CompTIA.CAS-005.v2026-06-01.q223

Exam Code:	CAS-005
Exam Name:	CompTIA SecurityX Certification Exam
Certification Provider:	CompTIA
Free Question Number:	223
Version:	v2026-06-01
# of views:	107
# of Questions views:	2434
https://www.freecram.net/torrent/CompTIA.CAS-005.v2026-06-01.q223.html	

NEW QUESTION: 1
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: 2
A malware analyst must examine the following partial file sample recovered from a Linux workstation:

```
[...]
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63
61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00
50 45 00 00 4c 01 03 00 34 6d be 66 00 00 00 00 00 00 00 00 e0 00 0f 03 0b 01 05 00 00 70 00 00 00 10 00 00 00 d0 00 00 70 4c 01 00 00 e0
00 00 00 50 01 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 01 00 00 02 00 00 00 00 00 00
03 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00
[...]
9f cf dd 11 42 e4 25 01 00 5a 6c 00 00 00 e8 00 00 26 01 00 4e fd ff ff ff 83 ec 1c 53 56 57 e8 01 00 01 cc 8b 3d b8 21 41 00 8d 4c 24 0c
33 db 8b f0 8b 44 24 2c 51 b6 b5 df be 1a 68 00 14 40 13 54 24 20 53 c7 10 19 00 00 f7 ed bf fb 89 5c 24 28 03 2c 52 89 46 0c ff d7 3b c3
06 10 75 39 53 00 ef ba b7 ed 6a 0a 2d 01 41 ff 15 b4 47 50 53 89 bc 83 c4 73 97 5d fb 0c 50 68 54 e0 42 0d
[...]
```

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: 3
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: 4
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

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: 5
An organization is researching the automation capabilities for systems within an OT network. A security analyst wants to assist with creating secure coding practices and would like to learn about the programming languages used on the PLCs. Which of the following programming languages is the most relevant for PLCs?
A. Ladder logic
B. Rust
C. C
D. Python
E. Java

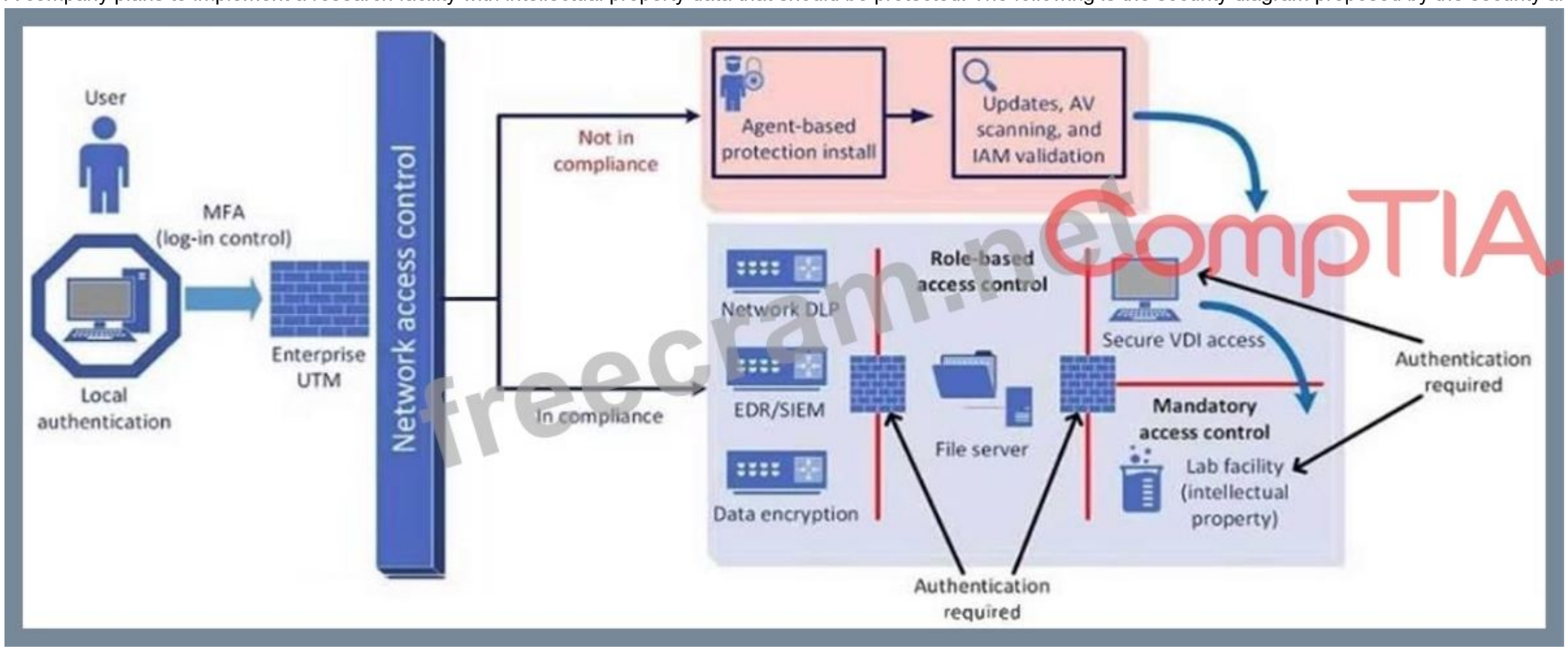
Answer: (SHOW ANSWER)

Programmable Logic Controllers (PLCs) in Operational Technology (OT) environments commonly use Ladder Logic, a graphical programming language resembling electrical relay logic diagrams.

It's the most relevant for PLCs due to its widespread use in industrial automation.

NEW QUESTION: 6

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: 7
A company wants to implement a three-tier approach to separate the web, database, and application servers. A security administrator must harden the environment. Which of the following is the best solution?
A. Deploying a VPN to prevent remote locations from accessing server VLANs
B. Configuring a SASE solution to restrict users to server communication
C. Implementing microsegmentation on the server VLANs
D. installing a firewall and making it the network core
Answer: (SHOW ANSWER)
Microsegmentation is the best solution to separate and harden the environment. It involves creating granular security controls within the network to restrict communication between servers in different tiers (web, database, application) while allowing necessary communication. This limits the attack surface and improves security by preventing lateral movement within the network.

NEW QUESTION: 8
Which of the following best explains why AI output could be inaccurate?
A. Model poisoning
B. Social engineering
C. Output handling
D. Prompt injections
Answer: (SHOW ANSWER)
Model poisoning involves deliberately feeding malicious or biased data into an AI model during training, leading to inaccurate or manipulated outputs. It directly affects the model's behavior and reliability.

NEW QUESTION: 9
While reviewing recent incident reports a security officer discovers that several employees were contacted by the same individual who impersonated a recruiter. Which of the following best describes this type of correlation?
A. Spear-phishing campaign
B. Threat modeling
C. Red team assessment
D. Attack pattern analysis
Answer: (SHOW ANSWER)
Attack pattern analysis involves identifying recurring techniques or behaviors used by threat actors - such as impersonating a recruiter - to correlate incidents and uncover broader campaigns. The security officer is recognizing a consistent method across multiple reports, which defines this as attack pattern analysis.

NEW QUESTION: 10

An organization must provide access to its internal system data. The organization requires that this access complies with the following:
- Access must be automated.
- Data confidentiality must be preserved.
- Access must be authenticated.
- Data must be preprocessed before it is retrieved.

Which of the following actions should the organization take to meet these requirements?

A. Configure a reverse proxy to protect the data.

B. Implement an on-demand VPN connection.

C. Deploy an API gateway protected with access tokens.

D. Continually publish all relevant data to a CDN.

Answer: (SHOW ANSWER)

An API gateway protected with access tokens enables automated and authenticated access while preserving confidentiality. It also supports preprocessing and transformation of data before delivery, fulfilling all the organization's requirements.

NEW QUESTION: 11

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

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: 12

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

www.mycompany.org

www.mycompany.com
campus.mycompany.com
wiki.mycompany.org
The solution must save costs and be able to protect all websites. Users should be able to notify the cloud security engineer of any on-path attacks. Which of the following is the best solution?
A. Purchase one SAN certificate.
B. Implement self-signed certificates.
C. Purchase one certificate for each website.
D. Purchase one wildcard certificate.
Answer: (SHOW ANSWER)
A Subject Alternative Name (SAN) certificate lets you bundle multiple distinct hostnames, including across different domains, in a single TLS certificate. With one SAN cert you can list:
www.mycompany.org
wiki.mycompany.org
www.mycompany.com
campus.mycompany.com
This keeps costs down (versus buying four separate certs) and avoids the domain restriction of a single wildcard, while still providing proper end-to-end HTTPS protection so that any interception triggers a browser warning and alerts users to on-path attacks.

NEW QUESTION: 13
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: 14
The principal security analyst for a global manufacturer is investigating a security incident related to abnormal behavior in the ICS network. A controller was restarted as part of the troubleshooting process, and the following issue was identified when the controller was restarted:
SECURE BOOT FAILED:
FIRMWARE MISMATCH EXPECTED UXFDC479 ACTUAL 0x79F31B
During the investigation, this modified firmware version was identified on several other controllers at the site. The official vendor firmware versions do not have this checksum. Which of the following stages of the MITRE ATT&CK framework for ICS includes this technique?
A. Evasion
B. Persistence
C. Collection
D. Lateral movement
Answer: (SHOW ANSWER)
The technique described in the scenario, where modified firmware with an altered checksum is found on multiple controllers, aligns with the Persistence stage of the MITRE ATT&CK framework for ICS (Industrial Control Systems). Persistence involves ensuring that an adversary can maintain access to a system even after reboots, credential changes, or other defensive measures. The manipulation of firmware is a classic method used by attackers to ensure that they can maintain control over a system or device across reboots or resets, which is a key characteristic of the Persistence stage.

NEW QUESTION: 15
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: 16
A cloud security architect has been tasked with selecting the appropriate solution given the following:
- The solution must allow the lowest RTO possible.
- The solution must have the least shared responsibility possible.
- Patching should be a responsibility of the CSP.
Which of the following solutions can best fulfill the requirements?
A. PaaS
B. IaaS
C. Private
D. SaaS
Answer: (SHOW ANSWER)
Of the models listed, a Software-as-a-Service solution places nearly all infrastructure, platform, and application management, and thus patching, squarely on the cloud provider. That minimizes your shared-responsibility footprint and gives you the fastest possible recovery (lowest RTO) since failovers and restorations are handled entirely by the CSP.

NEW QUESTION: 17
A security analyst received a report that an internal web page is down after a company-wide update to the web browser. Given the following error message:
Your connection is not private.
Attackers might be trying to steal your information for www.
internalwebsite.company.com.
NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM
Which of the following is the best way to fix this issue?
A. Rewriting any legacy web functions
B. Disabling all deprecated ciphers
C. Blocking all non-essential pons
D. Discontinuing the use of self-signed certificates
Answer: (SHOW ANSWER)
The error NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM indicates the site's certificate uses a deprecated/weak signing algorithm (commonly SHA-1). Modern browsers reject these.
The practical fix is to replace the certificate with one signed using a modern algorithm (e.g., SHA-
256) by a trusted CA (internal PKI or public). Moving away from self-signed certs ensures a valid trust chain and modern signatures.

NEW QUESTION: 18
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: 19

A security officer is requiring all personnel working on a special project to obtain a security clearance requisite with the level of all information being accessed. Data on this network must be protected at the same level of each clearance holder. The need to know must be verified by the data owner. Which of the following should the security officer do to meet these requirements?

A. Create a rule to authorize personnel only from certain IPs to access the files.

B. Assign labels to the files and require formal access authorization.

C. Assign attributes to each file and allow authorized users to share the files.

D. Assign roles to users and authorize access to files based on the roles.

Answer: (SHOW ANSWER)

To meet the requirement of ensuring that data is protected at the clearance level of each personnel member and that access is based on the need to know, labeling the files according to their classification level is an effective method. Labels indicate the sensitivity of the data and ensure that only individuals with the appropriate clearance and need-to-know access are authorized to view or modify the files.

By requiring formal access authorization from the data owner, the security officer ensures that access is explicitly verified before any personnel can access data at a given classification level.

NEW QUESTION: 20

An IT department is currently working to implement an enterprise DLP solution. Due diligence and best practices must be followed in regard to mitigating risk. Which of the following ensures that authorized modifications are well planned and executed?

A. Risk management

B. Network management

C. Configuration management

D. Change management

Answer: (SHOW ANSWER)

Change management establishes a formal process for planning, approving, testing, scheduling, and documenting all authorized modifications. This ensures that deploying or updating the DLP solution follows controlled steps, reducing the risk of unplanned disruptions or misconfigurations.

NEW QUESTION: 21

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: (SHOW ANSWER)
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: 22
A security engineer needs to create multiple servers in a company's private cloud. The servers should have a virtual network infrastructure that supports connectivity, as well as security configurations applied using predefined templates. Which of the following is the best option for the security engineer to consider for the deployment?
A. Installing a container orchestration solution locally, configuring the infrastructure, and cloning the solution
B. Creating templates on the cloud provider marketplace and modeling the solution using those templates
C. Using Terraform to implement an infrastructure as code model with the existing private cloud solution
D. Integrating the cloud provider API to the CI/CD pipeline model used by the company
Answer: C (LEAVE A REPLY)
Using Terraform allows the security engineer to implement Infrastructure as Code, enabling consistent creation of servers, virtual networking, and security configurations from predefined templates within the private cloud. This ensures repeatability, scalability, and security compliance.

NEW QUESTION: 23
An analyst has prepared several possible solutions to a successful attack on the company. The solutions need to be implemented with the least amount of downtime. Which of the following should the analyst perform?
A. Implement all the solutions at once in a virtual lab and then run the attack simulation. Collect the metrics and then choose the best solution based on the metrics.
B. Implement every solution one at a time in a virtual lab, running a metric collection each time.
After the collection, run the attack simulation, roll back each solution, and then implement the next. Choose the best solution based on the best metrics.
C. Implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics.
D. Implement all the solutions at once in a virtual lab and then collect the metrics. After collection, run the attack simulation. Choose the best solution based on the best metrics.
Answer: (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: 24
A software engineer is creating a CI/CD pipeline to support the development of a web application.
The DevSecOps team is required to identify syntax errors. Which of the following is the most relevant to the DevSecOps team's task?
A. Static application security testing
B. Software composition analysis
C. Runtime application self-protection
D. Web application vulnerability scanning
Answer: (SHOW ANSWER)
Static Application Security Testing (SAST) analyzes source code, bytecode, or binaries without executing the program, making it highly relevant for identifying syntax errors during the development process. This approach is ideal for the DevSecOps team's task of identifying errors before deployment.

NEW QUESTION: 25
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?
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: 26
A security analyst reviews the following event timeline from an EDR solution:

Time	File name	File action	Action verdict
4:08 p.m.	hr-reporting.docx	File save	Allowed
4:09 p.m.	hr-reporting.docx	Scan initiated	Pending
4:10 p.m.	hr-reporting.docx	File execute	Allowed
4:16 p.m.	paychecks.xlsx	File save	Allowed
4:16 p.m.	paychecks.xlsx	File shared	Allowed
4:17 p.m.	hr-reporting.docx	Script launched	Allowed
4:19 p.m.	hr-reporting.docx	Scan complete	Malware found
4:20 p.m.	paychecks.xlsx	File edit	Allowed

Which of the following has most likely occurred and needs to be fixed?
A. The DLP has failed to block malicious exfiltration, and data tagging is not being utilized properly.
B. A NIDS bypass was utilized by a threat actor, and updates must be installed by the administrator.
C. A logic flaw has introduced a TOCTOU vulnerability and must be addressed by the vendor.
D. A potential insider threat is being investigated and will be addressed by the senior management team.
Answer: (SHOW ANSWER)
The event timeline shows that hr-reporting.docx was executed and launched a script before the malware scan completed and detected it as malicious. This indicates a TOCTOU (Time-of- Check to Time-of-Use) vulnerability - where the file was checked after it was already used. This logic flaw needs to be fixed by the vendor to ensure scans complete before allowing execution.

