CuramSoftware.CS0-002.v2023-10-26.q112

Exam Code:	CS0-002
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	CompTIA
Free Question Number:	112
Version:	v2023-10-26
# of views:	1165
# of Questions views:	1120
https://www.freepdfdumps.com/CuramSoftware.CS0-002.v2023-10-26.q112.html	

NEW QUESTION: 1
A security analyst is reviewing port scan data that was collected over the course of several months. The following data represents the trends:
Which of the following is the BEST action for the security analyst to take after analyzing the trends?
A. Review the system configurations to determine if port 445 needs to be open.
B. Assume there are new instances of Apache in the environment.
C. Investigate why the number of open SSH ports varied during the six months.
D. Raise a concern to a supervisor regarding possible malicious use Of port 8443.
Answer: C (LEAVE A REPLY)
According to the CompTIA CySA+ Certification Exam Study guide, the best action for the security analyst to take after analyzing the trends is to investigate why the number of open SSH ports varied during the six months. This could indicate that malicious actors are attempting to gain access to the system, and it would be important to find out the root cause of this activity in order to prevent further intrusions. Additionally, raising a concern to a supervisor regarding possible malicious use of port 8443 would also be a prudent step, as this port is often used by attackers. As stated in the study guide, "Monitoring network ports and traffic can provide insight into suspicious activity and may be necessary to identify malicious activities". Additionally, "Ports can be used to gain unauthorized access to a system, so it is important to monitor the ports and to take steps to ensure that only necessary ports are open".

NEW QUESTION: 2
A security analyst wants to capture large amounts of network data that will be analyzed at a later time. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called "packetCapture." The capture must be as efficient as possible, and the analyst wants to minimize the likelihood that packets will be missed. Which of the following commands will best accomplish the analyst's objectives?

A. tcpdump -w packetCapture
B. tcpdump -a packetCapture
C. tcpdump -n packetCapture
D. nmap -v > packetCapture
E. nmap -oA > packetCapture
Answer: (SHOW ANSWER)
The tcpdump command is a network packet analyzer tool that can capture and display network traffic. The -w option specifies a file name to write the captured packets to, in a binary format that can be read by tcpdump or other tools later. This option is useful for capturing large amounts of network data that will be analyzed at a later time, as the question requires. The packet capture does not need to be in a format that is readable by humans, since it will be put into a binary file called "packetCapture". The capture must be as efficient as possible, and the -w option minimizes the processing and output overhead of tcpdump, reducing the likelihood that packets will be missed.

NEW QUESTION: 3
Due to a rise m cyberattackers seeking PHI, a healthcare company that collects highly sensitive data from millions of customers is deploying a solution that will ensure the customers' data is protected by the organization internally and externally Which of the following countermeasures can BEST prevent the loss of customers' sensitive data?
A. Implement privileged access management
B. Implement a risk management process
C. Implement multifactor authentication
D. Add more security resources to the environment
Answer: A (LEAVE A REPLY)
Implementing privileged access management (PAM) would be the best countermeasure to prevent the loss of customers' sensitive data due to a rise in cyberattackers seeking PHI (Protected Health Information). PAM is a solution that helps to control and monitor the access and use of privileged accounts, such as administrator or root accounts, that have elevated permissions or access to sensitive data. PAM can help prevent unauthorized or accidental use of privileged accounts by enforcing strict access policies, such as requiring approval, authentication, or auditing for each access request. PAM can also help rotate or expire the passwords of privileged accounts to reduce the risk of compromise2. PAM can help protect PHI from cyberattackers who may try to exploit privileged accounts to access or exfiltrate sensitive data.

NEW QUESTION: 4
At which of the following phases of the SDLC shoukJ security FIRST be involved?
A. Design
B. Maintenance
C. Implementation
D. Analysis

E. Planning
F. Testing
Answer: E (LEAVE A REPLY)
The software development life cycle (SDLC) is a process that consists of several phases that guide the development of software applications or systems. Security should be involved in every phase of the SDLC, but especially in the planning phase, which is the first phase where the scope, objectives, requirements, and resources of the project are defined. By involving security in the planning phase, potential risks and threats can be identified and mitigated early in the process, which can save time, money, and effort later on. Design, maintenance, implementation, analysis, and testing are other phases of the SDLC, but they are not the first phase where security should be involved. Reference: https://www.bmc.com/blogs/software-development-life-cycle-phases/

NEW QUESTION: 5
Which of the following BEST describes how logging and monitoring work when entering into a public cloud relationship with a service provider?
A. Logging and monitoring are not needed in a public cloud environment
B. Logging and monitoring are done by the data owners
C. Logging and monitoring duties are specified in the SLA and contract
D. Logging and monitoring are done by the service provider
Answer: C (LEAVE A REPLY)
A service level agreement (SLA) and a contract are documents that define the roles and responsibilities of the parties involved in a public cloud relationship. Logging and monitoring are important security activities that should be clearly specified in the SLA and contract, such as who will perform them, what data will be collected, how long will it be stored, and how will it be accessed or shared. Logging and monitoring are still needed in a public cloud environment, but they are not done solely by the data owners or the service provider. Reference: https://www.csoonline.com/article/2121595/what-to-look-for-in-a-cloud-security-sla.html

NEW QUESTION: 6
After a series of Group Policy Object updates, multiple services stopped functioning. The systems administrator believes the issue resulted from a Group Policy Object update but cannot validate which update caused the Issue. Which of the following security solutions would resolve this issue?
A. Privilege management
B. Group Policy Object management
C. Change management
D. Asset management
Answer: C (LEAVE A REPLY)
Change management is a process that ensures changes to systems or processes are introduced in a controlled and coordinated manner. Change management helps to minimize the impact of

changes on the business operations and avoid unintended consequences or errors1 Change management can help resolve the issue of Group Policy Object updates affecting multiple services by ensuring that the updates are properly planned, tested, approved, documented, communicated, and monitored.

NEW QUESTION: 7
An organization has a strict policy that if elevated permissions are needed, users should always run commands under their own account, with temporary administrator privileges if necessary. A security analyst is reviewing syslog entries and sees the following:
Which of the following entries should cause the analyst the MOST concern?
A. <100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM ' su vi httpd.conf' failed for joe
B. <100>2 2020-01-10T20:36:36.0010z financeserver su 201 32001 = BOM ' sudo vi users.txt success
C. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi syslog.conf failed for jos
D. <100> 2020-01-10T19:34..002z financeserver su 201 32001 = BOM ' su vi success
E. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi httpd.conf' success
Answer: D (LEAVE A REPLY)
The syslog entries show the attempts of users to run commands with elevated permissions on two servers: webserver and financeserver. The entries include the date and time, the server name, the command used (su or sudo), the user name, and the outcome (success or failed). The policy of the organization states that users should always run commands under their own account, with temporary administrator privileges if necessary. This means that users should use sudo to run commands as another user (usually root), rather than su to switch to another user's account. Therefore, the entry that should cause the analyst the most concern is D. <100> 2020-01-10T19:34...002z financeserver su 201 32001 = BOM ' su vi success. This entry shows that someone used su to switch to another user's account on the financeserver and successfully edited a file with vi. This could indicate an unauthorized access or a compromised account.

NEW QUESTION: 8
An organization has the following risk mitigation policies
* Risks without compensating controls will be mitigated first it the nsk value is greater than $50,000
* Other nsk mitigation will be pnontized based on risk value.
The following risks have been identified:
Which of the following is the ordei of priority for risk mitigation from highest to lowest?
A. A, C, D, B
B. B, C, D, A
C. C, B, A, D

D. C. D, A, B
E. D, C, B, A
Answer: C (LEAVE A REPLY)
The order of priority for risk mitigation from highest to lowest is C, B, A, D. This order is based on applying the risk mitigation policies of the organization. According to the first policy, risks without compensating controls will be mitigated first if the risk value is greater than $50,000. Risk C has no compensating controls and a risk value of $75,000, so it is the highest priority. Risk B also has no compensating controls, but a risk value of $40,000, so it is the second priority. According to the second policy, other risk mitigation will be prioritized based on risk value. Risk A has a risk value of $60,000 and a compensating control of encryption, so it is the third priority. Risk D has a risk value of $50,000 and a compensating control of backup power supply, so it is the lowest priority.

NEW QUESTION: 9
Which of the following types of controls defines placing an ACL on a file folder?
A. Technical control
B. Confidentiality control
C. Managerial control
D. Operational control
Answer: A (LEAVE A REPLY)
"Technical controls enforce confidentiality, integrity, and availability in the digital space. Examples of technical security controls include firewall rules, access control lists, intrusion prevention systems, and encryption." A technical control is a type of control that uses technology or software to protect data and systems from unauthorized access or misuse3. A technical control can include encryption, authentication, firewalls, antivirus software, and other mechanisms that rely on hardware or software. Placing an ACL (access control list) on a file folder is an example of a technical control. An ACL is a list of permissions that specifies who can access or modify a file or folder4. An ACL can help to enforce confidentiality, integrity, and availability of data by restricting access to authorized users only.

NEW QUESTION: 10
When of the following techniques can be implemented to safeguard the confidentiality of sensitive information while allowing limited access to authorized individuals?
A. Deidentification
B. Hashing
C. Masking
D. Salting
Answer: (SHOW ANSWER)
https://www.techtarget.com/searchsecurity/definition/data-masking
Masking is a technique that involves replacing or hiding some parts of sensitive information with symbols or characters, such as asterisks (*) or Xs. Masking can help safeguard the confidentiality

of sensitive information while allowing limited access to authorized individuals, because it obscures the original data without altering its format or structure. For example, masking can be used to hide some digits of a credit card number or a social security number. Deidentification, hashing, or salting are other techniques that involve transforming or modifying sensitive information, but they do not allow limited access to authorized individuals. Reference: https://www.ibm.com/docs/en/ims/14.1?topic=masking-data

NEW QUESTION: 11
An organization recently discovered that spreadsheet files containing sensitive financial data were improperly stored on a web server. The management team wants to find out if any of these files were downloaded by pubic users accessing the server. The results should be written to a text file and should induce the date. time, and IP address associated with any spreadsheet downloads. The web server's log file Is named webserver log, and the report We name should be accessreport.txt. Following is a sample of the web servefs.log file:
2017-0-12 21:01:12 GET /index.htlm - @4..102.33.7 - return=200 1622
Which of the following commands should be run if an analyst only wants to include entries in which spreadsheet was successfully downloaded?
A. more webserver.log | grep * xls > accessreport.txt
B. more webserver.log > grep "xls > egrep -E 'success' > accessreport.txt
C. more webserver.log | grep ' -E "return=200 | accessreport.txt
D. more webserver.log | grep -A *.xls < accessreport.txt
Answer: C (LEAVE A REPLY)
The grep command is a tool that searches for a pattern of characters in a file or input and prints the matching lines1 The egrep command is a variant of grep that supports extended regular expressions, which allow more complex and flexible pattern matching2 The more command is a filter that displays the contents of a file or input one screen at a time3 The pipe symbol (|) is used to redirect the output of one command to the input of another command. The redirection symbol (>) is used to redirect the output of a command to a file.
The command given in option C performs the following steps:
It uses the more command to display the contents of the webserver.log file.
It pipes the output of the more command to the grep command, which searches for lines that contain '*.xls', which is a pattern that matches any file name ending with .xls (a spreadsheet file extension).
It pipes the output of the grep command to the egrep command, which searches for lines that contain 'return=200', which is a pattern that matches any HTTP status code of 200 (which indicates a successful request).
It redirects the output of the egrep command to a file named accessreport.txt, which contains the date, time, and IP address associated with any spreadsheet downloads.

NEW QUESTION: 12

Industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacker was able to gain access to the SCADA by logging in to an account with weak credentials. Which of the following identity and access management solutions would help to mitigate this risk?

A. Multifactor authentication

B. Manual access reviews

C. Endpoint detection and response

D. Role-based access control

Answer: D (LEAVE A REPLY)

RBAC helps organizations manage access to critical infrastructure networks by assigning access based on roles. This allows organizations to control who can access specific resources and helps eliminate weak credentials that attackers could exploit. Manual reviews and endpoint detection and response can also help to mitigate risk, but role based access control is the best solution for this scenario.

NEW QUESTION: 13

Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?

A. To identify weaknesses in an organization's security posture

B. To identify likely attack scenarios within an organization

C. To build a business security plan for an organization

D. To build a network segmentation strategy

Answer: (SHOW ANSWER)

Threat intelligence can be used to identify likely attack scenarios within an organization based on the organization's specific vulnerabilities, assets, and threat landscape. Threat intelligence can help security teams anticipate and prepare for potential attacks, as well as detect and respond to ongoing attacks more effectively1. Threat intelligence can also provide insights into the threat actors, their motivations, and their tactics, techniques, and procedures (TTPs)2.

NEW QUESTION: 14

While conducting a cloud assessment, a security analyst performs a Prowler scan, which generates the following within the report:

Based on the Prowler report, which of the following is the BEST recommendation?

