

CuramSoftware.CS0-004.v2026-10-28.q41

Exam Code:	CS0-004
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	Curam Software
Free Question Number:	41
Version:	v2026-10-28
# of views:	143
# of Questions views:	410
https://www.freepdfdumps.com/CuramSoftware.CS0-004.v2026-10-28.q41.html	

NEW QUESTION: 1

A security analyst uses a full pcap solution to extract all traffic from the last two days associated with the 10.213.4.27 file server.

This file server is under investigation due to concerns about potential data exfiltration using Domain Name System (DNS) traffic. Which of the following commands should the analyst use to extract any potentially leaked data from the suspicious.pcap file?

A. strings suspicious.pcap | grep 10.213.4.27

B. zeek -r suspicious.pcap; grep 10.213.4.27 file.log

C. snort -r suspicious.pcap; grep eve.log 10.213.4.27

D. tcpdump -r suspicious.pcap port 53 and host 10.213.4.27

Answer: D (LEAVE A REPLY)

Option D applies the correct packet-filtering logic to isolate DNS-related traffic associated with the suspected server . The -r suspicious.pcap option directs tcpdump to read packets from the existing PCAP rather than capture live traffic. The expression port 53 and host 10.213.4.27 then limits output to packets involving the specified system and DNS's conventional port 53.

This is directly relevant to suspected DNS exfiltration. Attackers can encode data within DNS queries or responses, including unusually long subdomains or other manipulated DNS fields. Isolating the target's port 53 traffic dramatically reduces the dataset and allows the analyst to examine relevant queries and responses for encoded or anomalous information.

strings suspicious.pcap | grep treats the capture primarily as raw printable data and does not accurately perform protocol-aware packet filtering. The Zeek option searches file.log, which is focused on files observed in network traffic and is not the most direct location for DNS-query analysis. The Snort syntax shown is also inappropriate for the required extraction workflow.

The essential skill is translating an investigative hypothesis- possible DNS exfiltration by a known host - into a precise PCAP filter.

Study Guide Reference: Security Operations # Network Traffic Analysis # Full Packet Capture # tcpdump # BPF Filters # DNS Analysis # Data Exfiltration Detection.

NEW QUESTION: 2

A vulnerability analyst must perform a security assessment on an edge device running various services.

The analyst runs an Nmap port scan and sees the following output:

```

nmap scan report for 152.203.20.16
Host is up (0.0000050s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
500/udp   open  ikamsp

```

Which of the following should the analyst do next to validate the discovered remote access service is secure?

- A. Verify that the web server certificate is added to certificate store.
- B. Verify that the Border Gateway Protocol (BGP) route has been published.
- C. Verify that the virtual private network (VPN) service is utilizing Main Mode.
- D. Verify that the web server can be pinged.

Answer: C (LEAVE A REPLY)

The relevant follow-up is to assess the security configuration of the discovered VPN/IKE remote-access service , making option C the appropriate examination answer. Internet Key Exchange supports different negotiation modes, and Nmap includes specific capabilities for assessing IKE services. Nmap's ike-version script probes UDP port 500 and tests both Main and Aggressive Mode while identifying supported transforms and vendor characteristics.

Nmap's IKE library likewise explicitly supports generating either Main Mode or Aggressive Mode requests, enabling analysts to characterize the configuration of an exposed VPN endpoint. The security concern traditionally associated with this distinction is that Aggressive Mode exposes more negotiation information and has historically enabled offline attacks in some pre-shared-key configurations; Main Mode provides stronger identity protection during IKEv1 negotiation.

The other choices do not validate the security of the remote-access service. A web-server certificate is relevant to TLS-enabled HTTP services, BGP route publication relates to network routing, and ICMP ping only demonstrates basic reachability.

The analyst should therefore move from port discovery to service-specific configuration validation .

Study Guide Reference: Vulnerability Management # Nmap # Service Enumeration # VPN/IKE # UDP 500

Main Mode/Aggressive Mode # Configuration Validation.

NEW QUESTION: 3

Which of the following network architectures would best implement a perimeter-less network topology?

- A. Hybrid cloud networks
- B. Secure access service edge
- C. Cloud-native computing
- D. Content delivery networks

Answer: B (LEAVE A REPLY)

Secure access service edge is specifically designed for environments in which users, devices, applications, and workloads are distributed beyond a traditional enterprise network perimeter. SASE integrates networking and security functions into a service-oriented architecture so policy enforcement can follow the user or workload rather than depend solely on traffic traversing a centralized corporate boundary.

This makes SASE particularly suitable for a perimeter-less topology , where employees may work remotely, applications may reside in multiple cloud providers, and services may be accessed directly over the internet.

Typical SASE implementations combine software-defined wide-area networking with cloud-delivered security controls such as secure web gateways, cloud access security brokerage, firewall-as-a-service, and Zero Trust-oriented access controls.

A hybrid cloud network connects private and public cloud resources but can still operate using conventional network boundaries. Cloud-native computing describes an application and infrastructure design approach based on cloud technologies such as containers, microservices, and automation; it does not inherently define perimeter-less access security. A content delivery network distributes content geographically for performance and availability and is not an enterprise access-security architecture. The CS0-004 Security Operations objectives explicitly identify SASE, Zero Trust Network Architecture, and hybrid cloud as network architecture concepts analysts must understand.

Study Guide Reference: Security Operations # Network Architecture Concepts # SASE # Zero Trust Network Architecture # Distributed/Cloud Security.

NEW QUESTION: 4

An incident response team investigates a possible data leak. Various IT systems collect evidence.

Which of the following processes is required to ensure that evidentiary artifacts are properly recorded?

- A.** Packaging and labeling
- B.** Chain of custody
- C.** Post incident reporting
- D.** Storage and containment

Answer: ([SHOW ANSWER](#))

Chain of custody is the formal process used to document the collection, possession, transfer, handling, analysis, and disposition of evidentiary artifacts. Its purpose is to establish an auditable history demonstrating who controlled the evidence, when custody changed, why it was transferred, and what actions were performed on it.

NIST defines chain of custody as tracking evidence throughout its collection, safeguarding, and analysis lifecycle while documenting each individual who handled it, relevant timestamps, and the purpose of transfers. This is critical when multiple systems, analysts, forensic teams, or external parties participate in an investigation because undocumented handling could undermine confidence in the evidence's integrity or admissibility.

Packaging and labeling are important evidence-preservation procedures, but they represent only individual activities within the broader evidence-management process. Storage and containment protect artifacts from alteration or unauthorized access but do not provide the complete historical record of possession. Post-incident reporting documents investigation conclusions and response actions after the incident rather than tracking evidence throughout its lifecycle.

The decisive phrase is "properly recorded." A defensible record of every evidence transfer and handler is specifically the function of chain of custody.

Study Guide Reference: Incident Response and Management # Digital Forensics # Evidence Acquisition # Chain of Custody # Evidence Integrity # Documentation and Preservation.

NEW QUESTION: 5

A cybersecurity analyst receives an unstructured text document that contains advanced persistent threat (APT)-related indicators of compromise (IoCs). The analyst needs to extract the IPv4 addresses.

Which of the following is the best tool to accomplish this task?

- A.** CyberChef
- B.** Wireshark
- C.** Zeek
- D.** Open Cyber Threat Intelligence (OpenCTI)

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

CyberChef is the most appropriate option because the task involves parsing and extracting structured indicators from unstructured text, rather than inspecting network traffic or managing a threat-intelligence repository. CyberChef provides operations for text manipulation, pattern matching, regular expressions, decoding, extraction, and transformation. An analyst can therefore feed the document into CyberChef and identify IPv4 address patterns without manually reviewing potentially thousands of characters.

Wireshark is primarily a packet-analysis platform. It would be appropriate if the analyst needed to inspect packets from a PCAP or live network capture, but the scenario provides a text document. Zeek is a network security monitoring and traffic-analysis framework that converts network activity into structured logs; it is similarly unnecessary for static textual extraction. OpenCTI is a threat-intelligence platform designed to organize, correlate, and manage intelligence objects and relationships. It could store the resulting IoCs after extraction, but it is not the most efficient tool for extracting IPv4 strings from raw text.

The official CS0-004 objectives identify CyberChef under decoding/parsing tools, while Wireshark and Zeek are classified under packet analysis and OpenCTI under threat-intelligence platforms.

Study Guide Reference: Security Operations # Tools for Malicious-Activity Analysis # Decoding/Parsing # CyberChef # Pattern Recognition/Regular Expressions # IoC Analysis.

NEW QUESTION: 6

Which of the following is the most important component to include in the preparation phase of an incident response plan?

- A.** Roles and responsibilities
- B.** After action reports
- C.** Data integrity validation
- D.** Chain of custody

Answer: (SHOW ANSWER)

Clearly defined roles and responsibilities are foundational to incident-response preparation because responders must know in advance who has authority to make decisions and who performs specific technical, management, legal, communications, and recovery functions. Attempting to determine ownership while an active compromise is developing introduces delays, duplicated effort, communication failures, and potentially conflicting actions.