NEW QUESTION: 27
A company wants to perform threat modeling on an internally developed, business-critical application. The Chief Information Security Officer (CISO) is most concerned that the application should maintain 99.999% availability and authorized users should only be able to gain access to data they are explicitly authorized to view. Which of the following threat-modeling frameworks directly addresses the CISO's concerns about this system?

A. CAPEC
B. STRIDE
C. ATT&CK
D. TAXII
Answer: (SHOW ANSWER)
STRIDE is a threat-modeling framework that focuses on six key threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.
This directly addresses the CISO's concerns about ensuring high availability (99.999%) and restricting data access to only authorized users, making it the most suitable choice.

NEW QUESTION: 28
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: 29
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: 30
A security engineer wants to reduce the attack surface of a public-facing containerized application.
Which of the following will best reduce the application's privilege escalation attack surface?

A. Implementing the following commands in the Dockerfile:
RUN echo user:x:1000:1000:user:/home/user:/dev/null > /etc/passwd
B. Installing an EDR on the container's host, with reporting configured to log to a centralized SIEM, and implementing the following alerting rule:
IF PROCESS_USER==root ALERT_TYPE==critical
C. Designing a muiticontainer solution, with one set of containers that runs the mam application, and another set oi containers that perform automatic remediation by replacing compromised containers or disabling compromised accounts

D. Running the container in an isolated network and placing a load balancer in a public-facing network. Adding the following ACL to the load balancer:PERMIT HTTPS from 0.0.0.0/0 port 443

Answer: (SHOW ANSWER)

Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of privilege escalation attacks because even if an attacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access.

Implementing the following commands in the Dockerfile: This directly addresses the privilege escalation attack surface by ensuring the application does not run with elevated privileges.

NEW QUESTION: 31

A developer makes a small change to a resource allocation module on a popular social media website and causes a memory leak. During a peak utilization period, several web servers crash, causing the website to go offline. Which of the following testing techniques is the most efficient way to prevent this from reoccurring?

A. Load

B. Smoke

C. Regression

D. Canary

Answer: (SHOW ANSWER)

Load testing evaluates how a system performs under expected and peak utilization. It would have identified the memory leak during high traffic, preventing the web servers from crashing in production.

NEW QUESTION: 32

A security analyst reviews the following report:

	Location	Chassis manufacturer	OS	Application developer	Vendor
Product A	United States	Local company A	Debian 11	Unknown	Charlie Security Consulting
Product B	United States	Global company B	Red Hat Enterprise Linux	Developer B	BigBox Vulnerabilities

Which of the following assessments is the analyst performing?

A. System

B. Supply chain

C. Quantitative

D. Organizational

Answer: (SHOW ANSWER)
The analyst is reviewing information related to product origin, manufacturers, OS, developers, and vendors - key components of a supply chain assessment, which evaluates potential risks from third-party components and service providers.

NEW QUESTION: 33
During DAST scanning, applications are consistently reporting code defects in open-source libraries that were used to build web applications. Most of the code defects are from using libraries with known vulnerabilities. The code defects are causing product deployment delays.
Which of the following is the best way to uncover these issues earlier in the life cycle?
A. Directing application logs to the SIEM for continuous monitoring
B. Modifying the WAF polices to block against known vulnerabilities
C. Completing an IAST scan against the web application
D. Using a software dependency management solution
Answer: (SHOW ANSWER)
Using a software dependency management solution helps track and manage open-source libraries and their vulnerabilities. This solution can identify vulnerable libraries early in the development process, allowing developers to replace or patch them before deployment and reducing delays caused by code defects.

NEW QUESTION: 34
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: 35
Due to an infrastructure optimization plan, a company has moved from a unified architecture to a federated architecture divided by region. Long-term employees now have a better experience, but new employees are experiencing major performance issues when traveling between regions. The company is reviewing the following information:

Date and time	Region	Employee	System	Status
1/25/2024 8:00 a.m.	Americas	1	Building	Access granted
1/25/2024 8:05 a.m.	Americas	1	EMP1-LT	Log-in success
1/25/2024 4:55 p.m.	Americas	1	EMP1-LT	Log-out success
1/26/2024 9:00 a.m.	Europe	1	Building	Access granted
1/26/2024 9:15 a.m.	Europe	1	EMP1-LT	Log-in success
1/26/2024 4:55 p.m.	Europe	1	EMP1-LT	Log-out success

Date and time	Region	Employee	System	Status
1/25/2024 8:00 a.m.	Americas	2	Building	Access granted
1/25/2024 8:05 a.m.	Americas	2	EMP1-LT	Log-in success
1/25/2024 4:55 p.m.	Americas	2	EMP1-LT	Log-out success
1/26/2024 9:00 a.m.	Europe	2	Building	Access denied
1/26/2024 9:01 a.m.	Europe	2	Building	Access denied
1/26/2024 9:02 a.m.	Europe	2	Building	Access denied

Which of the following is the most effective action to remediate the issue?

A. Creating a new user entry in the affected region for the affected employee

B. Synchronizing all regions' user identities and ensuring ongoing synchronization

C. Restarting European region physical access control systems

D. Resyncing single sign-on application with connected security appliances

Answer: (SHOW ANSWER)

The performance issues for new employees traveling between regions are likely due to identity management inconsistencies in the federated architecture. Synchronizing user identities across regions ensures that user credentials are up-to-date and available in all regions, improving performance and access reliability when employees travel between regions.

NEW QUESTION: 36

An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

A. SASE

B. CMDB

C. SBoM

D. SLM

Answer: (SHOW ANSWER)

A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets.

NEW QUESTION: 37
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. Lightweight
D. Symmetric
Answer: (SHOW ANSWER)

NEW QUESTION: 38
A company recently experienced an incident in which an advanced threat actor was able to shim malicious code against the hardware stack of a domain controller. The forensic team cryptographically validated that both the underlying firmware of the box and the operating system had not been compromised. However, the attacker was able to exfiltrate information from the server using a steganographic technique within LDAP. Which of the following is the best way to reduce the risk of reoccurrence?
A. Enforcing allow lists for authorized network pons and protocols
B. Measuring and attesting to the entire boot chain
C. Rolling the cryptographic keys used for hardware security modules
D. Using code signing to verify the source of OS updates
Answer: A (LEAVE A REPLY)
Since the attacker used steganographic techniques within LDAP to exfiltrate data, the most effective way to reduce the risk of reoccurrence is to enforce allow lists for authorized network ports and protocols. This limits the ability of attackers to use unauthorized protocols or ports, which could help block hidden exfiltration methods like the one used in the incident.

NEW QUESTION: 39
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: 40
A systems administrator decides to take a programmatic approach in cataloging system resiliency to both new and existing attack patterns. Which of the following should the systems administrator use?

A. OWASP
B. ATT&CK
C. STRIDE
D. CAPEC
Answer: (SHOW ANSWER)
MITRE ATT&CK provides a programmatic framework of adversary tactics, techniques, and procedures. It enables cataloging system resiliency against known attack patterns, supporting structured testing and gap analysis.

NEW QUESTION: 41
A company was recently infected by malware. During the root cause analysis, the company determined that several users were installing their own applications. To prevent further compromises, the company has decided it will only allow authorized applications to run on its systems. Which of the following should the company implement?
A. Signing
B. Access control
C. HIPS
D. Permit listing
Answer: (SHOW ANSWER)
To prevent unauthorized applications from running, the company needs a mechanism to explicitly define and enforce which applications are allowed to execute. "Permit listing" (often referred to as
"whitelisting" in security contexts) is the most effective solution here. It involves creating a list of approved applications, and only those on the list are permitted to run, blocking all others by default. This directly addresses the root cause--users installing unapproved software--by restricting execution to only authorized programs.

NEW QUESTION: 42
A security engineer added a new server to the company email cluster. The server has a new external IP address associated with it. After a few days, the service desk started receiving complaints from users about their outgoing messages to customers being flagged as spam.
Which of the following records should the security engineer update to fix the issue? (Choose two.)
A. DMARC
B. PTR
C. MX
D. MIME
E. CNAME
F. SPF
Answer: (SHOW ANSWER)

NEW QUESTION: 43
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] = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
[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] }
```


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: 44

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: 45

A company currently uses manual processes to regularly address incidents occurring outside of working hours. Hiring or implementing a SOC is not an option because of budget limitations.

Which of the following solutions would most likely decrease the current risk?

A. Implement a NIPS integrated with the firewall, raising new rules to block any malicious access attempts coming from the external perimeter.

B. Improve logging capabilities, integrating those logs with the existing SIEM and creating better security dashboards.
C. Evaluate and implement new endpoint security tools, helping to prevent attack attempts.
D. Design proper runbooks and implement security orchestration and automation with integrated security tools.
Answer: (SHOW ANSWER)

NEW QUESTION: 46
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

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: 47
An organization would like to increase the effectiveness of its incident response process across its multiplatform environment. A security engineer needs to implement the improvements using the organization's existing incident response tools. Which of the following should the security engineer use?
A. Playbooks
B. Event collectors
C. Centralized logging
D. Endpoint detection

Answer: (SHOW ANSWER)
Playbooks standardize and automate incident response steps across a multiplatform environment using existing tools. This increases effectiveness and consistency in handling security incidents.

NEW QUESTION: 48
A security architect is onboarding a new EDR agent on servers that traditionally do not have internet access. In order for the agent to receive updates and report back to the management console, some changes must be made. Which of the following should the architect do to best accomplish this requirement? (Choose two.)
A. Create a firewall rule to only allow traffic from the subnet to the internet via a proxy.
B. Configure a proxy policy that blocks all traffic on port 443.
C. Configure a proxy policy that allows only fully qualified domain names needed to communicate to a portal.
D. Create a firewall rule to only allow traffic from the subnet to the internet via port 443.
E. Create a firewall rule to only allow traffic from the subnet to the internet to fully qualified names that are not identified as malicious by the firewall vendor.
F. Configure a proxy policy that blocks only lists of known-bad, fully qualified domain names.
Answer: (SHOW ANSWER)
Create a firewall rule to only allow traffic from the subnet to the internet via a proxy ensures that the servers can connect to the internet through a controlled channel, allowing the EDR agent to get updates and report back securely.
Configure a proxy policy that allows only fully qualified domain names needed to communicate to a portal ensures that the agent can reach only the necessary services for updates and reporting, minimizing exposure and enhancing security by limiting access to only trusted domains.

NEW QUESTION: 49
A central bank implements strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin. Which of the following best describes the cyberthreat to the bank?
A. Ability to obtain components during wartime
B. Fragility and other availability attacks
C. Physical Implants and tampering
D. Non-conformance to accepted manufacturing standards
Answer: (SHOW ANSWER)
The allow list for specific countries of origin as a risk mitigation indicates that the central bank is focused on preventing physical implants and tampering in hardware. This is a form of supply chain attack where malicious actors may insert malicious hardware components into devices, leading to potential compromises in security. By restricting the countries of origin, the bank is likely aiming to prevent such vulnerabilities.

NEW QUESTION: 50
A pharmaceutical lab hired a consultant to identify potential risks associated with Building 2, a new facility that is under construction. The consultant received the IT project plan, which includes the following VLAN design:

Name	VLAN	Subnet	Function	Regulated network?
Building 1 servers	111	10.1.11.0/25	Servers	No
Building 1 users	100	10.1.0.0/23	User Wi-Fi and LAN	No
Building 1 HVAC	105	10.1.5.0/27	HVAC controls	No
Building 1 lab	170	10.1.70.0/24	Lab	Yes
Building 1 QC	180	10.1.80.0/24	Lab	Yes
Building 2 servers	211	10.2.11.0/25	Servers	No
Building 2 users	200	10.2.0.0/22	Users and lab	Yes
Building 2 HVAC	215	10.2.15.0/27	HVAC controls	No

Which of the following TTPs should the consultant recommend be addressed first?

A. Zone traversal

B. Unauthorized execution

C. Privilege escalation

D. Lateral movement

Answer: (SHOW ANSWER)

The presence of both regulated (users and lab) and non-regulated (servers, HVAC) networks in Building 2 increases the risk of zone traversal, where traffic or attacks could cross from less secure to more secure network zones. Addressing zone traversal first helps protect regulated environments from unauthorized access originating in less protected VLANs.

NEW QUESTION: 51

An external threat actor attacks public infrastructure providers. In response to the attack and during follow-up activities, various providers share information obtained during response efforts.

After the attack, energy sector companies share their status and response data:

Company	SIEM	UEBA	DLP	ISAC member	TIP integration	Time to detect	Time to respond
1	Yes	No	Yes	Yes	Yes	10 minutes	20 minutes
2	Yes	Yes	Yes	Yes	No	20 minutes	40 minutes
3	Yes	Yes	No	No	Yes	12 minutes	24 minutes

Which of the following is the most important issue to address to defend against future attacks?

A. Failure to implement a UEBA system

B. Failure to implement a DLP system

C. Failure to join the industry ISAC

D. Failure to integrate with the TIP

Answer: D (LEAVE A REPLY)

Company 2, which has SIEM, UEBA, DLP, and ISAC membership-still shows the slowest detection (20 min) and response (40 min) times. Its only gap is lack of integration with a Threat Intelligence Platform (TIP). Automating the intake, normalization, and enrichment of shared indicators via a TIP lets the SIEM/UEBA/DLP correlate new threat data in real time, cutting both mean time to detect and mean time to respond.

NEW QUESTION: 52
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.

NEW QUESTION: 53
A company implemented a NIDS and a NIPS on the most critical environments. Since this implementation, the company has been experiencing network connectivity issues. Which of the following should the security architect recommend for a new NIDS/NIPS implementation?
A. Implementing the NIDS with a port mirror in the core switch and the NIPS in the main firewall
B. Implementing the NIDS and the NIPS together with the main firewall
C. Implementing a NIDS without a NIPS to increase the detection capability
D. Implementing the NIDS in the bastion host and the NIPS in the branch network router
Answer: (SHOW ANSWER)
Placing the NIDS on a port mirror allows it to passively monitor traffic without affecting performance, while deploying the NIPS at the firewall ensures it can actively block malicious traffic at a controlled chokepoint. This architecture balances detection, prevention, and network stability.

NEW QUESTION: 54
During an adversarial simulation exercise, an external team was able to gain access to sensitive information and systems without the organization detecting this activity. Which of the following mitigation strategies should the organization use to best resolve the findings?
A. Configuring a honeypot for adversary characterization
B. Leveraging simulators for attackers
C. Setting up a honey network for attackers
D. Utilizing decoy accounts and documents
Answer: (SHOW ANSWER)
Utilizing decoy accounts and documents (often referred to as honeytokens) is the best mitigation strategy in this scenario. Decoy accounts and documents are designed to look like legitimate, sensitive data or systems, but they are actually trapping. If an adversary accesses these decoys, it can trigger alerts and give the organization an early warning of the intrusion. This helps the organization detect unauthorized access more quickly and provides the opportunity to respond before actual damage is done.

NEW QUESTION: 55
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).
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: 56
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: 57
A customer requires secure communication of subscribed web services at all times, but the company currently signs its own certificate requests to an internal CA.
Which of the following approaches will best meet the customer's requirements?
A. Generate a CSR to the local CA for email encryption.
B. Submit a CSR for a wildcard certificate to a public CA.
C. Request a software signing certificate from a public CA.
D. Process a CSR for a server authentication certificate.
Answer: (SHOW ANSWER)
Server authentication certificates are used to secure web communication (e.g., HTTPS).
Submitting a CSR (Certificate Signing Request) for a server authentication certificate ensures the web services can securely establish encrypted communication. Other options, such as email encryption or software signing, do not apply in this scenario.

NEW QUESTION: 58
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: 59
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: 60
During a security review for the CI/CD process, a security engineer discovers the following information in a testing repository from the company:

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'floydtest_db');
/** MySQL database username */
define('DB_USER', 'root');
/** MySQL database password */
define('DB_PASSWORD', 'QW5vdGhlckJpbnRoZVdhbGwyMDEy');
/** MySQL hostname */
define('DB_HOST', 'localhost');
/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
/**#@+
* Authentication Unique Keys and Salts.
```


Which of the following options is the best countermeasure to prevent this issue in the future?