A. Delete CloudDev access key 1.

B. Delete BusinessUsr access key 1.

C. Delete access key 1.

D. Delete access key 2.

Answer: (SHOW ANSWER)

Prowler is a tool that can scan AWS environments for security issues and compliance violations. The Prowler report shows that there are two access keys for CloudDev user: access key 1 and access key 2. Access key 1 has not been used in more than 90 days, which violates the AWS

CIS benchmark 1.4 (Ensure access keys are rotated every 90 days or less). Therefore, the best recommendation is to delete access key 1 and use access key 2 instead. Deleting CloudDev access key 1, deleting BusinessUsr access key 1, or deleting access key 2 are not appropriate recommendations based on the Prowler report. Reference: https://github.com/toniblyx/prowler

NEW QUESTION: 15
A manufacturing company uses a third-party service provider lor Tier 1 security support One of the requirements is that the provider must only source talent from its own country due to geopolitical and national security interests Which of the following can the manufacturing company implement to ensure the third-party service provider meets this requirement?
A. Implement a secure supply chain program with governance
B. Implement blacklisting for IP addresses from outside the country
C. Implement strong authentication controls for all contractors
D. Implement user behavior analytics for key staff members
Answer: A (LEAVE A REPLY)
Implementing a secure supply chain program with governance would be the best way to ensure the third-party service provider meets the requirement of only sourcing talent from its own country. A secure supply chain program is a set of policies, procedures, and controls that aim to protect the integrity and security of the products and services delivered by third-party vendors. A secure supply chain program can help mitigate the risks of geopolitical and national security interests by verifying the origin, identity, and trustworthiness of the vendors and their employees1. Governance is a key component of a secure supply chain program, as it provides oversight, accountability, and enforcement of the policies and procedures.

NEW QUESTION: 16
A company has a cluster of web servers that is critical to the business. A systems administrator installed a utility to troubleshoot an issue, and the utility caused the entire cluster to 90 offline. Which of the following solutions would work BEST prevent to this from happening again?
A. Change management
B. Application whitelisting
C. Asset management
D. Privilege management
Answer: A (LEAVE A REPLY)
Change Management
o The process through which changes to the configuration of information systems are monitored and controlled, as part of the organization's overall configuration management efforts o Each individual component should have a separate document or database record that describes its initial state and subsequent changes
* Configuration information
* Patches installed
* Backup records

* Incident reports/issues
o Change management ensures all changes are planned and controlled to minimize risk of a service disruption Change management is a process that ensures changes to systems or processes are introduced in a controlled and coordinated manner. Change management helps to minimize the impact of changes on the business operations and avoid unintended consequences or errors3 Change management can help prevent the issue of utility installation affecting the web server cluster by ensuring that the utility is properly planned, tested, approved, documented, communicated, and monitored.

NEW QUESTION: 17
While monitoring the information security notification mailbox, a security analyst notices several emails were repotted as spam. Which of the following should the analyst do FIRST?
A. Block the sender In the email gateway.
B. Delete the email from the company's email servers.
C. Ask the sender to stop sending messages.
D. Review the message in a secure environment.
Answer: D (LEAVE A REPLY)
The security analyst should review the message in a secure environment first. This will help determine if the message is indeed spam or if it contains any malicious content, such as malware attachments or phishing links. Reviewing the message in a secure environment means using a sandbox or an isolated system that can prevent any potential harm to the analyst's system or network. If the message is confirmed to be spam or malicious, then the analyst can take further actions, such as blocking the sender, deleting the email, or notifying the users3.

NEW QUESTION: 18
You are a penetration tester who is reviewing the system hardening guidelines for a company. Hardening guidelines indicate the following.
There must be one primary server or service per device.
Only default port should be used
Non- secure protocols should be disabled.
The corporate internet presence should be placed in a protected subnet
Instructions :

Using the available tools, discover devices on the corporate network and the services running on these devices.
You must determine
ip address of each device
The primary server or service each device
The protocols that should be disabled based on the hardening guidelines
Answer:

NEW QUESTION: 19
A security analyst needs to provide the development learn with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?
A. CASB
B. VPC
C. Federation
D. VPN
Answer: D (LEAVE A REPLY)
What is the difference between VPN and VPC?
Just as a virtual private network (VPN) provides secure data transfer over the public Internet, a VPC provides secure data transfer between a private enterprise and a public cloud provider.
VPN (Virtual Private Network) is a technology that provides secure connectivity from the corporate network to a cloud environment. VPN creates an encrypted tunnel between the two networks, allowing developers to access servers in all three tiers of the cloud environment without exposing their traffic to interception or tampering. VPN can also provide authentication and authorization mechanisms to verify the identity and permissions of the developers.

NEW QUESTION: 20
A security analyst is reviewing the following server statistics:
Which of the following is MOST likely occurring?
A. Race condition
B. Privilege escalation
C. Resource exhaustion
D. VM escape
Answer: (SHOW ANSWER)
Resource exhaustion is most likely occurring on the server. Resource exhaustion is a condition where a system runs out of resources, such as CPU, memory, disk space, or network bandwidth, due to excessive demand or consumption by one or more processes. Resource exhaustion can cause performance degradation, system instability, or denial-of-service. The server statistics show that the CPU usage is 100%, the memory usage is 99%, and the disk usage is 98%. These

indicate that the server is under heavy load and has little or no resources available to handle incoming requests or perform other tasks.

NEW QUESTION: 21
A security analyst is reviewing the network security monitoring logs listed below:
Which of the following is the analyst most likely observing? (Select two).
A. 10.1.1.128 sent potential malicious traffic to the web server.
B. 10.1.1.128 sent malicious requests, and the alert is a false positive
C. 10.1.1.129 successfully exploited a vulnerability on the web server
D. 10.1.1.129 sent potential malicious requests to the web server
E. 10.1.1.129 can determine mat port 443 is being used
F. 10.1.1.130 can potentially obtain information about the PHP version
Answer: (SHOW ANSWER)
A security analyst is reviewing the network security monitoring logs listed below and is most likely observing that 10.1.1.129 sent potential malicious requests to the web server and that 10.1.1.130 can potentially obtain information about the PHP version. The logs show that 10.1.1.129 sent two requests to the web server with suspicious parameters, such as "union select" and "or 1=1", which are commonly used for SQL injection attacks. The logs also show that 10.1.1.130 sent a request to the web server with a parameter "phpinfo", which is a function that displays information about the PHP configuration and environment, which can be useful for attackers to find vulnerabilities or exploit them. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://owasp.org/www-community/attacks/SQL_Injection; https://www.php.net/manual/en/function.phpinfo.php

NEW QUESTION: 22
Which of the following lines from this output most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key?
A. TLS_RSA_WITH_DES_CBC_SHA 56
B. TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits)
C. TLS_RSA_WITH_AES_256_CBC_SHA 256
D. TLS_DHE_RSA_WITH_AES_256_GCM_SHA256 DH (2048 bits)
Answer: B (LEAVE A REPLY)
The line from this output that most likely indicates that attackers could quickly use brute force and determine the negotiated secret session key is TLS_DHE_RSA_WITH_AES_128_CBC_SHA 128 DH (1024 bits). This line indicates that the cipher suite uses Diffie-Hellman ephemeral (DHE) key exchange with RSA authentication, AES 128-bit encryption with cipher block chaining (CBC) mode, and SHA-1 hashing. The DHE key exchange uses a 1024-bit Diffie-Hellman group, which is considered too weak for modern security standards and can be broken by attackers using sufficient computing power. The other lines indicate stronger cipher suites that use longer key lengths or more secure algorithms. Reference: CompTIA Cybersecurity Analyst (CySA+)

Certification Exam Objectives (CS0-002), page 9; https://learn.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

NEW QUESTION: 23
A security analyst is supporting an embedded software team. Which of the following is the best recommendation to ensure proper error handling at runtime?
A. Perform static code analysis.
B. Require application fuzzing.
C. Enforce input validation.
D. Perform a code review.
Answer: (SHOW ANSWER)
Performing a code review is the best recommendation to ensure proper error handling at runtime for an embedded software team. A code review is a process of examining and evaluating source code by one or more developers other than the original author. A code review can help to identify and fix any errors, bugs, vulnerabilities, or inefficiencies in the code before it is deployed or executed. A code review can also help to ensure that the code follows the best practices, standards, and guidelines for error handling at runtime .

NEW QUESTION: 24
An organization announces that all employees will need to work remotely for an extended period of time. All employees will be provided with a laptop and supported hardware to facilitate this requirement. The organization asks the information security division to reduce the risk during this time. Which of the following is a technical control that will reduce the risk of data loss if a laptop is lost or stolen?
A. Requiring the use of the corporate VPN
B. Requiring the screen to be locked after five minutes of inactivity
C. Requiring the laptop to be locked in a cabinet when not in use
D. Requiring full disk encryption
Answer: (SHOW ANSWER)
Full disk encryption (FDE) is a technical control that encrypts all the data on a disk drive, including the operating system and applications. FDE prevents unauthorized access to the data if the disk drive is lost or stolen, as it requires a password or key to decrypt the data. FDE can be implemented using software or hardware solutions and can protect data at rest on laptops and other devices. The other options are not technical controls or do not reduce the risk of data loss if a laptop is lost or stolen. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 10; https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

NEW QUESTION: 25
A cybersecurity analyst is concerned about attacks that use advanced evasion techniques. Which of the following would best mitigate such attacks?

A. Keeping IPS rules up to date
B. Installing a proxy server
C. Applying network segmentation
D. Updating the antivirus software
Answer: A (LEAVE A REPLY)
Keeping IPS rules up to date is the best way to mitigate attacks that use advanced evasion techniques. An IPS (intrusion prevention system) is a security device that monitors network traffic and blocks or prevents malicious activity based on predefined rules or signatures. Advanced evasion techniques are cyberattacks that combine various evasion methods to bypass security detection and protection tools, such as IPS. Keeping IPS rules up to date can help to ensure that the IPS can recognize and block the latest advanced evasion techniques and prevent them from compromising the network .

NEW QUESTION: 26
During a company's most recent incident, a vulnerability in custom software was exploited on an externally facing server by an APT. The lessons-learned report noted the following:
* The development team used a new software language that was not supported by the security team's automated assessment tools.
* During the deployment, the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. Therefore, the vulnerability was not detected.
* The current IPS did not have effective signatures and policies in place to detect and prevent runtime attacks on the new application.
To allow this new technology to be deployed securely going forward, which of the following will BEST address these findings? (Choose two.)
A. Train the security assessment team to evaluate the new language and verify that best practices for secure coding have been followed
B. Work with the automated assessment-tool vendor to add support for the new language so these vulnerabilities are discovered automatically
C. Contact the human resources department to hire new security team members who are already familiar with the new language
D. Run the software on isolated systems so when they are compromised, the attacker cannot pivot to adjacent systems
E. Instruct only the development team to document the remediation steps for this vulnerability
F. Outsource development and hosting of the applications in the new language to a third-party vendor so the risk is transferred to that provider
Answer: A,B (LEAVE A REPLY)
The solution will address the findings that the development team used a new software language that was not supported by the security team's automated assessment tools and the security assessment team was unfamiliar with the new language and struggled to evaluate the software during advanced testing. The training of the security assessment team and working with the

automated assessment-tool vendor to add support for the new language will ensure that future deployments of the new technology are secure and the vulnerabilities are detected and prevented.

NEW QUESTION: 27
A new variant of malware is spreading on the company network using TCP 443 to contact its command-and-control server The domain name used for callback continues to change, and the analyst is unable to predict future domain name variance Which of the following actions should the analyst take to stop malicious communications with the LEAST disruption to service?
A. Implement a sinkhole with a high entropy level
B. Disable TCP/53 at the parameter firewall
C. Block TCP/443 at the edge router
D. Configure the DNS forwarders to use recursion
Answer: A (LEAVE A REPLY)
A sinkhole is a technique that redirects malicious network traffic to a controlled destination, such as a fake server or a black hole. A sinkhole can be used to stop malicious communications with a command-and-control server by preventing the malware from reaching its intended destination. A high entropy level means that the sinkhole can generate random domain names that match the changing domain name used by the malware for callback. Blocking TCP/443 at the edge router, disabling TCP/53 at the perimeter firewall, or configuring the DNS forwarders to use recursion are other possible actions that could stop malicious communications, but they could also disrupt legitimate services that use those protocols or settings. Reference: https://www.cisco.com/c/en/us/about/security-center/dns-sinkholing.html

NEW QUESTION: 28
An analyst receives an alert from the continuous-monitoring solution about unauthorized changes to the firmware versions on several field devices. The asset owners confirm that no firmware version updates were performed by authorized technicians, and customers have not reported any performance issues or outages. Which Of the following actions would be BEST for the analyst to recommend to the asset owners to secure the devices from further exploitation?
A. Change the passwords on the devices.
B. Implement BIOS passwords.
C. Remove the assets from the production network for analysis.
D. Report the findings to the threat intel community.
Answer: (SHOW ANSWER)
If were referring to other devices, yes - Implement BIOS passwords before they are compromised. But the ones that were already compromised, they need to be removed from the system to avoid further exploitation. Plus, if you put a password on there, the attacker may now have your password.
Remove the assets from the production network for analysis. If the analyst receives an alert about unauthorized changes to the firmware versions on several field devices, the best action to

recommend to the asset owners is to remove the assets from the production network for analysis. This would prevent further exploitation of the devices by isolating them from potential attackers and allow the analyst to investigate the source and nature of the unauthorized changes. Changing the passwords on the devices, implementing BIOS passwords, or reporting the findings to the threat intel community are other possible actions, but they are not as effective or urgent as removing the assets from the production network for analysis. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION: 29
As part of an Intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several detrains and reputational information that suggest the company's employees may be targeted for a phishing campaign. Which of the following configuration changes would be the MOST appropriate for Mergence gathering?
A. Update the whitelist.
B. Develop a malware signature.
C. Sinkhole the domains
D. Update the Blacklist
Answer: D (LEAVE A REPLY)
A blacklist is a list of domains, IP addresses, email addresses, or other identifiers that are known or suspected to be malicious or harmful. A blacklist can be used to block or filter unwanted or dangerous traffic from reaching a network or system2 Updating the blacklist can help prevent phishing campaigns by adding the domains or email addresses of the phishing sources to the list and preventing them from sending emails to the company's employees.

