

CuramSoftware.CS0-004.v2026-10-21.q86

Exam Code:	CS0-004
Exam Name:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam
Certification Provider:	Curam Software
Free Question Number:	86
Version:	v2026-10-21
# of views:	105
# of Questions views:	864
https://www.freecram.net/torrent/CuramSoftware.CS0-004.v2026-10-21.q86.html	

NEW QUESTION: 1

A security analyst reviews the following report:

1.15	Out-of-bounds write	CVSS4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/SC:N/SI:N/SA:N
1.16	Use of hard-coded credentials	CVSS4.0/AV:L/AC:L/AT:P/PR:H/UI:A/VC:N/VI:N/SC:L/SI:N/SA:N

Which of the following explain the reason the analyst gives 1.15 the highest priority for remediation? (Choose two.)

- A. Highly privileged user accounts can be used to gain access to the system.
- B. It requires the lowest level of permissions to execute.
- C. The attacker can use elevated privileges to execute arbitrary code.
- D. The vulnerable software can be accessed from remote networks.
- E. The system must be accessed with an interactive session for exploitation.
- F. It requires user interaction to exploit the vulnerability.

Answer: (SHOW ANSWER)

The CVSS vector for vulnerability 1.15 includes PR:N, which means no privileges are required to exploit the vulnerability. This makes exploitation easier and increases risk. The vector also includes AV:N, which indicates the vulnerability is exploitable over a network. Remote accessibility significantly increases exposure because attackers do not need local access to the target system.

NEW QUESTION: 2

An incident response team identifies a malicious uniform resource locator (URL) associated with a required business process and performs the following activities:

- Access to the URL has been restricted only to the necessary users through firewall rules and Cloud Security Group rules.
- Additional monitoring has been enabled for traffic related to that site and the allowed users.
- All application servers that need to access that site have been patched with the latest security and software updates.
- Application owners have been notified of the severity and need to remediate this reported issue.

Which of the following best describes the overall mitigation the security team is performing?

- A. Patching solutions
- B. Configuration management
- C. Compensating controls
- D. Attack surface management

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

The malicious URL cannot be completely blocked because it supports a required business process, so the team is applying alternative safeguards-restricted access, monitoring, patching, and notifications-to reduce the risk.

NEW QUESTION: 3

Which of the following is the best option for an IT administrator to deploy to ensure standardized permissions to a cloud environment?

- A. Automated onboarding tasks
- B. Threat feed correlation
- C. SaaS log enrichment
- D. Zero Trust platform APIs

Answer: (SHOW ANSWER)

Automated onboarding tasks help ensure that users are consistently assigned the correct roles, groups, and permissions when they are provisioned in a cloud environment. This standardization reduces configuration errors, enforces access policies, and supports role-based access control across cloud resources.

NEW QUESTION: 4

The Chief Information Security Officer wants to improve internal security measures by continuously validating and verifying access to the production environment. Which of the following concepts best describes this practice?

- A. Secure access service edge
- B. Next-generation firewall
- C. Zero Trust
- D. Privileged access management

Answer: (SHOW ANSWER)

Zero Trust follows the principle of "never trust, always verify," continuously validating users, devices, and access requests rather than trusting them based on network location.

NEW QUESTION: 5

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:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 18:52 UTC
Nmap scan report for 152.203.20.16
Host is up (0.0000050s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE      SERVICE
7/tcp     open      bgp
443/tcp   open      https
500/udp   open      ikamsp

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

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: ([SHOW ANSWER](#))

Open UDP port 500 indicates ISAKMP/IKE, commonly used by IPsec VPNs. Main Mode provides a more secure IKE negotiation by protecting peer identity information.

NEW QUESTION: 6

A vulnerability analyst runs a credentialed vulnerability scan covering all addressable enterprise assets. After running the scan, the analyst discovers a large number of critical vulnerabilities that cannot be immediately remediated. Which of the following are the most likely reasons why the vulnerabilities cannot be immediately addressed?

- A. Lack of technical skills, the absence of a test environment, and the absence of an asset inventory
- B. Physical access challenges, the absence of vendor support, and a lack of system documentation
- C. Inaccurate asset inventory, a lack of system documentation, and an absence of authorization
- D. Legacy and proprietary systems, a lack of patch availability, and vendor dependencies

Answer: ([SHOW ANSWER](#))

Legacy or proprietary systems may not support current patches, fixes may not yet exist, and remediation may depend on vendor testing or approval.

NEW QUESTION: 7

The website of a large retail chain is failing to enforce encrypted HTTPS connections, leaving customer account credentials exposed. Which of the following is the best corrective action for resolving this issue?

- A. Remove any redirect settings of HTTP connections to HTTPS.
- B. Implement HTTP Strict Transport Security Headers.
- C. Install a self-signed certificate on the web server.
- D. Reduce the default timeout period for all web-based sessions.

