CuramSoftware.CS0-002.v2023-03-21.q254

Exam Code:	CS0-002
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	CompTIA
Free Question Number:	254
Version:	v2023-03-21
# of views:	2961
# of Questions views:	2540
https://www.freepdfdumps.com/CuramSoftware.CS0-002.v2023-03-21.q254.html	

NEW QUESTION: 1
As part of the senior leadership team's ongoing nsk management activities the Chief Information Security Officer has tasked a security analyst with coordinating the right training and testing methodology to respond to new business initiatives or significant changes to existing ones The management team wants to examine a new business process that would use existing infrastructure to process and store sensitive data Which of the following would be appropnate for the security analyst to coordinate?
A. A tabletop exercise
B. A business impact analysis
C. A black-box penetration testing engagement
D. Threat modeling
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
A security analyst found an old version of OpenSSH running on a DMZ server and determined the following piece of code could have led to a command execution through an integer overflow;
Which of the following controls must be in place to prevent this vulnerability?
A. Use built-in functions from libraries to check and handle long numbers properly.
B. Implement float numbers instead of integers to prevent integer overflows.
C. Convert all integer numbers in strings to handle the memory buffer correctly.
D. Sanitize user inputs, avoiding small numbers that cannot be handled in the memory.
Answer: (SHOW ANSWER)

NEW QUESTION: 3
After a breach involving the exfiltration of a large amount of sensitive data a security analyst is reviewing the following firewall logs to determine how the breach occurred:
Which of the following IP addresses does the analyst need to investigate further?

A. 192.168.1.193
B. 192.168.1.12
C. 192.168.1.1
D. 192.168.1.10
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
An information security analyst is working with a data owner to identify the appropriate controls to preserve the confidentiality of data within an enterprise environment One of the primary concerns is exfiltration of data by malicious insiders Which of the following controls is the MOST appropriate to mitigate risks?
A. Data loss prevention
B. Data deduplication
C. OS fingerprinting
D. Digital watermarking
Answer: (SHOW ANSWER)

NEW QUESTION: 5
A Chief Information Secunty Officer has asked for a list of hosts that have critical and high-seventy findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?
A. Prowler
B. Nessus
C. Fuzzer
D. Nikto
E. Wireshark
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
The SOC has received reports of slowness across all workstation network segments. The currently installed antivirus has not detected anything, but a different anti-malware product was just downloaded and has revealed a worm is spreading Which of the following should be the NEXT step in this incident response?
A. Enable an ACL on all VLANs to contain each segment
B. Send a sample of the malware to the antivirus vendor and request urgent signature creation.
C. Compile a list of loCs so the IPS can be updated to halt the spread.
D. Begin deploying the new anti-malware on all uninfected systems.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 7
Which of the following is MOST closely related to the concept of privacy?

A. An individual's control over personal information
B. A policy implementing strong identity management processes
C. A system's ability to protect the confidentiality of sensitive information
D. The implementation of confidentiality, integrity, and availability
Answer: A (LEAVE A REPLY)
Explanation
"Privacy refers to whatever control you have over your personal information and how it is utilized."

NEW QUESTION: 8
In system hardening, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?
A. Unauthenticated
B. OWASP ZAP
C. Burp Suite
D. SCAP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
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)
Explanation
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

NEW QUESTION: 10
A hybrid control is one that:
A. is implemented at the enterprise and system levels
B. has operational and technical components
C. is implemented differently on individual systems
D. authenticates using passwords and hardware tokens
Answer: A (LEAVE A REPLY)

NEW QUESTION: 11

A cyber-security analyst is implementing a new network configuration on an existing network access layer to prevent possible physical attacks. Which of the following BEST describes a solution that would apply and cause fewer issues during the deployment phase?
A. Deploy network address protection with DHCP and dynamic VLANs.
B. Implement software-defined networking and security groups for isolation
C. Configure 802.1X and EAPOL across the network
D. Implement port security with one MAC address per network port of the switch.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12
A company wants to configure the environment to allow passive network monitonng. To avoid disrupting the sensitive network, which of the following must be supported by the scanner's NIC to assist with the company's request?
A. Promiscuous mode
B. Port mirroring
C. Full-duplex mode
D. Tunnel all mode
E. Port bridging
Answer: (SHOW ANSWER)

NEW QUESTION: 13
A security analyst reviews SIEM logs and discovers the following error event:
Which of the following environments does the analyst need to examine to continue troubleshooting the event?
A. DNS server
B. Windows domain controller
C. Proxy server
D. SQL server
E. WAF appliance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
An organization has not had an incident for several month. The Chief information Security Officer (CISO) wants to move to proactive stance for security investigations. Which of the following would BEST meet that goal?
A. Active response
B. Threat hunting
C. Information-sharing community
D. Root-cause analysis
E. Advanced antivirus
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.
Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?
A. Log correlation, monitoring, and automated reporting through a SIEM platform
B. Continuous compliance monitoring using SCAP dashboards
C. Development of a hypothesis as part of threat hunting
D. Quarterly vulnerability scanning using credentialed scans
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
During an incident investigation, a security analyst discovers the web server is generating an unusually high volume of logs The analyst observes the following response codes:
* 20% of the logs are 403
* 20% of the logs are 404
* 50% of the logs are 200
* 10% of the logs are other codes
The server generates 2MB of logs on a daily basis, and the current day log is over 200MB. Which of the following commands should the analyst use to identify the source of the activity?
A. cat access_log lgrep " 100 "
B. cat access_log lgrep " 204 "
C. cat access_log lgrep " 403 "
D. cat access_log lgrep " 200 "
E. cat access_log lgrep " 4 04 "
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
A security analyst is reviewing the following server statistics:
Which of the following Is MOST likely occurring?
A. Privilege escalation

B. Race condition
C. VM escape
D. Resource exhaustion
Answer: (SHOW ANSWER)

NEW QUESTION: 18
A development team signed a contract that requires access to an on-premises physical server. Access must be restricted to authorized users only and cannot be connected to the Internet. Which of the following solutions would meet this requirement?
A. Air gap the server.
B. Virtualize the server.
C. Establish a hosted SSO.
D. Implement a CASB.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Welcome to the Enterprise Help Desk System. Please work the ticket escalated to you in the desk ticket queue.
INSTRUCTIONS
Click on me ticket to see the ticket details Additional content is available on tabs within the ticket First, select the appropriate issue from the drop-down menu. Then, select the MOST likely root cause from second drop-down menu If at any time you would like to bring back the initial state of the simulation, please click the Reset All button
Answer:
Explanation

NEW QUESTION: 20
The help desk provided a security analyst with a screenshot of a user's desktop:
For which of the following is aircrack-ng being used?
A. Rainbow attack
B. Wireless access point discovery
C. Brute-force attack
D. PCAP data collection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?
A. Pause the virtual machine.
B. Shut down the virtual machine.
C. Take a snapshot of the virtual machine.

D. Remove the NIC from the virtual machine.

Answer: (SHOW ANSWER)

Explanation

Enumeration is the process of discovering and listing information. Network enumeration is the process of discovering pieces of information that might be helpful in a network attack or compromise. There are several techniques used to perform enumeration and several tools that make the process easier for both testers and attackers. Let's take a look at these techniques and tools.

NEW QUESTION: 22

A company's blocklist has outgrown the current technologies in place. The ACLs are at maximum, and the IPS signatures only allow a certain amount of space for domains to be added, creating the need for multiple signatures. Which of the following configuration changes to the existing controls would be the MOST appropriate to improve performance?

A. Implement a host-file-based solution that will use a list of all domains to deny for all machines on the network.

B. Create an IDS for the current blocklist to determine which domains are showing activity and may need to be removed

C. Review the current blocklist and prioritize it based on the level of threat severity. Add the domains with the highest severity to the blocklist.

D. Review the current blocklist to determine which domains can be removed from the list and then update the ACLs

Answer: D (LEAVE A REPLY)

Explanation

This is the most effective way to improve performance, as it allows you to reduce the amount of domains in the blocklist and reduce the size of the ACLs. By reviewing the blocklist and removing domains that are no longer active or no longer pose a threat, the blocklist can be reduced and the ACLs updated accordingly. This will reduce the amount of traffic and processing power required to manage the blocklist, and can help improve overall performance.

NEW QUESTION: 23

During an incident investigation, a security analyst acquired a malicious file that was used as a backdoor but was not detected by the antivirus application. After performing a reverse-engineering procedure, the analyst found that part of the code was obfuscated to avoid signature detection. Which of the following types of instructions should the analyst use to understand how the malware was obfuscated and to help deobfuscate it?

A. MOVL

B. XOR

C. ADD

D. MOV

E. SUB

Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
An analyst is working with a network engineer to resolve a vulnerability that was found in a piece of legacy hardware, which is critical to the operation of the organization's production line. The legacy hardware does not have third-party support, and the OEM manufacturer of the controller is no longer in operation. The analyst documents the activities and verifies these actions prevent remote exploitation of the vulnerability.
Which of the following would be the MOST appropriate to remediate the controller?
A. Install an IDS on the network between the switch and the legacy equipment.
B. Remove the legacy hardware from the network.
C. Replace the equipment that has third-party support.
D. Segment the network to constrain access to administrative interfaces.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
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: (SHOW ANSWER)
Explanation
https://www.stickmancyber.com/cybersecurity-blog/7-threat-hunting-misconceptions
https://www.simplilearn.com/skills-to-become-threat-hunter-article

NEW QUESTION: 26
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. MFA
B. TLS
C. IDS
D. SIEM
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
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. Perform input samtizaton
B. Increase the size of the file data buffer

C. Open the access.log file ri read/write mode.
D. Replace the strcpv function.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 28
Which of the following sources would a security analyst rely on to provide relevant and timely threat information concerning the financial services industry?
A. Real-time and automated firewall rules subscriptions
B. Common vulnerability and exposure bulletins
C. Open-source intelligence, such as social media and blogs
D. Information sharing and analysis membership
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
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. Clustering
B. Searching
C. Stack counting
D. Grouping
Answer: (SHOW ANSWER)

NEW QUESTION: 30
An organization's internal department frequently uses a cloud provider to store large amounts of sensitive data.
A threat actor has deployed a virtual machine to at the use of the cloud hosted hypervisor, the threat actor has escalated the access rights. Which of the following actions would be BEST to remediate the vulnerability?
A. Sandbox the virtual machine.
B. Implement an MFA solution.
C. Update lo the secure hypervisor version.
D. Implement dedicated hardware for each customer.
Answer: C (LEAVE A REPLY)
Explanation
MFA can be used to reduce the likelihood that the attacker gains access to the VM, however, the scenario specifically states that the attacker was able to escalate rights and the question asks what can be done to remediate the vulnerability. the vulnerability in this case would be the ability to escalate rights.