NEW QUESTION: 30
A security analyst discovers the company's website is vulnerable to cross-site scripting. Which of the following solutions will best remedy the vulnerability?
A. Prepared statements
B. Server-side input validation
C. Client-side input encoding
D. Disabled JavaScript filtering
Answer: B (LEAVE A REPLY)
Server-side input validation is a solution that can prevent cross-site scripting (XSS) vulnerabilities by checking and filtering any user input that is sent to the server before rendering it on a web page. Server-side input validation can help to ensure that the user input conforms to the expected format, length and type, and does not contain any malicious characters or syntax that may alter the logic or behavior of the web page. Server-side input validation can also reject or sanitize any input that does not meet the validation criteria .

NEW QUESTION: 31

A developer downloaded and attempted to install a file transfer application in which the installation package is bundled with acKvare. The next-generation antivirus software prevented the file from executing, but it did not remove the file from the device. Over the next few days, more developers tried to download and execute the offending file. Which of the following changes should be made to the security tools to BEST remedy the issue?

A. Blacklist the hash in the next-generation antivirus system.

B. Manually delete the file from each of the workstations.

C. Remove administrative rights from all developer workstations.

D. Block the download of the fie via the web proxy

Answer: (SHOW ANSWER)

Blocking the download of the file via the web proxy is the best change to make to the security tools to remedy the issue. A web proxy is a server that acts as an intermediary between a client and a web server, filtering or modifying requests and responses according to predefined rules1. Blocking the download of the file via the web proxy can prevent developers from accessing and executing the offending file that is bundled with adware. This can reduce the risk of infection or compromise of the developer workstations and improve their performance and security. Blacklisting the hash in the next-generation antivirus system (A) is not the best change to make to the security tools to remedy the issue. Blacklisting is a technique that involves blocking or denying access to known malicious or unwanted entities based on their identifiers, such as hashes, IP addresses, domains, etc2. Blacklisting the hash in the next-generation antivirus system can prevent developers from executing the offending file that is bundled with adware, but it does not prevent them from downloading it. This can still consume network bandwidth and disk space and expose developers to potential threats. Manually deleting the file from each of the workstations (B) is not the best change to make to the security tools to remedy the issue. Manually deleting the file from each of the workstations can remove the offending file that is bundled with adware, but it does not prevent developers from downloading it again. This can be a time-consuming and inefficient process that requires human intervention and coordination. Removing administrative rights from all developer workstations is not the best change to make to the security tools to remedy the issue. Removing administrative rights from all developer workstations can limit developers' ability to install or execute unauthorized or malicious applications, such as adware, but it does not prevent them from downloading them. This can also affect developers' productivity and functionality by restricting their access to legitimate applications or settings.

NEW QUESTION: 32
A security analyst is looking at the headers of a few emails that appear to be targeting all users at an organization:
Which of the following technologies would MOST likely be used to prevent this phishing attempt?
A. DNSSEC
B. DMARC
C. STP
D. S/IMAP
Answer: B (LEAVE A REPLY)
DMARC stands for Domain-based Message Authentication, Reporting and Conformance. It is an email authentication protocol that helps prevent spoofing and phishing attacks by verifying that the sender's domain matches the domain in the email header. DMARC also provides a way for domain owners to specify how receivers should handle unauthenticated messages from their domain1

NEW QUESTION: 33
During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following, should the analyst use to extract human-readable content from the partition?
A. strings
B. head
C. fsstat
D. dd
Answer: A (LEAVE A REPLY)
The strings command is a Linux utility that can extract human-readable content from any file or partition3. It can be used to analyze a Linux swap partition by finding text strings that may indicate malicious activity or compromise4. The head command (B) can only display the first few lines of a file or partition, which may not contain any useful information. The fsstat command can only display file system statistics such as size, type, and layout, which may not reveal any human-readable content. The dd command (D) can only copy or convert a file or partition, which may not extract any human-readable content.

NEW QUESTION: 34
A company frequently expenences issues with credential stuffing attacks Which of the following is the BEST control to help prevent these attacks from being successful?
A. SIEM
B. IDS

C. MFA
D. TLS
Answer: C (LEAVE A REPLY)
MFA stands for multi-factor authentication, which is a method of verifying a user's identity by requiring two or more pieces of evidence, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., fingerprint). MFA is the best control to help prevent credential stuffing attacks from being successful, because even if an attacker obtains a valid username and password from a breached site, they would still need another factor to access the target site. SIEM, IDS, and TLS are other security controls, but they are not as effective as MFA for preventing credential stuffing attacks. Reference: https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

NEW QUESTION: 35
A product manager is working with an analyst to design a new application that will perform as a data analytics platform and will be accessible via a web browser. The product manager suggests using a PaaS provider to host the application. Which of the following is a security concern when using a PaaS solution?
A. The use of infrastructure-as-code capabilities leads to an increased attack surface.
B. Patching the underlying application server becomes the responsibility of the client.
C. The application is unable to use encryption at the database level.
D. Insecure application programming interfaces can lead to data compromise.
Answer: (SHOW ANSWER)
Insecure application programming interfaces (APIs) can lead to data compromise when using a PaaS solution. APIs are interfaces that allow applications to communicate with each other and with the underlying platform. APIs can expose sensitive data or functionality to unauthorized or malicious users if they are not properly designed, implemented, or secured. Insecure APIs can result in data breaches, denial of service, unauthorized access, or code injection .

NEW QUESTION: 36
A forensic analyst is conducting an investigation on a compromised server Which of the following should the analyst do first to preserve evidence"
A. Restore damaged data from the backup media
B. Create a system timeline
C. Monitor user access to compromised systems
D. Back up all log files and audit trails
Answer: D (LEAVE A REPLY)
A forensic analyst is conducting an investigation on a compromised server. The first step that the analyst should do to preserve evidence is to back up all log files and audit trails. This will ensure that the analyst has a copy of the original data that can be used for analysis and verification. Backing up the log files and audit trails will also prevent any tampering or modification of the evidence by the attacker or other parties. The other options are not the first steps or may alter or

destroy the evidence. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 16; https://www.nist.gov/publications/guide-collection-and-preservation-digital-evidence

NEW QUESTION: 37
Forming a hypothesis, looking for indicators of compromise, and using the findings to proactively improve detection capabilities are examples of the value of:
A. vulnerability scanning.
B. threat hunting.
C. red learning.
D. penetration testing.
Answer: B (LEAVE A REPLY)
Threat hunting is a proactive process of searching for signs of malicious activity or compromise within a system or network, by using hypotheses, indicators of compromise, and analytical tools. Threat hunting can help improve detection capabilities by identifying unknown threats, uncovering gaps in security controls, and providing insights for remediation and prevention. Vulnerability scanning (A) is a reactive process of scanning systems or networks for known vulnerabilities or weaknesses that can be exploited by attackers. It can help identify and prioritize vulnerabilities, but not proactively hunt for threats. Red teaming is a simulated attack on a system or network by a group of ethical hackers who act as adversaries and try to breach security controls. It can help test the effectiveness of security defenses and response capabilities, but not proactively hunt for threats. Penetration testing (D) is similar to red teaming, but with a more defined scope and objective. It can help evaluate the security of a system or network by simulating real-world attacks and exploiting vulnerabilities, but not proactively hunt for threats.

NEW QUESTION: 38
An organization has a policy that requires servers to be dedicated to one function and unneeded services to be disabled. Given the following output from an Nmap scan of a web server:
Which of the following ports should be closed?
A. 22
B. 80
C. 443
D. 1433
Answer: A (LEAVE A REPLY)
Port 22 is the default port for Secure Shell (SSH), which is a protocol that allows remote access and administration of a server. If the server is dedicated to one function (web server) and unneeded services are disabled, then port 22 should be closed, because SSH is not necessary for a web server and could pose a security risk if exploited. Port 80, port 443, and port 1433 are ports that are needed for a web server, because they are used for HTTP, HTTPS, and SQL Server respectively. Reference: https://www.ssh.com/ssh/port

NEW QUESTION: 39
The Chief information Officer of a large cloud software vendor reports that many employees are falling victim to phishing emails because they appear to come from other employees. Which of the following would BEST prevent this issue
A. Induce digital signatures on messages originating within the company.
B. Require users authenticate to the SMTP server
C. Implement DKIM to perform authentication that will prevent this Issue.
D. Set up an email analysis solution that looks for known malicious links within the email.
Answer: C (LEAVE A REPLY)
DKIM, or DomainKeys Identified Mail, is an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent and authorized by the owner of a domain1 DKIM helps prevent phishing emails that spoof or impersonate other domains by verifying the identity and integrity of the sender. DKIM works by adding a DKIM signature header to each outgoing email message, which contains a hash value of selected parts of the message and the domain name of the sender. The sender's domain also publishes a public key in its DNS records, which can be used by the receiver to decrypt the DKIM signature and compare it with its own hash value of the message. If they match, it means that the message was not altered in transit and that it came from the claimed domain.

NEW QUESTION: 40
A security analyst performs a weekly vulnerability scan on a network that has 240 devices and receives a report with 2.450 pages. Which of the following would most likely decrease the number of false positives?
A. Manual validation
B. Penetration testing
C. A known-environment assessment
D. Credentialed scanning
Answer: (SHOW ANSWER)
Credentialed scanning is a method of vulnerability scanning that uses valid user credentials to access the target systems and perform a more thorough and accurate assessment of their security posture. Credentialed scanning can help to reduce the number of false positives by allowing the scanner to access more information and resources on the systems, such as configuration files, registry keys, installed software, patches, and permissions .

NEW QUESTION: 41
A security analyst is investigating a reported phishing attempt that was received by many users throughout the company The text of one of the emails is shown below:
Office 365 User.
It looks like you account has been locked out Please click this link and follow the pfompts to restore access Regards.
Security Team

Due to the size of the company and the high storage requirements, the company does not log DNS requests or perform packet captures of network traffic, but rt does log network flow data Which of the following commands will the analyst most likely execute NEXT?

A. telnet office365.com 25

B. tracert 122.167.40.119

C. curl http:// accountfix-office365.com/login. php

D. nslookup accountfix-office365.com

Answer: D (LEAVE A REPLY)

nslookup is a command-line tool that can query the Domain Name System (DNS) and display information about domain names and IP addresses. The security analyst can use nslookup to find out the IP address of the malicious domain accountfix-office365.com that was used in the phishing attempt. This could help the analyst to block or trace the source of the attack. telnet, tracert, and curl are other command-line tools, but they are not as useful as nslookup for investigating a phishing attempt based on a domain name. Reference: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup

NEW QUESTION: 42

An analyst determines a security incident has occurred Which of the following is the most appropnate NEXT step in an incident response plan?

A. Consult the malware analysis process

B. Consult the disaster recovery plan

C. Consult the data classification process

D. Consult the communications plan

Answer: D (LEAVE A REPLY)

A communications plan is a document that outlines who should be notified and how during an incident response. It can also specify the roles and responsibilities of the incident response team members, the escalation procedures, and the communication channels. Consulting the communications plan is the most appropriate next step in an incident response plan after determining a security incident has occurred. Consulting the malware analysis process, the disaster recovery plan, or the data classification process may be relevant at later stages of the incident response, but not as the next step. Reference: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION: 43

During a review of recent network traffic, an analyst realizes the team has seen this same traffic multiple times in the past three weeks, and it resulted in confirmed malware activity The analyst also notes there is no other alert in place for this traffic After resolving the security incident, which of the following would be the BEST action for the analyst to take to increase the chance of detecting this traffic in the future?

A. Share details of the security incident with the organization's human resources management team

B. Note the security incident so other analysts are aware the traffic is malicious
C. Communicate the security incident to the threat team for further review and analysis
D. Report the security incident to a manager for inclusion in the daily report
Answer: C (LEAVE A REPLY)
Communicate the security incident to the threat team for further review and analysis. This would allow the threat team to investigate the source and nature of the malicious traffic and create appropriate alerts or signatures to detect it in the future. Sharing details with human resources, noting the incident, or reporting it to a manager would not increase the chance of detection.