A. Performing an application penetration test over the testing environment before moving to production

B. Changing the repository technology to avoid inclusion of confidential information

C. Automating the upload process of code to the repository and improving the software development life cycle

D. Using a secrets management platform to share and manage confidential information

Answer: (SHOW ANSWER)

Using a secrets management platform ensures sensitive information like database credentials is stored securely and not hardcoded in code repositories, preventing accidental exposure during the CI/CD process.

NEW QUESTION: 61

A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients' charts. The hospital wants to ensure that if a tablet is identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within seconds. The tablets are configured as follows to meet hospital policy:

- Full disk encryption is enabled.
- "Always On" corporate VPN is enabled.
- eFuse-backed keystore is enabled/ready.
- Wi-Fi 6 is configured with SAE.
- Location services is disabled.
- Application allow list is unconfigured.

Assuming the hospital policy cannot be changed, which of the following is the best way to meet the hospital's objective?

A. Revoke the user VPN and Wi-Fi certificates

B. Cryptographically erase FDE volumes

C. Issue new MFA credentials to all users

D. Configure the application allow list

Answer: (SHOW ANSWER)

Cryptographically erasing FDE (Full Disk Encryption) volumes is the most effective way to mitigate data loss within seconds. It renders the encrypted data inaccessible by destroying the encryption key, which can be done instantly and remotely, meeting the hospital's objective without requiring changes to existing policy.

NEW QUESTION: 62
A water treatment plant uses specialized systems to control the balance of chemicals prior to adding them to the public water supply. The treatment plant has already isolated the system from both the internet and the company network. Which of the following additional controls is the best way to reduce the risk of a successful attack?
A. Storing the chemicals behind locked doors
B. Maintaining calibration of the chemical sensor system
C. Developing insider threat training
D. Implementing two-person control procedures
Answer: (SHOW ANSWER)

NEW QUESTION: 63
A security engineer performed a code scan that resulted in many false positives. The security engineer must find a solution that improves the quality of scanning results before application deployment. Which of the following is the best solution?
A. Limiting the tool to a specific coding language and tuning the rule set
B. Configuring branch protection rules and dependency checks
C. Using an application vulnerability scanner to identify coding flaws in production
D. Performing updates on code libraries before code development
Answer: (SHOW ANSWER)
To improve the quality of code scanning results and reduce false positives, the best solution is to limit the tool to a specific coding language and fine-tune the rule set. By configuring the code scanning tool to focus on the specific language used in the application, the tool can more accurately identify relevant issues and reduce the number of false positives. Additionally, tuning the rule set ensures that the tool's checks are appropriate for the application's context, further improving the accuracy of the scan results.

NEW QUESTION: 64
A security configure is building a solution to disable weak CBC configuration for remote access connections lo Linux systems. Which of the following should the security engineer modify?
A. The /etc/openssl.conffile, updating the virtual site parameter
B. The /etc/nsswitch.conf file, updating the name server
C. The /etc/hostsfile, updating the IP parameter
D. The /etc/sshd/ssh_configfile, updating the ciphers
Answer: (SHOW ANSWER)
The sshd_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed. By editing the
/etc/ssh/sshd_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the SSH server does not use insecure encryption methods.

NEW QUESTION: 65

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. APIs
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: 66
A company acquires a location with a large infrastructure of legacy devices. Because of the hardware's age and the legacy software's limitations, the OS cannot be upgraded, and the machines cannot be virtualized. These machines are not publicly facing, but they do have internet access. The following controls are currently in place:
- EDR
- Anti-malware
- Logging and monitoring
- Host-based firewall
- Proxied internet access
A security architect needs to supplement the existing control strategy with one that restricts unauthorized software. Which of the following controls should the architect recommend to best supplement the existing environment?
A. SIEM
B. Isolation
C. Conditional access
D. Application control
Answer: (SHOW ANSWER)
Application control restricts which software can run on a system, preventing unauthorized or malicious programs from executing. This is the most effective way to supplement existing controls for legacy systems that cannot be patched or virtualized.

NEW QUESTION: 67
Embedded malware has been discovered in a popular PDF reader application and is currently being exploited in the wild. Because the supply chain was compromised, this malware is present in versions 10.0 through 10.3 of the software's official versions. The malware is not present in version 10.4. Since the details around this malware are still emerging, the Chief Information Security Officer has asked the senior security analyst to collaborate with the IT asset inventory manager to find instances of the installed software in order to begin response activities. The asset inventory manager has asked an analyst to provide a regular expression that will identify the affected versions. The software installation entries are formatted as follows:
Reader 10.0
Reader 10.1
Reader 10.2
Reader 10.3
Reader 10.4

Which of the following regular expression entries will accurately identify all the affected versions?

A. Reader(*)[1][0].[0-4]:

B. Reader[1][0]X.[0-3]

C. Reader( )[1][0].[0-3]:

D. Reader( )[1][0] X.[1-3]:

Answer: (SHOW ANSWER)

This regex is valid and matches "Reader 10.0", "Reader 10.1", "Reader 10.2", and "Reader 10.3" while excluding "Reader 10.4".

Breakdown:

Reader: Matches the text "Reader".

[1][0]: Matches "10" as a combination of two characters.

\.: Matches the literal period.

[0-3]: Matches any single digit between 0 and 3.

NEW QUESTION: 68

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: 69

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. Cipher substitution attack

B. Pass- the-hash attack

C. Side-channel analysis

D. Supply chain attack

E. On-path attack

Answer: (SHOW ANSWER)

NEW QUESTION: 70

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: (SHOW ANSWER)
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: 71
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 prevent attempts to downgrade the protocol to legacy 3G
B. To defend from carrier OTA attack vectors
C. To filter directed electromagnetic interference
D. To block malicious radio connections
E. To protect against SIM hijack vulnerabilities
Answer: (SHOW ANSWER)

NEW QUESTION: 72
An organization handles sensitive information that must be displayed on call center technicians' screens to verify the identities of remote callers. The technicians use three randomly selected fields of information to complete the identity verification process. Some of the fields contain PII that are unique identifiers for the remote callers. Which of the following should be implemented to identify remote callers while also reducing the risk that technicians could improperly use the identification information?
A. Data masking
B. Encryption
C. Tokenization
D. Scrubbing
E. Substitution
Answer: (SHOW ANSWER)
Data masking allows call center technicians to view only the portions of sensitive fields necessary for identity verification (for example, showing the last four digits of an account number) while obscuring the rest. This approach strikes the balance between giving technicians enough information to confirm a caller's identity and preventing them from seeing or misusing the full PII.

NEW QUESTION: 73
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: (SHOW ANSWER)
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: 74
A company is developing a new service product offering that will involve the Security Officer (CISO) researching the relevant compliance regulations. Which of the following best describes the CISO's action?
A. Data retention
B. Data classification
C. Due diligence
D. Reference framework
Answer: (SHOW ANSWER)
Due diligence involves investigating and verifying processes, regulations, or environments to ensure compliance with laws and standards.

NEW QUESTION: 75
A company that relies on an COL system must keep it operating until a new solution is available.
Which of the following is the most secure way to meet this goal?
A. Isolating the system and enforcing firewall rules to allow access to only required endpoints
B. Enforcing strong credentials and improving monitoring capabilities
C. Restricting system access to perform necessary maintenance by the IT team
D. Placing the system in a screened subnet and blocking access from internal resources
Answer: (SHOW ANSWER)
To ensure the most secure way of keeping a legacy system (COL) operating until a new solution is available, isolating the system and enforcing strict firewall rules is the best approach. This method minimizes the attack surface by restricting access to only the necessary endpoints, thereby reducing the risk of unauthorized access and potential security breaches. Isolating the system ensures that it is not exposed to the broader network, while firewall rules control the traffic that can reach the system, providing a secure environment until a replacement is implemented.

NEW QUESTION: 76
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: 77

An organization has noticed an increase in phishing campaigns utilizing typosquatting. A security analyst needs to enrich the data for commonly used domains against the domains used in phishing campaigns. The analyst uses a log forwarder to forward network logs to the SIEM.

Which of the following would allow the security analyst to perform this analysis?

A. Use a cron job to regularly update and compare domains.
B. Create a parser that matches domains.
C. Develop a query that filters out all matching domain names.
D. Implement a dashboard on the SIEM that shows the percentage of traffic by domain.

Answer: (SHOW ANSWER)

To enrich the data for analysis, the security analyst needs to compare the legitimate domains against those used in phishing campaigns. Creating a parser that matches domains allows the SIEM to automatically identify and analyze the domains in the logs, helping detect typosquatting and other malicious domain usage. This method allows for efficient and automated processing of log data to identify potential threats.

NEW QUESTION: 78

A security engineer must integrate device attestation into user authentication and authorization workflows for mobile devices. Which of the following best meets the requirements?

A. Enforcing a security boundary for all devices outside the perimeter network
B. Enabling multifactor authentication using biometrics on access attempts
C. Implementing single sign-on to centralize access control enforcement
D. Configuring device profiling for patch level and jailbreak status

Answer: (SHOW ANSWER)

Configuring device profiling for patch level and jailbreak status ensures that the mobile device is compliant with security requirements before granting access. Device attestation checks the integrity of the device (such as whether it is jailbroken or up to date with security patches) to ensure that only trusted devices are allowed to authenticate and access resources. This solution directly addresses the requirement to integrate device attestation into user authentication workflows.

NEW QUESTION: 79
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: D (LEAVE A REPLY)
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: 80
A user tried to access a web page at http://10.1.1.1. Previously the web page did not require authentication, and now the browser is prompting for credentials. Which of the following actions would best prevent the issue from reoccurring and reduce the likelihood of credential exposure?

A. Implementing 802.1x EAP-TTLS on access points to reduce the risk of evil twins
B. Transitioning internal services to use DNS security
C. Modifying web server configuration and utilizing X509 certificates for authentication
D. Installing new rules for the IDS to detect impersonation attacks
Answer: (SHOW ANSWER)
The change from no authentication to requiring credentials suggests a shift in security posture for the web service. Using X.509 certificates for authentication provides a secure, certificate-based authentication method that can eliminate reliance on passwords and reduce the risk of credential exposure. This approach ensures encrypted and authenticated connections, preventing unauthorized access in the future.

NEW QUESTION: 81
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: (SHOW ANSWER)
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: 82
An analyst reviews a SIEM and generates the following report:

Host	Rule	Offense trigger
VM002	Network connection	TCP connection generated to web.corp.local
HOST002	Network connection	Web navigation to comptia.org
HOST002	File download	File download from web browser from web.corp.local
VM002	Network connection	Web navigation to web.corp.local
HOST002	Network connection	Web navigation to comptia.org/files
HOST002	Log-in activity	Log-in successful after two attempts

Only HOST002 is authorized for internet traffic. Which of the following statements is accurate?

A. The VM002 host is misconfigured and needs to be revised by the network team.

B. The HOST002 host is under attack, and a security incident should be declared.

C. The SIEM platform is reporting multiple false positives on the alerts.

D. The network connection activity is unusual, and a network infection is highly possible.

Answer: (SHOW ANSWER)

The activity seen aligns with authorized/expected behavior (HOST002 going external, VM002 staying internal). The "offenses" generated are not actual threats.

NEW QUESTION: 83

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

A. The client can seamlessly move data.

B. The vendor can change product offerings.

C. The client receives a sufficient level of service.

D. The client experiences decreased quality of service.

E. The client can leverage a multicloud approach.

F. The client experiences increased interoperability.

Answer: B,D (LEAVE A REPLY)

Vendor lock-in occurs when a client is overly dependent on a vendor, limiting flexibility. Risks include:

Option B: Vendors changing offerings (e.g., features, pricing) can disrupt the client, a key lock-in risk.

Option D: Decreased quality of service may result from reliance on a single vendor without alternatives.

NEW QUESTION: 84

A security analyst discovers a compromised internal server and finds that the attack vector was an application. When extracting a memory dump with the application process content, the analyst observes the following:

```
.....b4542/rgr...../x43/x64/x32/f3/x6b/x7a/x43/x64/x32/f3/x6b/x7a/x43/x64
/x32/f3/x6b/x7a/x43/x64/x32/f3/x6b/x7a/x43/x64/x32/f3/x6b/x7a/x90/x90/x90
/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x90/x76/x09/x67/xf5.....443.%43242
343/ge/452523/fgfdhgdh....gre
```

Which of the following solutions should the analyst recommend to best address this issue and avoid reoccurrence?

A. Implement address space layout randomization and canary stacks.

B. Reduce the buffer size to allow for less stored data.

C. Improve character filtering and input validation for user inputs.

D. Allow only the use of digitally signed and validated libraries.

Answer: (SHOW ANSWER)

The memory dump shows repeated /x90 (NOP sled), which is indicative of a buffer overflow exploit. Implementing address space layout randomization (ASLR) and stack canaries is the best defense, as they prevent attackers from reliably predicting memory addresses and detecting stack-based buffer overflows, thereby mitigating this type of attack.

NEW QUESTION: 85

A company is migrating from a Windows Server to Linux-based servers. A security engineer must deploy a configuration management solution that maintains security software across all the Linux servers. Which of the following configuration file snippets is the most appropriate to use?

A.

```
---
- name: deployment
  hosts: linux_servers
  remote_user: root

  tasks:
  - name: Install security software
    ansible.builtin.apt:
```

B.

```
<xml>

<hosts>linux_servers</hosts>
<os_type>Linux_3.1</os_type>
<SELinux>true</SELinux>
<source>com.canonical.io</source>
```

C.

```
{"name":"deployment",
  "hosts":"linux_servers,"
  "remote_user":"Administrator,"
}
{"tasks":"name":"Install security software",
    "com.microsoft.store.latest"
}
```

D.

```
{"task":"install",
 "hosts": "linux_servers"
 "remote_user": "root"
 "se_linux":"false"
 "application": "AppX"
```

Answer: (SHOW ANSWER)

Chosen option has YAML syntax for an Ansible playbook, which is the industry-standard configuration management tool for automating tasks on Linux servers. It is specifically designed for Linux environments and supports package installation and security software deployment at scale.

NEW QUESTION: 86

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: 87
A security team is creating tickets to track the progress of remediation. Which of the following is used to specify the due dates for high- and critical-priority findings?
A. MSA
B. SLA
C. ISA
D. MOU
Answer: (SHOW ANSWER)
A Service Level Agreement (SLA) defines the required response and resolution times (i.e., due dates) for different severity levels, such as high- and critical-priority findings. By embedding these timelines in the SLA, the security team and stakeholders share a clear expectation for how quickly each class of issue must be remediated.

