload traffic from your origin web servers, deploying a Content Delivery Network is the most effective solution.

NEW QUESTION: 159
A company wants to implement hardware security key authentication for accessing sensitive information systems. The goal is to prevent unauthorized users from gaining access with a stolen password.
Which of the following models should the company implement to solve this issue?
A. Rule based
B. Time-based
C. Role based

D. Context-based

Answer: (SHOW ANSWER)

Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user's current environment and behavior. This can include factors such as the user's location, the time of access, the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.

NEW QUESTION: 160

A security researcher tells a company that one of its solutions is vulnerable to buffer overflow, leading to a malicious coding execution. Which of the following is the best way to avoid this vulnerability in future versions?

Freecram.net

A. Testing for CSRF vulnerabilities before the application goes to production

B. Using SAST tools to find vulnerabilities as part of the pipeline

C. Implementing canary protection in an earlier life-cycle stage

D. Implementing pair programming to improve development capabilities

Answer: (SHOW ANSWER)

Static Application Security Testing (SAST) tools analyze source code during development to detect vulnerabilities like buffer overflows early in the software development lifecycle, allowing for proactive mitigation before deployment.

NEW QUESTION: 161

An administrator brings the company's fleet of mobile devices into its PKI in order to align device WLAN NAC configurations with existing workstations and laptops. Thousands of devices need to be reconfigured in a cost-effective, time-efficient, and secure manner. Which of the following actions best achieve this goal? (Choose two.)

A. Using the existing MDM solution to integrate with directory services for authentication and enrollment

B. Deploying netAuth extended key usage certificate templates

C. Deploying serverAuth extended key usage certificate templates

D. Deploying clientAuth extended key usage certificate templates

E. Configuring SCEP on the CA with an OTP for bulk device enrollment

F. Submitting a CSR to the CAto obtain a single certificate that can be used across all devices

Answer: (SHOW ANSWER)

Using the existing MDM solution integrated with directory services automates authentication and enrollment, making the process scalable, secure, and cost-effective. Configuring SCEP with a one-time password enables secure bulk enrollment of many devices efficiently.

NEW QUESTION: 162

Which of the following best describes the challenges associated with widespread adoption of homomorphic encryption techniques?

A. Incomplete mathematical primitives

B. No use cases to drive adoption

C. Quantum computers not yet capable

D. Insufficient coprocessor support

Answer: (SHOW ANSWER)

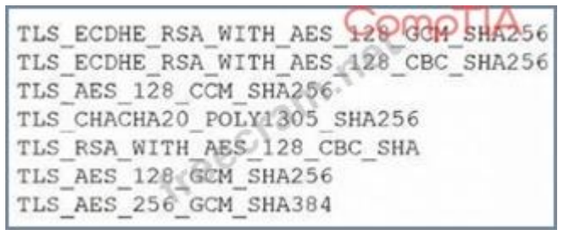
Fully homomorphic encryption schemes impose massive computational overhead, and without specialized hardware accelerators or co-processors to offload the heavy integer and polynomial arithmetic, performance remains prohibitive for broad deployment.

NEW QUESTION: 163
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. Static application security testing
B. Regression testing
C. Code signing
D. Sandboxing
Answer: (SHOW ANSWER)
Static application security testing (SAST) is the best tool for identifying security vulnerabilities in code early in the Software Development Life Cycle (SDLC). SAST tools analyze source code or binaries for vulnerabilities without executing the program, allowing teams to catch and address security issues before the code is pushed to production. This aligns with reducing the risk of vulnerable code being released.

NEW QUESTION: 164
Company A is merging with Company B. Company A is a small, local company. Company B has a large, global presence. The two companies have a lot of duplication in their IT systems, processes, and procedures. On the new Chief Information Officer's (CIO's) first day, a fire breaks out at Company B's main data center. Which of the following actions should the CIO take first?
A. Determine whether the incident response plan has been tested at both companies, and use it to respond.
B. Review the incident response plans, and engage the disaster recovery plan while relying on the IT leaders from both companies.
C. Ensure hot, warm, and mobile disaster recovery sites are available, and give an update to the companies' leadership teams.
D. Initiate Company A's IT systems processes and procedures, assess the damage, and perform a BIA.
Answer: (SHOW ANSWER)
When a disaster such as a fire occurs at a primary data center, the immediate priority is to review and implement the incident response plan (IRP) and the disaster recovery plan (DRP). These plans are designed to address and mitigate the impact of such incidents. Since the two companies have recently merged and may have differing systems and procedures, it is crucial to rely on the IT leaders from both companies who are familiar with their respective systems to ensure an effective response.
By reviewing and engaging the existing plans, the CIO can manage the situation efficiently and ensure minimal downtime and data loss while assessing how both companies' IT systems and processes will be integrated in the future.

NEW QUESTION: 165
A company that uses several cloud applications wants to properly identify:
- All the devices potentially affected by a given vulnerability.
- All the internal servers utilizing the same physical switch.
- The number of endpoints using a particular operating system.
Which of the following is the best way to meet the requirements?
A. SBoM
B. CASB
C. GRC
D. CMDB
Answer: (SHOW ANSWER)
CMDB (Configuration Management Database): Tracks assets, configurations, and relationships (e.g., switches, OS versions), meeting all requirements.

NEW QUESTION: 166
A vulnerability scan was performed on a website, and the following encryption suites were found:



Which of the following actions will remediate the vulnerability?

A. Removing any ciphers utilizing cipher block chaining

B. Rearranging the order of the ciphers from strongest to weakest

C. Deploying a WAF to monitor web traffic

D. Reissuing new SSL certificates for the website

Answer: (SHOW ANSWER)

Cipher suites that use CBC (Cipher Block Chaining), such as
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 and
TLS_RSA_WITH_AES_128_CBC_SHA, are vulnerable to padding oracle and related attacks.
Removing CBC-based ciphers ensures only modern and secure cipher suites (e.g., GCM, ChaCha20) are used, remediating the vulnerability.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:

https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 167

A news organization wants to implement workflows that allow users to request that untruthful data be retraced and scrubbed from online publications to comply with the right to be forgotten Which of the following regulations is the organization most likely trying to address'

A. GDPR

B. COPPA

C. CCPA

D. DORA

Answer: (SHOW ANSWER)

The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the "right to be forgotten," which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.

NEW QUESTION: 168

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)
When external technicians are granted access to printers and multifunction devices that buffer or store sensitive documents, there's a real risk they could view, copy, or exfiltrate data. Without a non-disclosure agreement in place, there is no contractual obligation preventing them from disclosing or misusing any confidential information they encounter. This gap presents a clear confidentiality risk that the information security manager should remediate.

NEW QUESTION: 169
A security administrator needs to develop a remediation plan to address a large number of vulnerability scan results. Which of the following should the administrator use to determine the vulnerabilities that should be addressed first?
A. CPE
B. CCE
C. CVSS
D. CVE
Answer: C (LEAVE A REPLY)
The Common Vulnerability Scoring System (CVSS) provides a standardized severity score for each vulnerability, reflecting its potential impact and exploitability. By sorting your scan results by CVSS score, focusing first on the highest-severity (e.g., critical and high) issues, you ensure your remediation plan targets the most dangerous vulnerabilities before lower-risk ones.

NEW QUESTION: 170
An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key. Which of the following would best secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?
Freecram.net
A. Sign the key with DSA
B. Deploy MFA for the service accounts
C. Utilize HMAC for the keys
D. Implement a VPN for all APIs
Answer: (SHOW ANSWER)

NEW QUESTION: 171
A company must build and deploy security standards for all servers in its on-premises and cloud environments based on hardening guidelines. Which of the following solutions most likely meets the requirements?
A. Develop a security baseline to integrate with the vulnerability scanning platform to alert about any server not aligned with the new security standards.
B. Create baseline images for each OS in use, following security standards, and integrate the images into the patching and deployment solution.
C. Build all new images from scratch, installing only needed applications and modules in accordance with the new security standards.
D. Run a script during server deployment to remove all the unnecessary applications as part of provisioning.
Answer: (SHOW ANSWER)
Creating secure baseline images ensures consistent, repeatable deployment aligned with hardening standards. These images can be used across on-premises and cloud environments, ensuring compliance and reducing misconfigurations.

NEW QUESTION: 172

An organization hires a security consultant to establish a SOC that includes a threat-modeling function. During initial activities, the consultant works with system engineers to identify antipatterns within the environment. Which of the following is most critical for the engineers to disclose to the consultant during this phase?

A. Results from the most recent infrastructure access review

B. A listing of unpatchable IoT devices in use in the data center

C. Network and data flow diagrams covering the production environment

D. Results from the most recent software composition analysis

E. A current inventory of cloud resources and SaaS products in use

Answer: (SHOW ANSWER)

In the context of establishing a Security Operations Center (SOC) with a threat-modeling function, it's crucial to understand how data flows within the organization's systems. Network and data flow diagrams provide a visual representation of the system's architecture, illustrating how data moves between components, which is essential for identifying potential security weaknesses and antipatterns. Antipatterns are common responses to recurring problems that are ineffective and risk- inducing. By analyzing these diagrams, the consultant can pinpoint areas where security controls may be lacking or misconfigured, thereby facilitating the development of effective threat models.

NEW QUESTION: 173

An organization is deploying a new data lake that will centralize records from several applications.

During the design phase, the security architect identifies the following requirements:

- The sensitivity levels of the data is different.
- The data must be accessed through stateless API calls after
authentication.
- Different users will have access to different data sets.

Which of the following should the architect implement to best meet these requirements?

A. Directory services

B. 802.1X with EAP-TLS

C. OpenID Connect

D. CASB

Answer: (SHOW ANSWER)

OpenID Connect provides federated authentication, enabling secure stateless API access. When combined with authorization frameworks (like OAuth 2.0), it supports fine-grained access control, ensuring different users can access only their permitted data sets in the data lake.

NEW QUESTION: 174

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)

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.

NEW QUESTION: 175

A compliance manager is planning an engagement to identify risks in the environment. The manager wants to discuss with business unit leaders essential aspects of the engagement that include identifying critical assets and processes as well as potential points of failure. Which of the following would be most relevant to consider during these conversations?

A. Subprocessor risks

B. Risk acceptance criteria

C. Remediation strategies

D. Risk appetite and tolerance

Answer: (SHOW ANSWER)

During risk identification discussions with business unit leaders, understanding the organization's risk appetite and tolerance is essential. These define how much risk the organization is willing to accept in pursuit of its objectives and help guide which assets, processes, and potential failure points are considered most critical. This context allows the security team to prioritize risks appropriately and align the engagement with the organization's strategic risk management expectations.