NEW QUESTION: 44
An analyst is reviewing the following output as part of an incident:
Which of the Wowing is MOST likely happening?
A. The hosts are part of a reflective denial -of -service attack.
B. Information is leaking from the memory of host 10.20 30.40
C. Sensitive data is being exfilltrated by host 192.168.1.10.
D. Host 291.168.1.10 is performing firewall port knocking.
Answer: (SHOW ANSWER)
The hosts are most likely part of a reflective denial-of-service attack. A reflective denial-of-service attack is a technique that allows attackers to both magnify the amount of malicious traffic they can generate and obscure the sources of the attack traffic. This type of distributed denial-of-service (DDoS) attack overwhelms the target, causing disruption or outage of systems and services. A reflective denial-of-service attack works by spoofing the target's IP address and sending requests to vulnerable servers that will respond to the target. The servers act as reflectors that bounce back the responses to the target, amplifying the attack volume and hiding the attacker's identity1. The output shows that host 10.20.30.40 is sending requests with a spoofed source IP address of 192.168.1.10 to host 203.0.113.15 on port 123, which is used by the Network Time Protocol (NTP). NTP is a common protocol used for reflection/amplification attacks, as it can generate large responses to small requests2.

NEW QUESTION: 45
A security administrator needs to provide access from partners to an Isolated laboratory network inside an organization that meets the following requirements:
* The partners' PCs must not connect directly to the laboratory network.
* The tools the partners need to access while on the laboratory network must be available to all partners
* The partners must be able to run analyses on the laboratory network, which may take hours to complete Which of the following capabilities will MOST likely meet the security objectives of the request?
A. Deployment of a jump box to allow access to the laboratory network and use of VDI in persistent mode to provide the necessary tools for analysis

B. Deployment of a firewall to allow access to the laboratory network and use of VDI in non-persistent mode to provide the necessary tools tor analysis
C. Deployment of a firewall to allow access to the laboratory network and use of VDI In persistent mode to provide the necessary tools for analysis
D. Deployment of a jump box to allow access to the Laboratory network and use of VDI in non-persistent mode to provide the necessary tools for analysis
Answer: D (LEAVE A REPLY)
A jump box is a system that is connected to two networks and acts as a gateway or intermediary between them1. A jump box can help to isolate and secure a network by limiting the direct access to it from other networks. A jump box can also help to monitor and audit the traffic and activity on the network. A VDI (Virtual Desktop Infrastructure) is a technology that allows users to access virtual desktops that are hosted on a server2. A VDI can help to provide users with the necessary tools and applications for analysis without installing them on their own PCs. A VDI can also help to reduce the maintenance and management costs of the desktops. A VDI can operate in two modes: persistent and non-persistent. In persistent mode, each user has a dedicated virtual desktop that retains its settings and data across sessions. In non-persistent mode, each user has a temporary virtual desktop that is deleted or reset after each session3. In this scenario, deploying a jump box to allow access to the laboratory network and using VDI in non-persistent mode can meet the security objectives of the request. The jump box can prevent the partners' PCs from connecting directly to the laboratory network and reduce the risk of unauthorized access or compromise. The VDI in non-persistent mode can provide the necessary tools for analysis without storing any data on the partners' PCs or the virtual desktops. The VDI in non-persistent mode can also allow the partners to run long analyses without losing their progress or results. Deploying a firewall (B) may not be sufficient or effective, as a firewall only filters or blocks traffic based on rules and does not provide access or tools for analysis. Using VDI in persistent mode (A) may not be secure or efficient, as persistent mode stores data on the virtual desktops that may be sensitive or confidential.

NEW QUESTION: 46
A company uses an FTP server to support its critical business functions The FTP server is configured as follows:
* The FTP service is running with (he data duectory configured in /opt/ftp/data.
* The FTP server hosts employees' home aVectories in /home
* Employees may store sensitive information in their home directories
An IoC revealed that an FTP director/ traversal attack resulted in sensitive data loss Which of the following should a server administrator implement to reduce the risk of current and future directory traversal attacks targeted at the FTP server?
A. Implement file-level encryption of sensitive files
B. Reconfigure the FTP server to support FTPS
C. Run the FTP server n a chroot environment
D. Upgrade the FTP server to the latest version

Answer: C (LEAVE A REPLY)
This would limit the FTP server's access to a specific directory tree and prevent directory traversal attacks that could access files outside of that tree. Implementing file-level encryption, supporting FTPS, or upgrading the FTP server would not prevent directory traversal attacks.

NEW QUESTION: 47
A security analyst identified one server that was compromised and used as a data making machine, and a few of the hard drive that was created. Which of the following will MOST likely provide information about when and how the machine was compromised and where the malware is located?
A. System timeline reconstruction
B. System registry extraction
C. Data carving
D. Volatile memory analysts
Answer: (SHOW ANSWER)
System timeline reconstruction is a forensic analysis technique that involves creating a chronological record of events that occurred on a system based on various sources of evidence such as log files, registry entries, file timestamps, network traffic, etc. System timeline reconstruction can provide information about when and how the machine was compromised and where the malware is located by showing when suspicious activities or changes took place on the system, such as unauthorized access attempts, file creation or modification, process execution, network connections, etc.

NEW QUESTION: 48
Given the output below:
#nmap 7.70 scan initiated Tues, Feb 8 12:34:56 2022 as: nmap -v -Pn -p 80,8000,443 --script http-* -oA server.out 192.168.220.42 Which of the following is being performed?
A. Cross-site scripting
B. Local file inclusion attack
C. Log4] check
D. Web server enumeration
Answer: D (LEAVE A REPLY)

Web server enumeration is the process of identifying information about a web server, such as its software version, operating system, configuration, services, and vulnerabilities. This can be done using tools like Nmap, which can scan ports and run scripts to gather information. In this question, the Nmap command is using the -p option to scan ports 80, 8000, and 443, which are commonly used for web services. It is also using the --script option to run scripts that start with http-*, which are related to web server enumeration. The output file name server.out also suggests that the purpose of the scan is to enumerate web servers. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives

NEW QUESTION: 49
During a review of the vulnerability scan results on a server, an information security analyst notices the following:
The MOST appropriate action for the analyst to recommend to developers is to change the web server so:
A. It only accepts TLSvl 2
B. It only accepts cipher suites using AES and SHA
C. It no longer accepts the vulnerable cipher suites
D. SSL/TLS is offloaded to a WAF and load balancer
Answer: (SHOW ANSWER)
A cipher suite is a set of algorithms that defines how the encryption, authentication, and integrity of data are performed during a secure communication session. Some cipher suites are considered vulnerable or weak because they use outdated or insecure algorithms that can be easily broken or compromised by attackers. The vulnerability scan results show that the web server accepts several vulnerable cipher suites, such as RC4, MD5, or DES. The best action for the analyst to recommend to developers is to change the web server so it no longer accepts the vulnerable cipher suites and only accepts the secure ones. Changing the web server so it only accepts TLSv1.2, only accepts cipher suites using AES and SHA, or offloading SSL/TLS to a WAF and load balancer are other possible actions, but they are not as specific or effective as changing the web server so it no longer accepts the vulnerable cipher suites. Reference: https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/

NEW QUESTION: 50
A company experienced a security compromise due to the inappropriate disposal of one of its hardware appliances. Sensitive information stored on the hardware appliance was not removed prior to disposal. Which of the following is the BEST manner in which to dispose of the hardware appliance?
A. Ensure the hardware appliance has the ability to encrypt the data before disposing of it.
B. Dispose of all hardware appliances securely, thoroughly, and in compliance with company policies.

C. Return the hardware appliance to the vendor, as the vendor is responsible for disposal.
D. Establish guidelines for the handling of sensitive information.
Answer: B (LEAVE A REPLY)
Secure and thorough disposal can involve deleting or wiping all data from the hardware appliances, physically destroying or shredding them, or recycling them through certified vendors or programs. Compliance with company policies can help to ensure that the disposal follows the best practices and standards for data protection and environmental responsibility .

NEW QUESTION: 51
A security analyst is correlating, ranking, and enriching raw data into a report that will be interpreted by humans or machines to draw conclusions and create actionable recommendations Which of the following steps in the intelligence cycle is the security analyst performing?
A. Analysis and production
B. Processing and exploitation
C. Dissemination and evaluation
D. Data collection
E. Planning and direction
Answer: (SHOW ANSWER)
Processing and exploitation is the step in the intelligence cycle that involves converting raw data into a format that can be used for analysis and producing intelligence products that can be disseminated to consumers. The security analyst is performing this step by correlating, ranking, and enriching raw data into a report. Analysis and production, dissemination and evaluation, data collection, and planning and direction are other steps in the intelligence cycle, but they do not match the description of the security analyst's task. Reference: https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-cycle.html

NEW QUESTION: 52
As a proactive threat-hunting technique, hunters must develop situational cases based on likely attack scenarios derived from the available threat intelligence information. After forming the basis of the scenario, which of the following may the threat hunter construct to establish a framework for threat assessment?
A. Critical asset list
B. Threat vector
C. Attack profile
D. Hypothesis
Answer: D (LEAVE A REPLY)
A hypothesis is a statement that can be tested by threat hunters to establish a framework for threat assessment. A hypothesis is based on situational awareness and threat intelligence information, and describes a possible attack scenario that may affect the organization. A hypothesis can help to guide threat hunters in their investigation by providing a clear and specific

question to answer, such as "Is there any evidence of lateral movement within our network?" or "Are there any signs of data exfiltration from our servers?".

NEW QUESTION: 53
A company stores all of its data in the cloud. All company-owned laptops are currently unmanaged, and all users have administrative rights. The security team is having difficulty identifying a way to secure the environment. Which of the following would be the BEST method to protect the company's data?
A. Implement UEM on an systems and deploy security software.
B. Implement DLP on all workstations and block company data from being sent outside the company
C. Implement a CASB and prevent certain types of data from being downloaded to a workstation
D. Implement centralized monitoring and logging for an company systems.
Answer: C (LEAVE A REPLY)
A CASB, or Cloud Access Security Broker, is a software tool or service that acts as an intermediary between an organization's cloud services and its users. A CASB can provide various security functions, such as visibility, compliance, threat protection, and data security2 A CASB can help protect the company's data stored in the cloud by preventing certain types of data from being downloaded to a workstation, such as sensitive or confidential information. This can reduce the risk of data leakage, theft, or loss if a workstation is compromised or stolen.
Reference:
Cloud Access Security Broker (CASB): An enterprise management software designed to mediate access to cloud services by users across all types of devices

NEW QUESTION: 54
A security analyst discovers suspicious host activity while performing monitoring activities. The analyst pulls a packet capture for the activity and sees the following:
Which of the following describes what has occurred?
A. The host attempted to download an application from utoftor.com.
B. The host downloaded an application from utoftor.com.
C. The host attempted to make a secure connection to utoftor.com.
D. The host rejected the connection from utoftor.com.
Answer: C (LEAVE A REPLY)
The packet capture shows that the host sent a Client Hello message to utoftor.com on port 443. This message is part of the TLS (Transport Layer Security) handshake protocol, which is used to establish a secure connection between a client and a server1. The Client Hello message contains information such as the supported TLS version, cipher suites, and extensions that the client can use for the secure connection. The server is expected to respond with a Server Hello message that selects the parameters for the secure connection. However, the packet capture does not show any response from the server, which means that the host only attempted to make a secure

connection to utoftor.com, but did not succeed. The host did not download (B) or reject (D) any application from utoftor.com.

NEW QUESTION: 55
In SIEM software, a security analysis selected some changes to hash signatures from monitored files during the night followed by SMB brute-force attacks against the file servers Based on this behavior, which of the following actions should be taken FIRST to prevent a more serious compromise?
A. Fully segregate the affected servers physically in a network segment, apart from the production network.
B. Collect the network traffic during the day to understand if the same activity is also occurring during business hours
C. Check the hash signatures, comparing them with malware databases to verify if the files are infected.
D. Collect all the files that have changed and compare them with the previous baseline
Answer: C (LEAVE A REPLY)
The first action that should be taken to prevent a more serious compromise is to check the hash signatures, comparing them with malware databases to verify if the files are infected. This will help to determine if the changes to hash signatures were caused by malicious software or legitimate updates. If the files are infected, they should be quarantined and removed from the network. Checking the hash signatures will also help to identify the type and source of the malware, which can inform further actions such as blocking malicious domains or IPs, updating antivirus signatures, or notifying users3.

NEW QUESTION: 56
industry partners from critical infrastructure organizations were victims of attacks on their SCADA devices. The attacks used privilege escalation to gain access to SCADA administration and access management solutions would help to mitigate this risk?
A. Multifactor authentication
B. Manual access reviews
C. Endpoint detection and response
D. Role-based access control
Answer: (SHOW ANSWER)
Role-based access control (RBAC) is a method of restricting access to resources based on the roles of users within an organization. RBAC assigns permissions and privileges to roles, rather than individual users, and grants access based on the principle of least privilege3 RBAC can help mitigate the risk of privilege escalation attacks on SCADA devices by ensuring that only authorized users have access to SCADA administration and management functions, and that they have the minimum level of access required to perform their tasks.

NEW QUESTION: 57

A company wants to ensure confidential data from its storage media files is sanitized so the drives cannot oe reused. Which of the following is the BEST approach?