NEW QUESTION: 88
During a recent security event, access from the non-production environment to the production environment enabled unauthorized users to:
- Install unapproved software
- Make unplanned configuration changes
During the investigation, the following findings were identified:
- Several new users were added in bulk by the IAM team
- Additional firewalls and routers were recently added
- Vulnerability assessments have been disabled for more than 30 days
- The application allow list has not been modified in two weeks
- Logs were unavailable for various types of traffic
- Endpoints have not been patched in over ten days
Which of the following actions would most likely need to be taken to ensure proper monitoring?
(Choose two.)
A. Disable bulk user creations by the IAM team
B. Extend log retention for all security and network devices to 180 days for all traffic
C. Review the application allow list daily
D. Routinely update all endpoints and network devices as soon as new patches/hot fixes are available
E. Ensure all network and security devices are sending relevant data to the SIEM
F. Configure firewall rules to only allow production-to-non-production traffic
Answer: (SHOW ANSWER)
Extend log retention for all security and network devices to 180 days for all traffic The incident investigation was hampered because "logs were unavailable for various types of traffic," which is a direct monitoring/forensics gap. Longer and more comprehensive retention is needed so security teams can reconstruct events and spot suspicious cross-environment access.

Ensure all network and security devices are sending relevant data to the SIEM Proper monitoring requires centralized, correlated visibility; without all firewalls, routers, and other security tools feeding events to the SIEM, lateral movement from non-prod to prod can go undetected. Centralized logging from "all services and infrastructure components" is a core monitoring best practice.

NEW QUESTION: 89

A company reduced its staff 60 days ago, and applications are now starting to fail. The security analyst is investigating to determine if there is malicious intent for the application failures. The security analyst reviews the following logs:

```
Mar 5 22:09:50 akj3 sshd[21502]: Success login for user01 from 192.168.2.5
Mar 5 22:10:00 akj3 sshd[21502]: Failed login for user10 from 192.168.2.5
Mar 5 22:10:40 akj3 sshd[21502]: Success login for user07 from 192.168.2.58
Mar 5 22:11:00 akj3 sshd[21502]: Failed login for user10 from 192.168.2.5
Mar 5 22:12:00 akj3 sshd[21502]: Failed login for user10 from 192.168.2.5
Mar 5 22:12:30 akj3 sshd[21502]: Success login for user03 from 192.168.2.27
Mar 5 22:13:00 akj3 sshd[21502]: Failed login for user10 from 192.168.2.5
```

Which of the following is the most likely reason for the application failures?

A. The user's account was set as a service account.

B. The user's home directory was deleted.

C. The user does not have sudo access.

D. The root password has been changed.

Answer: (SHOW ANSWER)

The logs show repeated failed logins for user10 from the same IP (192.168.2.5) at regular intervals, suggesting an automated process. This behavior is characteristic of a service account that is still active after a staff reduction, but likely disabled or removed, causing dependent applications to fail.

NEW QUESTION: 90

A security engineer receives reports through the organization's bug bounty program about remote code execution in a specific component in a custom application. Management wants to properly secure the component and proactively avoid similar issues. Which of the following is the best approach to uncover additional vulnerable paths in the application?

A. Leverage an exploitation framework to uncover vulnerabilities.

B. Use fuzz testing to uncover potential vulnerabilities in the application.

C. Utilize a software composition analysis tool to report known vulnerabilities.

D. Reverse engineer the application to look for vulnerable code paths.

E. Analyze the use of an HTTP intercepting proxy to dynamically uncover issues.

Answer: (SHOW ANSWER)

Fuzz testing is a technique used to identify vulnerabilities by inputting a large volume of random, unexpected, or malformed data into the application. It helps uncover vulnerabilities like buffer overflows, input validation issues, and other security flaws that may not be immediately apparent.

By systematically testing different inputs and paths in the application, fuzz testing can identify previously undiscovered vulnerabilities and help secure the component against potential exploits.

NEW QUESTION: 91

After a cybersecurity incident, a security analyst was able to collect a binary that the attacker used on the compromised server. Then the analyst ran the following command:

Which of the following options describes what the analyst is trying to do?

A. To reconstruct the timeline of commands executed by the binary

B. To extract IoCs from the binary used on the attack

C. To replicate the attack in a secure environment

D. To debug the binary to analyze low-level instructions

Answer: (SHOW ANSWER)

The command strings binary.exeis used to extract human-readable strings from a binary file. This can help the security analyst find indicators of compromise (IoCs), such as IP addresses (e.g., http://192.168.1.2/?=cmd.exe), file paths, and potentially malicious domain names or commands embedded in the binary. This process aids in identifying critical information that can be used for further investigation or remediation of the attack.

NEW QUESTION: 92

A company notices that cloud environment costs increased after using a new serverless solution based on API requests. Many invalid requests from unknown IPs were found, often within a short time. Which of the following solutions would most likely solve this issue, reduce cost, and improve security?

A. Using digital certificates for known customers and performing API authorization through those certificates

B. Defining request rate limits and comparing new requests from unknown IPs with a list of known- malicious IPs

C. Setting authentication processes for the API requests as well as proper rate limits according to regular usage

D. Only allowing API requests coming from regions with known customers

Answer: (SHOW ANSWER)

Implementing authentication for API requests ensures only legitimate users can access the service, while setting rate limits helps prevent abuse and controls costs associated with excessive or malicious traffic. This directly addresses both the security and cost concerns.

NEW QUESTION: 93

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.

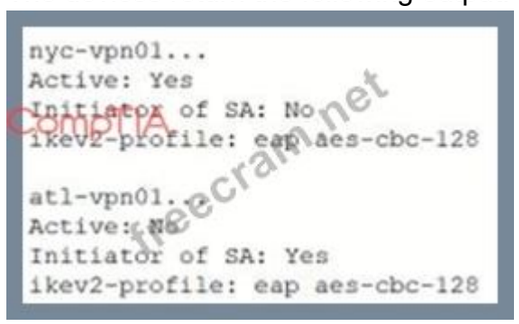
NEW QUESTION: 94
A malware researcher has discovered a credential stealer is looking at a specific memory register to harvest passwords that will be used later for lateral movement in corporate networks. The malware is using TCP 4444 to communicate with other workstations. The lateral movement would be best mitigated by:
A. Enabling an edge firewall
B. Enabling a host firewall
C. Enforcing all systems to use UEFI
D. Enabling ASLR on the Active Directory server
E. Configuring the CPU's NX bit
Answer: (SHOW ANSWER)

NEW QUESTION: 95
A hospital provides tablets to its medical staff to enable them to more quickly access and edit patients' charts. The hospital wants to ensure that if a tablet is identified as lost or stolen and a remote command is issued, the risk of data loss can be mitigated within seconds. The tablets are configured as follows to meet hospital policy:
- Full disk encryption is enabled.
- "Always On" corporate VPN is enabled.
- eFuse-backed keystore is enabled/ready.
- Wi-Fi 6 is configured with SAE.
- Location services is disabled.
- Application allow list is unconfigured.
Assuming the hospital policy cannot be changed, which of the following is the best way to meet the hospital's objective?
A. Revoke the user VPN and Wi-Fi certificates
B. Issue new MFA credentials to all users
C. Cryptographically erase FDE volumes
D. Configure the application allow list
Answer: (SHOW ANSWER)

NEW QUESTION: 96
A security manager is creating a connection between two networks that process data at different classification levels. The main goal of this connection is to pass data from the higher classification side to the lower classification side without causing spillage. Only approved fie types and content will be allowed. Which of the following technologies would best meet this objective?

A. Network access control
B. File integrity monitoring
C. Cross-domain solution
D. Microsegmentation
Answer: (SHOW ANSWER)
A cross-domain solution (CDS) is specifically designed to transfer data between networks of differing classification levels while enforcing strict content and file-type filtering to prevent spillage.
CDS implementations, such as data diodes or content-guarding proxies, ensure that only preapproved formats and sanitized content flow from the high side to the low side, meeting the requirement to allow safe data sharing without risking leakage.

NEW QUESTION: 97
A security engineer is troubleshooting an outage of a site-to-site VPN between New York City and Atlanta. The tunnel is configured with a pre-shared key on two VPN concentrators. The Atlanta site should be configured to always listen for connections from the New York City site. The security engineer issues the following command on both devices:
show crypto ike2 sa detailed
The devices return the following output:



Which of the following actions should the security engineer take to resolve the issue?
A. Modify cipher suites to use AES256-GCM.
B. Contact the Atlanta site's staff to restart the VPN concentrator.
C. Add a third VPN concentrator.
D. Configure the New York City site as the initiator.
Answer: (SHOW ANSWER)
The output shows that the Atlanta VPN is set as the initiator but is inactive, while the New York City VPN is active but not initiating the Security Association (SA). Since Atlanta is supposed to always listen, the New York City site must be configured as the initiator to establish the tunnel successfully.

NEW QUESTION: 98
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: 99
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?
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: 100
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: (SHOW ANSWER)
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: 101
A security engineer needs to remediate a SWEET32 vulnerability in an OpenSSH-based application and review existing configurations. Which of the following should the security engineer do? (Choose two.)
A. Disable Twofish algorithms
B. cat /etc/sshd/ssh_config | grep "HMAC"
C. Disable RSA algorithms
D. cat /etc/sshd/ssh_config | grep "PermitRootLogin"
E. Disable 3DES algorithms
F. cat /etc/sshd/ssh_config | grep "Ciphers"
Answer: (SHOW ANSWER)
SWEET32 exploits the 64-bit block size of 3DES, so disabling 3DES algorithms mitigates the vulnerability.
Reviewing the Ciphers configuration in ssh_config ensures only secure ciphers are enabled, confirming 3DES is removed and stronger algorithms are enforced.

NEW QUESTION: 102
A company's Chief Information Security Officer learns that the senior leadership team is traveling to a country accused of attempting to steal intellectual property saved on laptops. Which of the following is the best method to protect against this attack?
A. Configure Measured Boot to report any firmware changes.
B. Use sanitized devices with remote connections to VDI.
C. Deploy self-encrypting drives to protect company data.
D. Install tamper-evident stickers over any laptop screws.
Answer: (SHOW ANSWER)
Providing sanitized devices that connect only to a secure virtual desktop infrastructure (VDI) ensures no sensitive data is stored locally on laptops. This is the best protection against intellectual property theft when traveling to high-risk countries.

NEW QUESTION: 103
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: 104
A company wants to modify its process to comply with privacy requirements after an incident involving PII data in a development environment. In order to perform functionality tests, the QA team still needs to use valid data in the specified format. Which of the following best addresses the risk without impacting the development life cycle?
A. Encrypting the data before moving into the QA environment
B. Truncating the data to make it not personally identifiable
C. Using a large language model to generate synthetic data
D. Utilizing tokenization for sensitive fields
Answer: (SHOW ANSWER)
Tokenization replaces sensitive data (e.g., PII) with non-sensitive placeholders while maintaining format consistency, ensuring compliance without disrupting testing. This method is commonly used for PCI-DSS and GDPR compliance while preserving data structure for functional tests.

NEW QUESTION: 105
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: 106
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: 107
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: 108
Which of the following includes best practices for validating perimeter firewall configurations?
A. CIS controls
B. MITRE ATT&CK
C. NIST CSF
D. ISO 27001
Answer: (SHOW ANSWER)
CIS Controls provide prescriptive best practices for validating and hardening firewall configurations, including rule review, change management, and regular audits to ensure perimeter defenses are properly configured.

NEW QUESTION: 109
A Chief Information Security Officer (CISO) is concerned that a company's current data disposal procedures could result in data remanence. The company uses only SSDs. Which of the following would be the most secure way to dispose of the SSDs given the CISO's concern?
A. Shredding
B. Incinerating
C. Overwriting
D. Formatting
E. Degaussing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
A security engineer is implementing security measures on new hardware in preparation for its launch. During the development phase, a risk related to protections at the UEFI level was found. Which of the following should the engineer recommend to reduce this risk?

A. Configuring paravirtualization protection
B. Enabling Secure Boot
C. Installing cryptography at the operational system level
D. Implementing hardware root of trust
Answer: (SHOW ANSWER)
Enabling Secure Boot at the UEFI level helps ensure that only trusted and signed operating system loaders and boot files can be executed on the hardware. This prevents unauthorized code, such as bootkits or rootkits, from loading during the boot process, significantly reducing risks at the UEFI level. Secure Boot is an essential measure to ensure the integrity of the system from the very start of the boot process.

NEW QUESTION: 111
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: 112
A company finds logs with modified time stamps when compared to other systems. The security team decides to improve logging and auditing for incident response. Which of the following should the team do to best accomplish this goal?
A. Integrate a file-monitoring tool with the SIEM.

B. Change the log solution and integrate it with the existing SIEM.
C. Implement a central logging server, allowing only log ingestion.
D. Rotate and back up logs every 24 hours, encrypting the backups.
Answer: (SHOW ANSWER)
A central logging server ensures logs are collected in a tamper-proof manner and only ingested (not modified). This prevents attackers from altering logs locally.
Key concepts: Logs should be centrally stored to prevent tampering. Enabling log forwarding to a secure SIEM improves integrity.

NEW QUESTION: 113
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: B (LEAVE A REPLY)
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: 114
During a periodic internal audit, a company identifies a few new, critical security controls that are missing. The company has a mature risk management program in place, and the following requirements must be met:
The stakeholders should be able to see all the risks.
The risks need to have someone accountable for them.
Which of the following actions should the GRC analyst take next?
A. Add the risk to the risk register and assign the owner and severity.
B. Change the risk appetite and assign an owner to it.
C. Mitigate the risk and change the status to accepted.
D. Review the risk to decide whether to accept or reject it.
Answer: (SHOW ANSWER)
A risk register is a tool commonly used in risk management to document all identified risks, their assessment in terms of likelihood and impact, and the actions steps to manage them. By adding the newly identified risks to the risk register and assigning an owner and severity, the organization ensures that each risk is visible to stakeholders and has a designated individual responsible for its management. This aligns with the company's requirements for transparency and accountability in risk management.

NEW QUESTION: 115
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: 116
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?
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: 117
A company hired an email service provider called my-email.com to deliver company emails. The company started having several issues during the migration. A security engineer is troubleshooting and observes the following configuration snippet:

@	MX	10	email.company.com	45000
www	IN	CNAME	web01.company.com.	
email	IN	CNAME	srv01.company.com	
srv01	IN	A	192.168.1.10	
web01	IN	A	192.168.1.11	
@	IN	TXT	"v=dmarc include:company.com ~all"	

Which of the following should the security engineer modify to fix the issue? (Choose two.)
A. The email CNAME record must be changed to a type A record pointing to 192.168.1.11
B. The TXT record must be Changed to "v=dmarc ip4:192.168.1.10 include:my-email.com -all"
C. The srvo1 A record must be changed to a type CNAME record pointing to the email server
D. The email CNAME record must be changed to a type A record pointing to 192.168.1.10
E. The TXT record must be changed to "v=dkim ip4:l92.168.1.11 include my-email.com -ell"
F. The TXT record must be Changed to "v=dkim ip4:192.168.1.10 include:email-all"
G. The srv01 A record must be changed to a type CNAME record pointing to the web01 server
Answer: (SHOW ANSWER)

The security engineer should modify the following to fix the email migration issues:
Email CNAME Record: The email CNAME record must be changed to a type A record pointing to
192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required. Changing it to an A record ensures direct pointing to the correct IP.
TXT Record for DMARC: The TXT record must be changed to "v=dmarc ip4:192.168.1.10 include .com -all". This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting & Conformance) to include the correct IP address and the email service provider domain.
DMARC: Ensuring the DMARC record is correctly set up helps in preventing email spoofing and phishing, aligning with email security best practices.