NEW QUESTION: 176

Source code snippets for two separate malware samples are shown below:

Sample 1:

```
...
knockEmDown(String e)
{
  if(target.isAccessed())
  {
    target.toShell(e);
    System.out.println(e.toString());
    c2.sendTelemetry(target.hostname.toString + " is " + e.toString());
  } else {
    target.close();
  }
}
...
```

Sample 2:

```
...
targetSys(address a)
{
  if(address.isIpv4())
  {
    address.connect(1337);
    address.keepAlive("paranoid");
    String status = knockEmDown(address.current);
    remote.sendC2(address.current + " is " + status);
  } else {
    throw Exception e;
  }
}
...
```

freecram.net
CompTIA

Which of the following describes the most important observation about the two samples?

A. Telemetry is first buffered and then transmitted in paranoid mode.

B. The samples were probably written by the same developer.

C. Both samples use IP connectivity for command and control.

D. Sample 1 is the target agent while Sample 2 is the C2 server.

Answer: (SHOW ANSWER)
Both samples share similar naming conventions (knockEmDown, sendC2, toString()usage), structure, and coding style (e.g., address.keepAlive("paranoid"), target.toShell(e), etc.), suggesting a common author or coding template. These stylistic similarities are strong indicators that they were likely written by the same developer.

NEW QUESTION: 177
A company's SIEM is continuously reporting false positives and false negatives. The security operations team has implemented configuration changes to troubleshoot possible reporting errors.
Which of the following sources of information best supports the required analysis process?
(Choose two.)
A. Third-party reports and logs
B. Trends
C. Dashboards
D. Alert failures
E. Network traffic summaries
F. Manual review processes
Answer: (SHOW ANSWER)
The best sources of information to support the analysis process for troubleshooting false positives and false negatives in a SIEM are:
Trends - Analyzing trends helps identify patterns in alerts, such as recurring false positives or missed detections (false negatives), allowing the team to adjust rules or thresholds accordingly.
Alert failures - Reviewing alert failures (e.g., missed detections or incorrect alerts) provides direct insight into why the SIEM is generating false positives or negatives, helping refine detection logic.

NEW QUESTION: 178
A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization. Which of the following actions would best resolve the issue?
(Choose two.)
A. Conduct input sanitization.
B. Deploy a SIEM.
C. Use containers.
D. Patch the OS.
E. Deploy a WAF.
F. Deploy a reverse proxy.
G. Deploy an IDS.
Answer: (SHOW ANSWER)
Conduct input sanitization: The primary safeguard against LDAP injection is to validate and cleanse all user-supplied inputs before they're incorporated into LDAP queries. By enforcing strict whitelists (allowing only expected characters or patterns) and escaping or rejecting any special LDAP-filter metacharacters, you eliminate the injection vectors at the source.
Deploy a WAF: While you're remediating the code, a properly configured Web Application Firewall can provide an additional layer of defense by detecting and blocking known LDAP injection payloads (e.g., *)(uid=*))(|(uid=*) in incoming requests. This helps mitigate exploitation risk in the short term and serves as a compensating control until the application is fully secured.

NEW QUESTION: 179
A company SIEM collects information about the log sources. Given the following report information:

Device	Type	Time	Status	Function
VM001	Server	10:23:241	UP	Critical
VM002	Server	10:22:323	UP	Normal
NET002	Router	10:23:391	UP	Normal
NET003	IPS	1:45:312	DOWN	Normal
VM003	Server	9:53:783	DOWN	Critical

Which of the following actions should a security engineer take to enhance the security monitoring posture?

A. Calibrate the timing on the log sources to enhance event correlation.

B. Implement a centralized use case library to get alerts based on the type of log sources.

C. Perform a non-reporting device assessment to collect missing log sources.

D. Create a resiliency plan to prevent losing event logs from log sources.

Answer: (SHOW ANSWER)

The timestamps in the report are inconsistent in format and precision, which hinders accurate event correlation in the SIEM. Calibrating and synchronizing the timing on log sources (e.g., using NTP) ensures logs can be correlated reliably, enhancing the overall security monitoring posture.

NEW QUESTION: 180

An external SaaS solution user reports a bug associated with the role-based access control module. This bug allows users to bypass system logic associated with client segmentation in the multitenant deployment model. When assessing the bug report, the developer finds that the same bug was previously identified and addressed in an earlier release. The developer then determines the bug was reintroduced when an existing software component was integrated from a prior version of the platform. Which of the following is the best way to prevent this scenario?

A. Regression testing

B. Code signing

C. Automated test and retest

D. User acceptance testing

E. Software composition analysis

Answer: A (LEAVE A REPLY)

Regression testing is a software testing practice that ensures that recent code changes have not adversely affected existing functionalities. In this scenario, the reintroduction of a previously fixed bug indicates that changes or integrations brought back the old issue. Implementing comprehensive regression testing would help detect such reintroductions by systematically retesting the existing functionalities whenever changes are made to the codebase. This practice is crucial in maintaining the integrity of the application, especially in complex systems where multiple components interact.

NEW QUESTION: 181

A security engineer is assessing a new tool to segment data and communications between domains. The assessment must determine how data transmission controls can be bypassed without detection. Which of the following techniques should the security engineer use?

A. Machine-learning statistical analysis

B. Fuzz testing

C. Covert channel analysis

D. Protocol analysis

Answer: (SHOW ANSWER)

Covert channel analysis is the technique best suited for assessing how data transmission controls can be bypassed without detection. Covert channels involve using a system or communication protocol in unintended ways to transmit data secretly. This analysis helps identify potential hidden channels that might bypass security controls and allow unauthorized communication between domains.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 182
A security engineer reviews an after-action report from a previous security breach and notes a long lag time between detection and containment of a compromised account. The engineer suggests using SOAR to address this concern. Which of the following best explains the engineer's goal?
A. To prevent accounts from being compromised
B. To enable log correlation using machine learning
C. To orchestrate additional reporting for the security operations center
D. To prepare runbooks to automate future incident response
Answer: D (LEAVE A REPLY)
SOAR (Security Orchestration, Automation, and Response) platforms help automate and standardize incident response processes through runbooks, reducing response time and improving containment efficiency during future breaches.

NEW QUESTION: 183
A company runs a DAST scan on a web application. The tool outputs the following recommendations:
- Use Cookie prefixes.
- Content Security Policy - SameSite=strict is not set.
Which of the following vulnerabilities has the tool identified?
A. TOCTOU
B. XSS
C. RCE
D. CSRF
Answer: (SHOW ANSWER)

NEW QUESTION: 184
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: (SHOW ANSWER)

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.

NEW QUESTION: 185

The security team is looking into aggressive bot behavior that is resulting in performance issues on the web server. After further investigation, the security engineer determines that the bot traffic is legitimate. Which of the following is the best course of action to reduce performance issues without allocating additional resources to the server?

A. Block all bot traffic using the IPS.

B. Monitor legitimate SEO bot traffic for abnormalities.

C. Configure the WAF to rate-limit bot traffic.

D. Update robots.txt to slow down the crawling speed.

Answer: (SHOW ANSWER)

robots.txt provides a way to politely request that well-behaved bots reduce their crawling speed.

The Crawl-delay directive can be used to specify a delay (in seconds) between successive requests. This approach directly addresses the performance issue by reducing the load caused by the bots without completely blocking them or requiring complex WAF configurations.

NEW QUESTION: 186

An analyst needs to evaluate all images and documents that are publicly shared on a website.

Which of the following would be the best tool to evaluate the metadata of these files?

A. OllyDbg

B. ExifTool

C. Volatility

D. Ghidra

Answer: (SHOW ANSWER)

ExifTool is a powerful tool for reading, writing, and editing metadata in various types of files, including images and documents. It can extract metadata such as the creation date, software used, author information, GPS coordinates, and more, which can be useful for evaluating the characteristics of publicly shared files.

NEW QUESTION: 187

The device event logs sourced from MDM software are as follows:

Device	Date/Time	Location	Event	Description
ANDROID_1022	01JAN21 0255	38.9072N,77.0369W	PUSH	APPLICATION 1220 INSTALL QUEUED
ANDROID_1022	01JAN21 0301	38.9072N,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

CompTIAExam.net

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

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)

Due to line 4, a GPS spoofing could be in use either by the newly install app, or before the app was installed.

NEW QUESTION: 188

A company designs policies and procedures for hardening containers deployed in the production environment. However, a security assessment reveals that deployed containers are not complying with the security baseline. Which of the following solutions best addresses this issue throughout early life-cycle stages?

A. Installing endpoint agents on each container and setting them to report when configurations drift from the baseline

B. Finding hardened container images and enforcing them as the baseline for new deployments

C. Creating a pipeline to check the containers through security gates and validating the baseline controls before the final deployment

D. Running security assessments regularly and checking for the security baseline on containers already in production

Answer: (SHOW ANSWER)

The best solution is to integrate security checks into the CI/CD pipeline, where containers are validated against the security baseline before deployment. This proactive approach ensures that containers are hardening properly during the early stages of development and deployment, reducing the risk of non-compliance with security policies and preventing issues from reaching the production environment.

NEW QUESTION: 189

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	50
3	+ 10	60
4	- 10	50
5	- 40	(Below zero balance!) -10
6	+ 30	20
7	+ 10	60
8	+ 40	60

freecram.net
CompTIA

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. Ensure that the application is using memory-safe functions to prevent integer overflows.

B. Recommend thread-safe processes in the code to eliminate race conditions.

C. Require the developers to include exception handlers to accommodate out-of-bounds results.

D. Move the batch processing from client side to server side to remove client processing inconsistencies.

Answer: (SHOW ANSWER)

The issue described in the log shows that, at one point, the inventory goes below zero (transaction 5 where the operation is -40, resulting in a negative balance of -10). However, despite this, the final inventory is reported as 100 rather than 60, suggesting that the system is not correctly handling situations where the inventory goes below zero, or there is an error in reporting or updating the total.

By including exception handlers in the code to manage out-of-bounds results, the developers can ensure that the system correctly handles situations where negative inventory would otherwise occur or other logical errors take place. Exception handling can ensure that invalid operations are either prevented or properly logged and managed, which resolves the problem of inconsistent inventory reporting.

NEW QUESTION: 190

A Chief Information Security Officer requests an action plan to remediate vulnerabilities. A security analyst reviews the output from a recent vulnerability scan and notices hundreds of unique vulnerabilities. The output includes the CVSS score, IP address, hostname, and the list of vulnerabilities. The analyst determines more information is needed in order to decide which vulnerabilities should be fixed immediately. Which of the following is the best source for this information?

Freecram.net

A. Third-party risk review

B. Business impact analysis

C. Incident response playbook

D. Crisis management plan

Answer: (SHOW ANSWER)

A Business Impact Analysis (BIA) identifies the criticality of systems and the potential impact of their compromise. It helps prioritize which vulnerabilities to remediate first based on the business value and operational impact of the affected assets.