A. Degaussing

B. Shredding

C. Formatting

D. Encrypting

Answer: B (LEAVE A REPLY)

https://legalshred.com/degaussing-vs-hard-drive-shredding/

The best and most secure method of rendering hard drive information completely unusable is to completely destroy it through hard drive shredding Shredding is a method of physically destroying storage media files by cutting them into small pieces using a machine called a shredder. Shredding can ensure that confidential data from storage media files is sanitized so the drives cannot be reused, as it makes it impossible to recover any data from the shredded pieces.

NEW QUESTION: 58

During the forensic analysis of a compromised machine, a security analyst discovers some binaries that are exhibiting abnormal behaviors. After extracting the strings, the analyst finds unexpected content. Which of the following is the next step the analyst should take?

A. Only allow binaries on the approve list to execute.

B. Run an antivirus against the binaries to check for malware.

C. Use file integrity monitoring to validate the digital signature

D. Validate the binaries' hashes from a trusted source.

Answer: D (LEAVE A REPLY)

Validating the binaries' hashes from a trusted source is the next step the analyst should take after discovering some binaries that are exhibiting abnormal behaviors and finding unexpected content in their strings. A hash is a fixed-length value that uniquely represents the contents of a file or message. By comparing the hashes of the binaries on the compromised machine with the hashes of the original or legitimate binaries from a trusted source, such as the software vendor or repository, the analyst can determine whether the binaries have been modified or replaced by malicious code. If the hashes do not match, it indicates that the binaries have been tampered with and may contain malware.

NEW QUESTION: 59

A company offers a hardware security appliance to customers that provides remote administration of a device on the customer's network Customers are not authorized to alter the configuration The company deployed a software process to manage unauthorized changes to the appliance log them, and forward them to a central repository for evaluation Which of the following processes is the company using to ensure the appliance is not altered from its ongmal configured state?

A. CI/CD

B. Software assurance

C. Anti-tamper

D. Change management

Answer: C (LEAVE A REPLY)

Anti-tamper is a process that protects a system or device from unauthorized changes or modifications. It can also log and report any attempts to alter the system or device. The company is using anti-tamper to ensure the appliance is not altered from its original configured state. CI/CD, software assurance, and change management are not processes that specifically deal with unauthorized changes. Reference: https://www.acq.osd.mil/se/briefs/16943-DoD-AT-Overview-Brief.pdf

NEW QUESTION: 60

A security analyst is handling an incident in which ransomware has encrypted the disks of several company workstations. Which of the following would work BEST to prevent this type of Incident in the future?

A. Implement a UTM instead of a stateful firewall and enable gateway antivirus.

B. Back up the workstations to facilitate recovery and create a gold Image.

C. Establish a ransomware awareness program and implement secure and verifiable backups.

D. Virtualize all the endpoints with dairy snapshots of the virtual machines.

Answer: C (LEAVE A REPLY)

Ransomware is a type of malware that encrypts the files or disks of a victim's device and demands a ransom for the decryption key. Ransomware can cause significant damage, disruption, and data loss for individuals and organizations. To prevent this type of incident in the future, the best strategy is to combine user education and data protection. A ransomware awareness program can help users recognize and avoid potential ransomware attacks, such as phishing emails, malicious attachments, or compromised websites. A secure and verifiable backup system can help users recover their data in case of a ransomware infection, without paying the ransom or relying on the attackers. A backup system should be regularly tested and updated, and stored offline or in a separate location from the original data.

NEW QUESTION: 61

White reviewing incident reports from the previous night, a security analyst notices the corporate websites were defaced with po mcai propagand a. Which of the following BEST Describes this type of actor?

A. Hacktivist

B. Nation-state

C. insider threat

D. Organized crime

Answer: A (LEAVE A REPLY)

A hacktivist is a type of actor who uses hacking techniques to promote a political or social cause or agenda. Hacktivists often target websites or systems of organizations or governments that they oppose or disagree with, and deface them with messages or propaganda related to their cause. In this case, the hacktivist defaced the corporate websites with political propaganda.

NEW QUESTION: 62
A company's domain has been spooled in numerous phishing campaigns. An analyst needs to determine the company is a victim of domain spoofing, despite having a DMARC record that should tell mailbox providers to ignore any email that fails DMARC upon review of the record, the analyst finds the following:
Which of the following BEST explains the reason why the company's requirements are not being processed correctly by mailbox providers?
A. The DMARC record's DKIM alignment tag Is incorrectly configured.
B. The DMARC record's policy tag is incorrectly configured.
C. The DMARC record does not have an SPF alignment tag.
D. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.
Answer: B (LEAVE A REPLY)
The DMARC record's policy tag is incorrectly configured and explains why the company's requirements are not being processed correctly by mailbox providers. The policy tag (p) specifies how mailbox providers should handle messages from the domain that fail DMARC checks. The possible values for the policy tag are none, quarantine, or reject1. None means that no action is taken on failed messages and only reports are sent. Quarantine means that failed messages are treated as suspicious and may be filtered or marked as spam. Reject means that failed messages are rejected and not delivered. In this case, the company's DMARC record has a policy tag value of none, which means that mailbox providers will not ignore any email that fails DMARC as required by the company. Instead, mailbox providers will deliver all messages from the domain regardless of their DMARC status and only send reports to the company. To fix this issue, the company should change its policy tag value to reject, which means that mailbox providers will reject and ignore any email that fails DMARC as required by the company. The DMARC record's DKIM alignment tag (A) is not incorrectly configured and does not explain why the company's requirements are not being processed correctly by mailbox providers. The DKIM alignment tag (adkim) specifies how strictly mailbox providers should match DKIM identifiers with From domain identifiers2. The possible values for DKIM alignment tag are s or r. S means strict alignment, which means that DKIM identifiers must exactly match From domain identifiers. R means relaxed alignment, which means that DKIM identifiers must match From domain identifiers at an

organizational level (e.g., subdomain.example.com and example.com are considered aligned). In this case, the company's DMARC record has a DKIM alignment tag value of r, which means that mailbox providers will use relaxed alignment for DKIM verification.

NEW QUESTION: 63
Which of the following solutions is the BEST method to prevent unauthorized use of an API?
A. HTTPS
B. Geofencing
C. Rate liming
D. Authentication
Answer: (SHOW ANSWER)
Authentication is a method of verifying a user's identity by requiring some piece of evidence, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., fingerprint). Authentication is the best method to prevent unauthorized use of an API, because it ensures that only legitimate users can access or use the API functions or data. HTTPS, geofencing, or rate limiting are other methods that can enhance the security or performance of an API, but they do not prevent unauthorized use of an API. Reference: https://www.redhat.com/en/topics/api/what-is-api-security

NEW QUESTION: 64
Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)
A. Kitten
B. Panda
C. Tiger
D. Jackal
E. Bear
F. Spider
Answer: (SHOW ANSWER)
Kitten and Jackal are two APT (Advanced Persistent Threat) adversary archetypes that represent non-nation-state threat actors. APT adversary archetypes are categories of threat actors that share common characteristics, such as motivation, objectives, capabilities, or tactics. APT adversary archetypes can help security analysts understand and prioritize the threats they face2. Kitten is a term used to describe Iranian-based threat actors that are typically not backed by the Iranian government. They are motivated by ideological or religious beliefs and target political or regional adversaries3. Jackal is a term used to describe cybercriminal groups that operate as mercenaries or proxies for other threat actors. They are motivated by financial gain and target various sectors and regions.

NEW QUESTION: 65

Which of the following BEST explains the function of trusted firmware updates as they relate to hardware assurance?

A. Trusted firmware updates provide organizations with development, compilation, remote access, and customization for embedded devices.

B. Trusted firmware updates provide organizations with security specifications, open-source libraries, and custom toots for embedded devices.

C. Trusted firmware updates provide organizations with remote code execution, distribution, maintenance, and extended warranties for embedded devices

D. Trusted firmware updates provide organizations with secure code signing, distribution, installation. and attestation for embedded devices.

Answer: D (LEAVE A REPLY)

The CySA+ exam outline calls out "trusted firmware updates," but trusted firmware itself is more commonly described as part of trusted execution environments (TEEs). Trusted firmware is signed by a chip vendor or other trusted party, and then used to access keys to help control access to hardware. TEEs like those used by ARM processors leverage these technologies to protect the hardware by preventing unsigned code from using privileged features." Trusted firmware updates provide organizations with secure code signing, distribution, installation, and attestation for embedded devices. Embedded devices are devices that have a dedicated function and are part of a larger system or network, such as routers, cameras, sensors, etc. Embedded devices often run on firmware, which is a type of software that controls the device's hardware and functionality. Firmware updates are essential for improving the performance, security, and reliability of embedded devices. However, firmware updates also pose risks of introducing vulnerabilities or malware into the devices if they are not properly secured. Trusted firmware updates are firmware updates that use cryptographic techniques to ensure the integrity, authenticity, and confidentiality of the firmware code and data. Trusted firmware updates typically involve four steps1:

Code signing: The firmware code is digitally signed by the firmware developer or provider using a private key. The digital signature proves that the firmware code is from a trusted source and has not been tampered with.

Distribution: The signed firmware code is securely transmitted to the embedded device or a trusted intermediary (such as a cloud service or a gateway) using encryption or other methods. The transmission ensures that the firmware code is not intercepted or modified by unauthorized parties.

Installation: The embedded device verifies the digital signature of the firmware code using a public key that is stored in a secure location (such as a trusted platform module or TPM). The verification ensures that the firmware code is from a trusted source and has not been tampered with. The embedded device then installs the firmware code and reboots to apply the update.

Attestation: The embedded device reports its firmware status and configuration to a trusted verifier (such as a cloud service or a gateway) using a cryptographic proof. The proof ensures that the embedded device has installed the correct firmware update and has not been compromised.

Trusted firmware updates provide organizations with several benefits for hardware assurance, such as2:
Preventing unauthorized or malicious firmware updates that could compromise the security or functionality of embedded devices Detecting and mitigating firmware attacks or incidents that could affect the availability or performance of embedded devices Complying with regulatory or industry standards or best practices for firmware security Enhancing customer trust and satisfaction with embedded devices Trusted firmware updates do not provide organizations with development, compilation, remote access, or customization for embedded devices (A), as these are software engineering tasks that are not directly related to firmware security. Trusted firmware updates do not provide organizations with security specifications, open-source libraries, or custom tools for embedded devices (B), as these are software resources that are not directly related to firmware security. Trusted firmware updates do not provide organizations with remote code execution, distribution, maintenance, or extended warranties for embedded devices , as these are software features or services that are not directly related to firmware security.

NEW QUESTION: 66
An analyst is responding to an incident within a cloud infrastructure Based on the logs and traffic analysis, the analyst thinks a container has been compromised Which of the following should Ihe analyst do FIRST?
A. Perform threat hunting in other areas of the cloud infrastructure
B. Contact law enforcement to report the incident
C. Perform a root cause analysis on the container and the service logs
D. Isolate the container from production using a predefined policy template
Answer: D (LEAVE A REPLY)
The analyst should isolate the container from production using a predefined policy template first. Isolating the container is a containment measure that can help prevent the spread of the compromise to other containers or systems in the cloud infrastructure. Containment is an important step in the incident response process, as it can limit the impact and damage of an incident. Using a predefined policy template can help automate and standardize the isolation process, ensuring that it is done quickly and consistently1.

NEW QUESTION: 67
An organization wants to move non-essential services into a cloud computing environment. The management team has a cost focus and would like to achieve a recovery time objective of 12 hours. Which of the following cloud recovery strategies would work best to attain the desired outcome?
A. Duplicate all services in another instance and load balance between the instances.
B. Establish a hot site with active replication to another region within the same cloud provider.
C. Set up a warm disaster recovery site with the same cloud provider in a different region.
D. Configure the systems with a cold site at another cloud provider that can be used for failover.
Answer: (SHOW ANSWER)

Setting up a warm disaster recovery site with the same cloud provider in a different region can help to achieve a recovery time objective (RTO) of 12 hours while keeping the costs low. A warm disaster recovery site is a partially configured site that has some of the essential hardware and software components ready to be activated in case of a disaster. A warm site can provide faster recovery than a cold site, which has no preconfigured components, but lower costs than a hot site, which has fully configured and replicated components. Using the same cloud provider can help to simplify the migration and synchronization processes, while using a different region can help to avoid regional outages or disasters .

NEW QUESTION: 68
A security analyst needs to provide the development team with secure connectivity from the corporate network to a three-tier cloud environment. The developers require access to servers in all three tiers in order to perform various configuration tasks. Which of the following technologies should the analyst implement to provide secure transport?
A. CASB
B. VPC
C. Federation
D. VPN
Answer: D (LEAVE A REPLY)
A VPN is a secure network connection that allows users to access their private corporate networks over the internet, while keeping the connection encrypted and secure. This makes it an ideal solution for providing the development team with secure connectivity from the corporate network to a three-tier cloud environment.
https://www.comptia.org/content/virtual-private-networks

NEW QUESTION: 69
A developer is working on a program to convert user-generated input in a web form before it is displayed by the browser. This technique is referred to as:
A. output encoding.
B. data protection.
C. query parameterization.
D. input validation.
Answer: A (LEAVE A REPLY)
Output encoding is a technique that converts user-generated input in a web form before it is displayed by the browser. Output encoding is a form of data sanitization that prevents cross-site scripting (XSS) attacks, which occur when malicious scripts are injected into web pages and executed by unsuspecting users4. Output encoding works by replacing special characters in user input, such as <, >, ", ', &, etc., with their HTML-encoded equivalents, such as <, >, ", ', &, etc. This prevents the browser from interpreting the user input as HTML or JavaScript code and executing it.