Preparation should define escalation paths, decision-making authority, contact mechanisms, incident leadership, technical responsibilities, evidence-management responsibilities, and coordination with business, legal, privacy, communications, and external parties where applicable. NIST's current incident-response guidance emphasizes preparation across organizational risk-management activities so organizations can respond and recover efficiently when incidents occur.

An after-action report is produced after an incident and documents the event, response actions, recovery, and lessons learned. Data-integrity validation is important during evidence analysis and recovery but is not the primary organizational foundation of preparation. Chain of custody must be established when evidence is collected and transferred, particularly where legal proceedings may occur, but it represents one procedure within a broader incident-response capability.

Without predefined ownership, even technically sound procedures may fail operationally.

Study Guide Reference: Incident Response and Management # Preparation # Incident Response Plan # Roles and Responsibilities # Escalation # Communication # Authority and Coordination.

NEW QUESTION: 7

A binary file that might contain malicious code is hosted on an isolated machine. An analyst wants to quickly detect the malicious code.

Which of the following should the analyst use?

- A.** strings
- B.** VirusTotal
- C.** WHOIS
- D.** Yet Another Recursive Acronym (YARA)

Answer: D (LEAVE A REPLY)

YARA is specifically designed to identify and classify suspicious or malicious files through pattern-based rules. A YARA rule can contain textual strings, hexadecimal byte sequences, regular expressions, metadata, file characteristics, and Boolean conditions. This makes YARA particularly effective when an analyst already has a binary specimen on an isolated analysis system and needs to determine whether it contains patterns associated with malware.

The official YARA documentation describes YARA as a tool for helping malware researchers identify and classify malware samples using textual and binary patterns. Rules consist primarily of strings and logical conditions that determine whether a file matches the defined characteristics.

The strings utility can reveal printable characters embedded within a binary and is useful during preliminary static analysis, but it does not itself classify the file against structured malware-detection signatures.

VirusTotal can perform multi-engine analysis, but submitting a potentially sensitive binary from an isolated environment to an external service may be inappropriate and is unnecessary when local YARA detection is available. WHOIS provides registration information about internet resources and has no direct binary- malware detection capability.

Study Guide Reference: Security Operations # Malware Analysis # Static Analysis # YARA # Signature and Pattern Matching # Binary/File Analysis.

NEW QUESTION: 8

A vendor releases details of a new vulnerability. When an analyst reviews the scheduled scans, no vulnerabilities are identified. The vulnerability is only discovered after a configuration change.

Which of the following scan types did the analyst configure?

- A. External
- B. Credentialed
- C. Agent-based
- D. Network

Answer: C (LEAVE A REPLY)

An agent-based scan relies on software installed directly on the endpoint to collect local system state and report vulnerability or configuration information to the management platform. Because the agent has local visibility, its findings can be influenced by endpoint configuration, agent policy, update state, privileges, enabled assessment modules, or configuration changes that determine what information is collected and evaluated.

The scenario indicates that regularly scheduled assessment activity initially failed to identify the newly disclosed vulnerability, but the condition became visible after a configuration change. Among the available choices, that behavior most strongly aligns with an agent-based assessment whose local collection or assessment configuration had to be updated before the vulnerability could be detected.

An external scan evaluates systems from outside the organizational boundary and focuses primarily on externally reachable services. A network scan examines hosts and services remotely and is governed mainly by network reachability and scanner capabilities. A credentialed scan authenticates into a system to obtain deeper visibility, but the defining characteristic in the question is the persistent endpoint-based assessment affected by configuration.

CySA+ vulnerability-management objectives distinguish assessment techniques by perspective, authentication level, deployment method, and resulting visibility.

Analysts must understand why different scanning architectures can produce different findings.

Study Guide Reference: Vulnerability Management # Vulnerability Scanning Methods # Agent-Based Scanning # Network Scanning # Credentialed Scanning # Scan Configuration and Coverage.

NEW QUESTION: 9

An analyst reviews the following system logs from a recent breach attempt:

Time	User	Command	IP
12:51:11	Berry	whoami	10.10.12.13
12:51:12	Berry	netstat -tulpn	10.10.12.13
12:51:13	Berry	sudo su	10.10.12.13
12:51:14	Berry	./linpeas.sh	10.10.12.13
12:51:15	Berry	su Larry	10.10.12.13
12:51:16	Larry	sudo nano	10.10.12.13
12:51:19	Larry	reset; sh1>&0 2>&0	10.10.12.13
12:51:25	root	FreePDFdumps whoami	10.10.12.13

Which of the following techniques did the attacker attempt to use?

- A. Exfiltration
- B. Remote code execution
- C. Privilege escalation
- D. Spoofing

Answer: (SHOW ANSWER)

The observed activity corresponds to privilege escalation , meaning the attacker attempted to move from a lower level of authorization to a more powerful security context. Privilege escalation becomes important after initial compromise because an account or process obtained during initial access frequently lacks the permissions required to disable controls, access sensitive resources, modify protected system settings, dump credentials, or establish deeper persistence.

MITRE ATT & CK defines the Privilege Escalation tactic as adversary activity intended to obtain higher- level permissions on a system or network. Techniques can include exploiting vulnerabilities, manipulating access tokens, modifying accounts or group memberships, abusing misconfigurations, or executing processes under more privileged identities.

Exfiltration specifically concerns removing information from the compromised environment. Remote code execution describes obtaining the ability to execute attacker-controlled commands or code remotely; while RCE can sometimes lead to privilege escalation, they represent different objectives. Spoofing involves impersonating or falsifying an identity, address, or other trusted characteristic.

The critical analytical distinction is therefore the attacker's objective demonstrated by the logs : attempting to obtain elevated access indicates privilege escalation rather than merely establishing execution or transferring data.

Study Guide Reference: Security Operations # Malicious Activity Analysis # MITRE ATT & CK # Privilege Escalation # Account/Permission Changes # System Log Interpretation.

NEW QUESTION: 10

Which of the following does a phishing campaign click rate measure?

- A. The effectiveness of an organization's email filters
- B. The false-positive rate of data leakage prevention behavior
- C. The employees' security awareness
- D. The speed of responding to a social engineering attack

Answer: C (LEAVE A REPLY)

A phishing simulation click rate measures user susceptibility to phishing and is therefore primarily an indicator of employee security awareness and behavior . If a simulated phishing message is delivered to employees and a percentage of recipients click the embedded malicious-style link, that percentage provides evidence about how effectively users are recognizing and resisting social-engineering attempts.

NIST research specifically identifies phishing-simulation click rates as a commonly used measure for evaluating the effectiveness of phishing-related security-awareness programs. NIST also cautions that raw click rates should be interpreted in context because phishing messages differ substantially in difficulty; the Phish Scale was developed to provide context for click-rate and report-rate results.

The metric does not primarily measure email-filter effectiveness because a controlled simulation may intentionally bypass or be allowlisted through technical filtering so employee behavior can be evaluated. It is unrelated to data-loss prevention false positives. It also does not directly measure response speed; metrics such as reporting time or mean time to respond would be more appropriate for that purpose.

Therefore, click rate is fundamentally a human-risk and awareness metric .

Study Guide Reference: Reporting and Communication # Security Metrics # Security Awareness # Phishing Simulations # Click Rate # Reporting Rate # Human Risk Measurement.

NEW QUESTION: 11

Which of the following is the most likely reason an organization might implement compensating controls?

- A.** A vulnerability does not have a patch, and the system is mission critical.
- B.** A vulnerability has been fixed, tested, and deployed to production.
- C.** A vulnerability is being actively exploited in the wild, but the organization does not use the affected system.
- D.** A vulnerability was detected, but the organization has determined the result is a false positive.

Answer: A (LEAVE A REPLY)

Compensating controls are appropriate when the preferred remediation cannot currently be implemented but the organization must still reduce exposure. A mission-critical system with an unpatched vulnerability for which no vendor patch exists is a classic example. The system cannot simply be removed from service because the business requires it, and conventional patching is unavailable.

The organization may therefore deploy alternative controls such as network segmentation, restrictive firewall rules, application allowlisting, disabling unnecessary services, enhanced monitoring, IPS signatures, access restrictions, or isolation of affected functionality. These measures do not eliminate the underlying defect; instead, they reduce the probability or impact of exploitation while a permanent solution is developed.

NIST's control framework is designed to allow security controls to be selected and tailored according to organizational mission requirements and risk, supporting the broader principle that organizations may apply appropriate alternative safeguards when operational constraints exist.

Option B requires no compensating control because remediation has already occurred. Option C describes a vulnerability that is not applicable to the organization's systems. Option D represents a false positive and therefore does not constitute an actual exposure requiring mitigation.

Study Guide Reference: Vulnerability Management # Mitigation # Compensating Controls # Patch Availability # Mission-Critical Systems # Segmentation and Monitoring.

NEW QUESTION: 12

Which of the following is the best reason to heavily segment business-critical assets from within the network?