NEW QUESTION: 118
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: 119
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: 120
A security analyst is reviewing suspicious log-in activity and sees the following data in the SIEM:

Account	Application	Authorization server	Status	Risk
SALES1	Customer manager	LDAP-US	Success	Low
SALES1	Payroll	LDAP-US	Success	Low
ADMIN	Email	LDAP-US	Failure	High
SALES1	Email	LDAP-EU	Unknown	Unknown
MARKET1	Customer manager	LDAP-US	Success	Low
FINANCE1	Payroll	LDAP-EU	Unknown	Unknown

Which of the following is the most appropriate action for the analyst to take?

A. Update the log configuration settings on the directory server that Is not being captured properly.

B. Have the admin account owner change their password to avoid credential stuffing.

C. Block employees from logging in to applications that are not part of their business area.

D. implement automation to disable accounts that nave been associated with high-risk activity.

Answer: (SHOW ANSWER)

The ADMIN account is showing a failure to authenticate on LDAP-US and a high-risk level, which is a cause for concern. The most appropriate action would be to implement automation to disable accounts that have been associated with high-risk activity (like this one). This helps prevent further misuse or potential attacks using compromised credentials.

NEW QUESTION: 121

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: 122

An engineer wants to automate several tasks by running commands daily on a UNIX server. The engineer only has built-in default tools available. Which of the following should the engineer use to best assist with this endeavor? (Choose two.)

A. Python

B. Cron

C. Ansible

D. PowerShell

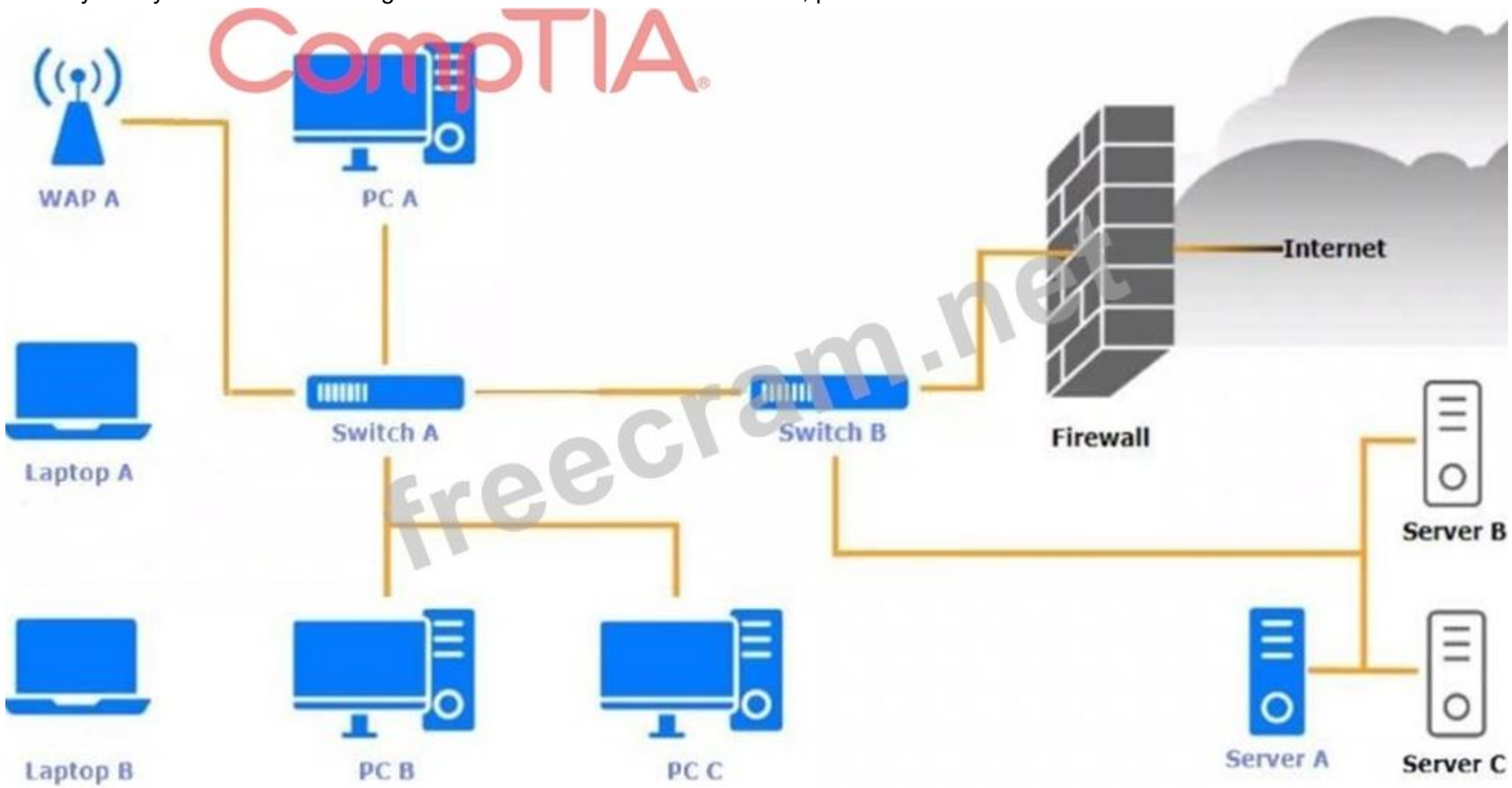
E. Bash
F. Task Scheduler
Answer: (SHOW ANSWER)
Cron is a built-in UNIX tool for scheduling tasks to run automatically at specified times.
Bash is the default command-line shell in UNIX systems, allowing engineers to write and execute scripts to automate tasks.

NEW QUESTION: 123
A security analyst collects the logs from the web server that is associated with a security incident.
The analyst finds the following entry in the logs:
SELECT user FROM Customers WHERE userID = "SRequest(userID)"
Which of the following will prevent this incident from reoccurring?
A. URL encoding
B. Query parameterization
C. Data sanitization
D. SQL output encoding
Answer: B (LEAVE A REPLY)
Query parameterization ensures that user input is treated strictly as data, not as executable SQL code. This prevents SQL injection attacks like the one shown in the log entry, thereby eliminating the vulnerability that led to the incident.

NEW QUESTION: 124
An organization is looking to establish more robust security measures by implementing PKI.
Which of the following should the security analyst implement when considering mutual authentication?
A. Perfect forward secrecy on both endpoints
B. Shared secret for both endpoints
C. Public keys on both endpoints
D. A common public key on each endpoint
E. A common private key on each endpoint
Answer: (SHOW ANSWER)
Mutual authentication in a PKI context requires each endpoint to present and validate the other's certificate, which contains its public key. Each side uses its private key to prove ownership of its certificate and uses the peer's public key to verify signatures, ensuring both parties authenticate each other.

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: (SHOW ANSWER)
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
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.



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

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

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

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
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

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
		☐ Enabled disk encryption
Default admin account	Default password has been changed	☐ 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

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

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

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

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
```

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 spt:ssh dpts:login:65535 state NEW,ESTABLISHED

1   28      DROP    all   --  any any anywhere  anywhere


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

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
```


Server A

Nmap | IP Tables

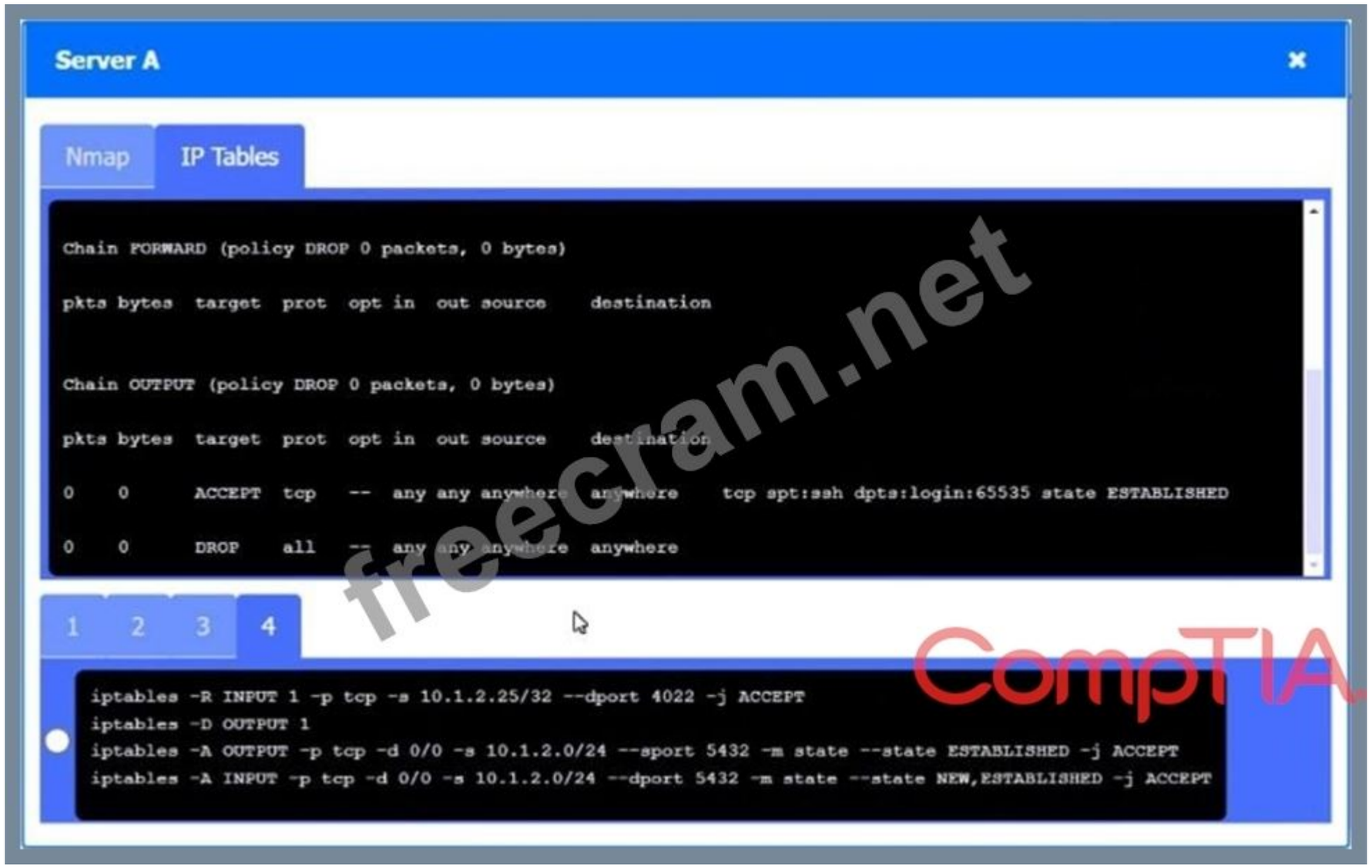
```
Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes  target  prot  opt in  out source    destination


Chain OUTPUT (policy DROP 0 packets, 0 bytes)

pkts bytes  target  prot  opt in  out source    destination

0    0      ACCEPT  tcp   --  any any anywhere  anywhere    tcp spt:ssh dpts:login:65535 state ESTABLISHED

0    0      DROP    all   --  any any anywhere  anywhere
```

1 | 2 | 3 | 4

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

freecram.net

CompTIA



Answer:

WAP-A- Disable unneeded services
Laptop A- Disable unneeded services
Laptop B- Enabled Disk encryption & Disable unneeded services
Switch A- Change default administrative password & Disable unneeded services
Switch B- Disable unneeded services
PC-A - Disable unneeded services
PC-B - Disable unneeded services
PC-C - Patch management, Disable unneeded services

NEW QUESTION: 127

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

Which of the following should the analyst use to address the vulnerabilities in the future?

A. Least privilege

B. Defense in depth

C. System image hardening

D. OS update

Answer: (SHOW ANSWER)

NEW QUESTION: 128

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: 129

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: 130

A DNS forward lookup zone named comptia.org must:
- Ensure the DNS is protected from on-path attacks.
- Ensure zone transfers use mutual authentication and are authenticated and negotiated.
Which of the following should the security architect configure to meet these requirements? (Choose two).

A. Public keys
B. Conditional forwarders
C. Root hints
D. DNSSEC
E. CNAME records
F. SRV records
Answer: (SHOW ANSWER)
By publishing the zone's DNSSEC public keys (and configuring the parent zone and any secondary servers to trust them), zone transfers will automatically be integrity-checked and authenticated. The mutual authentication during zone transfers relies on the underlying public-key signatures that DNSSEC provides.
Deploying DNSSEC for the comptia.org zone signs all records with cryptographic signatures and publishes the corresponding public keys, protecting against on-path tampering and spoofing.

NEW QUESTION: 131
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: 132
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: 133
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: 134
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.

NEW QUESTION: 135

A SIEM generated an alert after a third-party database administrator, who had recently been granted temporary access to the repository, accessed business-sensitive content in the database.
The SIEM had generated similar alerts before this incident. Which of the following best explains the cause of the alert?
A. Database field tokenization
B. Database decoy
C. Database activity monitoring
D. Database integrity enforcement
Answer: (SHOW ANSWER)
Database activity monitoring (DAM) tracks user actions within databases and generates alerts for anomalous behavior, such as unauthorized access to sensitive content. Database field tokenization protects sensitive data but does not monitor access. Database decoy involves creating fake data to detect misuse but is unrelated to monitoring. Database integrity enforcement ensures data accuracy but does not generate access alerts.

NEW QUESTION: 136
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: 137
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: B (LEAVE A REPLY)
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: 138
Due to budget constraints, an organization created a policy that only permits vulnerabilities rated high and critical according to CVSS to be fixed or mitigated. A security analyst notices that many vulnerabilities that were previously scored as medium are now breaching higher thresholds. Upon further investigation, the analyst notices certain ratings are not aligned with the approved system categorization. Which of the following can the analyst do to get a better picture of the risk while adhering to the organization's policy?
A. Align the exploitability metrics to the predetermined system categorization.
B. Align the remediation levels to the predetermined system categorization.
C. Align the impact subscore requirements to the predetermined system categorization.
D. Align the attack vectors to the predetermined system categorization.
Answer: (SHOW ANSWER)
CVSS's Environmental metrics let you tune the Base scores to your own environment by adjusting the Security Requirements (CR, IR, AR) for Confidentiality, Integrity, and Availability. By mapping those impact weights to your system classification (for example, marking Integrity as
"High" for systems that can't tolerate data corruption), you get a recalculated environmental score that more accurately reflects real-world risk, while still sticking to the organization's policy of only remediating high/critical CVSS scores.

NEW QUESTION: 139
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: D (LEAVE A REPLY)
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: 140
Audit findings indicate several user endpoints are not utilizing full disk encryption. During me remediation process, a compliance analyst reviews the testing details for the endpoints and notes the endpoint device configuration does not support full disk encryption. Which of the following is the most likely reason me device must be replaced?

A. The HSM is outdated and no longer supported by the manufacturer
B. The vTPM was not properly initialized and is corrupt.
C. The HSM is vulnerable to common exploits and a firmware upgrade is needed
D. The motherboard was not configured with a TPM from the OEM supplier.
E. The HSM does not support sealing storage
Answer: (SHOW ANSWER)
The most likely reason the endpoint cannot utilize full disk encryption is that the device lacks a TPM (Trusted Platform Module), which is often required for full disk encryption solutions. Many modern encryption technologies rely on the TPM to securely store encryption keys. If the motherboard was not configured with a TPM by the original equipment manufacturer (OEM), the device would not support full disk encryption and would need to be replaced or upgraded to a compatible device.