NEW QUESTION: 70
While reviewing system logs, a network administrator discovers the following entry:
Which of the following occurred?
A. An attempt was made to access a remote workstation.
B. The PsExec services failed to execute.
C. A remote shell failed to open.
D. A user was trying to download a password file from a remote system.
Answer: (SHOW ANSWER)
The output shows an entry from a system log that indicates a user was trying to download a password file from a remote system using PsExec. PsExec is a command-line tool that allows users to execute processes on remote systems. The entry shows that the user "administrator" tried to run PsExec with the following parameters: \192.168.1.100 -u administrator -p P@ssw0rd -c cmd.exe /c type c:\windows\system32\config\SAM > \192.168.1.101\c$\temp\sam.txt This means that the user tried to connect to the remote system with IP address 192.168.1.100 using the username "administrator" and password "P@ssw0rd", copy cmd.exe to the remote system, and execute it with the command "type c:\windows\system32\config\SAM > \192.168.1.101\c$ \temp\sam.txt". This command attempts to read the SAM file, which contains hashed passwords of local users, and write it to a file on another system with IP address 192.168.1.101. Reference: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives (CS0-002), page 8; https://docs.microsoft.com/en-us/sysinternals/downloads/psexec

NEW QUESTION: 71
A security analyst is concerned the number of security incidents being reported has suddenly gone down. Daily business interactions have not changed, and no following should the analyst review FIRST?
A. The DNS configuration
B. Privileged accounts
C. The IDS rule set
D. The firewall ACL
Answer: (SHOW ANSWER)
The security analyst should review the IDS rule set first. The IDS (Intrusion Detection System) is a tool that monitors network traffic and alerts on any suspicious or malicious activity. The IDS rule set is a set of conditions or patterns that define what constitutes normal or abnormal behavior on the network. The IDS rule set can affect the number of security incidents being reported, as it determines what triggers an alert or not3. The security analyst should review the IDS rule set to check if it is up to date, accurate, and comprehensive. If the IDS rule set is outdated, inaccurate, or incomplete, it may miss some incidents or generate false positives or negatives.

NEW QUESTION: 72

A consultant evaluating multiple threat intelligence leads to assess potential risks for a client. Which of the following is the BEST approach for the consultant to consider when modeling the client's attack surface?

A. Ask for external scans from industry peers, look at the open ports, and compare Information with the client.

B. Discuss potential tools the client can purchase lo reduce the livelihood of an attack.

C. Look at attacks against similar industry peers and assess the probability of the same attacks happening.

D. Meet with the senior management team to determine if funding is available for recommended solutions.

Answer: (SHOW ANSWER)

A good approach for modeling the client's attack surface is to look at attacks against similar industry peers and assess the probability of the same attacks happening. This can help the consultant to identify the most relevant and likely threats for the client based on their industry sector, size, location, and other factors. This can also help the consultant to prioritize the most critical risks and recommend appropriate mitigation strategies. Asking for external scans from industry peers (A) may not be feasible or reliable, as industry peers may not share their scan results or have different security configurations and vulnerabilities than the client. Discussing potential tools the client can purchase (B) may not be effective, as tools alone cannot reduce the likelihood of an attack without proper implementation and management. Meeting with senior management team (D) may not be helpful, as funding is not directly related to modeling the attack surface and may depend on other factors such as budget constraints and risk appetite.

NEW QUESTION: 73

A security analyst needs to determine the best method for securing access to a top-secret datacenter Along with an access card and PIN code, which of the following additional authentication methods would be BEST to enhance the datacenter's security?

A. Physical key

B. Retinal scan

C. Passphrase

D. Fingerprint

Answer: B (LEAVE A REPLY)

A retinal scan is a biometric authentication method that uses the unique pattern of blood vessels in the retina to verify a person's identity. It is considered a strong and reliable authentication method that would enhance the datacenter's security. A physical key, a passphrase, or a fingerprint are other authentication methods, but they are not as secure or reliable as a retinal scan. Reference: https://www.techopedia.com/definition/2586/retinal-scan

NEW QUESTION: 74

Which of the following is the software development process by which function, usability, and scenarios are tested against a known set of base requirements?

A. Security regression testing
B. Code review
C. User acceptance testing
D. Stress testing
Answer: C (LEAVE A REPLY)
"User acceptance testing (UAT) is the last phase of the software testing process. During UAT, actual software users test the software to make sure it can handle required tasks in real-world scenarios, according to specifications." https://www.plutora.com/blog/uat-user-acceptance-testing
User acceptance testing is the software development process by which function, usability, and scenarios are tested against a known set of base requirements. User acceptance testing (UAT) is the final stage of software development before production. It is used to get feedback from users who test the software and its user interface (UI). UAT is usually done manually, with users creating real-world situations and testing how the software reacts and performs. UAT is used to determine if end-users accept software before it's made public. Client or business requirements determine whether it fulfills the expectations originally set in its development2.

NEW QUESTION: 75
A company's security team recently discovered a number of workstations that are at the end of life. The workstation vendor informs the team that the product is no longer supported and patches are no longer available The company is not prepared to cease its use of these workstations
Which of the following would be the BEST method to protect these workstations from threats?
A. Deploy whitelisting to the identified workstations to limit the attack surface
B. Determine the system process centrality and document it
C. Isolate the workstations and air gap them when it is feasible
D. Increase security monitoring on the workstations
Answer: A (LEAVE A REPLY)
Deploying whitelisting to the identified workstations would be the best method to protect these workstations from threats. Whitelisting is a technique that allows only authorized applications, processes, or users to run or access a system or resource. Whitelisting can help limit the attack surface and prevent malware or unauthorized software from running on a system3. Deploying whitelisting to the workstations that are at the end of life can help mitigate the risk of exploitation due to lack of patches or support from the vendor.

NEW QUESTION: 76
Which of the following software assessment methods world peak times?
A. Security regression testing
B. Stress testing
C. Static analysis testing
D. Dynamic analysis testing
E. User acceptance testing
Answer: (SHOW ANSWER)

Stress testing is a software assessment method that tests how an application performs under peak times or extreme workloads. Stress testing can help to identify any performance issues, bottlenecks, errors or crashes that may occur when an application faces high demand or concurrent users. Stress testing can also help to determine the maximum capacity and scalability of an application .

NEW QUESTION: 77
A security analyst is running a tool against an executable of an unknown source. The Input supplied by the tool to the executable program and the output from the executable are shown below:
Which of the following should the analyst report after viewing this Information?
A. A dynamic library that is needed by the executable a missing
B. Input can be crafted to trigger an Infection attack in the executable
C. The toot caused a buffer overflow in the executable's memory
D. The executable attempted to execute a malicious command
Answer: (SHOW ANSWER)
A buffer overflow is a type of attack that exploits a vulnerability in an application or program that does not properly check the size or boundaries of an input. A buffer overflow occurs when an attacker supplies more data than the buffer can hold, causing the excess data to overwrite adjacent memory locations. This can result in unpredictable behavior, such as crashes, errors, data corruption, or execution of malicious code2 The tool that the analyst ran against the executable supplied an input that was too long for the buffer allocated by the executable. This caused a buffer overflow in the executable's memory, as indicated by the error message "Segmentation fault (core dumped)".

NEW QUESTION: 78
An organization prohibits users from logging in to the administrator account. If a user requires elevated permissions. the user's account should be part of an administrator group, and the user should escalate permission only as needed and on a temporary basis. The organization has the following reporting priorities when reviewing system activity:
* Successful administrator login reporting priority - high
* Failed administrator login reporting priority - medium

* Failed temporary elevated permissions - low
* Successful temporary elevated permissions - non-reportable
A security analyst is reviewing server syslogs and sees the following:
Which of the following events is the HIGHEST reporting priority?
A. Option A
B. Option B
C. Option C
D. Option D
Answer: A (LEAVE A REPLY)
Option A shows a successful administrator login from an IP address that is not part of the organization's network. This is a high reporting priority event, because it violates the organization's policy that prohibits users from logging in to the administrator account and it could indicate a compromise of the administrator credentials or a malicious insider. Option B shows a failed administrator login from an IP address that is part of the organization's network. This is a medium reporting priority event, because it could indicate an unauthorized attempt to access the administrator account. Option C shows a failed temporary elevated permission request from a user account that is part of the organization's network. This is a low reporting priority event, because it could indicate a user error or a legitimate need for elevated permission that was denied. Option D shows a successful temporary elevated permission request from a user account that is part of the organization's network. This is a non-reportable event, because it complies with the organization's policy that allows users to escalate permission only as needed and on a temporary basis. Reference: https://www.sans.org/reading-room/whitepapers/logging/detecting-attacks-systems-microsoft-windows-event-logs-2074

NEW QUESTION: 79
The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.
If the venerability is not valid, the analyst must take the proper steps to get the scan clean.
If the venerability is valid, the analyst must remediate the finding.
After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.
INTRUCTIONS:
The simulation includes 2 steps.
Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.
STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.
Answer:

NEW QUESTION: 80

A computer hardware manufacturer developing a new SoC that will be used by mobile devices. The SoC should not allow users or the process to downgrade from a newer firmware to an older one. Which of the following can the hardware manufacturer implement to prevent firmware downgrades?

A. Encryption

B. eFuse

C. Secure Enclave

D. Trusted execution

Answer: (SHOW ANSWER)

An eFuse, or electronic fuse, is a microscopic fuse put into a computer chip that can be blown by applying a high voltage or current. Once blown, an eFuse cannot be reset or repaired, and its state can be read by software or hardware2 An eFuse can be used by a hardware manufacturer to prevent firmware downgrades on a system-on-chip (SoC) that will be used by mobile devices. An eFuse can store information such as the firmware version, security level, or device configuration on the chip. When a newer firmware is installed, an eFuse can be blown to indicate the update and prevent reverting to an older firmware. This can help protect the device from security vulnerabilities, compatibility issues, or unauthorized modifications.

NEW QUESTION: 81

When investigating a compromised system, a security analyst finds the following script in the /tmp directory:

Which of the following attacks is this script attempting, and how can it be mitigated?

A. This is a password-hijacking attack, and it can be mitigated by using strong encryption protocols.

B. This is a password-spraying attack, and it can be mitigated by using multifactor authentication.

C. This is a password-dictionary attack, and it can be mitigated by forcing password changes every 30 days.

D. This is a credential-stuffing attack, and it can be mitigated by using multistep authentication.

Answer: B (LEAVE A REPLY)

https://owasp.org/www-community/attacks/Password_Spraying_Attack

A credential stuffing attack would be using the full credentials and most likely being used across many common platforms. A credential stuffing attack depends on the reuse of passwords. With so many people reusing their passwords for multiple accounts, just one set of credentials is enough to expose most or all of their accounts.

NEW QUESTION: 82

An organization wants to ensure the privacy of the data that is on its systems Full disk encryption and DLP are already in use Which of the following is the BEST option?

A. Require all remote employees to sign an NDA

B. Enforce geofencing to limit data accessibility

C. Require users to change their passwords more frequently

D. Update the AUP to restrict data sharing

Answer: B (LEAVE A REPLY)

Enforcing geofencing to limit data accessibility is the best option to ensure the privacy of the data that is on its systems. Geofencing is a technique that uses GPS or RFID technology to create a virtual geographic boundary around a specific location or area. Geofencing can be used to restrict data accessibility based on the location of the device or user that tries to access it. For example, geofencing can prevent employees from accessing sensitive data when they are outside the office premises or in a different country3. Geofencing can help protect data privacy and comply with data protection regulations that may vary across regions or jurisdictions.

NEW QUESTION: 83

A security analyst is reviewing the output of tcpdump to analyze the type of activity on a packet capture:

Which of the following generated the above output?

A. A port scan

B. A TLS connection

C. A vulnerability scan

D. A ping sweep

Answer: B (LEAVE A REPLY)

A port scan generated the output. A port scan is a type of attack that probes a host or a network for open ports or services. A port scan can help an attacker discover potential vulnerabilities or entry points for further exploitation. The output shows that tcpdump captured packets with different flags, such as SYN, ACK, RST, and FIN, which indicate different stages of the TCP three-way handshake or connection termination. The output also shows that the source IP address 192.168.1.100 sent packets to different destination ports on the target IP address 192.168.1.101, such as 22, 23, 25, 80, and 443. These are common ports that an attacker would scan to find out what services are running on the target.

NEW QUESTION: 84

An organization is developing software to match customers' expectations. Before the software goes into production, it must meet the following quality assurance guidelines

* Uncover all the software vulnerabilities.
* Safeguard the interest of the software's end users.
* Reduce the likelihood that a defective program will enter production.
* Preserve the Interests of me software producer

Which of me following should be performed FIRST?