NEW QUESTION: 191

A senior cybersecurity engineer is solving a digital certificate issue in which the CA denied certificate issuance due to failed subject identity validation. At which of the following steps within the PKI enrollment process would the denial have occurred?

A. RA

B. OCSP

C. CA

D. IdP

Answer: (SHOW ANSWER)

The Registration Authority (RA) is responsible for validating the identity of the certificate requestor before the Certificate Authority (CA) issues the certificate. If the identity validation fails during this step, the RA will deny the request, leading to a failure in certificate issuance. The CA will only issue the certificate after the RA has successfully validated the requestor's identity. Therefore, the denial of certificate issuance due to failed subject identity validation would have occurred at the RA stage.

NEW QUESTION: 192

A Chief Information Security Officer assigns a team to create malicious communications for a social engineering campaign. The purpose of this campaign is to determine the number of employees who might be susceptible to social engineering attacks. The following is a summary report from a previous campaign:

Department	Click rate
Sales	31%
Marketing	42%
Operations	71%
Finance	82%

Which of the following training modules would reduce click rates in the future?

A. Phishing

B. Whaling

C. Tailgating

D. Smishing

Answer: (SHOW ANSWER)

NEW QUESTION: 193

Which of the following best describes the reason PQC preparation is important?

A. To protect data against decryption due to increases in computational resource availability

B. To have larger key lengths available through key stretching

C. To improve encryption performance and speed using lightweight cryptography

D. To leverage asymmetric encryption for large amounts of data

Answer: (SHOW ANSWER)

Post-quantum cryptography (PQC) is about ensuring that encrypted data remains secure even when attackers have access to quantum computers, vastly more powerful computational resources than today's systems. Without PQC algorithms, future quantum capabilities could decrypt today's protected data, so preparing now safeguards information against that upcoming threat.

NEW QUESTION: 194

A system of globally distributed certificate servers connected to HSMs provide certificate security services for a publicly available PKI. These services include OCSP, certificate revocation list issuance, and certificate signing/issuance. The HSMs are all physical devices. All other servers are virtualized. Each global site has a network load balancer, and the sites are configured to load balance between sites.

Users report occasional but persistent log-on failures to different PKI-enabled websites. There is no apparent pattern to the failures. Some OCSP responses must be signed by the HSM. Each HSM is connected to a physical server containing multiple VMs for the local site with CAT 6e network cable. The backplane connecting the VMs is fiber based.

Which of the following would best reduce the OCSP response time in order to rule out the connection between the certificate server and HSM as a cause of the user-reported issues?

A. Virtualize the HSMs and convert the virtualized servers to physical systems.

B. Replace the copper-based network infrastructure with fiber.

C. Shorten the time the duration certificates are valid to 72 hours and implement ACME.

D. Reduce the number of global sites while increasing the number of HSMs.

Answer: (SHOW ANSWER)

Shortening the certificate validity period and implementing ACME reduces reliance on OCSP by enabling more frequent automated certificate issuance and renewal, thereby decreasing OCSP query load and response times. This approach helps rule out HSM-to-certificate server connection delays as the cause of user log-on failures.

NEW QUESTION: 195

A game developer wants to reach new markets and is advised by legal counsel to include specific age-related sign-up requirements. Which of the following best describes the legal counsel's concerns?
A. GDPR
B. LGPD
C. PCI DSS
D. COPPA
Answer: (SHOW ANSWER)
The Children's Online Privacy Protection Act (COPPA) requires online services, like games, to implement age-related sign-up requirements and obtain verifiable parental consent when collecting personal information from children under 13 in the U.S. This best aligns with the legal counsel's concerns.

NEW QUESTION: 196
A small number but steady series of attempts to breach the network has been occurring over a long period of time. During an investigation, a SOC analyst finds that traffic is exiting the network to known malicious hosts and is originating from a rogue network device. Which of the following attack vectors is most likely being used to breach the network?
A. Supply chain
B. Buffer overflow
C. Social engineering
D. Ransomware
Answer: (SHOW ANSWER)
A rogue network device generating outbound communication to known malicious hosts suggests that compromised or malicious hardware or embedded components were introduced into the environment. This type of intrusion commonly occurs through the supply chain, where tampered devices or equipment are delivered through vendors or procurement channels and later used to establish unauthorized network access or command-and-control communication over time.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 197
An organization's load balancers have reached EOL and are scheduled to be replaced. The organization identified a new, critical vulnerability that affects an unused function of the load balancers. Which of the following are the best ways to address the risk to the organization?
(Choose two.)
A. Exclude the devices from vulnerability scans.
B. Do not allow any network traffic to or from the hardware.
C. Immediately decommission the hardware.
D. Disable the vulnerable service.
E. Request a risk acceptance for the vulnerability indefinitely.
F. Request a risk acceptance for the vulnerability for 90 days.
Answer: (SHOW ANSWER)

NEW QUESTION: 198

A financial services organization is using AI to fully automate the process of deciding client loan rates. Which of the following should the organization be most concerned about from a regulatory perspective?

A. Model explainability

B. Credential Theft

C. Possible prompt Injections

D. Exposure to social engineering

Answer: (SHOW ANSWER)

Model explainability is a major concern from a regulatory perspective, particularly when AI is used to make critical decisions like loan rates. Regulatory bodies require that organizations be able to explain how decisions are made by AI models, especially when they impact financial outcomes. Without transparency into how the model arrives at its decisions, the organization could face regulatory scrutiny for potential biases, fairness issues, and lack of accountability.

NEW QUESTION: 199

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. 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)

Since the homegrown identity management system has already been flagged by an auditor as misaligned with industry best practices, and it must scale to handle dynamic, temporary user populations, the priority is to plan for a replacement that meets modern IAM standards (provisioning workflows, role-based access control, MFA support, audit logging, etc.). Starting with a clear requirements document ensures the new solution will address current gaps and support future needs.

NEW QUESTION: 200

After some employees are caught uploading data to online personal storage accounts, a company becomes concerned about data leaks related to sensitive, internal documentation.
Which of the following would the company most likely do to decrease this type of risk?

Freecram.net

A. Improve firewall rules to avoid access to those platforms

B. Implement a cloud access security broker

C. Create SIEM rules to raise alerts for access to those platforms

D. Deploy an internet proxy that filters certain domains

Answer: (SHOW ANSWER)

A CASB provides visibility and control over sanctioned and unsanctioned cloud services. By sitting between users and cloud providers, it can block or quarantine uploads to personal storage accounts in real time, preventing data exfiltration at the cloud access layer rather than relying solely on detection after the fact.

NEW QUESTION: 201

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 (also known as adversary or red-team simulation) involves deliberately mimicking insider tactics, techniques, and procedures to validate the playbook's controls and procedures in a controlled exercise. This approach directly tests whether the detection, containment, and response steps work as designed against realistic insider behaviors.

NEW QUESTION: 202

The results of an internal audit indicate several employees reused passwords that were previously included in a published list of compromised passwords.

The company has the following employee password policy:

Attribute	Requirement
Complexity	Enabled
Character class	Special character, number
Length	10 characters
History	8
Maximum age	60 days
Minimum age	0

freecram.net
CompTIA

Which of the following should be implemented to best address the password reuse issue?

(Choose two.)

A. Increase the minimum age to two days.

B. Increase the history to 20.

C. Increase the character length to 12.

D. Add case-sensitive requirements to character class.

E. Decrease the maximum age to 30 days.

F. Remove the complexity requirements.

G. Increase the maximum age to 120 days.

Answer: (SHOW ANSWER)

Increase the minimum age to two days: Setting a minimum age for passwords ensures that users cannot immediately change their password multiple times in succession to cycle through the password history and reuse a previous password. By increasing the minimum age to two days, it prevents this kind of behavior and enforces better password reuse discipline.

Increase the history to 20: The password history determines how many previous passwords are remembered by the system to prevent reuse. By increasing the history to 20, users are forced to create a significantly different password for a longer period, reducing the likelihood of reusing compromised passwords.

NEW QUESTION: 203

A security architect wants to prevent security impacts from input into data fields, such as the following:

'AND 1=1#

Which of the following would best accomplish this objective?

A. APIs

B. Coding standards

C. Base64 encoding

D. Sandboxing

Answer: (SHOW ANSWER)

The root of SQL injection (e.g., ' AND 1=1#) is unsafe string concatenation in application code. A robust secure-coding standard mandates parameterized queries (or stored procedures), strict input validation/whitelisting, and escaping of any user-supplied data. By embedding these practices into your development guidelines and enforcing them through code reviews and automated scans, you eliminate SQL injection and similar input-based attacks at the source.

NEW QUESTION: 204
A malicious actor exploited firmware vulnerabilities and used rootkits in an attack on an organization. After the organization recovered from the incident, an engineer needs to recommend a solution that reduces the likelihood of the same type of attack in the future. Which of the following is the most relevant solution?
A. Enabling software integrity checks
B. Installing self-encrypting drives
C. Implementing measured boot
D. Configuring host-based encryption
Answer: (SHOW ANSWER)
Implementing measured boot ensures that the system's firmware and boot process are verified for integrity before the OS is loaded. This prevents attacks that exploit firmware vulnerabilities or use rootkits, as any tampered components will be detected during the boot process. It is a crucial step to mitigate this type of attack in the future.

NEW QUESTION: 205
A security engineer discovers that some legacy systems are still in use or were not properly decommissioned. After further investigation, the engineer identifies that an unknown and potentially malicious server is also sending emails on behalf of the company.
The security engineer extracts the following data for review:

Server IP	DNS	Status	Auth. pass rate
200.100.50.25	marketing.company.com	Authorized	97%
200.50.25.10	29mail.mycrosoft.info	Unauthorized	0%
210.20.20.5	mail.google.com	Authorized	100%

Which of the following actions should the security engineer take next? (Choose two.)
A. Rotate the DKIM selector to use another key.
B. Change the DMARC policy to rejectand remove references to the server.
C. Remove the unnecessary servers from the SPF record.
D. Change the SPF record to enforce the hard fail parameter.
E. Update the MX record to contain only the primary email server.
F. Change the DMARC policy to noneand monitor email flow to establish a new baseline.
Answer: (SHOW ANSWER)
Changing the DMARC policy to "reject" and removing references to the unauthorized server will prevent malicious emails from being delivered, strengthening protection against spoofing.
Enforcing the hard fail parameter in the SPF record ensures that emails from unauthorized servers are rejected, further securing the organization's email infrastructure.