- A.** Legacy systems
- B.** Degraded functionality
- C.** Asset obfuscation
- D.** Proprietary server

Answer: A (LEAVE A REPLY)

Legacy systems present a significant security problem because they frequently cannot support current operating systems, security agents, encryption mechanisms, authentication controls, or vendor patches. When a business-critical legacy system cannot be remediated normally, strong network segmentation becomes an important compensating control. The objective is to reduce the system's reachable attack surface and restrict which users, hosts, protocols, and applications can communicate with it.

A segmented legacy asset might be placed in a dedicated VLAN or security zone and protected through restrictive firewall access-control rules, jump hosts, allowlisting, enhanced logging, and continuous monitoring. Even though segmentation does not remove the underlying vulnerability, it decreases exposure and makes exploitation or lateral movement considerably more difficult.

Degraded functionality is generally an effect or remediation constraint rather than the strongest reason for isolation. Asset obfuscation does not provide reliable security because hidden systems can still be discovered through enumeration or traffic analysis. A proprietary server is not automatically vulnerable merely because its implementation is proprietary; it may still support modern patches and security controls.

CS0-004 specifically covers segmentation as a vulnerability-scanning consideration, compensating controls as a mitigation strategy, and legacy systems as an important inhibitor to remediation.

Study Guide Reference: Vulnerability Management # Vulnerability Prioritization and Mitigation # Compensating Controls # Segmentation # Legacy-System Constraints.

NEW QUESTION: 13

The Chief Information Security Officer (CISO) reviews the following security operations metrics from the last month:

Metric	Value	Notes
Alerts	5701	Raw SIEM alerts
Investigations	491	Actively investigated events
Incidents	5	Number of times incident was declared
Analyst hours	1400	Hours analysts spent investigating
Junior analysts	4	Total number of junior analysts
Senior analysts	7	Total number of senior analysts

- Which of the following is the best action to improve overall security operations efficiency?
- A. Leverage a cloud security posture management tool to add asset context to alerts.
 - B. Analyze and tune the detections that are causing non-actionable alerts.
 - C. Implement playbooks for the junior analysts to use during investigations.
 - D. Perform internal incident training on the most common alerts from security information and event management (SIEM).

Answer: B (LEAVE A REPLY)

The most direct method for improving SOC efficiency when excessive alerts are non-actionable is to identify the detections generating that noise and perform rule and alert tuning . Non-actionable detections consume analyst time, increase queue depth, contribute to alert fatigue, and can obscure genuinely malicious activity. Tuning may include adjusting thresholds, refining correlation logic, adding exclusions for legitimate behavior, improving indicator context, modifying detection conditions, or disabling rules that consistently generate false positives without meaningful security value.

A cloud security posture management platform may improve context for cloud-related findings, but it does not directly correct poorly performing detection logic across the broader SOC. Playbooks improve consistency and reduce investigation variability, particularly for junior analysts, but they still force personnel to process alerts that should not have been generated. Training can improve analyst performance, yet it also fails to address the source of excessive non-actionable notifications.

The CS0-004 Security Operations objectives explicitly identify efficiency and process improvement , including standardized processes, automation and orchestration, data enrichment, rule/alert tuning , dashboard creation, and technology integration.

Therefore, the optimal operational improvement is to reduce unnecessary workload at the detection layer itself.

Study Guide Reference: Security Operations # Efficiency and Process Improvement # Data Enrichment # Rule/Alert Tuning # SOC Optimization.

NEW QUESTION: 14

A security analyst runs an Nmap scan against a host with multiple open ports using the following command:

```
nmap 10.10.10.1 -p-
```