A. Run source code against the latest OWASP vulnerabilities.

B. Document the life-cycle changes that look place.

C. Ensure verification and vacation took place during each phase.

D. Store the source code in a s oftware escrow.

E. Conduct a static analysis of the code.

Answer: (SHOW ANSWER)
Static analysis of the code is a technique that scans the source code or the compiled code of an application without executing it, to identify potential vulnerabilities, errors, or bugs. Static analysis can help uncover all the software vulnerabilities, safeguard the interest of the software's end users, reduce the likelihood that a defective program will enter production, and preserve the interests of the software producer by improving the quality and security of the code before it is deployed or run1

NEW QUESTION: 85
A company recently experienced a breach of sensitive information that affects customers across multiple geographical regions. Which of the following roles would be BEST suited to determine the breach notification requirements?
A. Legal counsel
B. Chief Security Officer
C. Human resources
D. Law enforcement
Answer: A (LEAVE A REPLY)
A breach notification is a communication to affected individuals or entities that informs them of a security incident involving their personal or sensitive information. A breach notification may include details such as what information was compromised, when and how the incident occurred, what actions are being taken to mitigate the impact, and what steps the recipients should take to protect themselves3 A breach notification may be required by law or regulation, depending on the type and location of the information involved and the jurisdiction of the affected parties. Different countries or regions may have different breach notification requirements, such as who must be notified, when, how, and what information must be disclosed4 Therefore, the best role to determine the breach notification requirements for a company that experienced a breach of sensitive information affecting customers across multiple geographical regions is legal counsel. Legal counsel can advise the company on its legal obligations and liabilities, as well as help draft and deliver appropriate breach notifications.

NEW QUESTION: 86
A security team has begun updating the risk management plan incident response plan and system security plan to ensure compliance with secunty review guidelines Which of the (olowing can be executed by internal managers to simulate and validate the proposed changes'?
A. Internal management review
B. Control assessment
C. Tabletop exercise
D. Peer review
Answer: C (LEAVE A REPLY)
A tabletop exercise is a simulation of a security incident or scenario that involves the participation of key stakeholders and decision-makers. It can be used to test and validate the effectiveness of

the organization's plans, policies, and procedures, such as the risk management plan, incident response plan, and system security plan. A tabletop exercise can also help identify gaps or weaknesses in the plans and improve the communication and coordination among the participants. An internal management review, a control assessment, a peer review, or a scripting are other possible methods to evaluate and validate a new product's security capabilities, but they are not as comprehensive or interactive as a tabletop exercise. Reference: https://www.csoonline.com/article/3444488/what-is-a-tabletop-exercise-how-to-run-a-security-scenario-in-6-steps.html

NEW QUESTION: 87
A security analyst is reviewing the following Internet usage trend report:
Which of the following usernames should the security analyst investigate further?
A. User1
B. User 2
C. User 3
D. User 4
Answer: D (LEAVE A REPLY)
The Internet usage trend report shows that User 4 has an unusually high amount of data downloaded compared to other users. User 4 downloaded 2.5 GB of data in one day, while the average data downloaded by other users was around 0.2 GB. This could indicate that User 4 is engaged in some suspicious or malicious activity, such as downloading unauthorized or illegal content, exfiltrating sensitive data, or installing malware. Therefore, the security analyst should investigate User 4 further to determine the nature and source of the data downloaded.

NEW QUESTION: 88
After a remote command execution incident occurred on a web server, a security analyst found the following piece of code in an XML file:
Which of the following it the BEST solution to mitigate this type of attack?
A. Implement a better level of user input filters and content sanitization.
B. Property configure XML handlers so they do not process sent parameters coming from user inputs.
C. Use parameterized Queries to avoid user inputs horn being processed by the server.
D. Escape user inputs using character encoding conjoined with whitelisting
Answer: A (LEAVE A REPLY)
The piece of code in the XML file is an example of a command injection attack, which is a type of attack that exploits insufficient input validation or output encoding to execute arbitrary commands on a server or system2 The attacker can inject malicious commands into an XML element that is processed by an XML handler on the server, and cause the server to execute those commands. The best solution to mitigate this type of attack is to implement a better level of user input filters and content sanitization, which means checking and validating any user input before processing it, and removing or encoding any potentially harmful characters or commands.

NEW QUESTION: 89
An organization's Cruel Information Security Officer is concerned the proper control are not in place to identify a malicious insider Which of the following techniques would be BEST to identify employees who attempt to steal data or do harm to the organization?
A. Place a text file named Passwords txt on the local file server and create a SIEM alert when the file is accessed
B. Segment the network so workstations are segregated from servers and implement detailed logging on the jumpbox
C. Perform a review of all users with privileged access and monitor web activity logs from the organization's proxy
D. Analyze logs to determine if a user is consuming large amounts of bandwidth at odd hours ol the day
Answer: D (LEAVE A REPLY)
Analyzing logs is a technique that involves collecting and examining data from various sources, such as network devices, servers, applications, or security tools. Analyzing logs can help identify malicious insiders by detecting anomalous or suspicious activities or behaviors, such as consuming large amounts of bandwidth at odd hours of the day, which could indicate data exfiltration or unauthorized access attempts. Placing a text file named Passwords.txt on the local file server and creating a SIEM alert when the file is accessed, segmenting the network so workstations are segregated from servers and implementing detailed logging on the jumpbox, or performing a review of all users with privileged access and monitoring web activity logs from the organization's proxy are other possible techniques to identify malicious insiders, but they are not as effective or reliable as analyzing logs. Reference: https://www.sans.org/reading-room/whitepapers/logging/detecting-attacks-systems-microsoft-windows-event-logs-2074

NEW QUESTION: 90
A code review reveals a web application is using lime-based cookies for session management. This is a security concern because lime-based cookies are easy to:
A. parameterize.
B. decode.
C. guess.
D. decrypt.
Answer: (SHOW ANSWER)
Lime-based cookies are a type of cookies that use lime encoding to store data in a web browser. Lime encoding is a simple substitution cipher that replaces each character in a string with another character based on a fixed key. Lime-based cookies are easy to decode because the key is publicly available and the encoding algorithm is simple. Anyone who intercepts or accesses the lime-based cookies can easily decode them and read the data stored in them. This is a security concern because lime-based cookies are often used for session management, which means they store information about the user's identity and preferences on a web application. If an attacker

can decode the lime-based cookies, they can impersonate the user or access their sensitive information.

NEW QUESTION: 91
A security analyst needs to provide a copy of a hard drive for forensic analysis. Which of the following would allow the analyst to perform the task?
A)
B)
C)
D)
A. Option A
B. Option B
C. Option C
D. Option D
Answer: (SHOW ANSWER)
Option C shows a device that can perform a forensic copy of a hard drive. A forensic copy, also known as a forensic image or a bit-stream image, is an exact, unaltered digital copy of a piece of digital evidence. A forensic copy captures everything on the hard drive, including active and latent data, and preserves the integrity of the original evidence. A forensic copy can be used for forensic analysis without risking any changes to the original drive1. Option C shows a device that can connect to two hard drives and create a forensic copy from one drive to another using a write-blocker. A write-blocker is a tool that prevents any data from being written to the destination drive, ensuring that only a read-only copy is made2.

NEW QUESTION: 92
Which of the following attack techniques has the GREATEST likelihood of quick success against Modbus assets?
A. Remote code execution
B. Buffer overflow
C. Unauthenticated commands
D. Certificate spoofing
Answer: C (LEAVE A REPLY)

Modbus is a communication protocol that is widely used in industrial control systems (ICS). Modbus does not have any built-in security features, such as authentication or encryption, which makes it vulnerable to various attacks. One of the most common and effective attack techniques against Modbus assets is to send unauthenticated commands to manipulate or disrupt the operation of the devices. Remote code execution, buffer overflow, and certificate spoofing are other attack techniques, but they have less likelihood of quick success against Modbus assets. Reference: https://www.sciencedirect.com/science/article/pii/S2405959517300045

NEW QUESTION: 93
An IT security analyst has received an email alert regarding a vulnerability within the new fleet of vehicles the company recently purchased. Which of the following attack vectors is the vulnerability MOST likely targeting?
A. SCADA
B. CAN bus
C. Modbus
D. IoT
Answer: B (LEAVE A REPLY)
The Controller Area Network - CAN bus is a message-based protocol designed to allow the Electronic Control Units (ECUs) found in today's automobiles, as well as other devices, to communicate with each other in a reliable, priority-driven fashion. Messages or "frames" are received by all devices in the network, which does not require a host computer.
CAN bus stands for Controller Area Network bus, which is a communication protocol that allows different devices and components in a vehicle to communicate and exchange data. The vulnerability within the new fleet of vehicles is most likely targeting the CAN bus, because it could allow an attacker to manipulate or disrupt the operation of the vehicle. SCADA, Modbus, and IoT are other terms related to communication protocols or systems, but they are not specific to vehicles. Reference: https://www.csoonline.com/article/3218104/what-is-a-can-bus-and-how-can-it-be-hacked.html

NEW QUESTION: 94
A company's Chief Information Officer wants to use a CASB solution to ensure policies are being met during cloud access. Due to the nature of the company's business and risk appetite, the management team elected to not store financial information in the cloud. A security analyst needs to recommend a solution to mitigate the threat of financial data leakage into the cloud. Which of the following should the analyst recommend?
A. Utilize the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises.
B. Do not utilize the CASB solution for this purpose, but add DLP on premises for data in motion.
C. Utilize the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud.
D. Do not utilize the CASB solution for this purpose, but add DLP on premises for data at rest.

Answer: (SHOW ANSWER)
"CASB solutions generally offer their own DLP policy engine, allowing you to configure DLP policies in a CASB and apply them to cloud services."
https://www.mcafee.com/blogs/enterprise/cloud-security/how-a-casb-integrates-with-an-on-premises-dlp-solution/ CASB stands for Cloud Access Security Broker, which is a solution that monitors and controls the access and usage of cloud services by an organization's users. DLP stands for Data Loss Prevention, which is a solution that prevents unauthorized disclosure or leakage of sensitive data. Utilizing the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud is the best recommendation for a security analyst to mitigate the threat of financial data leakage into the cloud, because it would prevent users from uploading or transferring financial information to cloud services that are not authorized or secure. Utilizing the CASB to enforce DLP data-at-rest protection for financial information that is stored on premises, not utilizing the CASB solution for this purpose but adding DLP on premises for data in motion or data at rest are other possible recommendations, but they are not as effective or relevant as utilizing the CASB to enforce DLP data-in-motion protection for financial information moving to the cloud. Reference: https://www.csoonline.com/article/3200344/what-is-a-casb-and-why-do-you-need-one.html

NEW QUESTION: 95
A security team has begun updating the risk management plan, incident response plan, and system security plan to ensure compliance with security review guidelines. Which of the following can be executed by internal managers to simulate and validate the proposed changes?
A. Internal management review
B. Control assessment
C. Tabletop exercise
D. Peer review
Answer: (SHOW ANSWER)
According to the CompTIA CySA+ Certification Exam (CS0-002) study guide, a tabletop exercise can be executed by internal managers to simulate and validate changes to the risk management plan, incident response plan, and system security plan. In a tabletop exercise, participants discuss and work through a simulated scenario, usually in a classroom or conference room setting, to evaluate their readiness and understanding of the proposed changes. This type of exercise can help to identify any potential issues or gaps in the proposed changes and can provide valuable insights for refining and improving the plans.

NEW QUESTION: 96
A security analyst is reviewing the following server statistics:
Which of the following Is MOST likely occurring?
A. Race condition
B. Privilege escalation
C. Resource exhaustion

D. VM escape

Answer: C (LEAVE A REPLY)

Resource exhaustion occurs when a system runs out of resources such as memory, CPU, disk space, or network bandwidth due to excessive demand or poor management1. In this case, the server statistics show that the CPU usage is 100%, the memory usage is 99%, and the disk usage is 98%, indicating that the system is suffering from resource exhaustion. This can affect the performance and availability of the system and its applications. A race condition (A) is a condition where the system's behavior depends on the sequence or timing of other uncontrollable events2. Privilege escalation (B) is a situation where an attacker gains unauthorized access to higher privileges or permissions on a system3. VM escape (D) is a technique where an attacker breaks out of a virtual machine and interacts with the host operating system.

NEW QUESTION: 97

Which of the following is MOST important when developing a threat hunting program?