NEW QUESTION: 206
A security architect is implementing more restrictive policies to improve secure coding practices.
Which of the following solutions are the best ways to improve the security coding practices?
(Choose two.)
A. Implement a SAST tool along the pipeline for every new commit.
B. Define security gates and tests along the CI/CD flow with strict exception rules.

C. Perform regular vulnerability assessments on production software, defining tight SLAs for treatment.
D. Hire a third-party company to perform regular software tests, including quality and unity tests.
E. Deliver regular training for the software developers based on best practices.
F. Perform regular code reviews and implement pair programming methodology.
Answer: (SHOW ANSWER)

NEW QUESTION: 207
A company experienced a data breach, resulting in the disclosure of extremely sensitive data regarding a merger. As a regulated entity, the company must comply with reporting and disclosure requirements. The company is concerned about its public image and shareholder values. Which of the following best supports the organization in addressing its concerns?
A. Data subject access request
B. Business impact analysis
C. Supply chain management program
D. Crisis management plan
Answer: (SHOW ANSWER)
A crisis management plan provides a structured approach to responding to a data breach and handling the subsequent public relations issues. This plan would allow the company to manage the disclosure of sensitive information, address regulatory compliance requirements, and protect its public image and shareholder values effectively.

NEW QUESTION: 208
An application security engineer is examining the IAM configuration for a workload. The following is a sample of the decoded payload and header:

```
{
  "alg": "None",
  "typ": "JWT"
}
{
  "sub": "user_98765",
  "iat": 1680000000,
  "exp": 1680003600,
  "role": "svc_account",
  "refresh": true,
  "token_id": "abc123"
}
```

Which of the following is the most concerning risk?
A. Lateral movement
B. Privilege escalation
C. Credential stuffing
D. RCE from deserialization
Answer: (SHOW ANSWER)
The JWT header shows the algorithm set to "None", which means the token is not cryptographically signed or verified. This allows an attacker to modify the token payload and change claims such as the role field to gain elevated permissions. Because the token could be altered to assign higher privileges, the most significant risk is unauthorized privilege escalation within the application.

NEW QUESTION: 209
A security analyst receives the following SIEM alert for review:

Time | Event
03/07/2025 UTC 13:54:06 | MACHINE: hr_talent_01.corp.local "cd" SUCCESS
03/07/2025 UTC 13:54:07 | MACHINE: hr_talent_01.corp.local "cd ../../" SUCCESS
03/07/2025 UTC 13:54:08 | MACHINE: hr_talent_01.corp.local "sudo cat /etc/shadow" SUCCESS
Which of the following best describes the incident that occurred on the device?
A. A file injection attack occurred on the device.
B. An attacker viewed password hashes on the device.
C. A sensitive file was exfiltrated from the device.
D. A directory traversal attack occurred on the device.
Answer: (SHOW ANSWER)
The decisive event is sudo cat /etc/shadow SUCCESS. On Linux systems, /etc/shadow stores password hashes and related account password data. The log therefore indicates successful privileged access to that file and successful viewing of its contents. CompTIA's SecurityX Security Operations domain includes analysis of indicators of malicious activity and investigation of suspicious system behavior; this command sequence is consistent with credential-access activity.

NEW QUESTION: 210
A company is planning to migrate all of its on-site-hosted applications to a public cloud provider. Which of the following is the best way to reduce the scope of security-relevant work that the company must address after the applications have been migrated to the cloud?
Freecram.net
A. Adopting cloud-native security solutions
B. Using a microservices architecture
C. Performing a lift-and-shift cloud migration
D. Implementing serverless cloud services
Answer: D (LEAVE A REPLY)
Implementing serverless cloud services shifts most of the infrastructure management and security responsibilities (such as patching, scaling, and OS hardening) to the cloud provider. This significantly reduces the company's security workload after migration.

NEW QUESTION: 211
A security analyst is performing threat modeling for a new AI chatbot. The AI chatbot will be rolled out to help customers develop configuration information within the company's SaaS offering. Which of the following issues would require involvement from the company's internal legal team?
A. An internal user finds a way to use prompt injection to disregard guardrails.
B. A DoS vulnerability exists that could impact all customers who use the chatbot.
C. A bug bounty of an exploitable model inversion vulnerability is submitted.
D. User consent is not being collected before training models on customer data.
E. An access control issue is allowing the model to be poisoned with incorrect information.
Answer: (SHOW ANSWER)
Training AI models on customer data without obtaining user consent raises legal and regulatory compliance issues related to privacy, data protection, and data usage rights. Laws and regulations governing personal and customer data often require explicit disclosure and consent before data can be used for purposes such as model training. This situation requires involvement from the legal team to ensure compliance with privacy regulations, contractual obligations, and proper data governance policies.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 212
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)
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.

NEW QUESTION: 213
A security administrator wants to detect a potential forged sender claim in the envelope of an email. Which of the following should the security administrator implement? (Choose two).
A. MX record
B. DMARC
C. SPF
D. DNSSEC
E. S/MIME
F. TLS
Answer: (SHOW ANSWER)
SPF (Sender Policy Framework): Validates the envelope sender (MAIL FROM) by checking that the sending IP is authorized in the domain's SPF record, detecting forged return-path addresses.
DMARC (Domain-based Message Authentication, Reporting & Conformance): Builds on SPF (and DKIM) to enforce alignment between the authenticated envelope sender and the "From:" header, providing policy enforcement and reporting on any failures.

NEW QUESTION: 214
A software developer is working on a piece of code required by a new software package. The code should use a protocol to verify the validity of a remote identity. Which of the following should the developer implement in the code?
A. RSA
B. OCSP
C. HSTS
D. CRL

Answer: (SHOW ANSWER)

The Online Certificate Status Protocol (OCSP) lets your application query a trusted responder in real time to confirm that a peer's X.509 certificate hasn't been revoked. Embedding OCSP checking in your TLS/SSL handshake ensures the remote identity you connect to remains valid without needing to download and parse full CRLs.

NEW QUESTION: 215

Based on the results of a SAST report on a legacy application, a security engineer is reviewing the following snippet of code flagged as vulnerable:

```
[01] #include <stdio.h>
[02] #include <string.h>
[03] ...
[04]  char input[256] = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
[05]  ...
[06]  char transmit[20] = "0000";
[07]  char *ret_xmit;
[08]  printf("To be submitted: \"%s\"\n", input);
[09]  result in ret_xmit
[10]  ret_xmit = strcpy(transmit, input);
[12]  return 0;
[13] }
```

CompTIA freecram.net

Which of the following is the vulnerable line of code that must be changed?

A. Line [02]

B. Line [04]

C. Line [07]

D. Line [08]

E. Line [10]

Answer: (SHOW ANSWER)

The use of strcpy in line 10 is vulnerable because it does not check the size of the destination buffer, leading to a potential buffer overflow when copying the large input string into the smaller transmit array.

NEW QUESTION: 216

A water power generation plant fails a security inspection. The controllers are distributed across a river that is 0.5mi (0.8km) wide. The controllers are connected via HTTP to the shoreside master controller. The distributed controllers and the shoreside controller communicate over the internet using a cellular network. The company cannot encrypt control traffic because the systems will not tolerate the additional overhead. Which of the following strategies is the best way to reduce the risk of compromise?

A. Monitoring control traffic for command sequences with out-of-range or unexpected values

B. Disconnecting cellular radios in favor of shielded Cat 5e cables to each of the controllers

C. Reviewing the ladder logic on the controllers to determine whether unauthorized changes have been introduced

D. Deploying a dedicated base station and reducing the footprint with highly directional antennas

Answer: (SHOW ANSWER)

The biggest risk in the scenario is that unencrypted control traffic is traversing the internet over a cellular network. Since encryption is not feasible, the best compensating control is to reduce exposure by making the wireless path more private, more local, and less accessible to unintended parties. A dedicated base station with directional antennas narrows the RF footprint and

reduces interception and unauthorized access opportunities compared with broad internet- based cellular exposure. CompTIA's SecurityX objectives emphasize Security Architecture, including secure boundaries, compensating controls, and resilient design choices when ideal controls cannot be used.

NEW QUESTION: 217
Which of the following AI concerns is most adequately addressed by input sanitization?
A. Model inversion
B. Prompt Injection
C. Data poisoning
D. Non-explainable model
Answer: (SHOW ANSWER)
Prompt injection occurs when attackers manipulate input to alter the behavior of an AI model.
Input sanitization helps prevent this by filtering or validating user input, ensuring that malicious commands or instructions don't reach or influence the model's processing logic.

NEW QUESTION: 218
A penetration tester is drafting a report of findings and recommendations. Multiple EOL biomedical devices were compromised using a combination of known-exploit payloads for CVEs and VLAN hopping. The tester acknowledges that the systems cannot be changed or replaced in the hospital due to regulatory, safety, and cost reasons. Which of the following are the most effective controls for this scenario? (Choose two.)
A. Deploying an IDS with active response for threat activities from a network tap
B. Implementing QoS that limits the throughput of the link speeds from some VLANs
C. Limiting trunking protocols to specific uplink ports of access switches
D. Adding a proxy and requiring medical staff to authenticate every connection
E. Inserting an in-line IPS between network segments of the affected hosts
F. Performing security awareness training for these devices users
Answer: (SHOW ANSWER)
Restricting trunking protocols to only designated uplink ports prevents attackers from exploiting switch trunk negotiation to perform VLAN hopping. Disabling trunking on access ports ensures they operate strictly as access interfaces assigned to a single VLAN, which mitigates the attack vector used to pivot between network segments.
Placing an in-line intrusion prevention system between the network segments hosting the vulnerable biomedical devices allows real-time inspection and blocking of exploit traffic targeting the known CVEs. Because the devices cannot be patched or replaced, compensating network controls that actively detect and block malicious traffic provide effective protection while maintaining device operation.

NEW QUESTION: 219
A company is migrating from company-owned phones to a BYOD strategy for mobile devices.
The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year.
Which of the following will most likely secure the data on the lost device?
A. Require a VPN to be active to access company data.
B. Set up different profiles based on the person's risk.
C. Remotely wipe the device.
D. Require MFA to access company applications.
Answer: (SHOW ANSWER)
Remotely wiping a lost mobile device ensures that any company data or credentials stored locally are erased, preventing unauthorized access even if the phone falls into the wrong hands. This control directly addresses the risk of data exposure on a lost device.