NEW QUESTION: 31
A system is experiencing noticeably slow response times, and users are being locked out frequently. An analyst asked for the system security plan and found the system comprises two servers: an application server in the DMZ and a database server inside the trusted domain. Which of the following should be performed NEXT to investigate the availability issue?
A. Review syslogs from critical servers.
B. Perform fuzzing.
C. Review the firewall logs.
D. Install a WAF in front of the application server.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
A cyber-incident response analyst is investigating a suspected cryptocurrency miner on a company's server.
Which of the following is the FIRST step the analyst should take?
A. Take a memory snapshot of the machine to capture volatile information stored in memory.
B. Start packet capturing to look for traffic that could be indicative of command and control from the miner.
C. Create a full disk image of the server's hard drive to look for the file containing the malware.
D. Run a manual antivirus scan on the machine to look for known malicious software.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
A security analyst received an email with the following key:
Xj3XJ3LLc
A second security analyst received an email with following key:
3XJ3xjcLLC
The security manager has informed the two analysts that the email they received is a key that allows access to the company's financial segment for maintenance. This is an example of:
A. separation of duties
B. private key encryption
C. dual control

D. two-factor authentication
E. public key encryption
Answer: C (LEAVE A REPLY)

NEW QUESTION: 34
During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect.
Which of the following is the BEST place to acquire evidence to perform data carving?
A. The system memory
B. The hard drive
C. Network packets
D. The Windows Registry
Answer: A (LEAVE A REPLY)
Reference: https://resources.infosecinstitute.com/memory-forensics/#gref
https://www.computerhope.com/jargon/d/data-carving.htm

NEW QUESTION: 35
A developer wrote a script to make names and other Pll data unidentifiable before loading a database export into the testing system Which of the following describes the type of control that is being used?
A. Data classification
B. Data loss prevention
C. Data masking
D. Data encoding
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
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. Add more security resources to the environment
B. Implement a risk management process
C. Implement privileged access management
D. Implement multifactor authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 37
A host is spamming the network unintentionally. Which of the following control types should be used to address this situation?
A. Corrective

B. Technical
C. Managerial
D. Operational
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
An organization developed a comprehensive modern response policy Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?
A. Completion of annual information security awareness training by ail employees
B. External and internal penetration testing by a third party
C. Completion of lessons-learned documentation by the computer security incident response team
D. Tabtetop activities involving business continuity team members
E. A simulated breach scenario evolving the incident response team
Answer: E (LEAVE A REPLY)

NEW QUESTION: 39
A development team is testing a new application release. The team needs to import existing client PHI data records from the production environment to the test environment to test accuracy and functionality.
Which of the following would BEST protect the sensitivity of this data while still allowing the team to perform the testing?
A. Encryption
B. Watermarking
C. Encoding
D. Deidentification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security To BEST complete this task, the analyst should place the:
A. firewall behind the VPN server
B. VPN on the firewall
C. VPN server behind the firewall
D. VPN server parallel to the firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
While investigating reports or issues with a web server, a security analyst attempts to log in remotely and recedes the following message:

The analyst accesses the server console, and the following console messages are displayed:
The analyst is also unable to log in on the console. While reviewing network captures for the server, the analyst sees many packets with the following signature:
Which of the following is the BEST step for the analyst to lake next in this situation?
A. Cryptomining malware is running on the server and utilizing an CPU and memory. Reboot the server and disable any cron Jobs or startup scripts that start the mining software.
B. After ensuring network captures from the server are saved isolate the server from the network take a memory snapshot, reboot and log in to do further analysis.
C. Corporate data is being exfilltrated from the server Reboot the server and log in to see if it contains any sensitive data.
D. Load the network captures into a protocol analyzer to further investigate the communication with
128.30.100.23, as this may be a botnet command server
Answer: D (LEAVE A REPLY)

NEW QUESTION: 42
A vulnerability assessment solution is hosted in the cloud This solution will be used as an accurate inventory data source for both the configuration management database and the governance nsk and compliance tool An analyst has been asked to automate the data acquisition
Which of the following would be the BEST way to acqutre the data'
A. CSV export
B. SOAR
C. API
D. Machine learning
Answer: (SHOW ANSWER)
Explanation
An example of API is google weather app, using the weather channel's API to collect accurate weather data and broadcast it on goggle weather app, so google doesn't have to do it their selves

NEW QUESTION: 43
A user receives a potentially malicious email that contains spelling errors and a PDF document. A security analyst reviews the email and decides to download the attachment to a Linux sandbox for review.
Which of the following commands would MOST likely indicate if the email is malicious?
A. file ~/Desktop/file.pdf
B. strings ~/Desktop/file.pdf | grep "<script"
C. cat < ~/Desktop/file.pdf | grep -i .exe
D. sha256sum ~/Desktop/file.pdf
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44

An organization was alerted to a possible compromise after its proprietary data was found for sale on the Internet. An analyst is reviewing the logs from the next-generation UTM in an attempt to find evidence of this breach. Given the following output:
Which of the following should be the focus of the investigation?
A. ftps.bluemed.net
B. webserver.org-dmz.org
C. sftp.org-dmz.org
D. 83hht23.org-int.org
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
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 BusinessUsr access key 1.
B. Delete access key 1.
C. Delete CloudDev access key 1.
D. Delete access key 2.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
A remote code-execution vulnerability was discovered in the RDP for the servers running a key-hosted application. While there is no automated check for this vulnerability from the vulnerability assessment vendor, the in-house technicians were able to evaluate manually whether this vulnerability was present through the use of custom scripts. This evaluation determined that all the hosts are vulnerable. A technician then tested the patch for this vulnerability and found that it can cause stability issues in the key-hosted application. The application is accessed through RDP to a jump host that does not run the application directly. To mitigate this vulnerability, the security operations team needs to provide remediation steps that will mitigate the vulnerability temporarily until the compatibility issues with the patch are resolved. Which of the following will BEST allow systems to continue to operate and mitigate the vulnerability in the short term?
A. Implement IPSec rules on the jump host server through a GPO that limits RDP access from only the other application servers. Do not patch the jump host. Since it does not run the application natively, it is at less risk of being compromised. Patch the application servers to secure them.
B. Implement IPSec rules on the application servers through a GPO that limits RDP access to only other application servers. Do not patch the jump host. Since it does not run the application natively, it is at less risk of being compromised. Patch the application servers to secure them.
C. Implement IPSec rules on the application servers through a GPO that limits RDP access from only the jump host. Patch the jump host. Since it does not run the application natively, it will not

affect the software's operation and functionality. Do not patch the application servers until the compatibility issue is resolved.
D. Implement firewall rules on the application servers through a GPO that limits RDP access to only other application servers. Manually check the jump host to see if it has been compromised. Patch the application servers to secure them.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
An organization is experiencing security incidents in which a systems administrator is creating unauthorized user accounts A security analyst has created a script to snapshot the system configuration each day. Following iss one of the scripts:
This script has been running successfully every day. Which of the following commands would provide the analyst with additional useful information relevant to the above script?
A)
B)
C)
D)
A. Option D
B. Option C
C. Option B
D. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 48
A security analyst is researching ways to improve the security of a company's email system to mitigate emails that are impersonating company executives. Which of the following would be BEST for the analyst to configure to achieve this objective?
A. A sandbox to check incoming mad
B. Domain Keys identified Man
C. DNSSEC keys to secure replication
D. A TXT record on the name server for SPF
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
A cybersecurity analyst is responding to an incident. The company's leadership team wants to attribute the incident to an attack group. Which of the following models would BEST apply to the situation?
A. Kill chain
B. MITRE ATT&CK
C. Diamond Model of Intrusion Analysis
D. Intelligence cycle
Answer: C (LEAVE A REPLY)

NEW QUESTION: 50
The steering committee for information security management annually reviews the security incident register for the organization to look for trends and systematic issues The steering committee wants to rank the risks based on past incidents to improve the security program for next year Below is the incident register for the organization.
Which of the following should the organization consider investing in FIRST due to the potential impact of availability?
A. Hire a managed service provider to help with vulnerability management
B. Build a warm site in case of system outages
C. Invest in a failover and redundant system, as necessary
D. Hire additional staff for the IT department to assist with vulnerability management and log review
Answer: C (LEAVE A REPLY)
Explanation
Both on July 31 and November 24, the organization could not restore multiple days due to missing disaster recovery plan. Therefore, failover systems are very important for this organization.

NEW QUESTION: 51
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 application is unable to use encryption at the database level.
B. The use of infrastructure-as-code capabilities leads to an increased attack surface.
C. Insecure application programming interfaces can lead to data compromise.
D. Patching the underlying application server becomes the responsibility of the client.
Answer: (SHOW ANSWER)

NEW QUESTION: 52

A security analyst needs to identify possible threats to a complex system a client is developing. Which of the following methodologies would BEST address this task?
A. Open Source Security Information Management (OSSIM)
B. Open Web Application Security Project (OWASP)
C. Software Assurance Maturity Model (SAMM)
D. Spoofing, Tampering. Repudiation, Information disclosure. Denial of service, Elevation of privileges (STRIDE)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
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. Input can be crafted to trigger an Infection attack in the executable
B. The executable attempted to execute a malicious command
C. The toot caused a buffer overflow in the executable's memory
D. A dynamic library that is needed by the executable a missing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 54
During an investigation, an analyst discovers the following rule in an executive's email client:
IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com> SELECT FROM 'sent' THEN DELETE FROM <executive@anycompany.com> The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?
A. Remove the rule from the email client and change the password
B. Recommend that management implement SPF and DKIM
C. Use the SIEM to correlate logging events from the email server and the domain server
D. Check the server logs to evaluate which emails were sent to <someaddress@domain.com>
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
Which of the following BEST describes HSM?
A. A computing device that manages cryptography, decrypts traffic, and maintains library calls
B. A computing device that manages digital keys, performs encryption/decryption functions, and maintains other cryptographic functions
C. A computing device that manages algorithms, performs entropy functions, and maintains digital signatures
D. A computing device that manages physical keys, encrypts devices, and creates strong cryptographic functions

Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
A security analyst has discovered trial developers have installed browsers on all development servers in the company's cloud infrastructure and are using them to browse the Internet. Which of the following changes should the security analyst make to BEST protect the environment?
A. Remove the administrator profile from the developer user group in identity and access management
B. Place a jumpbox m between the developers' workstations and the development VPC
C. Create an alert that is triggered when a developer installs an application on a server
D. Create a security rule that blocks Internet access in the development VPC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
The Cruel Executive Officer (CEO) of a large insurance company has reported phishing emails that contain malicious links are targeting the entire organza lion Which of the following actions would work BEST to prevent against this type of attack?
A. Turn on full behavioral analysis to avert an infection
B. Implement an EDR mail module that will rewrite and analyze email links.
C. Reconfigure the EDR solution to perform real-time scanning of all files
D. Ensure EDR signatures are updated every day to avert infection.
E. Modify the EDR solution to use heuristic analysis techniques for malware.
Answer: B (LEAVE A REPLY)
Explanation
If you're concerned about spear phishing and other advanced threats that may impact your organization, a next-gen EDR endpoint protection platform offers a lot of advantages over traditional antivirus.

NEW QUESTION: 58
Which of the following should be found within an organization's acceptable use policy?
A. Customer data must be handled properly, stored on company servers, and encrypted when possible
B. Administrator accounts must be audited monthly, and inactive accounts should be removed.
C. Passwords must be eight characters in length and contain at least one special character.
D. Consequences of violating the policy could include discipline up to and including termination.
Answer: (SHOW ANSWER)

NEW QUESTION: 59
During a review of SIEM alerts, a securrty analyst discovers the SIEM is receiving many alerts per day from the file-integrity monitoring toot about files from a newly deployed application that should

not change. Which of the following steps should the analyst complete FIRST to respond to the issue7

A. Check if temporary files are being monitored

B. Open a ticket informing the development team about the alerts

C. Warn the incident response team that the server can be compromised

D. Dismiss the alert, as the new application is still being adapted to the environment

Answer: C (LEAVE A REPLY)

NEW QUESTION: 60

Which of me following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

A. The devices may have weak or known passwords.

B. Message queuing telemetry transport does not support encryption.

C. The devices are not compatible with TLS 12.

D. The devices may cause a dramatic Increase in wireless network traffic.

E. The devices may utilize unsecure network protocols.

F. Multiple devices may interface with the functions of other IoT devices.

Answer: (SHOW ANSWER)

NEW QUESTION: 61

A security analyst reviews a recent network capture and notices encrypted inbound traffic on TCP port 465 was coming into the company's network from a database server. Which of the following will the security analyst MOST likely identify as the reason for the traffic on this port?

A. A connection from the database to the web front end is communicating on the port

B. Someone has configured an unauthorized SMTP application over SSL

C. The server is receiving a secure connection using the new TLS 1.3 standard

D. The traffic is common static data that Windows servers send to Microsoft

Answer: B (LEAVE A REPLY)

NEW QUESTION: 62

A threat feed notes malicious actors have been infiltrating companies and exfiltration data to a specific set of domains Management at an organization wants to know if it is a victim Which of the

following should the security analyst recommend to identity this behavior without alerting any potential malicious actors?