A. Understanding penetration testing techniques

B. Understanding how to build correlation rules within a SIEM

C. Understanding security software technologies

D. Understanding assets and categories of assets

Answer: D (LEAVE A REPLY)

Understanding assets and categories of assets is most important when developing a threat hunting program. Assets are anything that have value to an organization, such as data, systems, networks, applications, devices, people, processes, or reputation. Categories of assets are groups of assets that share common characteristics or attributes, such as type, function, location, owner, or criticality. Understanding assets and categories of assets can help to identify and prioritize the potential targets and impact of threats in an organization. Understanding assets and categories of assets can also help to determine and apply appropriate security controls and measures for each asset or category. Understanding assets and categories of assets can also help to collect and analyze relevant data and indicators for each asset or category during threat hunting activities. Understanding penetration testing techniques (A) is not most important when developing a threat hunting program. Penetration testing techniques are methods or tools that are used to simulate attacks on a system or network to evaluate its security posture and identify vulnerabilities or weaknesses. Penetration testing techniques can help to validate and improve the security of an organization, but they are not directly related to threat hunting activities. Penetration testing techniques are reactive rather than proactive approaches to security. Understanding how to build correlation rules within a SIEM (B) is also not most important when developing a threat hunting program. Correlation rules are logic statements that define relationships or patterns between different events or data points in a system or network. A SIEM (Security Information and Event Management) is a software solution that collects, analyzes, and correlates data from various sources in an organization to provide security monitoring and alerting capabilities1. Correlation rules can help to detect and respond to known threats in an organization, but they are not sufficient for threat hunting activities. Correlation rules are based on

predefined criteria rather than hypotheses or assumptions about unknown threats. Understanding security software technologies is also not most important when developing a threat hunting program. Security software technologies are applications or programs that provide security functions or features for an organization, such as antivirus software, firewalls, encryption software, VPNs (Virtual Private Networks), etc2. Security software technologies can help to protect an organization from various threats, but they are not essential for threat hunting activities. Security software technologies are based on signatures or heuristics rather than indicators of compromise or behavioral analysis.

NEW QUESTION: 98
A security engineer is reviewing security products that identify malicious actions by users as part of a company's insider threat program. Which of the following is the most appropriate product category for this purpose?
A. SCAP
B. SOAR
C. UEBA
D. WAF
Answer: C (LEAVE A REPLY)
UEBA stands for User and Entity Behavior Analytics, which is a category of security products that use machine learning and statistical analysis to identify malicious actions by users or entities on a network. UEBA products can detect anomalous or suspicious behaviors that deviate from normal patterns or baselines, such as data exfiltration, privilege escalation, unauthorized access, insider threats, or compromised accounts. UEBA products can also provide alerts, reports, or recommendations for response actions based on the detected behaviors.

NEW QUESTION: 99
A Chief Executive Officer (CEO) is concerned about the company's intellectual property being leaked to competitors. The security team performed an extensive review but did not find any indication of an outside breach. The data sets are currently encrypted using the Triple Data Encryption Algorithm. Which of the following courses of action is appropriate?
A. Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.
B. Enable data masking and reencrypt the data sets using AES-256.
C. Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.
D. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.
Answer: B (LEAVE A REPLY)
Data masking is a technique that replaces sensitive data with fictitious but realistic data, thus preventing unauthorized access to the original data. Reencrypting the data sets using AES-256

would provide a stronger level of encryption than Triple DES, which has been deprecated by NIST due to its vulnerability to attacks12

NEW QUESTION: 100
A security analyst is performing a Diamond Model analysis of an incident the company had last quarter. A potential benefit of this activity is that it can identify:
A. detection and prevention capabilities to improve.
B. which systems were exploited more frequently.
C. possible evidence that is missing during forensic analysis.
D. which analysts require more training.
E. the time spent by analysts on each of the incidents.
Answer: A (LEAVE A REPLY)
A Diamond Model analysis of an incident is a framework that identifies the four essential features of an attack: adversary, capability, infrastructure, and victim1 By analyzing these features and their relationships, a security analyst can gain insights into the attack's objectives, methods, sources, and targets. A potential benefit of this activity is that it can identify detection and prevention capabilities to improve, such as gaps in security controls, indicators of compromise, or mitigation strategies2

NEW QUESTION: 101
An internally developed file-monitoring system identified the following except as causing a program to crash often:
Which of the following should a security analyst recommend to fix the issue?
A. Open the access.log file ri read/write mode.
B. Replace the strcpv function.
C. Perform input samtizaton
D. Increase the size of the file data buffer
Answer: B (LEAVE A REPLY)
The security analyst should recommend replacing the strcpy function with a safer alternative. The strcpy function is a C library function that copies a string from one buffer to another. However, this function does not check the size of the destination buffer, which can lead to buffer overflow vulnerabilities if the source string is longer than the destination buffer. Buffer overflow vulnerabilities can allow attackers to execute arbitrary code or crash the program. A safer alternative to strcpy is strncpy, which limits the number of characters copied to the size of the destination buffer.

NEW QUESTION: 102
Which of the following BEST describes what an organizations incident response plan should cover regarding how the organization handles public or private disclosures of an incident?
A. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.

B. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures.
C. The disclosure section should include the names and contact information of key employees who are needed for incident resolution
D. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening m the future.
Answer: (SHOW ANSWER)
The disclosure section of an organization's incident response plan should cover how the organization handles public or private disclosures of an incident. The disclosure section should contain the organization's legal and regulatory requirements regarding disclosures, such as the type, content, format, timing, and recipients of the disclosures. The disclosure section should also specify the roles and responsibilities of the personnel involved in the disclosure process, such as who is authorized to make or approve disclosures, who is responsible for communicating with internal and external stakeholders, and who is accountable for ensuring compliance with the disclosure requirements. The disclosure section should not focus on how to reduce the likelihood customers will leave due to the incident (A), as this is a business objective rather than a disclosure requirement. The disclosure section should not include the names and contact information of key employees who are needed for incident resolution , as this is an operational detail rather than a disclosure requirement. The disclosure section should not contain language explaining how the organization will reduce the likelihood of the incident from happening in the future (D), as this is a remediation action rather than a disclosure requirement.

NEW QUESTION: 103
A security technician configured a NIDS to monitor network traffic. Which of the following is a condition in which harmless traffic is classified as a potential network attack?
A. True positive
B. True negative
C. False positive
D. False negative
Answer: C (LEAVE A REPLY)
A false positive is a condition in which harmless traffic is classified as a potential network attack by a NIDS. A NIDS is a network intrusion detection system that monitors network traffic for any signs of malicious or anomalous activity. A false positive can result in unnecessary alerts or actions by the NIDS, such as blocking legitimate traffic or generating false alarms. False positives can be caused by various factors, such as misconfigured rules, outdated signatures, noisy network traffic or benign anomalies3 .

NEW QUESTION: 104
The security team decides to meet informally to discuss and test the response plan for potential security breaches and emergency situations. Which of the following types of training will the security team perform?

A. Tabletop exercise
B. Red-team attack
C. System assessment implementation
D. Blue-team training
E. White-team engagement
Answer: A (LEAVE A REPLY)
A tabletop exercise is a type of training used to assess an organization's preparedness in responding to emergencies and security breaches. It involves discussing various scenarios and simulating how the organization would react in each situation.
https://www.comptia.org/content/tabletop-exercises.

NEW QUESTION: 105
A security analyst was transferred to an organization's threat-hunting team to track specific activity throughout the enterprise environment The analyst must observe and assess the number ot times this activity occurs and aggregate the results. Which of the following is the BEST threat-hunting method for the analyst to use?
A. Stack counting
B. Searching
C. Clustering
D. Grouping
Answer: A (LEAVE A REPLY)
Stack counting is the best threat-hunting method for the analyst to use to observe and assess the number of times a specific activity occurs and aggregate the results. Stack counting is a technique that involves collecting data from multiple sources, such as logs, events, or alerts, and grouping them by a common attribute, such as an IP address, a user name, or a process name. Stack counting can help identify patterns, trends, outliers, or anomalies in the data that may indicate malicious activity or compromise.

NEW QUESTION: 106
A product security analyst has been assigned to evaluate and validate a new products security capabilities Part of the evaluation involves reviewing design changes at specific intervals tor security deficiencies recommending changes and checking for changes at the next checkpoint Which of the following BEST defines the activity being conducted?
A. User acceptance testing
B. Stress testing
C. Code review
D. Security regression testing
Answer: C (LEAVE A REPLY)
Once the SDLC reached the development phase, code starts to be generated. That means that the ability to control the version of the software or component that your team is working on,

combined with check-in/check-out functionality and revision histories, is a necessary and powerful tool when developing software.
The question refers to a "new" product so I believe that is key. However, it also makes it seem that it is about the development of a product that could be in production.
Regression testing focuses on testing to ensure that changes that have been made do not create new issues, and ensure that no new vulnerabilities, misconfigurations, or other issues have been introduced.
A code review is a process that involves examining and evaluating the source code of a software application or system for security deficiencies, errors, bugs, or vulnerabilities. A code review can help improve the quality and security of the software product by identifying and fixing issues before they become operational problems. A code review is part of the evaluation and validation of a new product's security capabilities. User acceptance testing, stress testing, or security regression testing are other types of testing that can be used to evaluate and validate a new product's security capabilities, but they do not involve reviewing design changes at specific intervals for security deficiencies. Reference: https://www.synopsys.com/blogs/software-security/code-review/

NEW QUESTION: 107
A company's legal department is concerned that its incident response plan does not cover the countless ways security incidents can occur. The department has asked a security analyst to help tailor the response plan to provide broad coverage for many situations. Which of the following is the best way to achieve this goal?
A. Focus on incidents that have a high chance of reputation harm.
B. Focus on common attack vectors first.
C. Focus on incidents that affect critical systems.
D. Focus on incidents that may require law enforcement support.
Answer: C (LEAVE A REPLY)
An incident response plan should cover the most important and likely scenarios that could compromise the security and operations of an organization. According to various sources of best practices123, an incident response plan should start by conducting a risk assessment to identify potential threats and vulnerabilities, and prioritize the critical systems that need to be protected and restored in case of an incident. Focusing on incidents that affect critical systems ensures that

the incident response plan covers the most severe and impactful situations that could harm the organization's mission, reputation, or legal obligations.

NEW QUESTION: 108
An organizational policy requires one person to input accounts payable and another to do accounts receivable. A separate control requires one person to write a check and another person to sign all checks greater than $5,000 and to get an additional signature for checks greater than $10,000. Which of the following controls has the organization implemented?
A. Segregation of duties
B. Job rotation
C. Non-repudiaton
D. Dual control
Answer: (SHOW ANSWER)
Segregation of duties is a security control that requires multiple people to be involved with completing a task. This helps prevent fraud, as it ensures that no one individual has the ability to commit fraud or make mistakes without other people being aware of it

NEW QUESTION: 109
An incident response team is responding to a breach of multiple systems that contain Pll and PHI Disclosure of the incident to external entities should be based on:
A. the responder's discretion.
B. the public relations policy.
C. the communication plan.
D. the senior management team's guidance.
Answer: (SHOW ANSWER)
The communication plan is an important part of incident response, as it outlines how and when information about the incident should be shared with external entities.
A communication plan is a set of procedures and protocols that define how an organization should communicate with external entities during times of emergency or security incident. The plan typically outlines how and when information about the incident should be shared, and ensures that any relevant stakeholders are informed of the incident in a timely manner. It also serves as a guide for determining what information to share with outside parties. Here is a link to an article from CompTIA's website about the importance of a communication plan for incident response for your reference: https://www.comptia.org/content/incident-response-communication-plan

NEW QUESTION: 110
A security analyst identified some potentially malicious processes after capturing the contents of memory from a machine during incident response. Which of the following procedures is the NEXT step for further in investigation?
A. Data carving

B. Timeline construction
C. File cloning
D. Reverse engineering
Answer: D (LEAVE A REPLY)
Reverse engineering is a process of analyzing a system or a component to understand how it works and how it was made. Reverse engineering can be used to examine malicious processes captured from memory and determine their functionality, origin, and purpose. Reverse engineering can help identify the type of malware, its infection vector, its capabilities, its communication methods, and its indicators of compromise2

NEW QUESTION: 111
A security analyst is investigate an no client related to an alert from the threat detection platform on a host (10.0 1.25) in a staging environment that could be running a cryptomining tool because it in sending traffic to an IP address that are related to Bitcoin.
The network rules for the instance are the following:
Which of the following is the BEST way to isolate and triage the host?
A. Remove rules 1.2. and 3.
B. Remove rules 1.2. 4. and 5.
C. Remove rules 1.2. 3.4. and 5.
D. Remove rules 1.2. and 5.
E. Remove rules 1.4. and 5.
F. Remove rules 4 and 5
Answer: C (LEAVE A REPLY)
The best way to isolate and triage the host is to remove rules 1, 2, 3, 4, and 5. These rules allow inbound and outbound traffic on ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) from any source or destination. By removing these rules, the security analyst can block any network communication to or from the host, preventing any further data exfiltration or malware infection. This will also allow the security analyst to perform a forensic analysis on the host without any interference from external sources.

NEW QUESTION: 112
A SIEM analyst receives an alert containing the following URL:
Which of the following BEST describes the attack?
A. Password spraying
B. Buffer overflow
C. insecure object access
D. Directory traversal
Answer: D (LEAVE A REPLY)
A directory traversal attack is a type of web application attack that exploits insufficient input validation or filtering to access files or directories that are outside of the web root folder. A directory traversal attack can allow an attacker to read, modify, or execute files on the target

server that are not intended to be accessible via web requests. The URL in the alert contains an example of a directory traversal attack, as indicated by the use of ".../" sequences in the query string. These sequences are used to navigate up one level in the directory hierarchy, potentially reaching sensitive files or folders on the server. In this case, the attacker is trying to access /etc/passwd file, which contains user account information on Linux systems.