The following output is obtained after the scan:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 15:55 UTC
Note: Host seems down.
```

Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds

Which of the following is the most accurate way to scan the target IP for open ports?

- A. nmap 10.10.10.1 -p80, 443, 445, 9999, 135, 22, 21 -b --traceroute
- B. nmap -sn -p- 10.10.10.1
- C. nmap -p- -Pn 10.10.10.1
- D. nmap 10.10.10.1/24 -p- -R -O --script=ssl-enum-ciphers

Answer: ([SHOW ANSWER](#))

The original scan fails because Nmap's host-discovery process concludes that the target appears offline before conducting the intended full port scan. Option C adds -Pn , instructing Nmap to skip normal host discovery and proceed with scanning the target as though it is online. The -p- option then instructs Nmap to test the complete TCP port range rather than only its default set.

This is appropriate when a live host does not respond to discovery probes because ICMP echo traffic or other discovery packets may be filtered by firewalls, host-based controls, or network policy. A system can therefore appear "down" to Nmap's discovery phase while still exposing reachable TCP services.

Option B uses -sn, which performs host discovery without a port scan and therefore contradicts the requirement. Option A scans only a limited set of explicitly identified ports and includes unrelated functionality. Option D unnecessarily changes the scope to an entire /24, performs operating-system detection and DNS resolution, and invokes an SSL cipher script; none of those modifications addresses the immediate host-discovery problem.

Study Guide Reference: Vulnerability Management # Nmap # Host Discovery # -Pn # Full Port Scanning - p- # Firewall/ICMP Filtering # Scan Troubleshooting.

NEW QUESTION: 15

A Chief Information Security Officer (CISO) evaluates a threat heat map and notices a substantial increase in custom scanning and enumeration activities. The CISO wants to gather as much information as possible about the activities targeting the company to help prioritize mitigations.

Which of the following solutions is the best way to accomplish this goal?

- A. Configuring a honeypot in a separate environment to gather attacker techniques
- B. Leveraging canary tokens on all production systems to detect valid intrusion attempts
- C. Subscribing to information-sharing and threat intelligence reports for the industry
- D. Implementing a web application firewall in front of all applications and having it log attacks

Answer: ([SHOW ANSWER](#))

A honeypot is the strongest choice because the objective is not merely to block activity but to collect detailed intelligence about how adversaries are scanning, enumerating, and interacting with the organization. A properly isolated honeypot deliberately presents an attractive target while allowing defenders to observe attacker behavior without exposing legitimate production assets.

The resulting telemetry can reveal source infrastructure, targeted services, enumeration sequences, exploit attempts, command patterns, tools, payloads, and potentially broader TTPs. MITRE D3FEND defines a decoy environment as hosts and networks established specifically to deceive an attacker, and describes honeypots as decoy network resources that can expose an attacker's potential intent and strategy.

Canary tokens are valuable high-confidence tripwires but generally provide narrower detection evidence.

Threat-intelligence subscriptions provide external intelligence and may help with prioritization, yet they will not provide the same organization-specific visibility into actors actively interacting with the company's exposed environment. A WAF can log web attacks and block malicious requests, but its visibility is primarily limited to web application traffic.

Study Guide Reference: Security Operations # Threat Intelligence # Threat Hunting # Deception Technologies # Honeypots/Honeynets # Adversary TTP Collection.

NEW QUESTION: 16

A security analyst isolates a Windows 11 workstation from the network after known malware is detected. The list of security information and event management (SIEM) events during the malware installation and timeline does not identify a specific user who was logged in. The security analyst uses the local administrative account to log in and would like a list of logins to the machine.

Which of the following PowerShell commands should the analyst use?

A. Eventvwr.exe -LogType "Security" EventID "*" | Export-Csv c:\temp\Seclog.csv -NoTypeInfoInformation

B. Get-WinEvent -FilterHashTable @{ Logname="Security"

ED=4624;

} | Sort-Object TimeCreated -Descending | Export-Csv c:\temp\Seclog.csv -NoTypeInfoInformation

C. Get-WinEvent -FilterHashTable @{ Logname="System"

ED=9754;

} | Sort-Object TimeCreated -Descending | Export-Csv c:\temp\Seclog.csv -NoTypeInfoInformation

D. Get-WinEvent -FilterHashTable @{ Logname="Application"

ED=7124;

} | Sort-Object TimeCreated -Descending | Export-Csv c:\temp\Seclog.csv -NoTypeInfoInformation

Answer: B (LEAVE A REPLY)

Windows Security Event ID 4624 records a successful logon session. Therefore, querying the Security log for event 4624 provides the analyst with historical evidence of successful logins to the affected workstation.

Get-WinEvent is the appropriate PowerShell cmdlet for retrieving Windows event records. The FilterHashtable parameter allows efficient server-side filtering using attributes such as LogName and ID, rather than retrieving an entire event log and filtering the results afterward. Microsoft specifically documents LogName and ID as valid FilterHashtable keys and recommends this approach for efficient event-log querying.

The command then uses Sort-Object TimeCreated -Descending so the newest login events appear first, and Export-Csv preserves the resulting records for investigation.

Option A does not use the correct PowerShell event-query syntax shown. Options C and D search inappropriate log channels and unrelated event IDs. The evidence needed is authentication history, making the Windows Security log and successful-logon identifier 4624 the correct combination.

Study Guide Reference: Incident Response and Management # Evidence Collection # Windows Event Logs

PowerShell # Get-WinEvent # Security Event ID 4624 # Timeline Reconstruction.

Valid CS0-004 Dumps shared by Actual4test.com for Helping Passing CS0-004 Exam! Actual4test.com now offer the **newest CS0-004 exam dumps**, the Actual4test.com CS0-004 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CS0-004 dumps with Test Engine here: https://www.actual4test.com/CS0-004_examcollection.html (190 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 17

A security analyst receives a notice about a possible data breach. The report identifies unapproved, current access dates for files found in the following personnel archives:

Name	Date modified	Type	Size
Jones, P.	2/17/2022 10:21 AM	.zip	13Gb
Jones, R.	8/31/2025 3:15 PM	.zip	10Gb
Smith, A.	7/15/2024 1:45 PM	.zip	11Gb
Smith, D.	8/15/2025 9:23 AM	.zip	12Gb
Smith, J.	8/31/2025 3:36 PM	.zip	11Gb

Which of the following actions should the analyst take first?

- A. Perform log correlation.
- B. Reset user credentials.
- C. Restore files from backup.
- D. Establish a timeline.
- E. Establish a legal hold.

Answer: E (LEAVE A REPLY)

The analyst should first establish a legal hold because the suspected breach involves personnel records and evidence that may become relevant to regulatory, disciplinary, civil, or other legal proceedings. A legal hold prevents potentially relevant information from being deleted, overwritten, modified, rotated out under normal retention schedules, or otherwise destroyed before the organization's legal and investigative obligations are understood.

Preservation must precede destructive or potentially evidence-altering actions. NIST describes digital forensics as retrieving, storing, and analyzing electronic information while ensuring that evidence is captured reliably without alteration. RFC 3227 similarly emphasizes preserving evidence, following proper collection procedures, documenting handling, and maintaining chain of custody.

Log correlation and timeline construction are important investigative activities, but they should occur after preservation requirements have been established. Resetting credentials may subsequently be required for containment, but the scenario first raises an evidence-preservation obligation. Restoring files from backup would be especially premature because it could alter timestamps, overwrite artifacts, or otherwise complicate forensic analysis.

The examination principle is therefore preserve first when legal implications are reasonably foreseeable; analyze and remediate afterward under controlled procedures .

Study Guide Reference: Incident Response and Management # Evidence Acquisition # Legal Hold # Evidence Preservation # Chain of Custody # Timeline Analysis # Regulatory/Legal Considerations.

NEW QUESTION: 18

Which of the following best explains the purpose of the Pyramid of Pain in threat intelligence?

- A. To show that changing to different types of indicators and behaviors is difficult for an adversary
- B. To measure how much operational damage a threat actor can cause before detection occurs
- C. To compare open-source intelligence (OSINT) with closed-source intelligence based on collection cost
- D. To organize attack activity into categories such as spoofing, tampering, and repudiation

Answer: A (LEAVE A REPLY)

The Pyramid of Pain illustrates the increasing operational difficulty imposed on an adversary when defenders successfully detect and deny progressively more behavioral indicators. At the lower levels are artifacts that attackers can replace relatively easily, such as hash values and IP addresses. Higher levels include domain names, network or host artifacts, tools, and ultimately tactics, techniques, and procedures (TTPs) .

Its central defensive lesson is that not all indicators impose equal cost on an attacker. Blocking one IP address may require the attacker only to obtain another server. Detecting a specific malware hash can often be defeated by recompiling or modifying the file. Detecting the attacker's established behaviors and operational methods creates substantially greater difficulty because the adversary may need to redesign procedures, change tooling, retrain operators, or alter an established intrusion methodology.

The Pyramid of Pain was developed specifically to describe this relationship between indicators and the amount of operational "pain" defenders impose when those indicators are denied.

Option B describes impact measurement, not indicator durability. Option C concerns intelligence-source classification. Option D resembles threat-modeling approaches such as STRIDE rather than the Pyramid of Pain.

Study Guide Reference: Security Operations # Threat Intelligence # Pyramid of Pain # Indicators of Compromise # Tools # TTPs # Behavioral Detection.

NEW QUESTION: 19

The vulnerability management team must scan the cloud environment to establish security baselines.

Which of the following assessment tools should the team use to perform this task?

- A. Prowler
- B. Caldera
- C. Metasploit
- D. Maltego

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

NEW QUESTION: 20

Which of the following is the most comprehensive type of report associated with a closed incident?

- A. Lessons-learned
- B. Situation
- C. Root cause analysis
- D. After action

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

An after-action report (AAR) is the most comprehensive document associated with a closed incident because it consolidates the incident itself, the response activities performed, recovery actions, outcomes, deficiencies, and lessons identified during the event. NIST Cybersecurity Framework guidance specifically calls for preparing an after-action report that documents the incident, response and recovery activities, and lessons learned.

A lessons-learned document focuses primarily on what worked, what failed, and what should be improved.

Those observations are important, but they represent only one component of a complete post-incident record.

Root cause analysis has a narrower technical purpose: determining the fundamental condition that permitted the incident to occur or progress. A situation report is generally produced while an incident is ongoing to communicate current status, impact, actions, and outstanding issues.

An AAR is broader because it can incorporate the timeline, technical findings, containment and eradication actions, recovery results, stakeholder performance, root cause, lessons learned, and assigned corrective actions. NIST exercise guidance likewise treats lessons learned as information that becomes part of an after-action report.

Study Guide Reference: Reporting and Communication # Post-Incident Reporting # After-Action Reports

Lessons Learned # Root Cause Analysis # Corrective Actions.

NEW QUESTION: 21

Which of the following is the most important reason why tactics, techniques, and procedures (TTP) are beneficial to a defensive strategy?

- A. TTP provides useful insights on the hash values and internet protocol addresses attributed to an attacker.
- B. TTP provides useful insights on an attacker's indicators of compromise.
- C. TTP provides useful insights on the tools used by an attacker.
- D. TTP provides useful insights on the strategy and behavior of an attacker.

Answer: ([SHOW ANSWER](#))

Tactics, techniques, and procedures represent the behavioral characteristics of an adversary rather than merely individual technical artifacts. A tactic describes the adversary's objective, a technique identifies how that objective is achieved, and procedures represent the specific implementation observed during an intrusion. Consequently, TTP intelligence allows defenders to understand how an attacker operates , including patterns of reconnaissance, persistence, privilege escalation, lateral movement, command-and-control activity, and other operational behaviors.

Options A and B focus primarily on indicators of compromise such as IP addresses and hashes. These are useful for detection, but they are comparatively fragile because attackers can replace infrastructure, change domains, regenerate malware, or modify files to produce different hashes. Option C is broader than an individual IoC, but tools can likewise be replaced or modified. Behavioral knowledge is generally more durable because changing established operational methods imposes greater cost on an adversary.

The CS0-004 objectives explicitly place TTPs, Pyramid of Pain, MITRE ATT & CK, attribution, IoC analysis, and behavioral indicators within threat intelligence and threat-hunting concepts.

Study Guide Reference: Security Operations # Threat Intelligence and Threat Hunting # TTPs # Pyramid of Pain # MITRE ATT & CK # Behavioral IoCs.

NEW QUESTION: 22

An analyst performs Nmap scans to determine which hosts may need to be targeted to deploy a critical Windows patch. The patch for the vulnerability is to address a critical security flaw that targets open Server Message Block (SMB) ports on Windows systems only.

The analyst scans with the following command:

```
ost is up, received user-set (0.0065s latency)
canned at 2025-05-01 18:50:59 UTC for 8s
ot shown: 997 filtered tcp ports (no-response)
ORT STATE SERVICE REASON
2/tcp open ***** syn-ack ttl 128
35/tcp open ***** syn-ack ttl 128
45/tcp open ***** syn-ack ttl 128
389/tcp open ***** syn-ack ttl 128
```

```
map scan report for 10.203.10.12
ost is up, received user-set (0.0028s latency)
canned at 2025-05-01 18:50:59 UTC for 2s
ot shown: 995 closed tcp ports (reset)
ORT STATE SERVICE REASON
2/tcp open ***** syn-ack ttl 64
3/tcp filtered ***** no-response
0/tcp open ***** syn-ack ttl 64
389/tcp open ***** syn-ack ttl 64
080/tcp open ***** syn-ack ttl 64
```

```
map scan report for 10.203.10.13
ost is up, received user-set (0.0070s latency)
canned at 2025-05-01 18:50:59 UTC for 2s
ot shown: 995 closed tcp ports (reset)
ORT STATE SERVICE REASON
2/tcp open ***** syn-ack ttl 64
3/tcp filtered ***** no-response
0/tcp open ***** syn-ack ttl 64
389/tcp open ***** syn-ack ttl 64
080/tcp open ***** syn-ack ttl 64
```