A. Query DNS logs with a SIEM tool for any hosts requesting the malicious domains and create alerts based on this information

B. Look up the IP addresses for these domains and search firewall logs for any traffic being sent to those IPs over port 443

C. Create an IPS rule to block these domains and trigger an alert within the SIEM tool when these domains are requested

D. Add the domains to a DNS sinkhole and create an alert m the SIEM toot when the domains are queried

Answer: (SHOW ANSWER)

NEW QUESTION: 63

Which of the following policies would state an employee should not disable security safeguards, such as host firewalls and antivirus on company systems?

A. Account management policy

B. Password policy

C. Code of conduct policy

D. Acceptable use policy

Answer: (SHOW ANSWER)

NEW QUESTION: 64

When attempting to do a stealth scan against a system that does not respond to ping, which of the following Nmap commands BEST accomplishes that goal?

A. nmap -sS -O <system> -P0

B. nmap -sT -O <system> -P0

C. nmap -sQ -O <system> -P0

D. nmap -sA -O <system> -noping

Answer: A (LEAVE A REPLY)

NEW QUESTION: 65

Which of the following technologies can be used to store digital certificates and is typically used in high-security implementations where integrity is paramount?

A. eFuse

B. UEFI

C. Self-encrypting drive

D. HSM

Answer: (SHOW ANSWER)

NEW QUESTION: 66

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: A (LEAVE A REPLY)
Explanation
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: 67
In web application scanning, static analysis refers to scanning:
A. the system for vulnerabilities before installing the application.
B. the compiled code of the application to detect possible issues.
C. an application that is installed and active on a system.
D. an application that is installed on a system that is assigned a static IP.
Answer: (SHOW ANSWER)
Explanation
This type of analysis is performed before the application is installed and active on a system, and it involves examining the code without actually executing it in order to identify potential vulnerabilities or security risks.
As per CYSA+ 002 Study Guide: Static analysis is conducted by reviewing the code for an application. Static analysis does not run the program; instead, it focuses on understanding how the program is written and what the code is intended to do.

NEW QUESTION: 68
When reviewing a compromised authentication server, a security analyst discovers the following hidden file:
Further analysis shows these users never logged in to the server. Which of the following types of attacks was used to obtain the file and what should the analyst recommend to prevent this type of attack from reoccurring?
A. A rainbow tables attack was used to compromise the accounts. The analyst should recommend that future password hashes contains a salt.

B. A password spraying attack was used to compromise the passwords. The analyst should recommend that all users receive a unique password.
C. A rogue LDAP server is installed on the system and is connecting passwords. The analyst should recommend wiping and reinstalling the server.
D. A phishing attack was used to compromise the account. The analyst should recommend users install endpoint protection to disable phishing links.
Answer: (SHOW ANSWER)

NEW QUESTION: 69
An organization has several systems that require specific logons Over the past few months, the security analyst has noticed numerous failed logon attempts followed by password resets. Which of the following should the analyst do to reduce the occurrence of legitimate failed logons and password resets?
A. Adjust the current monitoring and logging rules
B. Perform a manual privilege review
C. Use SSO across all applications
D. Implement multifactor authentication
Answer: C (LEAVE A REPLY)

NEW QUESTION: 70
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. Retinal scan
B. Fingerprint
C. Passphrase
D. Physical key
Answer: (SHOW ANSWER)

NEW QUESTION: 71
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. Ask the sender to stop sending messages.
B. Delete the email from the company's email servers.
C. Review the message in a secure environment.
D. Block the sender In the email gateway.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
Which of the following is the BEST way to share incident-related artifacts to provide non-repudiation?

A. Secure email
B. Network folders
C. Encrypted USB drives
D. Cloud containers
Answer: (SHOW ANSWER)

NEW QUESTION: 73
A cybersecurity analyst is supposing an incident response effort via threat intelligence. Which of the following is the analyst MOST likely executing?
A. Containment and eradication
B. Requirements analysis and collection planning
C. Recovery and post-incident review
D. Indicator enrichment and research pivoting
Answer: D (LEAVE A REPLY)

NEW QUESTION: 74
A cybersecurity analyst is dissecting an intrusion down to the specific techniques and wants to organize them in a logical manner. Which of the following frameworks would BEST apply in this situation?
A. Pyramid of Pain
B. MITRE ATT&CK
C. CVSS v3.0
D. Diamond Model of Intrusion Analysts
Answer: B (LEAVE A REPLY)

NEW QUESTION: 75
A security analyst is reviewing the following requirements (or new time clocks that will be installed in a shipping warehouse:
* The clocks must be configured so they do not respond to ARP broadcasts.
* The server must be configured with static ARP entries for each clock.
Which of the following types of attacks will this configuration mitigate?
A. Spoofing
B. Sniffing
C. Rootkits
D. Overflows
Answer: A (LEAVE A REPLY)

NEW QUESTION: 76
Which of the following BEST identifies the appropriate use of threat intelligence as a function of detection and response?
A. To build a business security plan for an organization

B. To identify likely attack scenarios within an organization
C. To build a network segmentation strategy
D. To identify weaknesses in an organization's security posture
Answer: B (LEAVE A REPLY)

NEW QUESTION: 77
A company's marketing emails are either being found in a spam folder or not being delivered at all. The security analyst investigates the issue and discovers the emails in question are being sent on behalf of the company by a third party in1marketingpartners.com Below is the exiting SPP word:
Which of the following updates to the SPF record will work BEST to prevent the emails from being marked as spam or blocked?
A)
B)
C)
D)
A. Option B
B. Option A
C. Option D
D. Option C
Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
A security analyst is deploying a new application in the environment. The application needs to be integrated with several existing applications that contain SPI Pnor to the deployment, the analyst should conduct:
A. a tabletop exercise
B. an application stress test.
C. a business impact analysis
D. a PCI assessment
Answer: (SHOW ANSWER)

NEW QUESTION: 79
A newly appointed Chief Information Security Officer (CISO) has completed a risk assessment review of the organization and wants to reduce the numerous risks that were identified. Which of the following will provide a trend of risk mitigation?
A. Oversight
B. Planning
C. Continuous monitoring
D. Risk analysis
E. Risk response
Answer: (SHOW ANSWER)

NEW QUESTION: 80
A security analyst recently discovered two unauthorized hosts on the campus's wireless network segment from a man-m-the-middle attack .The security analyst also verified that privileges were not escalated, and the two devices did not gain access to other network devices Which of the following would BEST mitigate and improve the security posture of the wireless network for this type of attack?
A. Enable MAC filtering on the wireless router and create a whitelist that allows devices on the network
B. Conduct a wireless survey to determine if the wireless strength needs to be reduced.
C. Enable MAC filtering on the wireless router and suggest a stronger encryption for the wireless network,
D. Change the SSID, strengthen the passcode, and implement MAC filtering on the wireless router.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output:
Antivirus is installed on the remote host:
Installation path: C:\Program Files\AVProduct\Win32\
Product Engine: 14.12.101
Engine Version: 3.5.71
Scanner does not currently have information about AVProduct version 3.5.71. It may no longer be supported.
The engine version is out of date. The oldest supported version from the vendor is 4.2.11.
The analyst uses the vendor's website to confirm the oldest supported version is correct.
Which of the following BEST describes the situation?
A. This is a false positive, and the scanning plugin needs to be updated by the vendor.
B. This is a true positive, and the new computers were imaged with an old version of the software.

C. This is a true negative, and the new computers have the correct version of the software.
D. This is a false negative, and the new computers need to be updated by the desktop team.
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Following a recent security breach, a company decides to investigate account usage to ensure privileged accounts are only being utilized during typical business hours. During the investigation, a security analyst determines an account was consistently utilized in the middle of the night.
Which of the following actions should the analyst take NEXT?
A. Report the discrepancy to human resources.
B. Disable the privileged account
C. Review the activity with the user.
D. Initiate the incident response plan.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
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. Escape user inputs using character encoding conjoined with whitelisting
B. Property configure XML handlers so they do not process sent parameters coming from user inputs.
C. Implement a better level of user input filters and content sanitization.
D. Use parameterized Queries to avoid user inputs horn being processed by the server.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 84
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)
Explanation
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: 85
A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integration intelligence into hunt operations?
A. It enables the team to prioritize the focus area and tactics within the company's environment.
B. It supports rapid response and recovery during and followed an incident.
C. It allow analysis to receive updates on newly discovered software vulnerabilities.
D. It provide critically analyses for key enterprise servers and services.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 86
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: (SHOW ANSWER)
Explanation
"servers to be dedicated to one function..." http/s and SQL are two functions. I will select D, but agree with folks that the question is horribly written, and the person who wrote it was most likely drunk.

NEW QUESTION: 87
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)
Explanation
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

NEW QUESTION: 88
A company wants to outsource a key human-resources application service to remote employees as a SaaS-based cloud solution. The company's GREATEST concern should be the SaaS provider's:
A. SLA for system uptime.
B. DLP procedures.
C. data protection capabilities.
D. logging and monitoring capabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 89
Which of the following would MOST likely be included in the incident response procedure after a security breach of customer PII?
A. Human resources
B. Internal network operations center
C. Marketing
D. Public relations
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
During a forensic investigation, a security analyst reviews some Session Initiation Protocol packets that came from a suspicious IP address. Law enforcement requires access to a VoIP call that originated from the suspicious IP address. Which of the following should the analyst use to accomplish this task?
A. Wireshark
B. iptables
C. Tcpdump
D. Netflow
Answer: D (LEAVE A REPLY)
Explanation
https://learningnetwork.cisco.com/s/question/0D53i00000KszWaCAJ/netflow-vs-packet-analyzer

NEW QUESTION: 91
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. Establish a ransomware awareness program and implement secure and verifiable backups.
C. Virtualize all the endpoints with dairy snapshots of the virtual machines.
D. Back up the workstations to facilitate recovery and create a gold Image.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 92
A security analyst is required to stay current with the most recent threat data and intelligence reports. When gathering data, it is MOST important for the data to be:
A. relevant and accurate
B. proprietary and accurate
C. proprietary and timely
D. relevant and deep
Answer: (SHOW ANSWER)

NEW QUESTION: 93
A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?
A. Take the server offline to prevent continued SQL injection attacks.
B. Ask the developers to implement parameterized SQL queries.
C. Create a WAF rule In block mode for SQL injection
D. Modify the IDS rules to have a signature for SQL injection.
Answer: (SHOW ANSWER)

NEW QUESTION: 94
An organization supports a large number of remote users. Which of the following is the BEST option to protect the data on the remote users1 laptops?
A. Require the use of VPNs.
B. Use whole disk encryption.
C. implement a DLP solution.
D. Require employees to sign an NDA.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 95

A cybersecurity analyst is establishing a threat hunting and intelligence group at a growing organization.
Which of the following is a collaborative resource that would MOST likely be used for this purpose?
A. IoC feeds
B. VSS scores
C. Scrum
D. ISAC
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
A web-based front end for a business intelligence application uses pass-through authentication to authenticate users The application then uses a service account, to perform queries and look up data m a database A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?
A. Change the security model to force the users to access the database as themselves
B. Configure database security logging using syslog or a SIEM
C. Enforce unique session IDs so users do not get a reused session ID
D. Parameterize queries to prevent unauthorized SQL queries against the database
Answer: D (LEAVE A REPLY)

NEW QUESTION: 97
The security team at a large corporation is helping the payment-processing team to prepare for a regulatory compliance audit and meet the following objectives:
* Reduce the number of potential findings by the auditors.
* Limit the scope of the audit to only devices used by the payment-processing team for activities directly impacted by the regulations.
* Prevent the external-facing web infrastructure used by other teams from coming into scope.
* Limit the amount of exposure the company will face if the systems used by the payment-processing team are compromised.
Which of the following would be the MOST effective way for the security team to meet these objectives?
A. Limit the permissions to prevent other employees from accessing data owned by the business unit.
B. Segment the servers and systems used by the business unit from the rest of the network.
C. Implement full-disk encryption on the laptops used by employees of the payment-processing team.
D. Deploy patches to all servers and workstations across the entire organization.
Answer: (SHOW ANSWER)

NEW QUESTION: 98

Which of the following organizational initiatives would be MOST impacted by data severighty issues?