Answer: ([SHOW ANSWER](#))

Enabling HTTP Strict Transport Security forces browsers to use HTTPS exclusively, preventing any unencrypted HTTP connections. This ensures customer credentials cannot be transmitted in plaintext and corrects the failure to enforce secure connections.

NEW QUESTION: 8

A security operations center analyst receives an alert from the security information and event management system. The analyst quickly reviews the alert and sees a workstation infected with malware. The analyst then uses the endpoint detection and response tool to isolate the workstation from the network. Which of the following best describes the steps that occurred in this scenario?

- A. Analysis, containment, and eradication
- B. Analysis, eradication, and recovery
- C. Detection, analysis, and containment
- D. Isolation, mitigation, and analysis

Answer: ([SHOW ANSWER](#))

The SIEM alert represents detection, reviewing and confirming the malware is analysis, and isolating the workstation is containment.

NEW QUESTION: 9

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 using a compromised role to move from one cloud subscription to another, which is lateral movement between environments.

NEW QUESTION: 10

Which of the following best explains compensating controls?

- A. A compensating control is implemented when a vulnerability cannot be remediated.
- B. A compensating control is deployed after systems have been brought into compliance.
- C. A compensating control addresses the threat side of the risk equation rather than the vulnerability side.
- D. A compensating control completely remediates vulnerabilities that are too costly to fix.

Answer: ([SHOW ANSWER](#))

A compensating control is an alternative safeguard implemented when the primary control or recommended remediation cannot be applied, often due to technical, operational, or business constraints. Its purpose is to reduce the associated risk to an acceptable level when the underlying vulnerability cannot be directly remediated.

NEW QUESTION: 11

A SOC has SIEM configured to receive threat intelligence feeds from multiple external sources.

For certain tasks, there is no need for human interaction. Which of the following is the best solution to correlate events and provide valuable information to the analysts?

- A. Data enrichment
- B. Webhooks
- C. Single pane of glass
- D. Threat feed combination

Answer: ([SHOW ANSWER](#))

Data enrichment automatically adds context from threat intelligence feeds, asset inventories, geolocation databases, and other sources to security events. This correlation provides analysts with more meaningful and actionable information while reducing the need for manual investigation, making it ideal when human interaction is not required for certain tasks.

NEW QUESTION: 12

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: ([SHOW ANSWER](#))

ATT&CK Navigator visualizes adversary tactics and techniques, helping security teams map threat behavior and identify weaknesses in defensive coverage.

NEW QUESTION: 13

A Chief Information Security Officer (CISO) is notified of an ongoing incident. Which of the following explains why the CISO instructs the Chief Executive Officer not to discuss the incident over email?

- A. The security team discovered a vulnerability in the Short Message Service email gateway.
- B. The email system may be compromised.
- C. Emails are not encrypted in transit.
- D. The CISO has not notified the public relations team of the incident.

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

During an active incident, attackers may be monitoring a compromised email system. Incident communications should therefore use a secure, out-of-band channel.

NEW QUESTION: 14

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](#)**)**

A Cloud Access Security Broker (CASB) provides visibility into cloud application usage and user activity. It can monitor access to sanctioned and unsanctioned cloud storage services, track file uploads and downloads, and generate logs showing whether sensitive data was accessed or transferred to personal devices.

NEW QUESTION: 15

A new policy prohibits external access to database servers. A recent external port scan identified the following open Transmission Control Protocol (TCP) ports:

- 21
- 25
- 68
- 80
- 389
- 443
- 587
- 1514
- 3306
- 3389
- 8080

Which of the ports must be closed to be compliant with the new policy? (Choose two.)

- A. 25
- B. 587
- C. 1514
- D. 3306
- E. 3389
- F. 8080

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

Port 3306 is the default port used by MySQL database servers. Allowing external access to this port directly exposes the database service, which violates a policy that prohibits external access to database servers.

Port 3389 is used by Remote Desktop Protocol (RDP). External access through RDP allows direct administrative or user access to the server hosting the database, which effectively bypasses the restriction against external access to database servers and therefore must also be closed to comply with the policy.

NEW QUESTION: 16

Which of the following is the term for a predefined set of automated actions that incident responders and SOC analysts can use to enhance operations?

- A. Threat modeling
- B. Detection set
- C. CVSS
- D. Playbooks

Answer: (SHOW ANSWER)

Playbooks define predefined, often automated, response actions that incident responders and SOC analysts follow to standardize and enhance security operations.

Valid CS0-004 Dumps shared by EduDump.com for Helping Passing CS0-004 Exam! EduDump.com now offer the **newest CS0-004 exam dumps**, the EduDump.com CS0-004 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-004 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-004/premium/> (190 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 17

A SOC analyst scans a group of servers to search for vulnerabilities. After analyzing the output, the analyst realizes that some OS versions were not detected properly. Which of the following is the best option to increase the accuracy of the scan?

- A. Update the scan plug-ins.
- B. Upgrade the server OS.
- C. Use passive fingerprinting.
- D. Perform credentialed scans.