```
map scan report for 10.203.10.16
ost is up, received user-set (0.0065s latency)
canned at 2025-05-01 18:50:59 UTC for 8s
ot shown: 997 filtered tcp ports (no-response)
ORT STATE SERVICE REASON
2/tcp open ***** syn-ack ttl 128
35/tcp open ***** syn-ack ttl 128
```

\$sudo nmap -Pn 10.203.10.0/24

The analyst then receives the following output:

Which of the following hosts should the analyst prioritize for patching?

- A. 10.203.10.11
- B. 10.203.10.12

C. 10.203.10.13

D. 10.203.10.16

Answer: ([SHOW ANSWER](#))

The analyst should prioritize 10.203.10.11 because the scan output identifies that host as presenting the Windows SMB exposure relevant to the critical vulnerability. Vulnerability prioritization requires matching the vulnerability's technical prerequisites against the characteristics discovered on each host rather than simply patching every responding system indiscriminately.

Modern SMB services commonly use TCP port 445 . Microsoft documents TCP 445 as a required port for SMB-based file services, with port 139 associated with older NetBIOS-based implementations. Therefore, a Windows host exposing the affected SMB service satisfies an essential condition for applicability and should be prioritized when the vulnerability specifically targets open SMB ports.

The -Pn option is also significant operationally because it instructs Nmap to treat targets as online without relying on normal host-discovery probes. The analyst can consequently inspect reachable service ports even when systems do not respond to standard discovery methods.

The remaining hosts either do not expose the vulnerable SMB service or do not match the required Windows

/service profile described by the scenario. Priority should follow confirmed applicability, exposure, severity, and exploitability.

Study Guide Reference: Vulnerability Management # Nmap # Port Scanning # SMB # TCP 445/139 # Vulnerability Applicability # Remediation Prioritization.

NEW QUESTION: 23

Which of the following describes the main benefits of MITRE ATT & CK Navigator?

A. Replicating adversary behavior and blocking gaps in defenses

B. Monitoring adversary behavior and performing malware reverse engineering

C. Responding to adversary behavior and building security defense tools

D. Understanding adversary behavior and identifying gaps in defenses

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

MITRE ATT & CK Navigator is primarily a visualization and analytical tool for understanding adversary behavior and evaluating defensive coverage against ATT & CK tactics and techniques. Analysts can create layers over ATT & CK matrices, highlight techniques associated with specific threat groups, compare adversary profiles, record detection coverage, and identify techniques for which defensive visibility or controls are insufficient.

MITRE explicitly states that ATT & CK Navigator can be used to visualize defensive coverage, support red- team and blue-team planning, and represent the frequency of detected techniques. MITRE's ATT & CK design guidance also recognizes defensive gap assessment as a means of identifying areas where an enterprise lacks sufficient defenses or visibility.

Navigator itself does not replicate adversary behavior; adversary-emulation platforms and red-team tools perform that function. It is not a malware reverse-engineering platform, nor does it independently build defensive tools or execute incident-response actions.

Its major operational value is translating ATT & CK's behavioral knowledge base into a visual map that lets defenders answer two questions: What behaviors are relevant to the threats we face, and where do our detections or controls have gaps?

Study Guide Reference: Security Operations # MITRE ATT & CK # ATT & CK Navigator # Tactics and Techniques # Threat Mapping # Detection Coverage # Gap Analysis.

NEW QUESTION: 24

A security analyst responds to an alert regarding identity and access management activity within the cloud environment. The attacker is currently trying to gain access from one isolated cloud subscription to another via a compromised user role.

Which of the following aspects of the MITRE ATT & CK framework is the attacker trying to perform?

A. Privilege escalation

B. Lateral movement

- C. Persistence
- D. Execution
- E. Credential access

Answer: ([SHOW ANSWER](#))

The attacker is attempting lateral movement because an already compromised identity is being used to move from one cloud environment or subscription into another. Lateral movement describes adversary activity intended to reach additional systems, services, accounts, or resources after an initial foothold has been established. MITRE ATT & CK specifically includes cloud-oriented lateral movement. Its Lateral Movement tactic documents adversaries using valid accounts to access additional cloud services and resources within compromised environments. MITRE also documents cloud-role manipulation that may enable movement into additional accounts, demonstrating how identity and role relationships can become lateral-movement pathways in cloud architectures.

Privilege escalation would apply if the attacker were primarily attempting to obtain greater permissions within the current security context. Persistence concerns maintaining long-term access. Execution concerns running malicious code or commands. Credential access involves obtaining credentials or authentication material. In this scenario, the attacker already possesses a compromised user role. The objective is to use that existing access to traverse a trust boundary and reach another isolated subscription. That movement between security domains is the decisive indicator of the Lateral Movement tactic.

Study Guide Reference: Security Operations # MITRE ATT & CK # Lateral Movement # Cloud Services # Valid Accounts # IAM Roles # Cross-Subscription Access.

NEW QUESTION: 25

A new security operations center (SOC) manager joins a team that struggles to meet service-level agreements (SLAs). The alert backlog continues to increase daily. Which of the following will the manager most likely need to do?

- A. Automate escalation.
- B. Improve the triage processes.
- C. Upgrade threat intelligence.
- D. Enhance the customer service response.

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

Improving the triage process addresses the underlying operational bottleneck described in the scenario. SOC triage determines which alerts require investigation, their relative severity, whether they represent true or false positives, and which cases require escalation. When triage is inefficient, alerts accumulate faster than analysts can classify them, causing backlog growth and SLA violations.

A mature triage workflow applies consistent severity criteria, asset criticality, threat context, confidence levels, enrichment, deduplication, and predefined escalation thresholds. This reduces analyst effort spent on low-value events while ensuring genuinely dangerous alerts reach investigators quickly. Modern SIEM and security analytics platforms similarly emphasize grouping and correlating alerts into incidents to reduce unnecessary investigation workload. Microsoft Sentinel, for example, uses analytics and correlation to reduce noise and consolidate related alerts into incidents.

Automating escalation does not resolve poor initial classification and can simply transfer excessive noise downstream. Better threat intelligence may enrich alerts but will not inherently correct a dysfunctional queue.

Customer-service response is unrelated to SOC alert processing.

Study Guide Reference: Security Operations # SOC Operations # Alert Management # Triage # Prioritization # Escalation Procedures # Process Improvement.

NEW QUESTION: 26

A security operations center analyst is using the command line to display specific traffic.

The analyst uses the following command:

```
$tshark -r file.pcap -Y "http or udp"
```

Which of the following will the command line display?

- A. Encrypted web requests and Domain Name System (DNS) traffic

- B. Unencrypted web requests and DNS traffic
- C. Neither encrypted nor unencrypted web and DNS traffic
- D. Both encrypted and unencrypted web and DNS traffic

Answer: ([SHOW ANSWER](#))

The -r file.pcap argument instructs TShark to read packets from the specified capture file, while -Y applies a Wireshark display filter. The expression "http or udp" therefore displays packets recognized as HTTP or packets using UDP.

Traditional HTTP traffic is unencrypted and can be dissected directly as HTTP. HTTPS normally carries HTTP inside TLS encryption and therefore is not displayed merely because the filter specifies http. DNS commonly operates over UDP, particularly for standard queries and responses, so ordinary DNS traffic satisfies the udp portion of the expression. Consequently, B is the best answer in the context of the available choices.

A technical distinction is important: the expression does not mean "HTTP or DNS specifically." The udp portion matches UDP traffic generally, which can include protocols other than DNS. Nevertheless, within the examination scenario, the intended comparison is plaintext HTTP versus encrypted HTTPS together with standard UDP-based DNS.

Wireshark's documentation distinguishes display filters from capture filters, and TShark is the command-line network traffic analyzer within the Wireshark suite. CS0-004 places packet-analysis capabilities within Security Operations.

Study Guide Reference: Security Operations # Packet Analysis # Wireshark/TShark # PCAP Analysis # Display Filters # HTTP, UDP, and DNS.

NEW QUESTION: 27

Which of the following allows an organization to leverage AI in various forms while protecting business objectives and data?

- A. Usage policies
- B. Prompt engineering
- C. Non-disclosure agreement
- D. Incident response policy

Answer: ([SHOW ANSWER](#))

AI usage policies establish organizational boundaries for how artificial intelligence systems may be selected, accessed, configured, and used. They allow an organization to obtain operational benefits from AI while controlling risks involving confidential information, intellectual property, regulated data, model outputs, external AI services, and inappropriate automation. A strong policy can define approved platforms, prohibited data categories, validation requirements, human oversight, retention rules, acceptable use, and escalation procedures.

Prompt engineering is a technical method for constructing inputs that produce more useful model responses. It can improve output quality but does not establish enterprise-wide safeguards for protecting business objectives or sensitive information. A non-disclosure agreement establishes contractual confidentiality obligations between parties; it cannot govern the full technical and operational use of AI systems. An incident response policy determines how security incidents are managed and escalated, but it is reactive and not designed to establish routine AI governance.

CS0-004 explicitly addresses AI within Security Operations. The objectives identify AI risks including hallucinations, data exposure, model poisoning, and malicious prompts and identify governance considerations including legal or regulatory compliance and AI usage policies. AI use cases include log analysis, artifact comparison, incident investigation, event correlation, and automation.

Study Guide Reference: Security Operations # AI in Security Operations # AI Risks # Governance # AI Usage Policies # Data Protection.

NEW QUESTION: 28

An analyst is assigned to a new cybersecurity improvement project. The analyst wants to better understand the workflow processes and the skill set of the cybersecurity engineers on this task force. The analyst sets up a recurring, weekly conference call.

Which of the following best describes the purpose for the conference call?

- A. To conduct incident response training

- B. To create vendor information sessions
- C. To manage and facilitate team coordination
- D. To respond to customer requirements

Answer: C (LEAVE A REPLY)

The recurring weekly conference call is intended to manage and facilitate team coordination . The analyst's stated objectives are to understand workflow processes and the capabilities of the engineers participating in the cybersecurity improvement project. Regular coordination meetings provide a structured mechanism for sharing operational updates, clarifying responsibilities, identifying dependencies, communicating blockers, aligning technical activities, and understanding which personnel possess the expertise required for particular tasks.

Nothing in the scenario indicates an incident requiring formal incident-response training. Training would normally involve exercises, tabletop scenarios, simulations, procedures, or instruction designed to build response capability. There is also no vendor involvement, so a vendor information session would not satisfy the stated objective. Likewise, no customer request is identified.

The distinguishing clue is the combination of a cross-functional task force, workflow understanding, skills visibility, and recurring communication . These elements support internal project coordination rather than external communication or formal instruction.

Within CySA+, reporting and communication extends beyond writing final reports. Analysts must communicate effectively with technical teams, coordinate activities with relevant stakeholders, provide appropriate status information, and ensure security work is understood and actionable across organizational functions.

Study Guide Reference: Reporting and Communication # Stakeholder Communication # Team Coordination

Roles and Responsibilities # Workflow Management # Cross-Functional Collaboration.

NEW QUESTION: 29

A security analyst analyzes the output of a web application access log for a company based in the United States.

Given the following output:

datetime	username	status	ip_address	region
07-12-2025 09:01:00Z	tlindy	failed	63.102.4.78	US
07-12-2025 09:02:00Z	tlindy	success	63.102.4.78	US
07-12-2025 09:03:00Z	jschott	failed	185.23.154.24	RU
07-12-2025 09:07:00Z	ssanford	success	63.102.4.71	US
07-12-2025 09:08:00Z	mschultz	success	63.102.4.74	US
07-12-2025 09:08:00Z	jschott	failed	185.23.154.22	RU
07-12-2025 09:10:00Z	wlangey	success	63.102.4.79	US
07-12-2025 09:14:00Z	pking	failed	185.23.127.21	RU
07-12-2025 09:15:00Z	tlindy	success	185.87.14.12	RU
07-12-2025 09:13:00Z	jschott	failed	185.28.154.54	RU
07-12-2025 09:18:00Z	oohara	success	63.102.4.70	US
07-12-2025 09:18:00Z	jschott	failed	185.23.127.21	RU
07-12-2025 09:19:00Z	mschultz	success	63.102.4.74	US
07-12-2025 09:20:00Z	qjones	success	63.102.4.71	US
07-12-2025 09:23:00Z	jschott	success	63.102.4.78	US
07-12-2025 09:23:00Z	dmann	failed	185.23.127.21	RU
07-12-2025 09:25:00Z	tlindy	success	63.102.4.71	US
07-12-2025 09:25:00Z	jschott	failed	185.143.137.221	RU
07-12-2025 09:25:00Z	mschultz	success	63.102.4.74	US

Which of the following users should be investigated first?

- A. jschott
- B. dmann
- C. mschultz

D. tlindy

Answer: D (LEAVE A REPLY)

The analyst should prioritize tlindy because the activity associated with that account presents the strongest anomaly in the supplied access-log evidence. Web access-log analysis is fundamentally contextual: an analyst compares source information, request behavior, authentication activity, timestamps, response codes, geographic indicators, user-agent characteristics, and established behavioral expectations to determine which entry warrants immediate investigation.

The fact that the organization is explicitly identified as being based in the United States is an important contextual clue. Geographic or behavioral activity inconsistent with the expected operating profile of an account can raise investigative priority, particularly when combined with unusual authentication or web-request characteristics. Importantly, geographic deviation alone does not prove compromise; VPN services, business travel, cloud infrastructure, and remote-working arrangements can produce legitimate anomalies.

The correct SOC action is therefore investigation rather than immediate attribution.

This question tests the analyst's ability to distinguish normal activity from anomalous activity using log context, rather than simply searching for a particular HTTP status code or username. CySA+ expects analysts to correlate multiple data points before establishing whether activity represents an indicator of compromise.

The uploaded examination material identifies tlindy as the account requiring first investigation.

Study Guide Reference: Security Operations # Log Analysis # Web Application Logs # Behavioral Indicators # Anomaly Detection # User and Entity Context.

NEW QUESTION: 30

Which of the following actions should an incident response analyst take during the recovery phase of the incident response process?

A. Verify that malicious activity has occurred.

B. Reimage the disk.

C. Take the system offline.

D. Write the final report.

Answer: B (LEAVE A REPLY)

Reimaging the disk is a recovery activity because it restores the compromised endpoint to a trusted operational state after malicious activity has been identified and contained. Reimaging replaces the affected operating environment with a known-good system image, removing uncertainty about hidden persistence mechanisms, modified system files, unauthorized software, or other residual effects of compromise.

Verification that malicious activity occurred belongs to the detection and analysis stage. Taking the system offline is a containment measure intended to prevent additional propagation, command-and-control communication, or damage. Writing the final report occurs during post-incident documentation and lessons-learned activities rather than operational restoration.

NIST's Recover function focuses on restoring affected assets and operations and verifying that restored systems are suitable for return to normal business use. A clean reimage is particularly appropriate where the integrity of the compromised operating system cannot be reliably established through selective malware removal.

After rebuilding, analysts should verify configuration, patch levels, security controls, credentials, and monitoring before reconnecting the machine to production.

Study Guide Reference: Incident Response and Management # Recovery # Reimaging # Known-Good Baselines # Restoration Validation # Return to Production.

NEW QUESTION: 31

Which of the following is commonly used after an incident has been resolved to identify efficiencies and corrective actions related to activities performed during the incident response process?

A. Lessons learned

B. Key performance indicators (KPIs) and performance metrics

C. Executive summary

D. Root cause analysis

Answer: A (LEAVE A REPLY)

A lessons learned review evaluates how the incident was handled and identifies improvements that should be incorporated into future response activities. It examines what worked well, what created delays, where communications or escalation failed, whether tools and playbooks were effective, and which corrective actions should be assigned to reduce the likelihood or impact of similar incidents.

NIST's current incident-response guidance places strong emphasis on continuous improvement. It states that lessons identified during incident-response activities should feed into organizational improvement so policies, processes, practices, and security capabilities can be adjusted as necessary. NIST also notes that traditional post-incident activities identify required improvements and return them to preparation and broader cybersecurity risk management.

KPIs quantify operational performance but do not themselves provide the qualitative review necessary to identify process efficiencies and corrective actions. An executive summary communicates major incident facts and outcomes to leadership. Root cause analysis focuses on identifying the fundamental technical or organizational cause of the incident; it can contribute to lessons learned but is narrower in scope.