NEW QUESTION: 141
An organization that performs real-time financial processing is implementing a new backup solution.
Given the following business requirements:
- The backup solution must reduce the risk of potential backup
compromise.
- The backup solution must be resilient to a ransomware attack.
- The time to restore from backups is less important than backup data
integrity.
Multiple copies of production data must be maintained.
Which of the following backup strategies best meets these requirements?
A. Creating a secondary, immutable database and adding live data on a continuous basis
B. Utilizing two connected storage arrays and ensuring the arrays constantly sync
C. Enabling remote journaling on the databases to ensure real-time transactions are mirrored
D. Setting up anti-tampering on the databases to ensure data cannot be changed unintentionally
Answer: (SHOW ANSWER)
Creating a secondary, immutable database and adding live data continuously best meets the requirements because immutability ensures backup data cannot be altered or compromised, including during ransomware attacks. This approach preserves data integrity and maintains multiple copies, aligning with the priority on data integrity over restore speed.

NEW QUESTION: 142
An organization is increasing its focus on training that addresses new social engineering and phishing attacks. Which of the following is the organization most concerned about?
A. Meeting existing regulatory compliance
B. Overreliance on AI support bots
C. Generative AI tools increasing the quality of exploits
D. Differential analysis using AI models
Answer: C (LEAVE A REPLY)
The organization is concerned that generative AI tools can increase the quality and sophistication of phishing and social engineering attacks, making them harder to detect and more convincing to victims.

NEW QUESTION: 143
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. Certifications are typically issued against a formal standard.
C. Assessments are based on evidence, not judgments.
D. For standards like PCI, self-attestations are more reliable than certifications.
Answer: (SHOW ANSWER)

NEW QUESTION: 144

A global company's Chief Financial Officer (CFO) receives a phone call from someone claiming to be the Chief Executive Officer (CEO). The caller claims to be stranded and in desperate need of money. The CFO is suspicious, but the caller's voice sounds similar to the CEO's. Which of the following best describes this type of attack?

A. Smishing

B. Deepfake

C. Automated exploit generation

D. Spear phishing

Answer: (SHOW ANSWER)

The attacker used synthesized or AI-generated audio to mimic the CEO's voice convincingly over the phone. This is a form of "deepfake" attack, leveraging generative techniques to spoof a trusted individual's voice and manipulate the target into transferring funds.

NEW QUESTION: 145

A security analyst notices a number of SIEM events that show the following activity:

```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```

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

A. Configure the forward proxy to block 40.90.23.154

B. Disable local administrator privileges on the endpoints

C. Disable powershell.exe on all Microsoft Windows endpoints

D. Restart Microsoft Windows Defender

Answer: (SHOW ANSWER)

NEW QUESTION: 146

An audit finding reveals that a legacy platform has not retained logs for more than 30 days. The platform has been segmented due to its interoperability with newer technology. As a temporary solution, the IT department changed the log retention to 120 days. Which of the following should the security engineer do to ensure the logs are being properly retained?

A. Configure a scheduled task nightly to save the logs

B. Configure event-based triggers to export the logs at a threshold.

C. Configure the SIEM to aggregate the logs

D. Configure a Python script to move the logs into a SQL database.

Answer: (SHOW ANSWER)

A SIEM (Security Information and Event Management) solution is specifically designed to collect, store, and aggregate logs from various systems. By configuring the SIEM to aggregate the logs, the security engineer can ensure that the logs are properly retained, analyzed, and correlated for compliance and security purposes. This solution provides long-term storage and easier access to logs for investigations.

NEW QUESTION: 147

A company that provides services to clients who work with highly sensitive data would like to provide assurance that the data's confidentiality is maintained in a dynamic, low-risk environment.

Which of the following would best achieve this goal? (Choose two.)

A. Install a SOAR on all endpoints.

B. Hash all files.

C. Install SIEM within a SOC.

D. Encrypt all data and files at rest, in transit, and in use.
E. Configure SOAR to monitor and intercept files and data leaving the network.
F. Implement file integrity monitoring.
Answer: D,F (LEAVE A REPLY)
Encrypt all data and files at rest, in transit, and in use: Encryption ensures that sensitive data is protected and its confidentiality is maintained. By encrypting data at all stages- whether stored (at rest), transmitted (in transit), or actively being processed (in use)-the company can significantly reduce the risk of unauthorized access or exposure, ensuring the confidentiality of highly sensitive data.
Implement file integrity monitoring: File Integrity Monitoring (FIM) ensures that files containing sensitive data are not altered without authorization. By monitoring changes to critical files, it helps detect tampering, modifications, or potential data breaches, adding an extra layer of security to sensitive information in a dynamic environment.

NEW QUESTION: 148
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. Creating a site-to-site VPN tunnel and allowing restricted access to the system
B. Deploying a RDP jump box to allow remote system monitoring
C. Installing the vendor's monitoring appliance on the internal network and allowing outbound SSL connectivity
D. Implementing a reverse web proxy and allowing access from the internet
Answer: (SHOW ANSWER)

NEW QUESTION: 149
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: (SHOW ANSWER)
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: 150

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

A. Data integrity is protected by advanced hashing routines.
B. Resource utilization is lower.
C. Support for field-specific tokenization is added.
D. The need for a pre-shared key is removed.
Answer: (SHOW ANSWER)

NEW QUESTION: 151
An organization is developing an AI-enabled digital worker to help employees complete common tasks, such as template development, editing, research, and scheduling. As part of the AI workload, the organization wants to implement guardrails within the platform. Which of the following should the company do to secure the AI environment?
A. Limit the platform's abilities to only non-sensitive functions
B. Enhance the training model's effectiveness.
C. Grant the system the ability to self-govern
D. Require end-user acknowledgement of organizational policies.
Answer: (SHOW ANSWER)
Limiting the platform's abilities to only non-sensitive functions is the best way to secure the AI environment. By restricting the AI's scope to tasks that do not involve sensitive or critical information, the company can mitigate the risk of accidental data exposure or misuse while still allowing the AI to assist employees in non-sensitive activities. This approach helps implement guardrails that align with security best practices.

NEW QUESTION: 152
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: 153
A company's internal network is experiencing a security breach, and the threat actor is still active.
Due to business requirements, users in this environment are allowed to utilize multiple machines at the same time. Given the following log snippet:

Time	User	Process	Status	Machine
10:11	user-a	.exe	blocked	machine02
10:15	user-b	setup.exe	blocked	machine02
10:15	user-A	appwiz.exe	blocked	machine01
10:16	user-c	appwiz.CPL	blocked	machine03
11:17	user-c	cmd.exe	blocked	machine03
11:18	user-h	msconfig.exe	blocked	machine04
11:19	user-d	firefox.exe	blocked	machine04
11:19	user-d	cmd.com	blocked	machine01

Which of the following accounts should a security analyst disable to best contain the incident without impacting valid users?

A. user-a

B. user-b

C. user-c

D. user-d

Answer: (SHOW ANSWER)

User user-c is showing anomalous behavior across multiple machines, attempting to run administrative tools such as cmd.exe and appwiz.CPL, which are commonly used by attackers for system modification. The activity pattern suggests a lateral movement attempt, potentially indicating a compromised account.

NEW QUESTION: 154

A security team is responding to malicious activity and needs to determine the scope of impact.

The malicious activity appears to affect a certain version of an application used by the organization. Which of the following actions best enables the team to determine the scope of impact?

A. Performing a port scan

B. Inspecting egress network traffic

C. Reviewing the asset inventory

D. Analyzing user behavior

Answer: (SHOW ANSWER)

Reviewing the asset inventory allows the security team to identify all instances of the affected application versions within the organization. By knowing which systems are running the vulnerable versions, the team can assess the full scope of the impact, determine which systems might be compromised, and prioritize them for further investigation and remediation.

NEW QUESTION: 155

A security analyst wants to use lessons learned from a prior incident response to reduce dwell time in the future. The analyst is using the following data points:

User	Site visited	HTTP method	Filter status	Traffic status	Alert status
account1	tools.com	GET	Allowed	Allowed	No
admin1	hacking.com	GET	Allowed	Allowed	Yes
account5	payroll.com	GET	Allowed	Allowed	No
account2	p4yr0ll.com	GET	Blocked	Blocked	No
account2	p4yr0ll.com	POST	Blocked	Blocked	No
account2	139.40.29.21	POST	Allowed	Allowed	No
account5	payroll.com	GET	Allowed	Allowed	No

Which of the following would the analyst most likely recommend?

A. Adjusting the SIEM to alert on attempts to visit phishing sites

B. Allowing TRACE method traffic to enable better log correlation

C. Enabling alerting on all suspicious administrator behavior

D. utilizing allow lists on the WAF for all users using GFT methods

Answer: (SHOW ANSWER)

The data indicates that admin1 visited a suspicious domain (hacking.com), which triggered an alert. Adjusting the SIEM to alert on attempts to visit phishing sites would allow for faster identification of potentially malicious activity in the future. This approach directly addresses reducing dwell time by alerting on suspicious or malicious site visits, helping security teams to act quickly.

NEW QUESTION: 156

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?

(Choose two.)

A. EDR

B. HIDS

C. Web application firewall

D. Central logging

E. Host-based firewall

F. TPM

Answer: A,D (LEAVE A REPLY)

EDR provides endpoint telemetry and integrates with an XDR platform for extended detection and response.

Central logging ensures telemetry is forwarded to the SIEM, enabling SOC services to monitor the XDR platform effectively.

NEW QUESTION: 157

A security engineer is given the following requirements:

- An endpoint must only execute Internally signed applications
- Administrator accounts cannot install unauthorized software.
- Attempts to run unauthorized software must be logged

Which of the following best meets these requirements?

A. Maintaining appropriate account access through directory management and controls

B. Implementing a CSPM platform to monitor updates being pushed to applications

C. Deploying an EDR solution to monitor and respond to software installation attempts

D. Configuring application control with blocked hashes and enterprise-trusted root certificates

Answer: (SHOW ANSWER)

Application control with blocked hashes and enterprise-trusted root certificates ensures that only internally signed applications can be executed, aligning with the requirement to limit executable files to those signed by the organization. By blocking unauthorized hashes, the control prevents unauthorized software installations. This approach also meets the requirement to log attempts to run unauthorized software, as such events can be captured and logged by the application control solution.

NEW QUESTION: 158

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. Contact each user to reset their password.

C. Configure a privilege access management solution.

D. Migrate authentication methods to allow for OAuth 2.

Answer: (SHOW ANSWER)

NEW QUESTION: 159

Which of the following security risks should be considered as an organization reduces cost and increases availability of services by adopting serverless computing?

A. Vertical scalability of the infrastructure underpinning the serverless offerings

B. Type of virtualization or emulation technology used in the provisioning of services

C. Use of third-party monitoring of service provisioning and configurations

D. Level of control and influence governments have over cloud service providers

Answer: (SHOW ANSWER)

NEW QUESTION: 160

During a security assessment using an EDR solution, a security engineer generates the following report about the assets in the system:

Device	Type	EDR status
LN002	Linux SE	Enabled (unmanaged)
0WIN23	Windows 7	Enabled
0WIN29	Windows 10	Enabled (bypass)
MAC005	Mac OS	Enabled

After five days, the EDR console reports a blocked infection on the host 0WIN23 by a remote access Trojan. Which of the following most likely enabled the attempted infection?

A. 0W1N23 uses a legacy version of Windows that is not supported by the EDR
B. LN002 was not supported by the EDR solution and propagates the RAT
C. The EDR has an unknown vulnerability that was exploited by the attacker
D. 0W1N29 spreads the malware through other hosts in the network
Answer: (SHOW ANSWER)
The key clue is the "Enabled (bypass)" status on 0WIN29. That means the EDR agent was running but being bypassed, effectively allowing malicious code to execute unchecked. An attacker could exploit that bypass to install the RAT on 0WIN29, and then attempt lateral movement to 0WIN23. 0WIN23's EDR then detected and blocked the inbound infection, but the initial foothold was enabled by the vulnerability in the 0WIN29 deployment.

NEW QUESTION: 161
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
ozilla/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
ozilla/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
ozilla/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
ozilla/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
ozilla/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: 162
Employees use their badges to track the number of hours they work. The badge readers cannot be upgraded due to facility constraints. The software for the badge readers uses a legacy platform and requires connectivity to the enterprise resource planning solution. Which of the following is the best to ensure the security of the badge readers?
A. Segmentation
B. Vulnerability scans
C. Anti-malware
Answer: (SHOW ANSWER)
Segmentation is the best option to ensure the security of legacy badge readers that cannot be upgraded. Segmentation isolates the legacy devices on a separate network segment to minimize their exposure to potential threats. This approach reduces the attack surface by preventing unauthorized access from other parts of the network while still allowing necessary connectivity to the enterprise resource planning (ERP) system.

NEW QUESTION: 163
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. Web application firewall
D. Threat intelligence platforms
Answer: (SHOW ANSWER)

NEW QUESTION: 164
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.

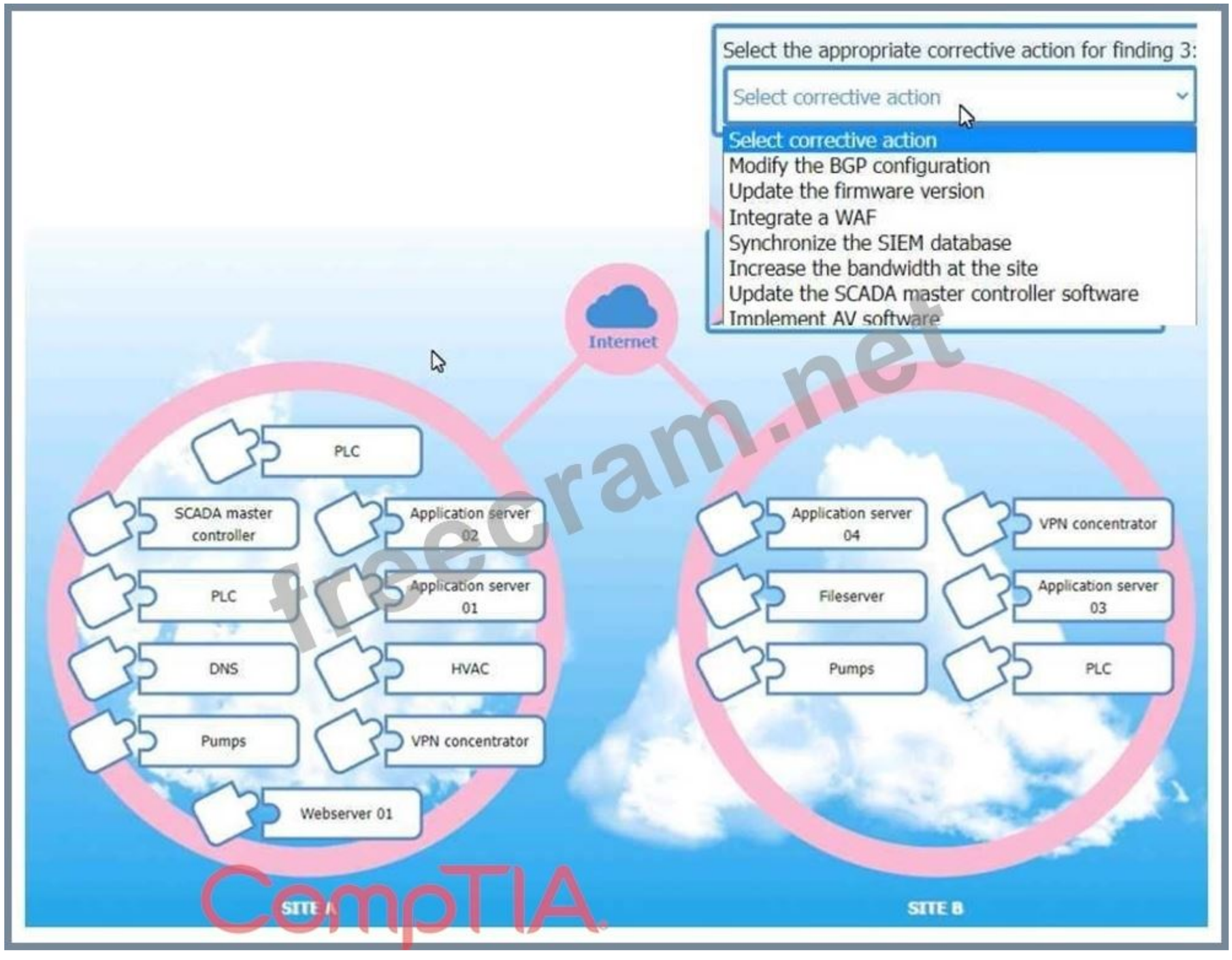
NEW QUESTION: 165
A security analyst detects a possible RAT infection on a computer in the internal network. After reviewing the details of the alert, the analyst identifies the initial vector of the attack was an email that was forwarded to multiple recipients in the same organizational unit. Which of the following should the analyst do first to minimize this type of threat in the future?
A. Move from an anti-malware software to an EDR solution.
B. Perform a penetration test to detect technology gaps on the anti-spam solution.
C. Configure an IPS solution in the internal network to mitigate infections.
D. Implement a security awareness program in the organization.
Answer: (SHOW ANSWER)
A security awareness program is the best initial step to minimize threats like this in the future. It helps employees recognize phishing emails, which are a common method for malware infections, and prevents them from forwarding malicious emails. Educating users is key in reducing human error, which is often the starting point for attacks like RAT infections.

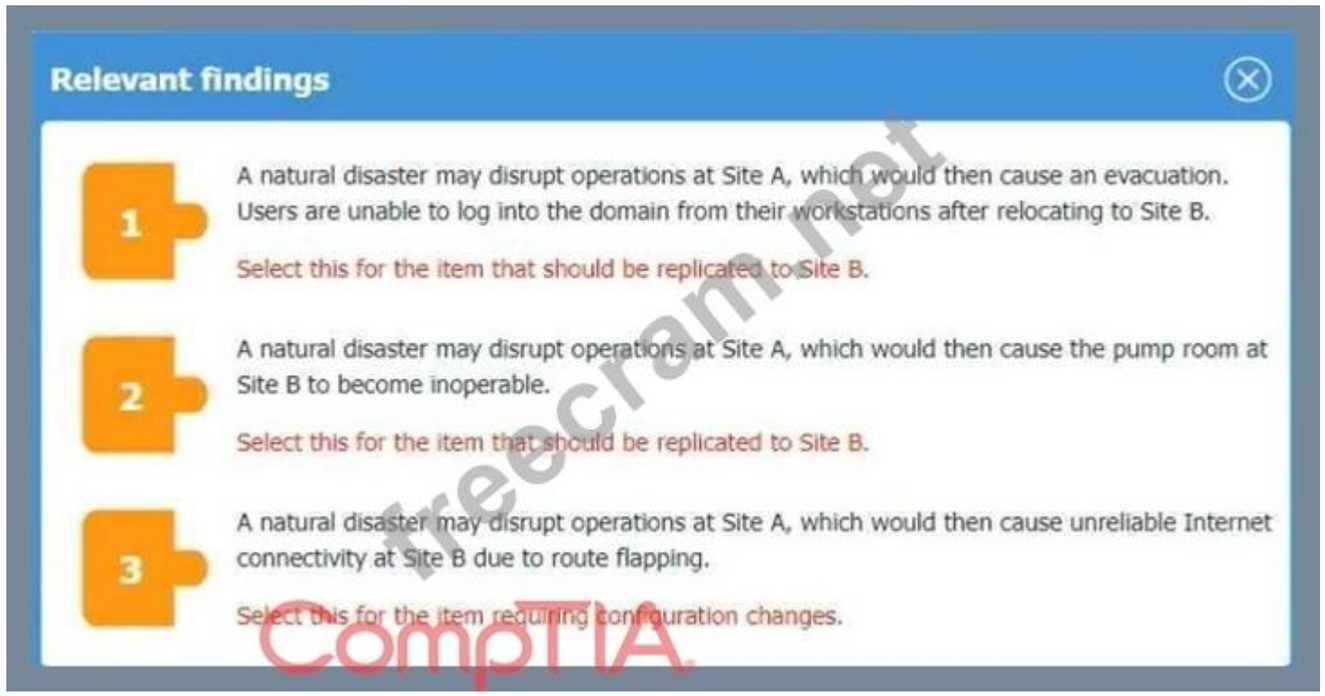
NEW QUESTION: 166
A company that provides kiosk workstations wants to improve the workstations' security implementation. The company is concerned that attackers can take control of the workstations during the boot process and change the flow of the data. Which of the following solutions best addresses the concerns?
A. Allowing only digitally signed modules to load
B. Setting controls to allow only specific operating systems
C. Removing any unused connection ports
D. Creating bootloader passwords

Answer: (SHOW ANSWER)

NEW QUESTION: 167
A recent security audit identified multiple endpoints have the following vulnerabilities:
- Various unsecured open ports
- Active accounts for terminated personnel
- Endpoint protection software with legacy versions
- Overly permissive access rules
Which of the following would best mitigate these risks? (Select three).
A. Unneeded services disabled
B. Secure boot
C. Address space layout randomization
D. Patching
E. Removal of unused accounts
F. Local drive encryption
G. Enabling BIOS password
H. Logging
Answer: (SHOW ANSWER)

NEW QUESTION: 168
SIMULATION
An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:
1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation.
Users are unable to log into the domain from-their workstations after relocating to Site B.
2. A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet connectivity at Site B due to route flapping.
INSTRUCTIONS
Match each relevant finding to the affected host by clicking on the host name and selecting the appropriate number.
For findings 1 and 2, select the items that should be replicated to Site B. For finding 3, select the item requiring configuration changes, then select the appropriate corrective action from the drop- down menu.





Answer:

Matching Relevant Findings to the Affected Hosts:

Finding 1:

Affected Host: DNS

Reason: Users are unable to log into the domain from their workstations after relocating to Site B, which implies a failure in domain name services that are critical for user authentication and domain login.

Finding 2:

Affected Host: Pumps

Reason: The pump room at Site B becoming inoperable directly points to the critical infrastructure components associated with pumping operations.

Finding 3:

Affected Host: VPN Concentrator

Reason: Unreliable internet connectivity at Site B due to route flapping indicates issues with network routing, which is often managed by VPN concentrators that handle site-to-site connectivity.

Corrective Actions for Finding 3:

Finding 3 Corrective Action:

Action: Modify the BGP configuration

Reason: Route flapping is often related to issues with Border Gateway Protocol (BGP) configurations. Adjusting BGP settings can stabilize routes and improve internet connectivity reliability.

Replication to Site B for Finding 1:

Affected Host: DNS

Domain Name System (DNS) services are essential for translating domain names into IP addresses, allowing users to log into the network. Replicating DNS services ensures that even if Site A is disrupted, users at Site B can still authenticate and access necessary resources.

Replication to Site B for Finding 2:

Affected Host: Pumps

The operation of the pump room is crucial for maintaining various functions within the infrastructure. Replicating the control systems and configurations for the pumps at Site B ensures that operations can continue smoothly even if Site A is affected.
Configuration Changes for Finding 3:
Affected Host: VPN Concentrator
Route flapping is a situation where routes become unstable, causing frequent changes in the best path for data to travel. This instability can be mitigated by modifying BGP configurations to ensure more stable routing. VPN concentrators, which manage connections between sites, are typically configured with BGP for optimal routing.

NEW QUESTION: 169
An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories best describes this type of vendor risk?
A. Remote code signing
B. Supply chain attack
C. Side-load attack
D. SDLC attack
Answer: (SHOW ANSWER)

NEW QUESTION: 170
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: 171
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)
...
...
...
```