A. Moving to a cloud-based environment

B. Implementing non-repudiation controls

C. Migrating to locally hosted virtual servers

D. Encrypting local database queries

Answer: (SHOW ANSWER)

NEW QUESTION: 99

A threat intelligence analyst has received multiple reports that are suspected to be about the same advanced persistent threat. To which of the following steps in the intelligence cycle would this map?

A. Requirements

B. Analysis

C. Collection

D. Dissemination

E. Feedback

Answer: C (LEAVE A REPLY)

NEW QUESTION: 100

A pharmaceutical company's marketing team wants to send out notifications about new products to alert users of recalls and newly discovered adverse drug reactions. The team plans to use the names and mailing addresses that users have provided.

Which of the following data privacy standards does this violate?

A. Purpose limitation

B. Sovereignty

C. Data minimization

D. Retention

Answer: (SHOW ANSWER)

Reference:

http://www.isitethical.eu/portfolio-item/purpose-limitation/

NEW QUESTION: 101

A development team has asked users to conduct testing to ensure an application meets the needs of the business. Which of the fallowing types of testing docs This describe?

A. Regression testing

B. Penetration testing

C. Stress testing

D. Acceptance testing

Answer: D (LEAVE A REPLY)

NEW QUESTION: 102
A user reports a malware alert to the help desk A technician verifies the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do NEXT?
A. Reverse engineer the malware to determine its purpose and risk to the organization.
B. Document the procedures and walk through the incident training guide.
C. Sanitize the workstation and verify countermeasures are restored
D. Isolate the workstation and issue a new computer to the user.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 103
While conoXicting 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 BusinessUsr access key 1.
B. Delete Cloud Dev access key 1
C. Delete access key 2.
D. Delete access key 1.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 104
The Chief Information Officer (CIO) of a large healthcare institution is concerned about all machines having direct access to sensitive patient information. Which of the following should the security analyst implement to BEST mitigate the risk of sensitive data exposure?
A. MFA on all workstations
B. NAC to ensure minimum standards are met
C. Network segmentation
D. A cloud access service broker system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
Which of the following technologies can be used to store digital certificates and is typically used in highsecurity implementations where integrity is paramount?
A. eFuse
B. UEFI
C. HSM
D. Self-encrypting drive
Answer: C (LEAVE A REPLY)

NEW QUESTION: 106

While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security. To provide the MOST secure access model in this scenario, the jumpbox should be.
A. bridged between the IT and operational technology networks to allow authenticated access.
B. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.
C. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.
D. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.
Answer: (SHOW ANSWER)

NEW QUESTION: 107
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 contain the organization's legal and regulatory requirements regarding disclosures.
B. The disclosure section should include the names and contact information of key employees who are needed for incident resolution
C. The disclosure section should focus on how to reduce the likelihood customers will leave due to the incident.
D. The disclosure section should contain language explaining how the organization will reduce the likelihood of the incident from happening m the future.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 108
A company's legal and accounting teams have decided it would be more cost-effective to offload the risks of data storage to a third party. The IT management team has decided to implement a cloud model and has asked the security team for recommendations. Which of the following will allow all data to be kept on the third-party network?
A. VDI
B. SaaS
C. CASB

D. FaaS
Answer: B (LEAVE A REPLY)
Explanation
Which of the follawing activities is designed to handle a control failure that leads to a breach?
* Risk assessment
* Incident management
* Root cause analysis
* Vulnerability management Software as a Service (SaaS)
-Provides all the hardware, operating system, software, and applications needed for a complete application service to be delivered
-Cloud service providers are responsible for the security of the platform and infrastructure
-Consumers are responsible for application security, account provisioning, and authorizations
Cloud Access Security Broker (CASB)
- Enterprise management software designed to mediate access to cloud services by users across all types of devices Single sign-on Malware and rogue device detection Monitor/audit user activity Mitigate data exfiltration
- Cloud Access Service Brokers provide visibility into how clients and another network nodes use cloud services Forward Proxy Reverse Proxy API

NEW QUESTION: 109
Which of the following factors would determine the regulations placed on data under data sovereignty laws?
A. The company's data security policy
B. The type of data the company stores
C. The data laws of the country in which the company is located
D. What the company intends to do with the data it owns
Answer: C (LEAVE A REPLY)

NEW QUESTION: 110
While reviewing log files, a security analyst uncovers a brute-force attack that is being performed against an external webmail portal. Which of the following would be BEST to prevent this type of attack from beinq successful?
A. Configure a WAF with brute force protection rules in block mode
B. Implement MFA on the email portal using out-of-band code delivery.
C. Create a new rule in the IDS that triggers an alert on repeated login attempts
D. Leverage password filters to prevent weak passwords on employee accounts from being exploited.
E. Alter the lockout policy to ensure users are permanently locked out after five attempts.
Answer: (SHOW ANSWER)

NEW QUESTION: 111

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

A. insider threat

B. Nation-state

C. Hacktivist

D. Organized crime

Answer: C (LEAVE A REPLY)

NEW QUESTION: 112

When investigating a report of a system compromise, a security analyst views the following /var/log/secure log file:

Which of the following can the analyst conclude from viewing the log file?

A. The comptia user knows the sudo password.

B. The comptia user executed the sudo su command.

C. The comptia user knows the root password.

D. The comptia user added himself or herself to the /etc/sudoers file.

Answer: C (LEAVE A REPLY)

Explanation

the user is not in the sudoers file. you use your own password for that. the user used the su command to switch user accounts. when no user is specified, the su command defaults to the root account. the user is now logged into the root account. you need to know the root password to log into the root account.

NEW QUESTION: 113

Clients are unable to access a company's API to obtain pricing data. An analyst discovers sources other than clients are scraping the API for data, which is causing the servers to exceed available resources. Which of the following would be BEST to protect the availability of the APIs?

A. IP whitelisting

B. Web application firewall

C. Certificate-based authentication

D. Virtual private network

Answer: A (LEAVE A REPLY)

NEW QUESTION: 114

The help desk noticed a security analyst that emails from a new email server are not being sent out. The new email server was recently added to the existing ones. The analyst runs the following command on the new server.

Given the output, which of the following should the security analyst check NEXT?

A. The IP address of the new email server

B. The DNS name of the new email server

C. The version of SPF that is being used
D. The DMARC policy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 115
An organization's network administrator uncovered a rogue device on the network that is emulating the charactenstics of a switch. The device is trunking protocols and inserting tagging va the flow of traffic at the data link layer Which of the following BEST describes this attack?
A. VLAN hopping
B. Spoofing
C. DNS pharming
D. Injection attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 116
Which of the following assessment methods should be used to analyze how specialized software performs during heavy loads?
A. API compatibility lest
B. Input validation
C. Stress test
D. User acceptance test
E. Code review
Answer: C (LEAVE A REPLY)

NEW QUESTION: 117
During an investigation, an incident responder intends to recover multiple pieces of digital mediA. Before removing the media, the responder should initiate:
A. chain of custody forms.
B. secure communications.
C. decryption tools.
D. malware scans.
Answer: (SHOW ANSWER)

NEW QUESTION: 118
An analyst is investigating an anomalous event reported by the SOC. After reviewing the system logs the analyst identifies an unexpected addition of a user with root-level privileges on the endpoint. Which of the following data sources will BEST help the analyst to determine whether this event constitutes an incident?
A. Patching logs
B. Data classification matrix
C. Change requests

D. Backup logs
E. Threat feed
Answer: (SHOW ANSWER)

NEW QUESTION: 119
Which of the following is a reason to use a nsk-based cybersecunty framework?
A. A risk-based approach better allocates an organization's resources against cyberthreats and vulnerabilities
B. A risk-based approach always requires quantifying each cyber nsk faced by an organization
C. A risk-based approach is driven by regulatory compliance and es required for most organizations
D. A risk-based approach prioritizes vulnerability remediation by threat hunting and other qualitative-based processes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 120
A company's senior human resources administrator left for another position, and the assistant administrator was promoted into the senior position. On the official start day, the new senior administrator planned to ask for extended access permissions but noticed the permissions were automatically granted on that day. Which of the following describes the access management policy in place at the company?
A. Host-based
B. Mandatory-based
C. Federated access
D. Role-based
Answer: D (LEAVE A REPLY)

NEW QUESTION: 121
A security analyst received an alert from the SIEM indicating numerous login attempts from users outside their usual geographic zones, all of which were initiated through the web-based mail server. The logs indicate all domain accounts experienced two login attempts during the same time frame.
Which of the following is the MOST likely cause of this issue?
A. A password-spraying attack was performed against the organization.
B. A DDoS attack was performed against the organization.
C. This was normal shift work activity; the SIEM's AI is learning.
D. A credentialed external vulnerability scan was performed.
Answer: A (LEAVE A REPLY)
Reference: https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

NEW QUESTION: 122
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: C (LEAVE A REPLY)

NEW QUESTION: 123
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: (SHOW ANSWER)
This is based from the Info "(Application/octet-stream) https://isotropic.co/what-is-octet-stream/ "Connection: close" mean when used in the response message? Bookmark this question. Show activity on this post. When the client uses the Connection: close header in the request message, this means that it wants the server to close the connection after sending the response message. 200 OK is the most common HTTP status code. It generally means that the HTTP request succeeded. https://evertpot.com/http/200-ok
https://evertpot.com/http/200-ok

NEW QUESTION: 124
Which of the following, BEST explains the function of TPM?
A. To provide hardware-based security features using unique keys

B. To implement encryption algorithms for hard drives
C. To ensure platform confidentiality by storing security measurements
D. To improve management of the OS installation.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 125
As part of an exercise set up by the information security officer, the IT staff must move some of the network systems to an off-site facility and redeploy them for testing. All staff members must ensure their respective systems can power back up and match their gold image. If they find any inconsistencies, they must formally document the information.
Which of the following BEST describes this test?
A. Simulation
B. Full interruption
C. Walk through
D. Parallel
Answer: A (LEAVE A REPLY)

NEW QUESTION: 126
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: (SHOW ANSWER)
Explanation
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."

NEW QUESTION: 127
A company recently experienced a break-in whereby a number of hardware assets were stolen through unauthorized access at the back of the building. Which of the following would BEST prevent this type of theft from occurring in the future?
A. Monitored security cameras

B. Perimeter fencing
C. Motion detection
D. Badged entry
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
An analyst is responding 10 an incident involving an attack on a company-owned mobile device that was being used by an employee to collect data from clients in the held. Maiware was loaded on the device via the installation of a third-party software package The analyst has baselined the device Which of the following should the analyst do to BEST mitigate future attacks?
A. Update the maiware catalog
B. Patch the mobile device's OS
C. Implement MDM
D. Block third-party applications
Answer: C (LEAVE A REPLY)

NEW QUESTION: 129
Which of the following is MOST dangerous to the client environment during a vulnerability assessment penetration test?
A. There is a shorter period of time to assess the environment
B. No status reports are included with the assessment.
C. The testing is outside the contractual scope
D. There is a longer period of time to assess the environment.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
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 firewall ACL
B. Privileged accounts
C. The DNS configuration
D. The IDS rule set
Answer: D (LEAVE A REPLY)

NEW QUESTION: 131
A security analyst was alerted to a tile integrity monitoring event based on a change to the vhost-paymonts
.conf file The output of the diff command against the known-good backup reads as follows
Which of the following MOST likely occurred?
A. The file was altered to harvest credit card numbers

B. The file was altered to accept payments without charging the cards
C. The file was altered to avoid logging credit card information
D. The file was altered to verify the card numbers are valid.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
An organization discovers motherboards within the environment that appear to have been physically altered during the manufacturing process. Which of the following is the BEST course of action to mitigate the risk of this reoccurring?
A. Work with IT to replace the devices with the known-altered motherboards.
B. Perform an assessment of the firmware to determine any malicious modifications.
C. Coordinate a supply chain assessment to ensure hardware authenticity.
D. Conduct a trade study to determine if the additional risk constitutes further action.
Answer: (SHOW ANSWER)

NEW QUESTION: 133
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. curl
http:// accountfix-office365.com/login. php
B. nslookup accountfix-office365.com
C. tracert 122.167.40.119
D. telnet office365.com 25
Answer: B (LEAVE A REPLY)