NEW QUESTION: 220
A security architect is performing threat-modeling activities related to an acquired overseas software company that will be integrated with existing products and systems. Once its software is integrated, the software company will process customer data for the acquiring company. Given the following:

ID	Threat	STRIDE	Criticality
01	Attacker performs denial of service against public-facing endpoints	Denial of service	High
02	Malicious insider puts a backdoor into source code	Tampering	Critical
03	Attacker injects malicious code into third-party library	Tampering	Critical
04	Attacker escalates privilege to administrator in web system	Elevation of privilege	High
05	Attacker performs successful password spraying	Spoofing	High

CompTIA
Pdfexam.net

Which of the following mitigations would reduce the risk of the most significant threats?
A. Privileged access management system with conditional access capabilities to prevent unauthorized access
B. Rate-limiting capabilities on all authentication systems and leveraging single sign-on through federation
C. Secure development process with gate checks and appropriate code scanning
D. Zero Trust architecture for all assets from the acquired company using microsegmentation against sensitive applications
Answer: (SHOW ANSWER)
The most significant threats listed (IDs 02 and 03) involve tampering with source code or third- party libraries, both rated as Critical. Implementing a secure development process with gate checks and code scanning directly mitigates these risks by detecting backdoors, malicious code, and integrity issues before integration.

NEW QUESTION: 221
A developer needs to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module. Which of the following is the most appropriate technique?
A. Key splitting
B. Key escrow
C. Key rotation
D. Key encryption
E. Key stretching
Answer: (SHOW ANSWER)
Key stretching enhances the security of stored passwords by applying computationally intensive algorithms (e.g., bcrypt, PBKDF2) to make brute-force attacks more difficult, without replacing the underlying crypto-module.ks.

NEW QUESTION: 222
Which of the following explains why an organization should carefully consider whether to use AI to automate processes that interact with healthcare data?
A. The model may be susceptible to AI pipeline injections.
B. The model may be susceptible to information disclosure.
C. The model may be susceptible to social engineering.

D. The model may be susceptible to model inversion.
Answer: (SHOW ANSWER)
Healthcare data involves sensitive and regulated information. Using AI to automate processes with such data raises the primary concern of information disclosure, where private medical records or personally identifiable information could be exposed if the model or its handling of data is not properly secured.

NEW QUESTION: 223
A security engineer needs to select the architecture for a cloud database that will protect an organization's sensitive data. The engineer has a choice between a single-tenant or a multitenant database architecture offered by a cloud vendor. Which of the following best describes the security benefits of the single-tenant option? (Choose two.)
A. Most cost-effective
B. Ease of backup and restoration
C. High degree of privacy
D. Low resilience to side-channel attacks
E. Full control and ability to customize
F. Increased geographic diversity
Answer: (SHOW ANSWER)
High degree of privacy: Single-tenant deployments isolate your data and metadata entirely from other customers, eliminating risks of accidental or malicious cross-tenant access.
Full control and ability to customize: You retain administrative control over configurations, patching schedules, encryption settings, and network policies, allowing to tailor security controls precisely to your requirements.

NEW QUESTION: 224
An analyst is using the Diamond Model of Intrusion Analysis to identify the likely chain of activities associated with an attacker's activities. The threat hunter has completed the core components of the model but needs to consider meta factors to more deeply understand the situation. Which of the following should the threat hunter seek to understand within the model?
A. Direction
B. Velocity
C. Capabilities
D. Infrastructure
Answer: B (LEAVE A REPLY)
Within the Diamond Model of Intrusion Analysis, meta features provide additional context about adversary activity beyond the four core elements. Velocity is a meta feature that describes the speed and rate at which adversary activities occur across events in the intrusion chain.
Understanding this factor helps analysts better interpret how quickly an attack progresses and how the adversary operates over time.

NEW QUESTION: 225
A multinational enterprise is planning to implement a centralized authentication solution across its global offices. The risk team identifies that some regional offices operate in areas with high latency and some data centers experience intermittent connectivity issues. The Chief Information Officer requests a solution that minimizes authentication disruptions without compromising security. Which of the following is the best risk treatment strategy?
A. Implement a hybrid identity solution with local failover authentication
B. Require that all users authenticate only during on-site visits to headquarters
C. Accept the risk due to the low probability of simultaneous authentication failures
D. Outsource authentication to a third-party cloud provider
Answer: (SHOW ANSWER)
A hybrid identity architecture allows authentication services to operate both centrally and locally.

Local authentication services or cached credentials provide failover capability when connectivity to central identity infrastructure is disrupted due to latency or intermittent network issues. This approach maintains strong centralized identity management while ensuring users in remote regions can still authenticate securely during connectivity interruptions, minimizing operational disruption without weakening security controls.

NEW QUESTION: 226
A cloud engineer wants to configure mail security protocols to support email authenticity and enable the flow of email security information to a third-party platform for further analysis. Which of the following must be configured to achieve these requirements? (Choose two.)
A. DMARC
B. DKIM
C. TLS
D. SPF
E. DNSSEC
F. MX
Answer: (SHOW ANSWER)
DKIM (DomainKeys Identified Mail) adds a cryptographic signature to outbound messages, ensuring recipients can verify they haven't been tampered with and truly originated from your domain. DMARC (Domain-based Message Authentication, Reporting & Conformance) leverages both DKIM (and SPF) to validate incoming mail and critically provides reporting ("rua"/"ruf" tags) so you can forward delivery, failure, and forensic data to any third-party analytics or threat-intel platform.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)

NEW QUESTION: 227
A company wants to prevent a partner company from denying agreement to a transaction. Which of the following is the best solution for the company?
A. Federation
B. Key escrow
C. Salting hashes
D. Digital signatures
Answer: D (LEAVE A REPLY)
Digital signatures provide non-repudiation, ensuring that the sender cannot deny signing a transaction. This mechanism ties the transaction to the entity through cryptographic assurance. Federation involves identity management and authentication but does not address non- repudiation. Key escrow is used for securely storing encryption keys and is unrelated to transaction agreements. Salting hashes enhances password security but does not support transactional non-repudiation.

NEW QUESTION: 228
A Chief Information Security Officer is concerned about the operational impact of ransomware. In the event of a ransomware attack, the business requires the integrity of the data to remain intact and an RPO of less than one hour. Which of the following storage strategies best satisfies the business requirements?
A. Full disk encryption
B. Remote journaling
C. Immutable

D. RAID 10
Answer: C (LEAVE A REPLY)
Immutable storage prevents data from being altered or deleted, ensuring integrity even during a ransomware attack. Combined with frequent snapshots, it can achieve an RPO of less than one hour, best meeting the business requirements.

NEW QUESTION: 229
A company is decommissioning old servers and hard drives that contain sensitive data. Which of the following best protects against data leakage?
A. Purging
B. Clearing
C. Shredding
D. Degaussing
Answer: (SHOW ANSWER)
Purging is the best option for protecting against data leakage when decommissioning old servers and hard drives that contain sensitive data. Purging involves the removal of data in such a way that it cannot be recovered by any known means, even by advanced forensic techniques. This typically involves overwriting the data multiple times or using specialized software to ensure it is completely erased.

NEW QUESTION: 230
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.)
Freecram.net
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)
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.

NEW QUESTION: 231
A company's BIA indicates that any loss of more than one hour of data would be catastrophic to the business. Which of the following must be in place to meet this requirement?
A. RPO
B. RTO
C. SLA
D. DRP
E. BCP
Answer: (SHOW ANSWER)

RPO (Recovery Point Objective): Specifies the maximum acceptable amount of data loss measured in time. If data loss of more than one hour is unacceptable, the RPO should be set to less than or equal to one hour.
RTO (Recovery Time Objective): Refers to the acceptable duration of system downtime, which is not relevant to the question.
The BCP, DRP, and SLA do not directly address data loss.

NEW QUESTION: 232
During an audit at an organization, auditors find that developers are able to promote code to production. The auditors request a full review of all production changes. Which of the following should the organization implement to prevent a full review in the future?
A. Branch protection
B. Centralized code repositories
C. Interactive application security testing
D. Change control board
Answer: (SHOW ANSWER)
A Change Control Board (CCB) enforces structured review and approval processes for changes before they reach production. Implementing a CCB ensures that all production changes are formally reviewed, preventing audit issues in the future.

NEW QUESTION: 233
A cyberanalyst has been tasked with recovering PDF files from a provided image file. Which of the following is the best file-carving tool for PDF recovery?
A. objdump
B. Strings
C. dd
D. Foremost
Answer: (SHOW ANSWER)
Foremost is a dedicated file-carving utility that scans raw disk images for known file headers and footers, such as PDF's %PDF- and %%EOF, and extracts intact documents without relying on filesystem metadata. This makes it the go-to tool for recovering PDFs from a forensic image.

NEW QUESTION: 234
A company's help desk is experiencing a large number of calls from the finance department stating access issues to www.bank.com. The security operations center reviewed the following security logs:

User	User IP & Subnet	Location	Website	DNS Resolved IP (public)	HTTP Status Code
User12	10.200.2.52/24	Finance	www.bank.com	65.146.76.34	495
User31	10.200.2.213/24	Finance	www.bank.com	65.146.76.34	495
User46	10.200.5.76/24	IT	www.bank.com	98.17.62.78	200
User23	10.200.2.156/24	Finance	www.bank.com	65.146.76.34	495
User51	10.200.4.138/24	Legal	www.bank.com	98.17.62.78	200

freecram.net CompTIA
Which of the following is most likely the cause of the issue?
A. Recursive DNS resolution is failing
B. The DNS record has been poisoned.
C. DNS traffic is being sinkholed.
D. The DNS was set up incorrectly.

Answer: (SHOW ANSWER)
Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination.
This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.
In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.

NEW QUESTION: 235
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: (SHOW ANSWER)
An immutable infrastructure approach ensures that VM images are never altered in place. All state and data live externally (for example in object storage or managed databases), and any required change, be it patching or configuration, happens by building and rolling out a fresh VM image. This guarantees no unauthorized drift or in-place modification on running instances.

NEW QUESTION: 236
A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location. Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?
A. Execute never
B. No-execute
C. Total memory encryption
D. Virtual memory protection
Answer: (SHOW ANSWER)
ARM's "Execute Never" (XN) feature is the architecture's equivalent of a no-execute (NX) or Data Execution Prevention (DEP) bit. By marking all writable memory regions as non-executable, you block any injected code, such as that placed in another process's heap or stack, from ever running. This prevents the malware from inserting itself into memory and then executing its payload.

NEW QUESTION: 237
The material findings from a recent compliance audit indicate a company has an issue with excessive permissions. The findings show that employees changing roles or departments results in privilege creep. Which of the following solutions are the best ways to mitigate this issue?
(Choose two.)
A. Setting different access controls defined by business area
B. Implementing a role-based access policy
C. Designing a least-needed privilege policy
D. Establishing a mandatory vacation policy
E. Performing periodic access reviews

F. Requiring periodic job rotation

Answer: (SHOW ANSWER)

Role-based access control (RBAC) ensures that permissions are tied to job roles rather than individuals, making it easier to update or change access when someone switches roles. Periodic access reviews help detect and correct excessive permissions by regularly reviewing who has access to what and removing any unnecessary privileges.