Therefore, the broader mechanism for reviewing the entire response process and developing improvement actions is the lessons-learned process.

Study Guide Reference: Reporting and Communication # Post-Incident Reporting # Lessons Learned # Corrective Actions # Process Improvement # Stakeholder Feedback.

Valid CS0-004 Dumps shared by Actual4test.com for Helping Passing CS0-004 Exam! Actual4test.com now offer the **newest CS0-004 exam dumps**, the Actual4test.com CS0-004 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CS0-004 dumps with Test Engine here: https://www.actual4test.com/CS0-004_examcollection.html (190 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 32

Which of the following best describes why operational technology (OT) devices use compensating controls?

- A. Industrial control systems use significant network bandwidth.
- B. Outage windows are usually scheduled.
- C. Traditional IT security solutions may not be compatible.
- D. OT devices are typically not encrypted.

Answer: C (LEAVE A REPLY)

Operational technology environments frequently contain specialized controllers, industrial control systems, supervisory control and data acquisition equipment, embedded operating systems, and vendor-specific devices that were designed primarily for availability, safety, deterministic operation, and long service life. Traditional enterprise security controls-such as endpoint detection agents, vulnerability scanners, host-based firewalls, aggressive patching mechanisms, or modern authentication software-may not be supported and can potentially interfere with operational processes.

For this reason, organizations often implement compensating controls around OT assets when the preferred security control cannot be deployed directly. Examples include network segmentation, tightly controlled firewall rules, protocol allowlisting, passive monitoring, secure jump servers, access restrictions, enhanced logging, and additional physical controls. These measures reduce risk without requiring unsupported software to be installed on sensitive industrial devices.

High network bandwidth consumption is not the defining reason for compensating controls. Scheduled outage windows can actually facilitate maintenance rather than explain why alternative controls are required.

Likewise, lack of encryption may be a weakness in some environments, but it does not explain the broader compatibility problem.

CS0-004 specifically places OT, ICS, and SCADA under critical-infrastructure concepts in Security Operations and separately recognizes compensating controls as a formal vulnerability mitigation strategy.

Study Guide Reference: Security Operations # Critical Infrastructure # OT/ICS/SCADA # Security Architecture # Compatibility Constraints and Compensating Controls.

NEW QUESTION: 33

Which of the following occurs during the analysis phase of the incident response process?

- A. Triage
- B. Alert writing
- C. Reimaging
- D. Isolation

Answer: (SHOW ANSWER)

Triage occurs during the analysis phase because responders must determine what an alert represents, how serious it is, which assets are affected, and what response priority should be assigned before taking broader containment or recovery actions.

Triage typically involves validating the alert, gathering supporting telemetry, establishing whether the event is a true positive, determining scope and impact, identifying affected identities or systems, correlating indicators, and assigning severity. The outcome provides the evidence required to decide whether an event should be escalated into formal incident handling and what subsequent actions are justified. NIST incident- handling guidance has historically emphasized analyzing incident-related information in order to determine the appropriate response, while the current NIST framework continues to emphasize efficient incident detection, response, and recovery.

Isolation belongs to containment because it restricts the compromised asset's ability to communicate or spread malicious activity. Reimaging normally occurs during recovery after the environment has been contained and malicious persistence addressed. Alert writing is part of detection engineering or security- monitoring operations rather than a defining incident-analysis activity.

The sequence is therefore important: detect # analyze/triage # contain # eradicate # recover # conduct post-incident activities .

Study Guide Reference: Incident Response and Management # Incident Response Process # Detection # Analysis/Triage # Containment # Eradication # Recovery.

NEW QUESTION: 34

A cybersecurity analyst is reviewing static application security testing scan results and notices a finding for hard-coded credentials.

Which of the following should the analyst recommend to the application team to resolve this concern?

- A. Implement a privileged access management solution.
- B. Enable single sign-on.
- C. Obfuscate application programming interface keys.
- D. Integrate secrets management.

Answer: D (LEAVE A REPLY)

The correct remediation is to integrate a secrets-management solution and remove credentials from application source code. Hard-coded passwords, API keys, access tokens, certificates, and similar secrets create serious exposure because anyone who obtains the source repository, package, build artifact, backup, or configuration may recover the credential.

OWASP specifically identifies hard-coded secrets in source code and configuration files as a secrets- management problem and recommends centralized controls for securely storing, retrieving, rotating, auditing, and managing secrets throughout their lifecycle.

A secrets-management platform allows applications to retrieve sensitive values securely during execution instead of embedding them directly in code. Proper implementation also supports rotation and revocation when credentials are exposed.

PAM primarily governs privileged human or service access and is not the most direct application-code remediation. Single sign-on reduces repeated user authentication but does not remove embedded application credentials. Obfuscation is inadequate because an application that needs an API key must ultimately be capable of recovering and using it; attackers can often reverse that transformation.

The correct secure-development principle is therefore separation of secrets from application code .

Study Guide Reference: Vulnerability Management # SAST # Hard-Coded Credentials # Secrets Management # API Keys # Credential Rotation # Secure Software Development.

NEW QUESTION: 35

A security team reviews a penetration testing report of a web application that contains multiple cross-site scripting (XSS) and Structured Query Language injection (SQLi) vulnerabilities.

Which of the following is most likely causing these to occur?

- A. Misconfigured web application firewall (WAF)
- B. Lack of secure input validation
- C. Lack of a Hypertext Transfer Protocol (HTTP) Strict Transport Security (HSTS) header
- D. Lack of endpoint protection in the environment

Answer: B (LEAVE A REPLY)

The common underlying weakness is insufficient handling and validation of untrusted application input .

XSS occurs when attacker-controlled content is processed and subsequently rendered in a manner that allows script execution. SQL injection occurs when untrusted values become part of database commands without appropriate separation between code and data.

OWASP recommends validating untrusted input early in the processing workflow and applying syntactic and semantic validation. For SQL injection specifically, OWASP identifies parameterized queries as the primary defensive technique and recommends allow-list input validation as an additional defensive layer. For XSS, context-appropriate output encoding and sanitization must also be applied; therefore input validation should be viewed as part of secure application handling rather than the sole technical control.

A WAF can provide defense in depth but does not correct vulnerable application code. HSTS forces browsers to use HTTPS and protects transport security; it does not prevent malicious input from being interpreted by an application. Endpoint protection similarly operates on hosts and does not repair web application data-handling flaws.

Study Guide Reference: Vulnerability Management # Application Vulnerabilities # XSS # SQL Injection # Input Validation # Output Encoding # Parameterized Queries # Secure Coding.

NEW QUESTION: 36

A security operations center (SOC) analyst investigates the results of a password spray test conducted by the vulnerability management team.

The analyst must:



Identify Linux systems that have successful and unsuccessful logins with username "User1".

Create an output report named "linux-events" of all the events to a flat file.

The analyst issues the following console command:

ls /var/log/

The shortened output of the command is below:

Which of the following commands should the analyst use to meet the report output requirements?

- A. cat /var/log/ssslog | grep "User1" > linux-events.txt
- B. cat /var/log/faillog.log | grep "User1" > linux-events.txt
- C. cat /var/log/syslog | grep "User1" > linux-events.txt
- D. cat /var/log/auth.log | grep "User1" > linux-events.txt

Answer: D (LEAVE A REPLY)

/var/log/auth.log is the appropriate source because it records authentication and authorization activity on Debian/Ubuntu-style Linux systems, including password-related events, SSH logins, PAM authentication, and other authorization events. Canonical's Ubuntu documentation specifically identifies /var/log/auth.log as the authorization log used for password prompts, sudo, and remote logins.

The command performs three operations. `cat /var/log/auth.log` sends the log contents to standard output. The pipe forwards that data to `grep "User1"`, which selects records containing the required username. Finally, `> linux-events.txt` redirects the resulting matching records into the requested flat-file report. Because `auth.log` can contain both accepted and rejected authentication activity, the command can capture successful and unsuccessful events associated with User1.

`sssd` is not the general authentication log path shown in the scenario and may contain only SSSD-specific events. A faillog-oriented source emphasizes failed logins and therefore does not satisfy the requirement to collect both successful and failed activity. `/var/log/syslog` contains broad system messages but is less precise than the dedicated authentication log.

Study Guide Reference: Security Operations # Linux Log Analysis # /var/log/auth.log # cat # grep # Output Redirection # Authentication Investigation.

NEW QUESTION: 37

Before merging with a software company, the acquiring company's legal team requires a detailed software scan to determine if all code base is using open-source or paid licensed libraries. The vulnerability management analyst needs to provide this report.

Which of the following scan methods will best meet this requirement?

- A. Static application security testing (SAST)
- B. Dynamic application security testing (DAST)
- C. Software composition analysis (SCA)
- D. Runtime application self-protection (RASP)
- E. Credentialed vulnerability scan

Answer: C (LEAVE A REPLY)

Software Composition Analysis (SCA) is specifically designed to identify third-party and open-source components incorporated into software. It can enumerate libraries and dependencies, identify their versions, associate components with known vulnerabilities, and provide licensing information. This directly satisfies the legal team's requirement to determine whether the codebase contains open-source or commercially licensed libraries.

CISA's software supply-chain guidance recognizes software composition analysis and software bills of materials as mechanisms for obtaining visibility into software components. CISA guidance also notes that SBOM information can include both open-source and commercial third-party software and licensing information.