NEW QUESTION: 134
A security analyst wants to identify which vulnerabilities a potential attacker might initially exploit if the network is compromised Which of the following would provide the BEST results?
A. Uncredentialed scan
B. Network ping sweep
C. Baseline configuration assessment
D. External penetration test
Answer: D (LEAVE A REPLY)

NEW QUESTION: 135
Which of the following APT adversary archetypes represent non-nation-state threat actors? (Select TWO)
A. Tiger
B. Panda
C. Jackal
D. Bear
E. Spider
F. Kitten
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 136
A team of security analysts has been alerted to potential malware activity. The initial examination indicates one of the affected workstations is beaconing on TCP port 80 to five IP addresses and attempting to spread across the network over port 445. Which of the following should be the team's NEXT step during the detection phase of this response process?
A. Identify potentially affected systems by creating a correlation search in the SIEM based on the network traffic.
B. Engage the engineering team to block SMB traffic internally and outbound HTTP traffic to the five IP addresses.
C. Escalate the incident to management, who will then engage the network infrastructure team to keep them informed.
D. Depending on system criticality, remove each affected device from the network by disabling wired and wireless connections.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 137
A Chief Information Security Officer has asked for a list of hosts that have critical and high-severity findings as referenced in the CVE database. Which of the following tools would produce the assessment output needed to satisfy this request?
A. Nessus
B. Nikto

C. Fuzzer
D. Wireshark
E. Prowler
Answer: (SHOW ANSWER)
Explanation
Nessus is a vulnerability scanning and assessment tool that can be used to scan systems for potential vulnerabilities and weaknesses. It provides detailed reports on any critical and high-severity findings as referenced in the CVE database, making it the ideal tool for fulfilling the Chief Information Security Officer's request. Nikto, fuzzer, wireshark, and prowler are all security tools, but they are not applicable for the scenario described in the question. Here is a link to an article from CompTIA's website about Nessus for your reference: https://www.comptia.org/content/nessus-vulnerability-scanning-and-assessment-tool.

NEW QUESTION: 138
A cybersecurity analyst routinely checks logs, querying for login attempts. While querying for unsuccessful login attempts during a five-day period, the analyst produces the following report:
Which of the following BEST describes what the analyst Just found?
A. A bot is running a brute-force attack in an attempt to log in to the domain.
B. An unauthorized user is using login credentials in a script.
C. Users 4 and 5 are using their credentials to transfer files to multiple servers.
D. Users 4 and 5 are using their credentials to run an unauthorized scheduled task targeting some servers In the cloud.
Answer: (SHOW ANSWER)

NEW QUESTION: 139
An analyst is reviewing the following code output of a vulnerability scan:
Which of the following types of vulnerabilities does this MOST likely represent?
A. A credential bypass vulnerability
B. An HTTP response split vulnerability
C. A XSS vulnerability
D. A insecure direct object reference vulnerability
Answer: A (LEAVE A REPLY)

NEW QUESTION: 140
A general contractor has a list of contract documents containing critical business data that are stored at a public cloud provider. The organization's security analyst recently reviewed some of the storage containers and discovered most of the containers are not encrypted. Which of the following configurations will provide the MOST security to resolve the vulnerability?
A. Implementing the Triple Data Encryption Algorithm at the file level
B. Implementing AES-256 encryption on the containers
C. Upgrading TLS 1.2 connections to TLS 1.3

D. Enabling SHA-256 hashing on the containers
Answer: (SHOW ANSWER)

NEW QUESTION: 141
Which of the following should a database administrator implement to BEST protect data from an untrusted server administrator?
A. Data masking
B. Data deidentification
C. Data minimization
D. Data encryption
Answer: D (LEAVE A REPLY)

NEW QUESTION: 142
The majority of a company's employees have stated they are unable to perform their job duties due to outdated workstations, so the company has decided to institute BYOD. Which of the following would a security analyst MOST likely recommend for securing the proposed solution?
A. A Linux-based system and mandatory training on Linux for all BYOD users
B. A firewalled environment for client devices and a secure VDI for BYOO users
C. A standardized anti-malware platform and a unified operating system vendor
D. 802.1X lo enforce company policy on BYOD user hardware
Answer: (SHOW ANSWER)
Explanation
VDI means virtual desktop interface. Using VDI, you can maintain a standard image and remove the threat of an infected machine plugging into your network.

NEW QUESTION: 143
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future.
Which of the following would be the BEST solution to recommend to the director?
A. Install a data loss prevention system, and train human resources employees on its use. Provide PII training to all employees at the company. Encrypt PII information.
B. Install specific equipment to create a human resources policy that protects PII datA. Train company employees on how to handle PII datA. Outsource all PII to another company. Send the human resources director to training for PII handling.
C. Train all employees. Encrypt data sent on the company network. Bring in privacy personnel to present a plan on how PII should be handled.
D. Enforce encryption on all emails sent within the company. Create a PII program and policy on how to handle datA. Train all human resources employees.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 144
An organization suspects it has had a breach, and it is trying to determine the potential impact. The organization knows the following:
* The source of the breach is linked to an IP located in a foreign country.
* The breach is isolated to the research and development servers.
* The hash values of the data before and after the breach are unchanged.
* The affected servers were regularly patched, and a recent scan showed no vulnerabilities.
Which of the following conclusions can be drawn with respect to the threat and impact? (Choose two.)
A. The confidentiality of the data is unaffected.
B. The threat is an APT.
C. The source IP of the threat has been spoofed.
D. The threat is an insider.
E. The integrity of the data is unaffected.
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 145
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: D (LEAVE A REPLY)
Explanation
When transitioning over to a cloud solution, an organization may lose visibility of certain points on the technology stack, particularly if it's subscribing to PaaS or SaaS solutions. Because the responsibility of protecting portions of the stack falls to the service provider, it does sometimes mean the organization loses monitoring capabilities, for better or worse. Chapman, Brent; Maymi, Fernando. CompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002) (p. 158).
McGraw Hill LLC. Kindle Edition.

NEW QUESTION: 146
An information security analyst is reviewing backup data sets as part of a project focused on eliminating archival data sets.
Which of the following should be considered FIRST prior to disposing of the electronic data?
A. Sanitization policy
B. Retention standards
C. Data sovereignty
D. Encryption policy

Answer: B (LEAVE A REPLY)

NEW QUESTION: 147
A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:
Which of the following is the MOST likely reason for this vulnerability?
A. The developer did not set proper cross-site request forgery protections.
B. The developer set input validation protection on the specific field of search.aspx.
C. The developer did not implement default protections in the web application build.
D. The developer did not set proper cross-site scripting protections in the header.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 148
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> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi httpd.conf' success
B. <100> 2020-01-10T19:33:48.002z webserver sudo 201 32001 = BOM ' su vi syslog.conf failed for jos
C. <100>2 2020-01-10T19:33:41.002z webserver su 201 32001 = BOM ' su vi httpd.conf' failed for joe
D. <100>2 2020-01-10T20:36:36.0010z financeserver su 201 32001 = BOM ' sudo vi users.txt success
E. <100> 2020-01-10T19:34..002z financeserver su 201 32001 = BOM ' su vi success
Answer: C (LEAVE A REPLY)

NEW QUESTION: 149
A security analyst is responding to an incident on a web server on the company network that is making a large number of outbound requests over DNS Which of the following is the FIRST step the analyst should take to evaluate this potential indicator of compromise'?
A. Reimage the machine to remove the threat completely and get back to a normal running state.
B. Run an anti-malware scan on the system to detect and eradicate the current threat
C. Shut down the system to prevent further degradation of the company network
D. Isolate the system on the network to ensure it cannot access other systems while evaluation is underway.
E. Start a network capture on the system to look into the DNS requests to validate command and control traffic.
Answer: E (LEAVE A REPLY)

NEW QUESTION: 150
For machine learning to be applied effectively toward security analysis automation, it requires.
A. a multicore, multiprocessor system.
B. a threat feed API.
C. anomalous traffic signatures.
D. relevant training data.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 151
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)
Explanation
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: 152
An organization recently discovered some inconsistencies in the motherboards it received from a vendor. The organization's security team then provided guidance on how to ensure the authenticity of the motherboards it received from vendors.
Which of the following would be the BEST recommendation for the security analyst to provide'?

A. The organization should maintain the relationship with the vendor and enforce vulnerability scans.
B. The organization should use a certified, trusted vendor as part of the supply chain.
C. The organization should evaluate current NDAs to ensure enforceability of legal actions.
D. The organization should ensure all motherboards are equipped with a TPM.
Answer: (SHOW ANSWER)

NEW QUESTION: 153
A security analyst working in the SOC recently discovered Balances m which hosts visited a specific set of domains and IPs and became infected with malware. Which of the following is the MOST appropriate action to take in the situation?
A. Implement a change request to the firewall setting to not allow traffic to and from the IPs and domains
B. Implement an IPS signature for the malware and a change request to the firewall setting to not allow traffic to and from the IPs and domains
C. implement an IPS signature for the malware and update the blacklisting for the associated domains and IPs
D. Implement an IPS signature for the malware and another signature request to Nock all the associated domains and IPs
Answer: A (LEAVE A REPLY)

NEW QUESTION: 154
An analyst performs a routine scan of a host using Nmap and receives the following output:
Which of the following should the analyst investigate FIRST?
A. Port 21
B. Port 80
C. Port 22
D. Port 23
Answer: A (LEAVE A REPLY)

NEW QUESTION: 155
Legacy medical equipment, which contains sensitive data, cannot be patched. Which of the following is the BEST solution to improve the equipment's security posture?
A. Move the legacy systems behind a WAF
B. Implement an air gap for the legacy systems.
C. Place the legacy systems in the DMZ
D. Implement a VPN between the legacy systems and the local network.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 156

A Chief Information Security Officer (CISO) is concerned the development team, which consists of contractors, has too much access to customer datA. Developers use personal workstations, giving the company little to no visibility into the development activities.
Which of the following would be BEST to implement to alleviate the CISO's concern?
A. Test data
B. NDA
C. DLP
D. Encryption
Answer: B (LEAVE A REPLY)

NEW QUESTION: 157
The IT department is concerned about the possibility of a guest device infecting machines on the corporate network or taking down the company's singe internet connection. Which of the following should a security analyst recommend to BEST meet the requirements outlined by the IT Department?
A. Place a firewall In between the corporate network and the guest network
B. Require the guest machines to install the corporate-owned EDR solution.
C. Configure NAC to only allow machines on the network that are patched and have active antivirus.
D. Configure the IPS with rules that will detect common malware signatures traveling from the guest network.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 158
The inability to do remote updates of certificates, keys, software, and firmware is a security issue commonly associated with:
A. firewalls and UTM devices
B. web servers on private networks
C. HVAC control systems
D. smartphones
Answer: C (LEAVE A REPLY)

NEW QUESTION: 159
A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?
A. Regression testing
B. Dynamic analysis
C. User acceptance testing
D. Static analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 160
An analyst must review a new cloud-based SIEM solution. Which of the following should the analyst do FIRST prior to discussing the company's needs?
A. Download the product security white paper.
B. Perform a vulnerability scan against a test instance.
C. Check industry news feeds for product reviews.
D. Ensure a current non-disclosure agreement is on file
Answer: D (LEAVE A REPLY)

NEW QUESTION: 161
Which of the following BEST explains the function of a managerial control?
A. To help design and implement the security planning, program development, and maintenance of the security life cycle
B. To guide the development of training, education, security awareness programs, and system maintenance
C. To create data classification, risk assessments, security control reviews, and contingency planning
D. To ensure tactical design, selection of technology to protect data, logical access reviews, and the implementation of audit trails
Answer: C (LEAVE A REPLY)
Explanation
Managerial controls are procedural mechanisms that focus on the mechanics of the risk management process.
Examples of administrative controls include periodic risk assessments, security planning exercises, and the incorporation of security into the organization's change management, service acquisition, and project management practices

NEW QUESTION: 162
A security analyst sees the following OWASP ZAP output from a scan that was performed against a modern version of Windows while testing for client-side vulnerabilities:
Which of the following is the MOST likely solution to the listed vulnerability?
A. Enable the browser's XSS filter.
B. Enable the browser's protected pages mode
C. Enable Windows XSS protection
D. Enable server-side XSS protection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 163

A security analyst is reviewing a suspected phishing campaign that has targeted an organisation. The organization has enabled a few email security technologies in the last year: however, the analyst believes the security features are not working. The analyst runs the following command:
> dig domain._domainkey.comptia.orq TXT
Which of the following email protection technologies is the analyst MOST likely validating?
A. DNSSEC
B. DKIM
C. DMARC
D. SPF
Answer: D (LEAVE A REPLY)

NEW QUESTION: 164
Which of the following is an advantage of SOAR over SIEM?
A. SOAR is much less expensive.
B. SOAR reduces the amount of human intervention required.
C. SOAR can aggregate data from many sources.
D. SOAR uses more robust encryption protocols.
Answer: C (LEAVE A REPLY)
Explanation
SOAR systems and services tend to add a layer of workflow management. That means that SOAR deployments may actually ingest SIEM alerts and other data and then apply workflows and automation to them. SIEM and SOAR tools can be difficult to distinguish from each other, with one current difference being the broader range of tools that SOAR services integrate with. The same vendors who provide SIEM capabilities also provide SOAR systems in many cases with Splunk, Rapid7, and IBM (QRadar) all included.
There are differences, however, as ITSM tools like ServiceNow play in the space as well. As an analyst, you need to know that SOAR services and tools exist and can be leveraged to cover additional elements beyond what traditional SIEM systems have historically handled.