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: B (LEAVE A REPLY)
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: 172
Due to reports of malware targeting companies in the same industry, an organization wants to develop a comprehensive list of IoCs to determine if its systems might be affected in a similar attack. Which of the following would be best to use to develop this list?
A. Simulators
B. Sandbox detonation
C. Antivirus
D. Endpoint detection and response
Answer: (SHOW ANSWER)
By detonating threat samples in a sandbox environment, you can safely execute the malware and extract a full spectrum of indicators of compromise - file and payload hashes, dropped filenames and registry keys, network IOCs (domains, IPs, URLs), mutex names, and more. These artifacts form a comprehensive IoC list you can then feed into your monitoring tools (EDR, SIEM, firewalls) to hunt for and block any matching activity across your environment.

NEW QUESTION: 173
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: (SHOW ANSWER)
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: 174
A systems administrator needs to address risks associated with corporate brand impersonation via email. The systems administrator wants a method that permits recipient servers to validate the source authenticity of emails received. Which of the following is the most appropriate?
A. SPF

B. S/MIME
C. DMARC
D. DKIM
Answer: (SHOW ANSWER)

NEW QUESTION: 175
After an organization met with its ISAC, the organization decided to test the resiliency of its security controls against a small number of advanced threat actors. Which of the following will enable the security administrator to accomplish this task?
A. Adversary emulation
B. Reliability factors
C. Deployment of a honeypot
D. Internal reconnaissance
Answer: (SHOW ANSWER)
Adversary emulation involves simulating advanced threat actors using tactics, techniques, and procedures (TTPs) derived from real-world attacks. This approach helps test the effectiveness of an organization's security controls in a controlled environment, allowing the administrator to evaluate how well the system can withstand advanced threats.

NEW QUESTION: 176
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: (SHOW ANSWER)

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: 177
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: 178
A pharmaceutical company acquired a growing startup. The pharmaceutical company has a comprehensive OT stack, while the startup allows employees to install IoT devices without oversight. Both companies will continue to operate independently with some systems shared and others separated. Which of the following considerations are the most important when designing the new combined systems? (Choose two.)
A. Environmental
B. Data privacy
C. Regulation
D. Segmentation
E. Aggregation
F. Safety monitoring
Answer: (SHOW ANSWER)

NEW QUESTION: 179
A systems administrator needs to identify new attacks that could be carried out against the environment. The administrator plans to proactively seek out and observe new attacks. Which of the following is the best way to accomplish this goal?
A. Configuring an IPS
B. Implementing sandboxing
C. Scanning for IoCs
D. Deploying a honeypot
Answer: (SHOW ANSWER)
A honeypot is a decoy system designed to attract attackers and observe their techniques and tactics in a controlled environment. This allows the administrator to proactively observe new attacks and learn from them without putting actual production systems at risk.

NEW QUESTION: 180

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. Define security gates and tests along the CI/CD flow with strict exception rules.
B. Perform regular code reviews and implement pair programming methodology.
C. Implement a SAST tool along the pipeline for every new commit.
D. Hire a third-party company to perform regular software tests, including quality and unity tests.
E. Perform regular vulnerability assessments on production software, defining tight SLAs for treatment.
F. Deliver regular training for the software developers based on best practices.
Answer: (SHOW ANSWER)

NEW QUESTION: 181
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: 182
An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key. Which of the following would best secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?
A. Deploy MFA for the service accounts
B. Utilize HMAC for the keys
C. Sign the key with DSA
D. Implement a VPN for all APIs
Answer: (SHOW ANSWER)

NEW QUESTION: 183

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: A (LEAVE A REPLY)

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: 184

Users are experiencing a variety of issues when trying to access corporate resources. Examples include:

- Connectivity issues between local computers and file servers within
branch offices
- Inability to download corporate applications on mobile endpoints
while working remotely
- Certificate errors when accessing internal web applications

Which of the following actions are the most relevant when troubleshooting the reported issues?
(Choose two.)

A. Review VPN throughput

B. Check IPS rules

C. Restore static content on lite CDN.

D. Enable secure authentication using NAC

E. Implement advanced WAF rules.

F. Validate MDM asset compliance

Answer: A,F (LEAVE A REPLY)

Review VPN throughput helps identify remote access issues, such as slow or failed application downloads.

Validate MDM asset compliance ensures mobile devices meet security requirements, which can affect access to apps and certificates.

NEW QUESTION: 185

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: 186
A security engineer wants to enhance the security posture of end-user systems in a zero trust environment. Given the following requirements:
- Reduce the ability for potentially compromised endpoints to contact
C2 infrastructure.
- Track the requests that the malware makes to the IPs.
- Avoid the download of additional payloads.
Which of the following should the engineer deploy to meet these requirements?
A. DNS sinkholing
B. Browser isolation
C. Zone transfer protection
D. HIDS
Answer: (SHOW ANSWER)
DNS sinkholing is the best solution to meet these requirements. By redirecting malicious DNS requests (such as those from compromised endpoints attempting to contact command and control (C2) infrastructure) to a "sinkhole" server, the security engineer can prevent communication between the malware and the attacker's infrastructure. Additionally, DNS sinkholing allows for tracking and logging of the requests that the malware attempts to make, while also preventing the malware from downloading additional payloads by blocking these connections.

NEW QUESTION: 187
A global company with a remote workforce implemented a new VPN solution. After deploying the VPN solution to several hundred users, the help desk starts receiving reports of slow access to both internally and externally available applications. A security analyst reviews the following:
VPN client routing:
0.0.0.0/0 eth1
Which of the following solutions should the analyst use to fix this issue?
A. Move the servers to a screened subnet.
B. Enable split tunneling.
C. Configure an NAC solution.
D. Implement DNS over HTTPS.
Answer: (SHOW ANSWER)
Enable split tunneling to resolve the issue of slow access. The current VPN client routing (0.0.0.0/0 routing through the VPN) forces all traffic, both internal and external, through the VPN, leading to slow performance for external applications. Split tunneling allows only internal traffic to go through the VPN, while external traffic bypasses the VPN, improving performance for external applications.

NEW QUESTION: 188
A vulnerability can on a web server identified the following:

```
* TLS 1.2 Cipher Suites:
The server accepted the following 4 cipher suites:
TLS_RSA_WITH_DES_CBC_SHA                56
TLS_RSA_WITH_AES_128_CBC_SHA            128
TLS_RSA_WITH_3DES_EDE_CBC_SHA           168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA       168 DH (1024 bits)
```

Which of the following actions would most likely eliminate on path decryption attacks? (Select two).
A. Disallowing cipher suites that use ephemeral modes of operation for key agreement
B. Removing support for CBC-based key exchange and signing algorithms
C. Adding TLS_ECDHE_ECDSA_WITH_AE3_256_GCMS_HA256
D. Implementing HIPS rules to identify and block BEAST attack attempts
E. Restricting cipher suites to only allow TLS_RSA_WITH_AES_128_CBC_SHA
F. Increasing the key length to 256 for TLS_RSA_WITH_AES_128_CBC_SHA
Answer: (SHOW ANSWER)
On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:
Removing support for CBC-based key exchange and signing algorithms: CBC mode is vulnerable to certain attacks like BEAST. By removing support for CBC-based ciphers, you can eliminate one of the primary vectors for these attacks. Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.
Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256: This cipher suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC.
SHA-256 is a strong hash function that ensures data integrity.