NEW QUESTION: 238

A building camera is remotely accessed and disabled from the remote console application during off-hours. A security analyst reviews the following logs:

```
.1 Dec 16:03:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
lozilla/5.0 (Windows NT 5.1) Gecko
.1 Dec 16:33:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
lozilla/5.0(Windows NT 5.1) Gecko
.1 Dec 22:30:23 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
lozilla/5.0 (X11.Linux x86_64) Applewebkit
.1 Dec 23:00:23 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
.1 Dec 23:05:43 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
lozilla/5.0 (X11.Linux x86_64) Applewebkit
.1 Dec 23:35:43 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
.2 Dec 00:30:53 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
lozilla/5.0 (X11.Linux x86_64) Applewebkit
```

Which of the following actions should the analyst take to best mitigate the threat?

A. Implement WAF protection for the web application.

B. Upgrade the firmware on the camera.

C. Only allow connections from approved IPs.

D. Block IP 104.18.16.29 on the firewall.

Answer: (SHOW ANSWER)

The logs show successful admin access from both an internal IP (192.168.2.5) and an external IP (104.18.16.29). Since external access during off-hours indicates compromise, the best long-term mitigation is to restrict remote access so only approved IPs can connect. This prevents unauthorized external access while maintaining legitimate internal management.

NEW QUESTION: 239

SIMULATION

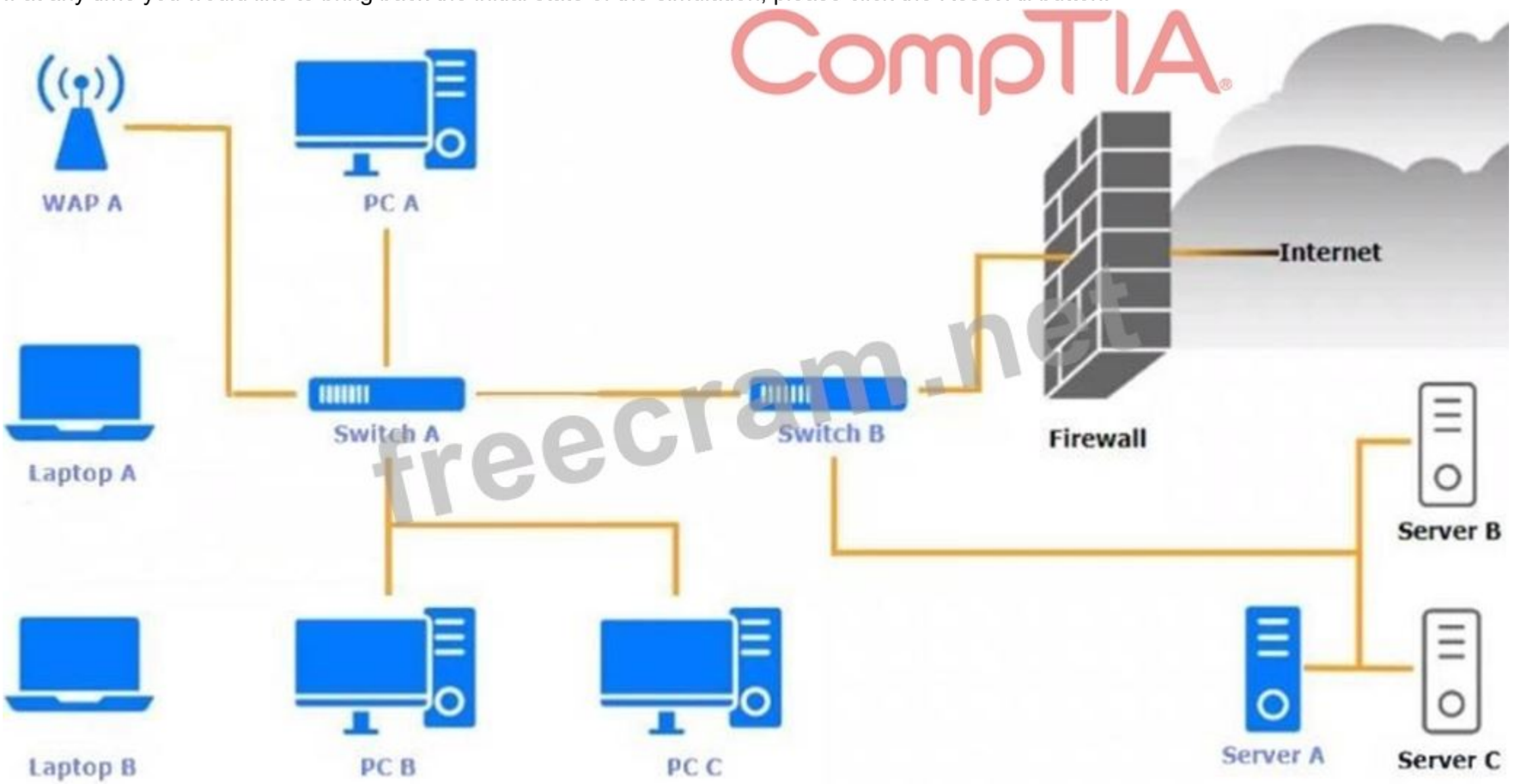
A security engineer needs to review the configurations of several devices on the network to meet the following requirements:

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

INSTRUCTIONS

Click on the various workstations and network devices to review the posture assessment results.

Remediate any possible issues or indicate that no issue is found.
Click on Server A to review output data. Select commands in the appropriate tab to remediate connectivity problems to the PostgreSQL database via SSH.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



freecram.net

WAP A

Finding	Status	Remediation
Firmware	Updated 5 days ago	☐ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
SSID broadcast	Disabled	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ 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

Laptop A

Finding	Status	Remediation
OS updates	Updated 3 days ago, last checked 6:08 a.m.	☐ No issue
Endpoint protection	Last checked in 6:13 a.m.	☐ Patch management
Browser version	91.2.5 (7/25/2023)	☐ 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	Medium	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	☐ Change default administrative password
Wireless	Enabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

freecram.net

CompTIA®

Laptop B

Finding	Status	Remediation
OS updates	Updated 3 days ago, last checked 8:08 a.m.	☐ No issue
Endpoint protection	Last checked in 8:11 a.m.	☐ Patch management
Browser version	81.2.5 (7/25/2023)	☐ Update endpoint protection
Disk encryption	Disabled	☐ Enabled disk encryption
Password Complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	Normal	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 8080, 53	☐ Change default administrative password
Wireless	Enabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

CompTIA
freecram.net

Switch A

Finding	Status	Remediation
Firmware	Updated 7 days ago	☐ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 12)	4	☐ Update endpoint protection
Default admin account	Default password has not been changed	☐ Enabled disk encryption
		☐ Enable port security on network device
HTTP server	Disabled	☐ 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®

Switch B

Finding	Status	Remediation
Firmware	Updated 7 days ago	☐ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 6)	1	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ 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

CompTIA
freecram.net

PC A

Finding	Status	Remediation
OS updates	Updated 2 days ago, last checked 5:08 a.m.	☐ No issue
Endpoint protection	Last checked 6:11 a.m.	☐ Patch management
Browser version	91.2.5 (7/25/2023)	☐ 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	Normal	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

freecram.net
CompTIA

PC B

Finding	Status	Remediation
OS updates	Updated 2 days ago, last checked 5:10 a.m.	☐ No issue
Endpoint protection	Last checked in 6:13 a.m.	☐ Patch management
Browser version	91.2.5 (7/25/2023)	☐ 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	Medium	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 389, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

freecram.net
CompTIA

PC C

Finding	Status	Remediation
OS updates	Updated 22 days ago	☐ No issue
Endpoint protection	Last checked 6:19 a.m.	☐ Patch management
Browser version	91.2.5 (7/25/2022)	☐ 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
		☐ Enable all connectivity settings

freecram.net
CompTIA

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
```

freecram.net

CompTIA

Server A

Nmap | IP Tables

```
#iptables --list --verbose

Chain INPUT (policy DROP 5 packets, 341 bytes)

pkts bytes  target  prot  opt in  out source    destination

0    0      ACCEPT  tcp   --  any any anywhere  anywhere    tcp dpts:login:65535 dpt:ssh state NEW,ESTABLISHED

1   28      DROP    all   --  any any anywhere  anywhere

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

freecram.net

CompTIA

1 | 2 | 3 | 4

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



CompTIA
freecram.net

Answer:



NEW QUESTION: 240

A firewall administrator needs to ensure all traffic across the company network is inspected. The administrator gathers data and finds the following information regarding the typical traffic in the network:

Port	Protocol	Traffic in (bytes)	Traffic out (bytes)	% of traffic
80	TCP	1,250,482	2,165,482	3.12
443	TCP	58,395,746	75,847,219	91.4
	ICMP	334,562	444,119	.9
445	TCP	7,658,433	568,234	4.11
123	UDP	54,645	55,181	.08

Which of the following is the best solution to ensure the administrator can complete the assigned task?

A. A full-tunnel VPN

B. Web content filtering

C. An endpoint DLP solution

D. SSL/TLS decryption

Answer: (SHOW ANSWER)

With over 91% of your traffic on TCP/443, virtually all of your users' web sessions are encrypted HTTPS. Without decrypting that traffic, your firewall (or proxy) can't perform deep inspection. Enabling SSL/TLS decryption (often via a transparent proxy or decryption appliance) lets you terminate and re-encrypt sessions so you can apply your security policies, ensuring that the bulk of your network traffic is fully inspected.

NEW QUESTION: 241

As part of a security audit in the software development life cycle, a product manager must demonstrate and provide evidence of a complete representation of the code and modules used within the production-deployed application prior to the build. Which of the following best provides the required evidence?

A. Software composition analysis

B. Runtime application inspection

C. Static application security testing

D. Interactive application security testing

Answer: (SHOW ANSWER)

Software Composition Analysis (SCA) is the best method for identifying all components, dependencies, and open-source libraries used in an application. It ensures that organizations track and manage vulnerabilities in third-party code before deployment. SCA tools generate a Software Bill of Materials (SBOM), which provides a full representation of the code and modules used in the application.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 242
A security analyst was monitoring the networks of a group of companies. The analyst identified several periods of concentrated, coordinated activity by unknown actors. The activity repeated at regular intervals and affected all the companies. Minor hardware outages that correlated with the same times as the discovered activity escalated in severity. Which of the following threat actors was most likely involved?
A. An organized crime collective running a ransomware campaign
B. A group of politically motivated hackers
C. Disgruntled employees who were recently terminated
D. An advanced persistent threat financed by a nation-state
Answer: D (LEAVE A REPLY)
The described activity - concentrated, coordinated attacks that happen at regular intervals and affect multiple companies - suggests the involvement of an advanced persistent threat (APT). APTs are often well-funded and organized, typically backed by nation-states. They focus on long- term, stealthy campaigns to achieve strategic goals, which might include espionage or disruption.
The fact that the attacks correlate with minor hardware outages and increasing severity indicates a well-planned and ongoing attack that escalates over time, a hallmark of nation-state- backed APTs. These attackers often have the resources, skill, and persistence to operate over extended periods without detection, making them a likely candidate for this type of activity.