NEW QUESTION: 165
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: (SHOW ANSWER)
Explanation

change management - process through which changes to the configuration of information systems are monitored and controlled. Each individual component should have a separate document or database record that describes its initial state and subsequent changes

NEW QUESTION: 166
A company has contracted with a software development vendor to design a web portal for customers to access a medical records database. Which of the following should the security analyst recommend to BEST control the unauthorized disclosure of sensitive data when sharing the development database with the vendor?
A. Establish an NDA with the vendor.
B. Enable data masking of sensitive data tables in the database.
C. Set all database tables to read only.
D. Use a de-identified data process for the development database.
Answer: D (LEAVE A REPLY)
Explanation
https://privacy-analytics.com/resources/videos/what-is-the-difference-between-data-masking-de-identification-an

NEW QUESTION: 167
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 whitelisted binaries to execute.
B. Use file integrity monitoring to validate the digital signature.
C. Run an antivirus against the binaries to check for malware.
D. Validate the binaries' hashes from a trusted source.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 168
A security analyst has received reports of very slow, intermittent access to a public-facing corporate server.
Suspecting the system may be compromised, the analyst runs the following commands:

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

A. Examine the server logs for further indicators of compromise of a web application.

B. Run kill -9 1325 to bring the load average down so the server is usable again.

C. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.

D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 169

A security analyst is trying to determine if a host is active on a network. The analyst first attempts the following:

The analyst runs the following command next:

Which of the following would explain the difference in results?

A. ICMP is being blocked by a firewall.

B. The routing tables for ping and hping3 were different.

C. The original ping command needed root permission to execute.

D. hping3 is returning a false positive.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 170

A cybersecurity analyst needs to determine whether a large file named access log from a web server contains the following loC:

../../../../bin/bash

Which of the following commands can be used to determine if the string is present in the log?

A. echo access.log | grep "../../../../bin/bash"

B. cat access.log > grep "../../../ ../bin/bash"

C. grep "../../../../bin/bash" 1 cat access.log

D. grep "../../../. ./bin/bash" < access.log

Answer: D (LEAVE A REPLY)

NEW QUESTION: 171

A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:

Which of the following commands would work BEST to achieve the desired result?

A. grep -v chatter14 chat.log

B. grep -v pythonfun chat.log

C. grep -i javashark chat.log

D. grep -i chatter14 chat.log

E. grep -i pythonfun chat.log

F. grep -v javashark chat.log

Answer: (SHOW ANSWER)

NEW QUESTION: 172
You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not.
The company's hardening guidelines indicate the following:
* TLS 1.2 is the only version of TLS running.
* Apache 2.4.18 or greater should be used.
* Only default ports should be used.
INSTRUCTIONS
Using the supplied data, record the status of compliance with the company's guidelines for each server.
The question contains two parts: make sure you complete Part 1 and Part 2. Make recommendations for issues based ONLY on the hardening guidelines provided.

Answer:
See explanation below.
Explanation
Part 1 Answer:
Check on the following:
AppServ1 is only using TLS.1.2
AppServ4 is only using TLS.1.2
AppServ1 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater
Part 2 answer:
Recommendation:
Recommendation is to disable TLS v1.1 on AppServ2 and AppServ3. Also upgrade AppServ2 Apache to version 2.4.48 from its current version of 2.3.48

NEW QUESTION: 173
The computer incident response team at a multinational company has determined that a breach of sensitive data has occurred in which a threat actor has compromised the organization's email system. Per the incident response procedures, this breach requires notifying the board immediately. Which of the following would be the BEST method of communication?
A. Corporate-hosted encrypted email
B. Summary sent by certified mail
C. VoIP phone call
D. Post of the company blog
E. Externally hosted instant message

Answer: C (LEAVE A REPLY)

NEW QUESTION: 174
A customer notifies a security analyst that a web application is vulnerable to information disclosure The analyst needs to indicate the seventy of the vulnerability based on its CVSS score, which the analyst needs to calculate When analyzing the vulnerability the analyst realizes that tor the attack to be successful, the Tomcat configuration file must be modified Which of the following values should the security analyst choose when evaluating the CVSS score?
A. Local
B. Network
C. Physical
D. Adjacent
Answer: B (LEAVE A REPLY)

NEW QUESTION: 175
Which of the following is the use of tools to simulate the ability for an attacker to gain access to a specified network?
A. Penetration testing
B. Fuzzing
C. Network mapping
D. Reverse engineering
Answer: A (LEAVE A REPLY)

NEW QUESTION: 176
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 C
B. Option D
C. Option B
D. Option A
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
A vulnerability scanner has identified an out-of-support database software version running on a server. The software update will take six to nine months to complete. The management team has agreed to a one-year extended support contract with the software vendor. Which of the following BEST describes the risk treatment in this scenario?

A. The extended support mitigates any risk associated with the software.
B. The extended support contract changes this vulnerability finding to a false positive.
C. The company is transferring the risk for the vulnerability to the software vendor.
D. The company is accepting the inherent risk of the vulnerability.
Answer: D (LEAVE A REPLY)
Explanation
Risk Acceptance
o A risk response that involves determining that a risk is within the organization's risk appetite and no countermeasures other than ongoing monitoring will be needed Mitigation Control Avoidance Changing plans Transference Insurance Acceptance Low risk

NEW QUESTION: 178
A security analyst is reviewing vulnerability scan results and notices new workstations are being flagged as having outdated antivirus signatures. The analyst observes the following plugin output: The analyst uses the vendor's website to confirm the oldest supported version is correct. Which of the following BEST describes the situation?
A. This is a true negative and the new computers have the correct version of the software
B. This is a false positive and the scanning plugin needs to be updated by the vendor
C. This is a false negative and the new computers need to be updated by the desktop team
D. This is a true positive and the new computers were imaged with an old version of the software
Answer: D (LEAVE A REPLY)

NEW QUESTION: 179
Risk management wants IT to implement a solution that will permit an analyst to intercept, execute, and analyze potentially malicious files that are downloaded from the Internet.
Which of the following would BEST provide this solution?
A. Decomposition of malware
B. Risk evaluation
C. File fingerprinting
D. Sandboxing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 180
An organization wants to move non-essential services into a cloud computing environment. Management 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: C (LEAVE A REPLY)

Explanation
A hot site is always ready to take over the primary site's workload, so wouldn't it be more cost-effective in the long run? Additionally, a hot site would provide faster recovery times and better protection against data loss compared to a warm site.

NEW QUESTION: 181
To validate local system-hardening requirements, which of the following types of vulnerability scans would work BEST to verify the scanned device meets security policies?
A. SCAP
B. SAST
C. DAST
D. DACS
Answer: A (LEAVE A REPLY)
Explanation
SCAP is a protocol designed to assess the security compliance of computers and other devices. It works by scanning systems against security policies, and can help verify that the scanned device meets security requirements. Here is a link to the CompTIA CySA+ Guide's Chapter 5 - Access Controls for more information: https://certification.comptia.org/docs/default-source/exam-objectives/cs0-002.pdf

NEW QUESTION: 182
Due to continued support of legacy applications, an organization's enterprise password complexity rules are inadequate for its required security posture. Which of the following is the BEST compensating control to help reduce authentication compromises?
A. Multifactor authentication
B. Biometrics
C. Increased password-rotation frequency
D. Smart cards
Answer: C (LEAVE A REPLY)

NEW QUESTION: 183

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: (SHOW ANSWER)

Explanation

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.

NEW QUESTION: 184

A security analyst is reviewing the following log from an email security service.

Which of the following BEST describes the reason why the email was blocked?

A. The To address is invalid.

B. The email originated from the www.spamfilter.org URL.

C. The IP address and the remote server name are the same.

D. The IP address was blacklisted.

E. The From address is invalid.

Answer: C (LEAVE A REPLY)

Reference: https://www.webopediA.com/TERM/R/RBL.html

NEW QUESTION: 185

A company creates digitally signed packages for its devices. Which of the following BEST describes the method by which the security packages are delivered to the company's customers?

A. eFuse

B. SELinux

C. Trusted firmware updates

D. Anti-tamper mechanism

Answer: C (LEAVE A REPLY)

NEW QUESTION: 186

A security analyst is investigating a compromised Linux server. The analyst issues the ps command and receives the following output.

Which of the following commands should the administrator run NEXT to further analyze the compromised system?

A. rpm -V openash-server

B. /bin/la -1 /proc/1301/exe

C. kill -9 1301
D. strace /proc/1301
Answer: (SHOW ANSWER)

NEW QUESTION: 187
An analyst receives artifacts from a recent Intrusion and is able to pull a domain, IP address, email address, and software version. When of the following points of the Diamond Model of Intrusion Analysis does this intelligence represent?
A. Adversary
B. Victims
C. Capabilities
D. Infrastructure
Answer: A (LEAVE A REPLY)

NEW QUESTION: 188
As part of a merger with another organization, a Chief Information Security Officer (CISO) is working with an assessor to perform a risk assessment focused on data privacy compliance. The CISO is primarily concerned with the potential legal liability and fines associated with data privacy. Based on the CISO's concerns, the assessor will MOST likely focus on:
A. quantitative magnitude.
B. qualitative magnitude.
C. quantitative probabilities.
D. qualitative probabilities.
Answer: (SHOW ANSWER)

NEW QUESTION: 189
A security analyst is reviewing the following server statistics:
Which of the following is MOST likely occurring?
A. VM escape
B. Race condition
C. Privilege escalation
D. Resource exhaustion
Answer: D (LEAVE A REPLY)

NEW QUESTION: 190
An organization has not had an incident for several months. The Chief Information Security Officer (CISO) wants to move to a more proactive stance for security investigations. Which of the following would BEST meet that goal?
A. Root-cause analysis
B. Information-sharing community
C. Threat hunting

D. Active response
E. Advanced antivirus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 191
During routine monitoring a security analyst identified the following enterpnse network traffic:
Packet capture output:
Which of the following BEST describes what the security analyst observed?
A. 192.168.12.21 made a TCP connection to 66 187 224 210
B. 209.132.177.50 set up a TCP reset attack to 192 168 12 21
C. 192.168.12.21 made a TCP connection to 209 132 177 50
D. 66.187.224.210 set up a DNS hijack with 192.168.12.21.
Answer: (SHOW ANSWER)