SAST examines source or compiled code for security weaknesses such as unsafe functions, data-flow problems, or coding vulnerabilities, but dependency licensing is not its primary purpose. DAST tests a running application from the outside and generally cannot inventory the complete component dependency tree. RASP operates within a running application to detect or prevent attacks. Credentialed infrastructure scanning identifies system-level vulnerabilities and configuration issues rather than software-license composition.

The strongest clue is the requirement to identify libraries and their licensing status , which directly maps to SCA.

Study Guide Reference: Vulnerability Management # Application Security Testing # SCA # Third-Party Components # Open-Source Dependencies # SBOM # Licensing and Vulnerability Analysis.

NEW QUESTION: 38

A security operations center (SOC) manager reviews a document signed by the Chief Financial Officer (CFO), the sales director, and a customer to decide whether a contract breach occurred.

Which of the following best describes the document that includes key performance indicators (KPIs)?

- A. Tactics, techniques, and procedures (TTPs)
- B. Return on investment report
- C. Service-level agreement (SLA)

- D. Risk management plan
- E. Memorandum of understanding

Answer: C (LEAVE A REPLY)

A service-level agreement (SLA) formally establishes measurable service expectations between a provider and a customer. These expectations commonly include availability targets, response times, resolution times, service quality thresholds, escalation conditions, reporting requirements, and other measurable performance indicators. NIST describes an SLA as a document that specifies technical performance promises and how performance or disputes will be handled. NIST security-control guidance also notes that service-level agreements can define performance expectations and measurable outcomes.

That makes an SLA the appropriate document when management needs to determine whether contractual performance requirements were violated. KPIs contained in the agreement provide objective measures against which actual service performance can be compared.

TTPs describe adversary behavior and have no contractual purpose. A return-on-investment report evaluates financial effectiveness rather than service obligations. A risk management plan describes how organizational risks will be identified and treated. A memorandum of understanding records cooperation or intent between parties, but it typically does not provide the detailed operational performance guarantees associated with an SLA.

The clues are customer, signed agreement, contractual breach, and measurable KPIs -all of which strongly identify a service-level agreement.

Study Guide Reference: Reporting and Communication # Service-Level Agreements # KPIs # Contractual Requirements # Performance Metrics # Compliance and Escalation.

NEW QUESTION: 39

A cybersecurity analyst requests a paid subscription to a threat intelligence feed relevant to a company's industry.

Which of the following best describes this type of feed?

- A. Open-source intelligence
- B. Threat mapping
- C. Threat modeling
- D. Closed-source intelligence

Answer: (SHOW ANSWER)

A paid, subscription-based threat intelligence service is best classified as closed-source intelligence because access is restricted to authorized subscribers rather than being freely available to the public. Commercial threat-intelligence providers typically collect, analyze, correlate, and curate indicators and adversary information before distributing that intelligence through authenticated portals, APIs, or feeds.

NIST identifies several external intelligence-source categories, including open-source repositories, commercial threat feeds, and external information-sharing partners .

A commercial feed relevant to a company's specific industry may provide higher-context intelligence regarding threat actors, infrastructure, malware, vulnerabilities, campaigns, and indicators affecting that vertical.

OSINT, by contrast, originates from publicly accessible sources and normally does not require restricted subscription access. Threat mapping is the activity of associating adversary behavior or intelligence with infrastructure, campaigns, frameworks, or organizational assets. Threat modeling is a structured process used to identify potential threats and weaknesses in systems or applications; it is not an intelligence-source classification.

The examination clue is "paid subscription." Restricted commercial access distinguishes the feed from publicly obtainable OSINT.

Study Guide Reference: Security Operations # Threat Intelligence # Intelligence Sources # Open-Source Intelligence # Closed/Commercial Intelligence # Industry-Specific Threat Feeds.

NEW QUESTION: 40

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.

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

Vulnerability remediation timeframes

Environment

Output

CVSS risk level	Standard	Applies to		
		OPS	TEST	STAGE
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 followed.
- If a patch requires a reboot for installation, the reboot must occur within the timeframes outlined above.
- All mitigations must be tested in the lower environments before being promoted to operations.
- Appropriate risk management processes should be considered when an applicable timeframe is not required for an environment.



FreePDFDumps

Environment name	Environment location	Subnets	Domain	Publicly accessible	NGFW	Load balancer	MFA required
ops.comptia.org	External	203.17.18.20 203.17.18.30 192.168.60.0/24 192.168.61.0/24	comptia.org	Yes	Yes	Yes	No
stage.comptia.org	Internal	192.168.76.0/24 192.168.75.0/24	comptia.org	No	No	Yes	Yes
test.comptia.org	External	192.168.50.0/24 192.168.51.0/24	comptia.org	No	Yes	Yes	Yes

Title: Microsoft IIS: Unsupported software version detected

Description: The software version detected is no longer supported.

Affected asset: 192.168.76.50

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: 192.168.76.60

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.

Affected asset: 192.168.51.32

Risk: May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).

Reference: CVE-2021-1234, CVSS 8.1

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: 192.168.60.45

Risk: Session sidejacking

Reference: CVE-2021-0462, CVSS 7.4

Title: Web server is susceptible to TLS downgrade attacks

Description: The server permits the web client to select and use its own preferences.

Affected asset: 192.168.60.90

Risk: May allow data to be vulnerable

Reference: CVE-2021-1234, CVSS 8.1

Title: Basic authentication

Description: Website is configured to permit use of .htaccess files on directories.

Affected asset: 192.168.51.90

Risk: May allow privileged access to sensitive data.

Reference: CVE-2021-38361, CVSS 5.1

Answer Area

Select the server to be patched within 14 calendar days:

- | | |
|--|--|
| ☐ 192.168.51.32 | ☐ 192.168.76.50 |
| ☐ 192.168.76.60 | ☐ 192.168.60.45 |
| ☐ 192.168.60.90 | ☐ 192.168.51.90 |

Select the appropriate technique and mitigation:

- Select
- Select
- Compensating control; implement secure session tokens
 - Compensating control; create new ACL on firewall to block port 443
 - Compensating control; implement MFA on the application
 - Reconfigure; transition to a new identity and access manager
 - Request exception; organization needs time to procure a PKI
 - Reconfigure; restrict to use only modern cipher suites
 - Reconfigure; upgrade IIS to current release
 - Request exception; legacy protocol could have operational impact

Answer:

Answer Area



FreePDFDumps

Select the server to be patched within 14 calendar days:

- | | |
|--|--|
| ☐ 192.168.51.32 | ☐ 192.168.76.50 |
| ☐ 192.168.76.60 | ☐ 192.168.60.45 |
| ☐ 192.168.60.90 | ☐ 192.168.51.90 |

Select the appropriate technique and mitigation:

- Select
- Select
- Compensating control; implement secure session tokens
 - Compensating control; create new ACL on firewall to block port 443
 - Compensating control; implement MFA on the application
 - Reconfigure; transition to a new identity and access manager
 - Request exception; organization needs time to procure a PKI
 - Reconfigure; restrict to use only modern cipher suites
 - Reconfigure; upgrade IIS to current release
 - Request exception; legacy protocol could have operational impact

Explanation:

192.168.76.5 - Patch; upgrade IIS to the current release

The correct remediation target is 192.168.76.5, which is associated with an unsupported Microsoft IIS version and a CVSS score of 9.2 in the matching hotspot data.

The remediation standard assigns vulnerabilities above 9.0 to the shortest remediation window, meaning the system requires action in seven days and therefore necessarily falls within the requested fourteen-day maximum. The corresponding remediation is to patch or upgrade IIS to a currently supported release.

The key vulnerability-management principle is that remediation priority is not determined exclusively by the existence of a vulnerability. Analysts must consider severity, asset context, exposure, business importance, exploitability, available remediation, and organizational service-level requirements. A product that has reached an unsupported state represents additional risk because standard security updates may no longer be supplied.

Upgrading the affected IIS installation directly removes the unsupported software condition rather than merely reducing exposure around it. A compensating control would be appropriate when remediation cannot immediately be performed, but it would not supersede a supported upgrade when that upgrade is operationally available.

Study Guide Reference: Vulnerability Management # Vulnerability Prioritization # CVSS # Remediation Timeframes # End-of-Life/Unsupported Software # Patching and Upgrading.

NEW QUESTION: 41

An analyst prepares an after action report following an incident in which multiple systems were compromised over several days.

The analyst provides raw event logs from each compromised system in the report and determines that a patient-zero system cannot be found.

Which of the following should the analyst do to determine the patient-zero system?

- A. Establish an accurate timeline of events.
- B. Enable monitoring on the compromised systems.
- C. Isolate the compromised systems before remediation.
- D. Improve the content for incident updates during shift handoff.
- E. Perform a reverse composition analysis on malware packages.

Answer: A (LEAVE A REPLY)

The analyst must construct an accurate incident timeline. Patient zero is the earliest compromised system from which subsequent malicious activity originated or propagated. Determining it requires ordering events chronologically across all affected hosts and correlating authentication activity, process execution, network

connections, malware creation times, lateral movement, and other evidence.

Raw logs alone do not communicate this sequence effectively. Logs from different systems must first use reliable timestamps and then be normalized and correlated. Once events are ordered, the analyst can work backward from known compromises to determine which host displayed the earliest credible signs of intrusion and whether subsequent systems were reached from that host.

Enabling additional monitoring helps detect future activity but does not reconstruct historical sequence by itself. Isolation is necessary during containment but does not establish which system was initially compromised. Shift-handoff improvements are useful organizationally but do not answer the forensic question. Malware composition analysis may identify relationships between samples, but it does not establish system-level chronology.

NIST's incident-response guidance emphasizes analysis, documentation, root-cause understanding, and after- action reporting as inputs to continuous improvement.

Study Guide Reference: Incident Response and Management # Timeline Analysis # Event Correlation # Patient Zero # Root Cause Analysis # After-Action Review.

Valid CS0-004 Dumps shared by Actual4test.com for Helping Passing CS0-004 Exam! Actual4test.com now offer the **newest CS0-004 exam dumps**, the Actual4test.com CS0-004 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CS0-004 dumps with Test Engine here: https://www.actual4test.com/CS0-004_examcollection.html (190 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)