NEW QUESTION: 243
A security engineer receives an alert from the threat intelligence platform with the following information:

Email	Source	Date	Data
jane@corporg.com	Third-party leakage	4 weeks ago	Email, name
john@corporg.com	Pastebin	3 weeks ago	Email, password, cell phone
alice@corporg.com	Deep web website	2 months ago	Name, address, cell phone
ann12@hotmail.com	Deep web forum	5 days ago	Email, password
joe@corporg.com	Initial access broker	1 week ago	Email, password

freecram.com CompTIA

Which of the following actions should the security engineer do first?
A. Reset John's and Joe's passwords and investigate any potential unauthorized access
B. Contact John, Ann, and Joe to inform them about the incident and schedule a password reset
C. Reset John's, Ann's, and Joe's passwords and disconnect all users' active sessions
D. Reset John's and Joe's passwords and inform authorities about the leakage
Answer: (SHOW ANSWER)
The threat intelligence data shows that credentials for two corporate accounts were exposed, including both email and password. These accounts are at immediate risk of unauthorized access because valid credentials may already be circulating in public or criminal sources. The first response should be to reset those passwords and investigate for suspicious login activity or misuse to determine whether the credentials were already used by attackers.

NEW QUESTION: 244
A security consultant recommends that a solution be deployed to increase awareness of APTs throughout the IT and OT environments. The consultant's requirements state that the solution must:
- Be capable of collecting data from both OT and IT protocols.
- Operate within new microsegmented and air-gapped network architecture
- Provide both correlation of events and retention of raw log data and
incidents
- Integrate with the ITSM platform and employee paging system
Which of the following solutions best meets these requirements?
A. SASE deployment with an Always On VPN
B. A next-generation firewall with intrusion prevention services
C. A vulnerability scanner with agentless scanning
D. SIEM with remote collectors
Answer: (SHOW ANSWER)
A SIEM with remote collectors can gather logs and telemetry from both IT and OT systems across segmented or air-gapped networks by placing collectors locally in each segment. These collectors forward events to the central SIEM for correlation, long-term log retention, and incident tracking. SIEM platforms also commonly integrate with ITSM systems and notification tools such as paging systems, enabling automated ticketing and alerting while providing visibility into advanced persistent threats across the environment.

NEW QUESTION: 245
A security engineer is reviewing the SIEM logs after a server crashed. The following list of events represents the timeline of actions collected from the SIEM:

```
(1:30:01:231) System : PID: 334 - Explorer.exe
(1:30:03:523) System : PID: 1231 - Msbuild.exe as child from 334
(1:33:12:312) System : PID: 3324 - Powershell.exe as child from 1231
(1:34:34:864) System : PID: 4554 - LSSASS.exe as child from 3324
(1:35:56:131) System : PID: 7662 - LSSASS.exe - SAM access from 3324
```

Which of the following TTPs is most likely associated with this SIEM log?
A. Lateral movement
B. Credential dumping
C. Data exfiltration
D. LOLBins use
Answer: (SHOW ANSWER)
The logs show processes associated with credential dumping, specifically LSASS.exe access, which is commonly targeted to extract stored credentials from memory for later use by attackers.

NEW QUESTION: 246
During post-incident analysis of a recent website outage, an incident response team identifies the following commands that were run from a compromised internal machine:

```
bad@globalcorp.com:~$ host -l globalcorp.com
Host globalcorp.com not found: 5(REFUSED); Transfer failed.

bad@globalcorp.com:~$ host globalcorp.com
globalcorp.com has address 52.94.236.0 globalcorp.com has address 54.239.28.0 globalcorp.com has address 205.251.242.0 globalcorp.com mail is
handled by 5 globalcorp-smtp.globalcorp.com.

bad@globalcorp.com:~$ dig axfr globalcorp.com globalc0rp.com
; <<>> DiG 9.18.24-0ubuntu5-Ubuntu <<>> axfr globalcorp.com
;
; global options: +cmd
; globalcorp.com 7200 IN SOA globalc0rp.com 20170402001 172800 900 1 209600 (...)
```

Which of the following should the team do?

A. Sinkhole suspicious DNS traffic

B. Implement DKIM

C. Restrict host and dig command executions

D. Prevent successful zone transfers

Answer: (SHOW ANSWER)

The commands show attempts to perform a DNS zone transfer using dig axfr. Zone transfers allow retrieval of the entire DNS zone database, revealing internal hostnames, IP addresses, and infrastructure details. The output indicates the transfer succeeded, which means the DNS server is improperly allowing zone transfers to unauthorized hosts. Restricting zone transfers so they are only permitted between authorized DNS servers prevents attackers from enumerating internal infrastructure through DNS.

NEW QUESTION: 247

A company runs a DAST scan on a web application. The tool outputs the following recommendations:

- Use Cookie prefixes.
- Content Security Policy - SameSite=strict is not set.

Which of the following vulnerabilities has the tool identified?

A. RCE

B. XSS

C. CSRF

D. TOCTOU

Answer: (SHOW ANSWER)

The recommendations to use Cookie prefixes and set SameSite=strict relate directly to mitigating Cross-Site Request Forgery (CSRF) attacks by restricting how cookies are sent with cross-site requests.

NEW QUESTION: 248

A security officer received several complaints from users about excessive MFA push notifications at night. The security team investigates and suspects malicious activities regarding user account authentication. Which of the following is the best way for the security officer to restrict MFA notifications?

A. Provisioning FID02 devices

B. Deploying a text message based on MFA

C. Enabling OTP via email

D. Configuring prompt-driven MFA

Answer: (SHOW ANSWER)

Prompt-driven MFA means that MFA prompts are triggered only when there is suspicious activity or a specific need for authentication, rather than being sent regularly. This approach would reduce the excessive notifications while still ensuring security, addressing the user's complaints effectively.

NEW QUESTION: 249
A company hosts a platform-as-a-service solution with a web-based front end, through which customers interact with data sets. A security administrator needs to deploy controls to prevent application-focused attacks. Which of the following most directly supports the administrator's objective?
A. improving security dashboard visualization on SIEM
B. Rotating API access and authorization keys every two months
C. Implementing application toad balancing and cross-region availability
D. Creating WAF policies for relevant programming languages
Answer: D (LEAVE A REPLY)
A Web Application Firewall (WAF) provides specific protection against application-focused attacks (such as SQL injection, cross-site scripting, etc.) by analyzing and filtering HTTP requests. Creating WAF policies tailored to the application's programming languages will directly support the security administrator's objective of preventing application-specific attacks.

NEW QUESTION: 250
After a recent outage, a software engineering company performed an audit of its development processes. The audit findings include the following:
- The use of local branches were not enforced for software development.
- Two-person review was not required for merges with production pipelines.
- There was a lack of pre-production pipelines and insufficient bake times between stages.
Which of the following changes would best improve the company's practices?

Freecram.net

A. Regression testing
B. Architecture and integration review
C. Formal specification and verification
D. Coding standards and linting
Answer: B (LEAVE A REPLY)
Architecture and integration review enforces structured development workflows, including branch management, peer reviews, and proper pre-production pipelines. This directly addresses the audit findings and improves software reliability and security.

NEW QUESTION: 251
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. Tabletop exercise
B. Walk-through review
C. Lessons learned
D. Business impact analysis
Answer: A (LEAVE A REPLY)
A tabletop exercise is a discussion-based simulation where key stakeholders, including management and technical teams, gather to walk through a hypothetical cybersecurity incident.
The goal is to identify security gaps, assess response strategies, and prepare for real-world incidents. During this exercise, participants typically discuss their roles and decisions in handling the incident, but no actual systems are impacted.

NEW QUESTION: 252
An organization purchased a new manufacturing facility and the security administrator needs to:
- Implement security monitoring.
- Protect any non-traditional device(s)/network(s).
- Ensure no downtime for critical systems.
Which of the following strategies best meets these requirements?
A. Configuring honeypots in the internal network to capture malicious activity
B. Analyzing system behavior and responding to any increase in activity
C. Applying updates and patches soon after they have been released
D. Observing the environment and proactively addressing any malicious activity
Answer: (SHOW ANSWER)
Observing the environment and proactively addressing malicious activity provides continuous monitoring for non-traditional devices and networks while avoiding downtime for critical systems. This strategy aligns with OT/ICS environments where availability is crucial and active measures must not disrupt operations.

NEW QUESTION: 253
A Chief Information Security Officer (CISO) is developing a third-party risk management program and wants to establish an order of preference for solicitation and acceptance of audit and assessment results from business partners. The CISO prefers a formal certification against an established framework, which should be considered more reliable than self-attestations. Which of the following is most likely the reason for this perspective?
A. A certification audit is managed by a central authority.
B. Assessments are based on evidence, not judgments.
C. Certifications are typically issued against a formal standard.
D. For standards like PCI, self-attestations are more reliable than certifications.
Answer: (SHOW ANSWER)

NEW QUESTION: 254
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: A (LEAVE A REPLY)
By implementing structured error-handling routines (e.g., try/catch blocks with generic user-facing error messages and internal logging of detailed debug information), you prevent the application from exposing sensitive interpreter details to end users. This practice ensures that, even when an unexpected condition occurs, only a sanitized error page is shown, mitigating information-leakage risks at their source.

NEW QUESTION: 255
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)
Obtaining file hashes from a confiscated laptop is primarily done to ensure that the integrity of each file can be validated later. By generating a hash of each file, investigators can later compare the hash values to ensure that no files have been altered or tampered with during the investigation process. This helps confirm that the files remain unchanged from the time they were seized.

NEW QUESTION: 256
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)
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.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF Special Discount Code: freecram**)

NEW QUESTION: 257
A company established a new process for business analysts to receive emails that contain links for purchase requests. The new process requires links to be submitted through new emails. Which of the following is the best way to secure this process without disrupting order fulfillment?
A. Deploying a browser isolation solution
B. Blocking all potentially malicious links
C. Enforcing security awareness training
D. Implementing DNS filtering
Answer: (SHOW ANSWER)
Deploying a browser isolation solution would be the best way to secure this process without disrupting order fulfillment. It allows users to click on links within emails while keeping any potentially harmful content isolated from the rest of the network. This prevents malicious links from affecting internal systems while still enabling users to complete their tasks without disruption.