NEW QUESTION: 192
A security analyst discovers a vulnerability on an unpatched web server that is used for testing machine learning on Bing Data sets. Exploitation of the vulnerability could cost the organization $1.5 million in lost productivity. The server is located on an isolated network segment that has a 5% chance of being compromised. Which of the following is the value of this risk?
A. $75.000
B. $1.425 million
C. $300.000
D. $1.5 million
Answer: A (LEAVE A REPLY)

NEW QUESTION: 193
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. Use data tokenization on sensitive fields, reencrypt the data sets using AES-256, and then create an MD5 hash.
B. Limit all access to the sensitive data based on geographic access requirements with strict role-based access controls.
C. Enable data masking and reencrypt the data sets using AES-256.
D. Ensure the data is correctly classified and labeled, and that DLP rules are appropriate to prevent disclosure.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 194

A proposed network architecture requires systems to be separated from each other logically based on defined risk levels. Which of the following explains the reason why an architect would set up the network this way?
A. To reduce the number of IP addresses that are used on the network
B. To create a design that simplifies the supporting network
C. To reduce the attack surface of those systems by segmenting the network based on risk
D. To complicate the network and frustrate a potential malicious attacker
Answer: C (LEAVE A REPLY)

NEW QUESTION: 195
An organization is moving its infrastructure to the cloud in an effort to meet the budget and reduce staffing requirements. The organization has three environments: development, testing, and production. These environments have interdependencies but must remain relatively segmented. Which of the following methods would BEST secure the company's infrastructure and be the simplest to manage and maintain?
A. Create one cloud account with one VPC for all environments. Purchase a virtual firewall and create granular security rules.
B. Create three separate cloud accounts for each environment and a single core account for network services. Route all traffic through the core account.
C. Create three separate cloud accounts for each environment. Configure account peering and security rules to allow access to and from each environment.
D. Create one cloud account and three separate VPCs for each environment. Create security rules to allow access to and from each environment.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 196
A security analyst is conceded that a third-party application may have access to user passwords during authentication. Which of the following protocols should the application use to alleviate the analyst's concern?
A. SHA-1
B. SAML
C. LADPS
D. MFA
Answer: B (LEAVE A REPLY)

NEW QUESTION: 197
Approximately 100 employees at your company have received a phishing email. As a security analyst you have been tasked with handling this situation.
INSTRUCTIONS
Review the information provided and determine the following:
1. How many employees clicked on the link in the phishing email?
2. On how many workstations was the malware installed?
3. What is the executable file name or the malware?

Answer:
Explanation
6 infected
7 clicked
isass.exe

NEW QUESTION: 198
A forensic analyst took an image of a workstation that was involved in an incident To BEST ensure the image is not tampered with me analyst should use:
A. a legal hold
B. hashing
C. backup tapes
D. chain of custody.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 199
As part of a review of modern response plans, which of the following is MOST important for an organization lo understand when establishing the breach notification period?
A. Legal requirements
B. Organizational policies
C. Service-level agreements
D. Vendor requirements and contracts
Answer: A (LEAVE A REPLY)

NEW QUESTION: 200
A security analyst notices the following entry while reviewing the server togs OR 1=1' ADD USER attacker' PW 1337password' ---- Which of the following events occurred?
A. RCE
B. SQLi

C. XSS
D. CSRF
Answer: B (LEAVE A REPLY)

NEW QUESTION: 201
A security analyst is generating a list of recommendations for the company's insecure API. Which of the following is the BEST parameter mitigation rec
A. Validate all incoming data.
B. Implement parameterized queries.
C. Use effective authentication and authorization methods.
D. Use TLs for all data exchanges.
Answer: (SHOW ANSWER)

NEW QUESTION: 202
A security analyst has received information from a third-party intelligence-sharing resource that indicates employee accounts were breached.
Which of the following is the NEXT step the analyst should take to address the issue?
A. Set up privileged access management to ensure auditing is enabled.
B. Audit access permissions for all employees to ensure least privilege.
C. Configure SSO to prevent passwords from going outside the local network.
D. Force a password reset for the impacted employees and revoke any tokens.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 203
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. Remove administrative rights from all developer workstations.
C. Manually delete the file from each of the workstations.
D. Block the download of the fie via the web proxy
Answer: (SHOW ANSWER)

NEW QUESTION: 204
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 .129 successfully exploited a vulnerability on the web server.
B. 10.1.1.128 sent potential malicious traffic to the web server.
C. 10.1.1.128 sent malicious requests, and the alert is a false positive.

D. 10.1.1.129 sent potential malicious requests to the web server.
E. 10.1.1.129 sent non-malicious requests, and the alert is a false positive.
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 205
A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:
Which of the following should the analyst review to find out how the data was exfilltrated?
A. Tuesday's logs
B. Thursday's logs
C. Wednesday's logs
D. Monday's logs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 206
A security technician is testing a solution that will prevent outside entities from spoofing the company's email domain, which is comptiA.org. The testing is successful, and the security technician is prepared to fully implement the solution.
Which of the following actions should the technician take to accomplish this task?
A. Add TXT @ "v=spf1 mx include:_spf.comptiA.org all" to the DNS record.
B. Add TXT @ "v=spf1 mx include:_spf.comptiA.org all" to the email server.
C. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the domain controller.
D. Add TXT @ "v=spf1 mx include:_spf.comptiA.org +all" to the web server.
Answer: A (LEAVE A REPLY)
Reference: https://blog.finjan.com/email-spoofing/

NEW QUESTION: 207
An organization's Chief Information Security Officer (CISO) has asked department leaders to coordinate on communication plans that can be enacted in response to different cybersecurity incident triggers.
Which of the following is a benefit of having these communication plans?
A. They can help to keep the organization's senior leadership informed about the status of patching during the recovery phase.
B. They can help to limit the spread of worms by coordinating with help desk personnel earlier in the recovery phase.
C. They can help to prevent the inadvertent release of damaging information outside the organization.
D. They can quickly inform the public relations team to begin coordinating with the media as soon as a breach is detected.
Answer: (SHOW ANSWER)

NEW QUESTION: 208
A team of network security analysts is examining network traffic to determine if sensitive data was exfitrated Upon further investigation, the analysts believe confidential data was compromised. Which of me following capattlnes would BEST defend against tnts type of sensitive data eifiitraUon?
A. Deploy an edge firewal.
B. Deploy EDR.
C. Implement DLP
D. Enaypi the hard drives
Answer: B (LEAVE A REPLY)

NEW QUESTION: 209
An organization wants to implement a privileged access management solution to belter manage the use ot emergency and privileged service accounts Which of the following would BEST satisfy the organization's goal?
A. Policy-based access controls
B. Discretionary access controls
C. Access control lists
D. Credential vaulting
Answer: A (LEAVE A REPLY)

NEW QUESTION: 210
An organization has the following policies:
*Services must run on standard ports.
*Unneeded services must be disabled.
The organization has the following servers:
*192.168.10.1 - web server
*192.168.10.2 - database server
A security analyst runs a scan on the servers and sees the following output:
Which of the following actions should the analyst take?
A. Disable IIS on 192.168.10.1.
B. Disable MSSQL on 192.168.10.2.
C. Disable DNS on 192.168.10.2.
D. Disable SSH on both servers.
E. Disable HTTPS on 192.168.10.1.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
Which of the following secure coding techniques can be used to prevent cross-site request forgery attacks?

A. Output encoding
B. Tokenization
C. Input validation
D. Parameterized queries
Answer: B (LEAVE A REPLY)

NEW QUESTION: 212
A security team is implementing a new vulnerability management program in an environment that has a historically poor security posture. The team is aware of issues patch management in the environment and expects a large number of findings. Which of the following would be the MOST efficient way to increase the security posture of the organization in the shortest amount of time?
A. Create an SLA stating that remediation actions must occur within 30 days of discovery for all levels of vulnerabilities.
B. Implement a change control policy that allows the security team to quickly deploy patches in the production environment to reduce the risk of any vulnerabilities found.
C. Incorporate prioritization levels into the remediation process and address critical findings first.
D. Create classification criteria for data residing on different servers and provide remediation only for servers housing sensitive data.
Answer: (SHOW ANSWER)

NEW QUESTION: 213
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 no longer accepts the vulnerable cipher suites
B. It only accepts cipher suites using AES and SHA
C. It only accepts TLSvl 2
D. SSL/TLS is offloaded to a WAF and load balancer
Answer: (SHOW ANSWER)

NEW QUESTION: 214

A company's security administrator needs to automate several security processes related to testing for the existence of changes within the environment Conditionally other processes will need to be created based on input from prior processes Which of the following is the BEST method for accomplishing this task?

A. Machine learning and process monitoring

B. Workflow orchestration and scripting

C. Continuous integration and configuration management

D. API integration and data enrichment

Answer: B (LEAVE A REPLY)

NEW QUESTION: 215

After examine a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?

A. Header analysis

B. File carving

C. Metadata analysis

D. Data recovery

Answer: B (LEAVE A REPLY)

Explanation

Three common types of file carving methods are as follows: Header- and footer-based carving, which focuses on headers like those found in JPEG files. For example, JPEGs can be found by looking for \xFF\xD8 in the header and \xFF\xD9 in the footer. Content-based carving techniques look for information about the content of a file such as character counts and text recognition. File structure-based carving techniques that use information about the structure of files.

NEW QUESTION: 216

During the threal modeling process for a new application that a company is launching, a security analyst needs to define methods and items to take into consideralion Wtiich of the following are part of a known threat modeling method?

A. Threat profile, infrastructure and application vulnerabilities, security strategy and plans

B. Spoofing tampering, repudiation, information disclosure, denial of service elevation of privilege

C. Purpose, objective, scope, (earn management, cost, roles and responsibilities

D. Human impact, adversary's motivation, adversary's resources, adversary's methods

Answer: B (LEAVE A REPLY)

NEW QUESTION: 217

A monthly job to install approved vendor software updates and hot fixes recently stopped working. The security team performed a vulnerability scan, which identified several hosts as having some critical OS vulnerabilities, as referenced in the common vulnerabilities and exposures (CVE) database.

Which of the following should the security team do NEXT to resolve the critical findings in the most effective manner? (Choose two.)
A. Patch the required hosts with the correct updates and hot fixes, and rescan them for vulnerabilities.
B. Remove the servers reported to have high and medium vulnerabilities.
C. Resolve the monthly job issues and test them before applying them to the production network.
D. Tag the computers with critical findings as a business risk acceptance.
E. Harden the hosts on the network, as recommended by the NIST framework.
F. Manually patch the computers on the network, as recommended on the CVE website.
Answer: (SHOW ANSWER)

NEW QUESTION: 218
An analyst has been asked to provide feedback regarding the control required by a revised regulatory framework At this time, the analyst only needs to focus on the technical controls. Which of the following should the analyst provide an assessment of?
A. Establishment o' data classifications
B. Formal identification of data ownership
C. Execution of NDAs
D. Tokenization of sensitive data
E. Reporting on data retention and purging activities
Answer: D (LEAVE A REPLY)

NEW QUESTION: 219
Which of the following solutions is the BEST method to prevent unauthorized use of an API?
A. Authentication
B. Geofencing
C. Rate liming
D. HTTPS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 220
Which of the following roles is ultimately responsible for determining the classification levels assigned to specific data sets?
A. Data custodian
B. Data owner
C. Data processor
D. Senior management
Answer: B (LEAVE A REPLY)
Reference: https://www.pearsonitcertification.com/articles/article.aspx?p=2731933&seqNum=3

NEW QUESTION: 221

Given the Nmap request below:
Which of the following actions will an attacker be able to initiate directly against this host?
A. An SQL injection
B. Password sniffing
C. ARP spoofing
D. A brute-force attack
Answer: (SHOW ANSWER)

NEW QUESTION: 222
A development team uses open-source software and follows an Agile methodology with two-week sprints.
Last month, the security team filed a bug for an insecure version of a common library. The DevOps team updated the library on the server, and then the security team rescanned the server to verify it was no longer vulnerable. This month, the security team found the same vulnerability on the server.
Which of the following should be done to correct the cause of the vulnerability?
A. Install a HIPS on the server.
B. Deploy a WAF in front of the application.
C. Implement a software repository management tool.
D. Instruct the developers to use input validation in the code.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 223
After examining a header and footer file, a security analyst begins reconstructing files by scanning the raw data bytes of a hard disk and rebuilding them. Which of the following techniques is the analyst using?
A. Data recovery
B. Metadata analysis
C. File carving
D. Header analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 224
In response to an audit finding, a company's Chief information Officer (CIO) instructed the security department to Increase the security posture of the vulnerability management program. Currency, the company's vulnerability management program has the following attributes:
Which of the following would BEST Increase the security posture of the vulnerably management program?
A. Expand the ports being scanned to Include all ports. Keep the scan interval at its current level Enable authentication and perform credentialed scans.