NEW QUESTION: 189
An incident response team completed recovery from offline backup for several workstations. The workstations were subjected to a ransomware attack after users fell victim to a spear-phishing campaign, despite a robust training program. Which of the following questions should be considered during the lessons-learned phase to most likely reduce the risk of reoccurrence?
(Choose two.)
A. Are there opportunities for legal recourse against the originators of the spear-phishing campaign?
B. What internal and external stakeholders need to be notified of the breach?
C. Which methods can be implemented to increase speed of offline backup recovery?
D. What measurable user behaviors were exhibited that contributed to the compromise?
E. Which technical controls, if implemented, would provide defense when user training fails?
F. Which user roles are most often targeted by spear phishing attacks?
Answer: (SHOW ANSWER)
What measurable user behaviors were exhibited that contributed to the compromise?
During the lessons-learned phase, it's important to analyze the specific user behaviors that led to the successful spear-phishing attack, even after a robust training program. This could involve understanding patterns such as clicking on suspicious links, failing to verify emails, or not reporting unusual activity. By identifying these behaviors, the organization can target specific areas for improvement in training or behavior modification.
Which technical controls, if implemented, would provide defense when user training fails?

Since users fell victim to the spear-phishing attack despite training, it's critical to implement technical controls that can provide an additional layer of defense. This may include email filtering to block phishing attempts, multi-factor authentication (MFA), endpoint detection and response (EDR) tools, and sandboxing for suspicious attachments. These controls will help prevent or mitigate attacks when training alone is insufficient.

NEW QUESTION: 190

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: (SHOW ANSWER)
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: 191
A security analyst wants to keep track of all outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT, which of the following would be the best option to inject in the HTTP header to include the real source IP from workstations?
A. X-Forwarded-Proto
B. X-Forwarded-For
C. Cache-Control
D. Strict Transport Security
E. Content-Security-Policy
Answer: (SHOW ANSWER)
The X-Forwarded-For header is specifically designed to carry the original client's IP address through proxy or NAT devices. By having the web filter inject the workstation's real source IP into this header on each HTTP request, downstream systems (like your firewall logs or SIEM) can extract the true client IP instead of the filter's translated address.

NEW QUESTION: 192
The identity and access management team is sending logs to the SIEM for continuous monitoring.
The deployed log collector is forwarding logs to the SIEM. However, only false positive alerts are being generated.
Which of the following is the most likely reason for the inaccurate alerts?
A. The compute resources are insufficient to support the SIEM
B. The SIEM indexes are 100 large
C. The data is not being properly parsed
D. The retention policy is not property configured
Answer: C (LEAVE A REPLY)

Proper parsing of data is crucial for the SIEM to accurately interpret and analyze the logs being forwarded by the log collector. If the data is not parsed correctly, the SIEM may misinterpret the logs, leading to false positives and inaccurate alerts. Ensuring that the log data is correctly parsed allows the SIEM to correlate and analyze the logs effectively, which is essential for accurate alerting and monitoring.

NEW QUESTION: 193
Developers have been creating and managing cryptographic material on their personal laptops fix use in production environment. A security engineer needs to initiate a more secure process.
Which of the following is the best strategy for the engineer to use?
A. Disabling the BIOS and moving to UEFI
B. Managing secrets on the vTPM hardware
C. Employing shielding lo prevent LMI
D. Managing key material on a HSM
Answer: (SHOW ANSWER)
Managing key material on a Hardware Security Module (HSM) is the best strategy to secure cryptographic material. HSMs are specialized devices designed to generate, store, and manage cryptographic keys securely. By using an HSM, the security engineer can ensure that cryptographic keys are protected in a secure, tamper-resistant environment, rather than being stored on developers' personal laptops where they are more vulnerable to theft or mishandling.

NEW QUESTION: 194
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: 195
A compliance officer is facilitating a business impact analysis and wants business unit leaders to collect meaningful data. Several business unit leaders want more information about the types of data the officer needs. Which of the following data types would be the most beneficial for the compliance officer? (Choose two.)
A. Inventory details
B. Applicable contract obligations
C. Costs associated with downtime
D. Network diagrams
E. Contingency plans
F. Critical processes
Answer: (SHOW ANSWER)
Costs associated with downtime help quantify the financial impact of disruptions, which is essential for a business impact analysis (BIA).
Critical processes identify essential functions that must be prioritized for recovery, allowing the compliance officer to assess the consequences of interruptions effectively.

NEW QUESTION: 196
Which of the following best describes a risk associated with using facial recognition to locally authenticate to a mobile device?
A. Data remanence
B. Deepfake
C. Metadata scraping
D. Biometric impersonation
Answer: (SHOW ANSWER)
Biometric impersonation refers to the risk of someone using a photo, video, or other methods to spoof or trick a facial recognition system into authenticating them as the legitimate user. This is a significant concern with facial recognition used for local authentication on mobile devices, as attackers might exploit this vulnerability to gain unauthorized access. Other options such as
"deepfake" could be a method used in biometric impersonation, but the best description of the risk is biometric impersonation itself.

NEW QUESTION: 197
A security manager at a local hospital wants to secure patient medical records. The manager needs to:
- Choose an access control model that clearly defines who has access to sensitive information.
- Prevent those who enter new patient information from specifying who
has access to this data.
Which of the following access control models is the best way to ensure the lowest risk of granting unintentional access?
A. Rule-based
B. Attribute-based
C. Mandatory
D. Discretionary
Answer: C (LEAVE A REPLY)
Mandatory Access Control (MAC) enforces centrally defined policies that determine access to sensitive data, such as medical records. It prevents users who create or enter new data from assigning permissions, thereby reducing the risk of unintentional or improper access.

NEW QUESTION: 198
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: 199
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: 200
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: 201
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: 202
After the latest risk assessment, the Chief Information Security Officer (CISO) decides to meet with the development and security teams to find a way to reduce the security task workload. The CISO would like to:
- Have a solution that uses an API to communicate with other security
tools.
- Use the latest technology possible.
- Have the highest controls possible on the solution.
Which of following is the best option to meet these requirements?
A. EDR
B. CSP
C. SOAR
D. CASB
Answer: (SHOW ANSWER)
A SOAR platform is explicitly built to integrate via APIs with your existing security tools (EDR, SIEM, firewalls, ticketing systems, etc.), orchestrate automated workflows, and apply rich, customizable controls (playbooks, role-based access, audit logging). It's also one of the newest
"X as a Service" technologies in the market for reducing manual security tasks and streamlining incident response.

NEW QUESTION: 203
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: 204

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

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: A,B (LEAVE A REPLY)
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: 205
An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry. Which of the following should the security analyst use to perform threat modeling?
A. ATT&CK
B. OWASP
C. CAPEC
D. STRIDE
Answer: (SHOW ANSWER)
The MITRE ATT&CK framework provides a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs) that can be used for threat modeling. It helps identify gaps in detection capabilities by mapping real-world attack behaviors specific to the industry, making it the most relevant for the task.

NEW QUESTION: 206
A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped. The files were transferred via TLS-protected HTTP sessions from systems that do not normally send traffic to those sites. The technician will define this threat as:
A. A decrypting RSA using an obsolete and weakened encryption attack.
B. A zero-day attack.

C. An advanced persistent threat.
D. An on-path attack.
Answer: (SHOW ANSWER)
The scenario describes a prolonged, stealthy operation where files were exfiltrated over three months via secure channels (TLS-protected HTTP) from unexpected systems, then ceased. This aligns with an Advanced Persistent Threat (APT), characterized by long-term, targeted attacks aimed at data theft or surveillance, often using sophisticated methods to remain undetected.

NEW QUESTION: 207
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: 208
After a vendor identified a recent vulnerability, a severity score was assigned to the vulnerability.
A notification was also publicly distributed. Which of the following would most likely include information regarding the vulnerability and the recommended remediation steps?
A. CCE
B. CPE
C. CVE
D. CVSS
Answer: (SHOW ANSWER)

NEW QUESTION: 209
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: 210

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

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: 211

A security professional is investigating a trend in vulnerability findings for newly deployed cloud systems. Given the following output:

Date	IP address	System name	Finding	Criticality rating
10/13/2023	10.123.34.98	System1	OpenSSL version 1.01	Medium
10/13/2023	10.3.114.72	System6	OpenSSL version 1.01	Medium
10/13/2023	10.12.134.45	System12	Java 11 runtime environment found	Medium
10/13/2023	10.68.65.11	System36	OpenSSL version 1.01	Medium
10/13/2023	10.23.74.9	System37	Java 11 runtime environment found	Medium
10/13/2023	10.13.124.3	System45	OpenSSL version 1.01	Medium

Which of the following actions would address the root cause of this issue?

A. Automating the patching system to update base Images

B. Recompiling the affected programs with the most current patches

C. Disabling unused/unneeded ports on all servers

D. Deploying a WAF with virtual patching upstream of the affected systems

Answer: (SHOW ANSWER)

The output shows that multiple systems have outdated or vulnerable software versions (OpenSSL 1.01 and Java 11 runtime). This suggests that the systems are not being patched regularly or effectively.

Automating the patching system to update base images: Automating the patching process ensures that the latest security updates and patches are applied to all systems, including newly deployed ones. This addresses the root cause by ensuring that base images used for deployment are always up-to-date with the latest security patches.

NEW QUESTION: 212

SIMULATION

You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.

The company's hardening guidelines indicate the following:

- There should be one primary server or service per device.
- Only default ports should be used.
- Non-secure protocols should be disabled.

INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.
For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:
- The IP address of the device
- The primary server or service of the device (Note that each IP should by associated with one service/port only)
- The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines) If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

NMAP Scan Output

```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT     STATE  SERVICE  VERSION
25/tcp   closed smtp     Barracuda Networks Spam Firewall smtpd
415/tcp  open   ssl/smtp smtpd
587/tcp  open   ssl/smtp smtpd
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE  VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp      FileZilla ftpd 0.9.39 beta
22/tcp   closed ssh
80/tcp   open   http     Microsoft IIS httpd 7.5
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
```

Devices Discovered (0)

Add Device For

10.1.45.65
10.1.45.66
10.1.45.67
10.1.45.68

Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Pure-FTPd
443/tcp	open	ssl/http-proxy	SonicWALL SSL-VPN http proxy

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux 2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).

NMAP Scan Output

Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	CrushFTP sftpd (protocol 2.0)
8080/tcp	open	http	CrushFTP web interface

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports

PORT	STATE	SERVICE	VERSION
25/tcp	closed	smtp	Barracuda Networks Spam Firewall smtpd
415/tcp	open	ssl/smtp	smtpd
587/tcp	open	ssl/smtp	smtpd
443/tcp	open	ssl/http	Microsoft IIS httpd 7.5

Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6

Devices Discovered (1)

Add Device For 10.1.45.66

IP Address 10.1.45.65

Role

- SFTP Server
- Email Server
- FTP Server
- UTM Appliance
- Web Server
- Database Server
- AD Server

Disable Protocols

- 20/tcp
- 21/tcp
- 22/tcp
- 25/tcp
- 80/tcp
- 415/tcp

(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9 (Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux 2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE: cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports

PORT	STATE	SERVICE	VERSION
20/tcp	closed	ftp-data	
21/tcp	open	ftp	FileZilla ftpd 0.9.39 beta
22/tcp	closed	ssh	
80/tcp	open	http	Microsoft IIS httpd 7.5
443/tcp	open	ssl/http	Microsoft IIS httpd 7.5
2001/tcp	closed	dc	
2047/tcp	closed	dls	
2196/tcp	closed	unknown	
6001/tcp	closed	X11:1	

Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Pure-FTPd
443/tcp	open	ssl/http-proxy	SonicWALL SSL-VPN http proxy

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux

443/tcp
8080/tcp

Answer:
10.1.45.65 SFTP Server Disable 8080
10.1.45.66 Email Server Disable 415 and 443
10.1.45.67 Web Server Disable 21, 80
10.1.45.68 UTM Appliance Disable 21

NEW QUESTION: 213
A security analyst detected unusual network traffic related to program updating processes. The analyst collected artifacts from compromised user workstations. The discovered artifacts were binary files with the same name as existing valid binaries but with different hashes. Which of the following solutions would most likely prevent this situation from reoccurring?
A. Improving patching processes
B. Implementing digital signature
C. Performing manual updates via USB ports
D. Allowing only dies from internal sources
Answer: (SHOW ANSWER)
Digital signatures ensure the integrity and authenticity of binaries. If binaries are tampered with or replaced by malicious versions, signature verification will fail. This would prevent malicious files with the same name but different hashes from executing, thereby mitigating such attacks.

NEW QUESTION: 214
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

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: 215
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: (SHOW ANSWER)
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: 216
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: A (LEAVE A REPLY)
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: 217
An organization with a remote workforce has a new client with the following requirements:
- Consultants need to travel to the client site.
- The company has proprietary information on its hard drives.
- The company prohibits BYOD.
Which of the following would be the most beneficial for the organization to implement?
A. Measured boot
B. Host-based encryption
C. Secure enclave
D. Virtual hardware
Answer: (SHOW ANSWER)

NEW QUESTION: 218
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: 219
After an incident response exercise, a security administrator reviews the following table:

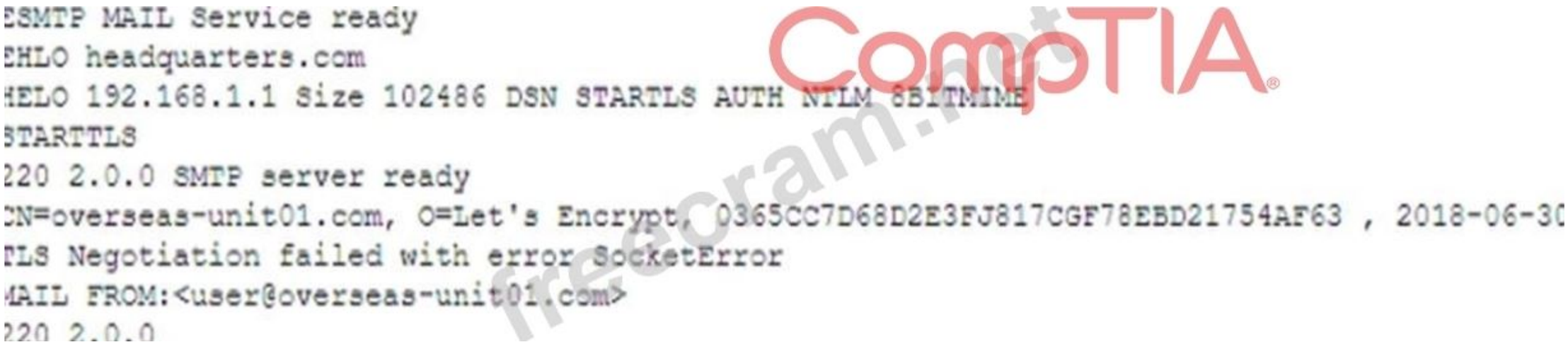
Service	Risk rating	Criticality rating	Alert severity
Public website	Medium	Low	Low
Email	High	High	High
Human resources systems	High	Medium	Medium
Phone system	High	Critical	Critical
Intranet	Low	Low	Low

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: B (LEAVE A REPLY)
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: 220
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: 221
A company that operates in different countries has local email infrastructure for each of its business units. A breach occurred in which email communications were intercepted between the headquarters and one of the overseas business units.
During an investigation, the security analyst finds the following email log:



Which of the following actions should the security analyst take to best address the issue?

A. Revoke the expired TLS certificate and replace it with a valid one

B. Disable the NTLM authentication and replace it with TLS 1.2

C. Change the TLS configuration from opportunistic to enforced

D. Create a new TLS certificate using a stronger algorithm and larger key

Answer: (SHOW ANSWER)

The log shows a STARTTLS negotiation failure followed by email transmission without encryption. This indicates the mail server is using opportunistic TLS, which falls back to plaintext if encryption fails - leaving email vulnerable to interception. Enforcing TLS ensures communication only proceeds if encryption is successful, effectively mitigating this risk.

NEW QUESTION: 222

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: 223

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.