NEW QUESTION: 258
Which of the following is the best way to protect the website browsing history for an executive who travels to foreign countries where internet usage is closely monitored?
A. DOH
B. EAP-TLS

C. Geofencing
D. Private browsing mode
Answer: (SHOW ANSWER)
DNS over HTTPS (DOH) encrypts DNS queries, which protects the browsing history from being monitored or intercepted by third parties, such as internet service providers or government authorities. This is especially important in countries where internet usage is closely monitored.
DOH ensures that DNS requests (which resolve domain names into IP addresses) are encrypted and sent over HTTPS, preventing external parties from seeing which websites the executive is visiting.

NEW QUESTION: 259
The security team is receiving escalated support tickets stating that one of the company's publicly available websites is not loading as expected. Given the following observations:

Server	URL	Installed certificate	Age of installed certificate
SALES10	www.sales.com	*.sales.com	282 days
SALES10	fulfillment.sales.com	*.sales.com	282 days
WEB27	www.website.com	website.com	418 days
SALES20	tracking.sales.com	tracking.sales.com	240 days
EVENT2	event.sales.com	event.sales.com	57 days

Which of the following is most likely the root cause?
A. A certificate signed by a global root certification authority has expired.
B. A protocol mismatch error is expected to occur when using outdated browsers.
C. One certificate is being bound to multiple websites on the same server.
D. Subject alternative names were not used appropriately for subdomains.
Answer: (SHOW ANSWER)
The certificate for www.website.comon WEB27 is 418 days old, which likely exceeds its validity period (commonly 398 days per current industry standards). This suggests the certificate has expired, causing the website to fail to load properly.

NEW QUESTION: 260
A security engineer is reviewing logs and summarizes the following:
- The target host communicates to an external IP address over HTTPS.
- The external IP address was not categorized as malicious.
- The company has a deep packet inspection system that supports HTTPS traffic.
- The attack uses a known command-and-control tool to beacon from an affected host.
Which of the following techniques did the attacker most likely use?
A. Redirection
B. Custom BOF
C. EDR evasion
D. Steganography
Answer: (SHOW ANSWER)
The attacker used EDR evasion by tunneling command-and-control traffic over HTTPS to a non- malicious IP. This hides the beaconing within legitimate encrypted traffic, bypassing detection even with deep packet inspection in place.

NEW QUESTION: 261
Which of the following is the reason why security engineers often cannot upgrade the security of embedded facility automation systems?
A. They are constrained by available compute.
B. They lack x86-64 processors.
C. They lack EEPROM.
D. They are not logic-bearing devices.
Answer: (SHOW ANSWER)
Embedded facility automation systems, such as those used for controlling HVAC, lighting, or security, are often constrained by limited computational resources. These systems are designed to be low-cost and energy-efficient, which means they typically have limited processing power, memory, and storage capacity. As a result, security engineers often face difficulties when trying to upgrade or implement additional security measures, such as more sophisticated encryption or security patches, because these systems lack the necessary compute resources to handle such upgrades.

NEW QUESTION: 262
While investigating a security event an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware. Which of the following is the next step the analyst should take after reporting the incident to the management team?
A. Pay the ransom within 48 hours
B. Isolate the servers to prevent the spread
C. Notify law enforcement
D. Request that the affected servers be restored immediately
Answer: (SHOW ANSWER)

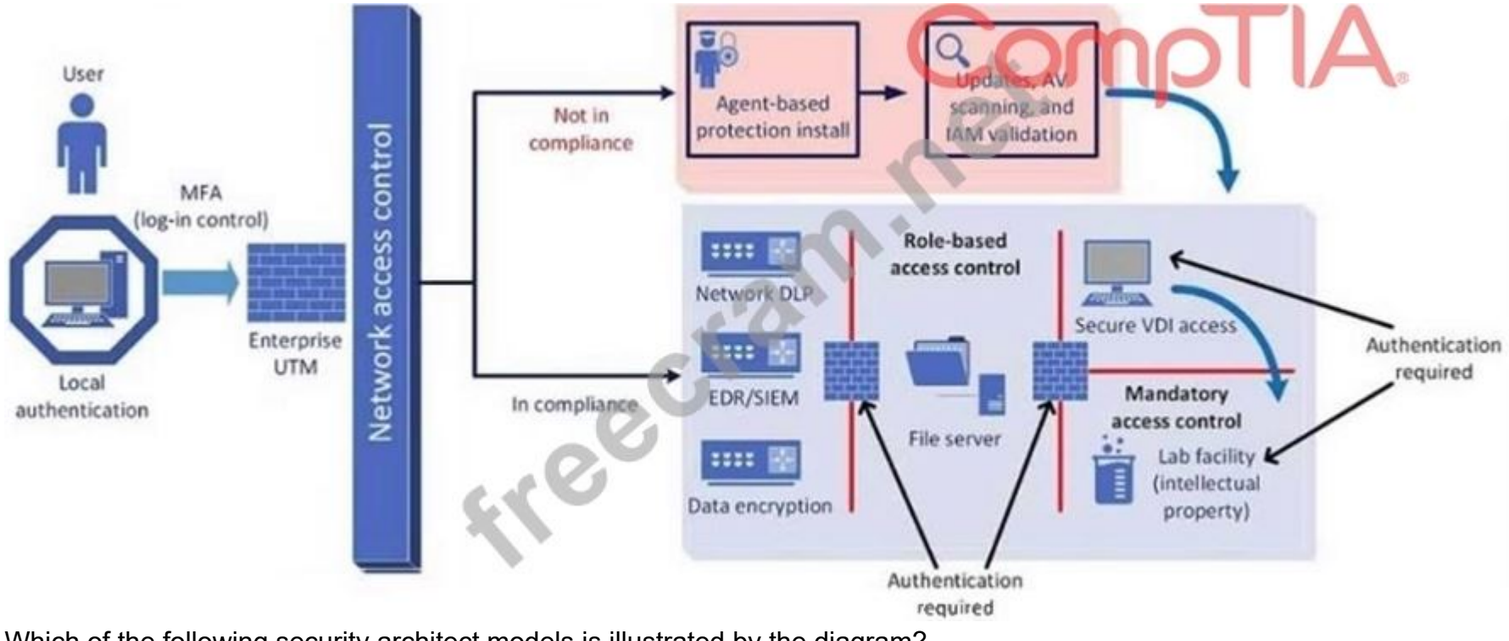
NEW QUESTION: 263
Which of the following describes how a risk assessment is performed when an organization has a critical vendor that provides multiple products?
A. At the individual product level
B. Through the selection of a random product
C. Using a third-party audit report
D. By choosing a major product
Answer: (SHOW ANSWER)
A risk assessment should be performed at the individual product level when an organization has a critical vendor providing multiple products. This approach ensures that each product is evaluated for its specific risks, vulnerabilities, and impact on the organization. By assessing each product separately, the organization can identify and prioritize the risks associated with each product rather than making assumptions based on a single product or a general overview.

NEW QUESTION: 264
A systems administrator is working with clients to verify email-based services are performing properly. The administrator wants to have the email server digitally sign outbound emails using the organization's private key. Which of the following should the systems administrator configure?
A. SPF
B. DKIM
C. DMARC

D. TLS
Answer: (SHOW ANSWER)
DKIM (DomainKeys Identified Mail) uses a private key to digitally sign outbound emails, allowing recipients to verify the authenticity of the sender using the corresponding public key published in DNS.

NEW QUESTION: 265
A company's headquarters is in an area with a high rate of severe weather. An engineer must update the enterprise architecture to meet the following requirements:
- Critical services must remain functional without downtime.
- Backups of data and configurations must be securely implemented.
- Company workstations must be highly available and remotely reachable.
Which of the following solutions is the best way to meet these requirements?
A. Transition physical resources to virtual resources with standby redundant servers, and install a high capacity, diesel-powered backup generator.
B. Open and staff a second data center at least 100 miles away with robust, network-attached storage, and include DAR encryption for offline backups of customer data to enable rapid recovery.
C. Lease a cross-country workspace to support as-needed relocation of staff and equipment, and continuously back up and test VM images with automatic recovery orchestration.
D. Implement a geographically distributed allocation of physical resources and VDI with continuous replication connected via site-to-site and load-balanced IPSec VPNs.
Answer: (SHOW ANSWER)
A geographically distributed deployment of physical resources provides site resilience against severe weather by preventing a single location from becoming a point of failure. VDI makes company workstations highly available and remotely reachable, allowing users to access their environments from alternate locations without depending on local office hardware. Continuous replication supports service continuity and secure recovery of data and configurations, while site- to-site and load-balanced IPSec VPNs maintain secure connectivity between locations and users with minimal disruption.

NEW QUESTION: 266
A company plans to implement a research facility with intellectual property data that should be protected. The following is the security diagram proposed by the security architect:



Which of the following security architect models is illustrated by the diagram?
A. Identity and access management model
B. Agent based security model

C. Perimeter protection security model
D. Zero Trust security model
Answer: (SHOW ANSWER)
The security diagram proposed by the security architect depicts a Zero Trust security model. Zero Trust is a security framework that assumes all entities, both inside and outside the network, cannot be trusted and must be verified before gaining access to resources.
Key Characteristics of Zero Trust in the Diagram:
Role-based Access Control: Ensures that users have access only to the resources necessary for their role.
Mandatory Access Control: Additional layer of security requiring authentication for access to sensitive areas.
Network Access Control: Ensures that devices meet security standards before accessing the network.
Multi-factor Authentication (MFA): Enhances security by requiring multiple forms of verification.
This model aligns with the Zero Trust principles of never trusting and always verifying access requests, regardless of their origin.

NEW QUESTION: 267
While performing threat-hunting functions, an analyst is using the Diamond Model of Intrusion Analysis. The analyst identifies the likely adversary, the infrastructure involved, and the target.
Which of the following must the threat hunter document to use the model effectively?
A. Knowledge
B. Capabilities
C. Phase
D. Methodologies
Answer: B (LEAVE A REPLY)
The Diamond Model of Intrusion Analysis requires the documentation of capabilities, as this refers to the adversary's tools, techniques, and procedures (TTPs) used during the attack.
Identifying and documenting the adversary's capabilities is essential for effective threat-hunting, as it helps understand how the adversary operates and can guide the detection of similar future attacks.

Valid CAS-005 Dumps shared by ExamDiscuss.com for Helping Passing CAS-005 Exam! ExamDiscuss.com now offer the **newest CAS-005 exam dumps**, the ExamDiscuss.com CAS-005 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com CAS-005 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/CAS-005/premium/ (**604** Q&As Dumps, **35%OFF Special Discount Code: freecram**)