B. Continue scanning the well-known ports increase the scan interval to a number the business will accept without causing service Interruption. Enable authentication and perform credentialed scans.
C. Expand the ports Being scanned lo Include al ports increase the scan interval to a number the business win accept without causing service interruption. Enable authentication and perform credentialed scans
D. Expand the ports being scanned to Include at ports increase the scan interval to a number the business will accept without causing service Interruption. Continue unauthenticated scans.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 225
An organization has been seeing increased levels of malicious traffic. A security analyst wants to take a more proactive approach to identify the threats that are acting against the organization's network. Which of the following approaches should the security analyst recommend?
A. Use the MITRE ATT&CK framework to develop threat models.
B. Conduct internal threat research and establish indicators of compromise.
C. Use SCAP scans to monitor for configuration changes on the network.
D. Review the perimeter firewall rules to ensure rule-set accuracy.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 226
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 policy tag is incorrectly configured.
B. The DMARC record's version tag is set to DMARC1 instead of the current version, which is DMARC3.
C. The DMARC record's DKIM alignment tag Is incorrectly configured.
D. The DMARC record does not have an SPF alignment tag.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 227
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. Enforce input validation
B. Require application fuzzing.
C. Perform a code review
D. Perform static code analysis.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 228
After detecting possible malicious external scanning, an internal vulnerability scan was performed, and a critical server was found with an outdated version of JBoss. A legacy application that is running depends on that version of JBoss. Which of the following actions should be taken FIRST to prevent server compromise and business disruption at the same time?
A. Make a backup of the server and update the JBoss server that is running on it.
B. Contact the vendor for the legacy application and request an updated version.
C. Create a proper DMZ for outdated components and segregate the JBoss server.
D. Apply visualization over the server, using the new platform to provide the JBoss service for the legacy application as an external service.
Answer: (SHOW ANSWER)
Explanation
What is that application for? "The DMZ is a special network zone designed to house systems that receive connections from the outside world, such as web and email servers. Sound firewall designs place these systems on an isolated network where, if they become compromised, they pose little threat to the internal network because connections between the DMZ and the internal network must still pass through the firewall and are subject to its security policy"

NEW QUESTION: 229
A company's security officer needs to implement geographical IP blocks for nation-state actors from a foreign country On which of the following should the blocks be implemented'?
A. Access control list
B. Data loss prevention
C. Web content filter
D. Network access control
Answer: (SHOW ANSWER)

NEW QUESTION: 230

A user reports the system is behaving oddly following the installation of an approved third-party software application. The application executable was sourced from an internal repository Which of the following will ensure the application is valid?

A. Hash the application's installation file and compare it to the hash provided by the vendor

B. Perform a malware scan on the file in the internal repository

C. Ask the user to refresh the existing definition file for the antivirus software

D. Remove the user's system from the network to avoid collateral contamination

Answer: A (LEAVE A REPLY)

NEW QUESTION: 231

A financial organization has offices located globally. Per the organization's policies and procedures, all executives who conduct Business overseas must have their mobile devices checked for malicious software or evidence of tempering upon their return. The information security department oversees the process, and no executive has had a device compromised. The Chief information Security Officer wants to Implement an additional safeguard to protect the organization's data. Which of the following controls would work BEST to protect the privacy of the data if a device is stolen?

A. Install a DLP solution to track data now

B. Implement a mobile device wiping solution for use if a device is lost or stolen.

C. Install an encryption solution on all mobile devices.

D. Train employees to report a lost or stolen laptop to the security department immediately

Answer: C (LEAVE A REPLY)

NEW QUESTION: 232

At which of the following phases of the SDLC shoukJ security FIRST be involved?

A. Analysis

B. Planning

C. Maintenance

D. Design

E. Testing

F. Implementation

Answer: D (LEAVE A REPLY)

NEW QUESTION: 233

A large software company wants to move as source control and deployment pipelines into a cloud-computing environment. Due to the nature of the business management determines the recovery time objective needs to be within one hour. Which of the following strategies would put the company in the BEST position to achieve the desired recovery time?

A. Set up every cloud component with duplicated copies and auto scaling turned on

B. Create a duplicate copy on premises that can be used for failover in a disaster situation

C. Configure a duplicate environment in the same region and load balance between both instances
D. Establish an alternate site with active replication to other regions
Answer: (SHOW ANSWER)

NEW QUESTION: 234
Which of following allows Secure Boot to be enabled?
A. eFuse
B. MSM
C. UEFI
D. PAM
Answer: B (LEAVE A REPLY)

NEW QUESTION: 235
A company was recently awarded several large government contracts and wants to determine its current risk from one specific APT.
Which of the following threat modeling methodologies would be the MOST appropriate to use during this analysis?
A. Attack vectors
B. Adversary capability
C. Diamond Model of Intrusion Analysis
D. Kill chain
E. Total attack surface
Answer: B (LEAVE A REPLY)
Reference: https://www.secureworks.com/blog/advanced-persistent-threats-apt-b

NEW QUESTION: 236
Ann, a user, reports to the security team that her browser began redirecting her to random sites while using her Windows laptop. Ann further reports that the OS shows the C: drive is out of space despite having plenty of space recently. Ann claims she not downloaded anything. The security team obtains the laptop and begins to investigate, noting the following:
* File access auditing is turned off.
* When clearing up disk space to make the laptop functional, files that appear to be cached web pages are immediately created in a temporary directory, filling up the available drive space.
* All processes running appear to be legitimate processes for this user and machine.
* Network traffic spikes when the space is cleared on the laptop.
* No browser is open.
Which of the following initial actions and tools would provide the BEST approach to determining what is happening?
A. Disable the network connection, check Sysinternals Process Explorer, and review netstat output.

B. Delete the temporary files, run an Nmap scan, and utilize Burp Suite.
C. Review logins to the laptop, search Windows Event Viewer, and review Wireshark captures.
D. Perform a hard power down of the laptop, take a dd image, and analyze with FTK.
Answer: (SHOW ANSWER)

NEW QUESTION: 237
During a cyber incident, which of the following is the BEST course of action?
A. Restrict customer communication until the severity of the breach is confirmed.
B. Switch to using a pre-approved, secure, third-party communication system.
C. Keep the entire company informed to ensure transparency and integrity during the incident.
D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 238
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. Collect all the files that have changed and compare them with the previous baseline
B. Check the hash signatures, comparing them with malware databases to verify if the files are infected.
C. Fully segregate the affected servers physically in a network segment, apart from the production network.
D. Collect the network traffic during the day to understand if the same activity is also occurring during business hours
Answer: C (LEAVE A REPLY)

NEW QUESTION: 239
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: C (LEAVE A REPLY)
Explanation

"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-solutio

NEW QUESTION: 240
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. Peer review
D. Tabletop exercise
Answer: B (LEAVE A REPLY)

NEW QUESTION: 241
Which of the following describes the mam difference between supervised and unsupervised machine-learning algorithms that are used in cybersecurity applications?
A. Unsupervised algorithms produce more false positives. Than supervised algorithms.
B. Unsupervised algorithms are not suitable for IDS systems, white supervised algorithms are
C. Supervised algorithms can be used to block attacks, while unsupervised algorithms cannot.
D. Supervised algorithms require security analyst feedback, while unsupervised algorithms do not.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 242
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)
Explanation
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: 243
An incident response team is responding to a breach of multiple systems that contain PII 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)
Explanation
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: 244
A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system.
After several attempts to remediate the issue, the system went down. A root cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources.
Which of the following BEST describes this attack?
A. Injection attack
B. Memory corruption
C. Denial of service
D. Array attack

Answer: C (LEAVE A REPLY)
Reference: https://economictimes.indiatimes.com/definition/memory-corruption

NEW QUESTION: 245
A network attack that is exploiting a vulnerability in the SNMP is detected.
Which of the following should the cybersecurity analyst do FIRST?
A. Apply the required patches to remediate the vulnerability.
B. Escalate the incident to senior management for guidance.
C. Disable all privileged user accounts on the network.
D. Temporarily block the attacking IP address.
Answer: (SHOW ANSWER)
Reference: https://beyondsecurity.com/scan-pentest-network-vulnerabilities-snmp-protocol-version- detection.html

NEW QUESTION: 246
During a review of vulnerability scan results an analyst determines the results may be flawed because a control-baseline system which is used to evaluate a scanning tools effectiveness was reported as not vulnerable Consequently, the analyst verifies the scope of the scan included the control-baseline host which was available on the network during the scan. The use of a control-baseline endpoint in this scenario assists the analyst in confirming.
A. false negatives
B. hardening validation.
C. verification of mitigation
D. false positives
E. the criticality index
Answer: (SHOW ANSWER)

NEW QUESTION: 247
An analyst needs to provide a recommendation that will allow a custom-developed application to have full access to the system's processors and peripherals but still be contained securely from other applications that will be developed. Which of the following is the BEST technology for the analyst to recommend?
A. Hardware security module
B. Software-based drive encryption
C. Trusted execution environment
D. Unified Extensible Firmware Interface
Answer: (SHOW ANSWER)

NEW QUESTION: 248
A cybersecurity analyst is currently checking a newly deployed server that has an access control list applied.

When conducting the scan, the analyst received the following code snippet of results:
Which of the following describes the output of this scan?
A. The analyst has discovered a False Positive, and the status code is incorrect providing an OK message.
B. The analyst has discovered a False Positive, and the status code is incorrect providing a server error message.
C. The analyst has discovered a True Positive, and the status code is correct providing a file not found error message.
D. The analyst has discovered a True Positive, and the status code is incorrect providing a forbidden message.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 249
Which of the following is the BEST way to gather patch information on a specific server?
A. Event Viewer
B. Custom script
C. CI/CD
D. SCAP software
Answer: D (LEAVE A REPLY)

NEW QUESTION: 250
A software developer is correcting the error-handling capabilities of an application following the initial coding of the fix. Which of the following would the software developer MOST likely performed to validate the code poor to pushing it to production?
A. Penetration test
B. Web-application vulnerability scan
C. Static analysis
D. Packet inspection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 251
The inability to do remote updates of certificates. keys software and firmware is a security issue commonly associated with:
A. web servers on private networks.
B. HVAC control systems
C. smartphones
D. firewalls and UTM devices
Answer: (SHOW ANSWER)

NEW QUESTION: 252
A security analyst is reviewing the following DNS logs as part of security-monitoring activities:

Which of the following MOST likely occurred?
A. The attack used encryption to obfuscate the payload and bypass detection by an IDS.
B. The attack caused an internal host to connect to a command and control server.
C. The attack attempted to contact www.gooqle com to verify Internet connectivity.
D. The attack used an algorithm to generate command and control information dynamically.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 253
An employee was found to have performed fraudulent activities. The employee was dismissed, and the employee's laptop was sent to the IT service desk to undergo a data sanitization procedure. However, the security analyst responsible for the investigation wants to avoid data sanitization. Which of the following can the security analyst use to justify the request?
A. Data retention
B. GDPR
C. Evidence retention
D. Data correlation procedure
Answer: A (LEAVE A REPLY)

NEW QUESTION: 254
A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets.
Which of the following is the BEST example of the level of sophistication this threat actor is using?
A. IP addresses used by the threat actor for command and control
B. Network assets used in previous attacks attributed to the threat actor
C. Social media accounts attributed to the threat actor
D. Email addresses and phone numbers tied to the threat actor
E. Custom malware attributed to the threat actor from prior attacks
Answer: E (LEAVE A REPLY)