Answer: D (LEAVE A REPLY)

Credentialed scans authenticate to the target systems and can directly query the operating system for detailed configuration and version information. This provides much more accurate results than unauthenticated scanning and helps correctly identify OS versions, installed software, and vulnerabilities.

NEW QUESTION: 18

A sales application was remediated to address a critical vulnerability. The process took five business hours and was ultimately successful. However, the change advisory board informed the company's leadership team that the process resulted in a considerable financial loss. Which of the following best explains the reason for the financial loss?

- A. The loss is a normal cost of operations that relies on IT
- B. The Chief Information Officer did not notify the board members
- C. The IT team should have hired a penetration test assessment before patching
- D. The maintenance window was not properly communicated or scheduled

Answer: (SHOW ANSWER)

Even though the vulnerability remediation was successful, a critical sales application being unavailable during business operations can result in lost revenue and business disruption.

Properly scheduling and communicating a maintenance window helps minimize operational impact by ensuring affected stakeholders are aware of the outage and can plan accordingly.

Failure to do so can lead to significant financial losses despite a technically successful change.

NEW QUESTION: 19

Based on recent alerts, a security analyst thinks a web application server was compromised. The analyst reviews the following server output:

```
09:59:57 up 1:19, 4 users, load average: 2.01, 0.75, 0.27
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
comptias   -        0.0.0.0         09:28    29:28  0.00s   0.03s   gdm-session-worker
www        tty2     89.123.222.5    03:28    25:28  0.00s   0.03s   /var/www/apache2
gdm        tty1     -              08:38    1:19   5.80s   0.09s   /usr/bin/gjs
comptia2   -        0.0.0.0         09:25    39:09  0.05s   0.09s   gdm-session-worker
```

Which of the following best describes what has occurred?

- A. An initiated unauthorized session
- B. Too many users logged in at the same time
- C. High resource consumption
- D. Abnormal idle times for each user

Answer: ([SHOW ANSWER](#))

The web-service account www has an interactive tty2 session originating from an external IP address. A service account should not normally have an interactive remote login, indicating unauthorized access.

NEW QUESTION: 20

Which of the following best explains the importance of security orchestration, automation, and response for security operation activities?

- A. Implementing infrastructure as code in the organization
- B. Supporting the team's management of remediation tasks
- C. Deploying general scripts for automating security engineering operations
- D. Collecting threat intelligence feeds for improved threat response

Answer: ([SHOW ANSWER](#))

Security orchestration, automation, and response streamlines and coordinates incident response workflows, enabling the SOC team to efficiently manage, prioritize, and execute remediation tasks at scale.

NEW QUESTION: 21

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: ([SHOW ANSWER](#))

An SLA is a formal agreement that defines measurable service requirements, KPIs, responsibilities, and consequences when agreed performance levels are not met.

NEW QUESTION: 22

A security analyst is investigating an unusually high volume of requests received on a web server.

Based on the following command and output:

```
$ grep " 404 " access_log
...snip...
10.203.10.23 - - [21/May/2024 13:19:06] "GET /goodmorningsun HTTP/1.1" 404 -
10.203.10.23 - - [21/May/2024 13:19:06] "GET /newyddion HTTP/1.1" 404 -
10.203.10.23 - - [21/May/2024 13:19:06] "GET /heartsandminds HTTP/1.1" 404 -
10.203.10.23 - - [21/May/2024 13:19:06] "GET /1970 HTTP/1.1" 404 -
10.203.10.23 - - [21/May/2024 13:19:06] "GET /dopey HTTP/1.1" 404 -
10.203.10.23 - - [21/May/2024 13:19:06] "GET /ilovewales HTTP/1.1" 404 -
10.203.10.23 - - [21/May/2024 13:19:06] "GET /n_ireland HTTP/1.1" 404 -
10.203.10.23 - - [21/May/2024 13:19:06] "GET /heavenandearth HTTP/1.1" 404 -
10.203.10.23 - - [21/May/2024 13:19:06] "GET /gormenghast HTTP/1.1" 404 -
10.203.10.23 - - [21/May/2024 13:19:06] "GET /clue HTTP/1.1" 404 -
...snip...
```

Which of the following best describes the activity that the analyst will confirm?

- A. SQL injection
- B. Directory brute force
- C. Remote command execution
- D. Cross-site scripting

Answer: (SHOW ANSWER)

The log shows a rapid sequence of GET requests for many different paths that do not exist, all returning 404 errors. This pattern is characteristic of directory or resource brute forcing, where an attacker scans for valid files or directories by requesting numerous possibilities.

NEW QUESTION: 23

Which of the following uses simulated traffic to a website to evaluate performance?

- A. Log analysis
- B. War gaming
- C. Synthetic monitoring
- D. Packet inspection

Answer: (SHOW ANSWER)

Synthetic monitoring evaluates website performance by generating simulated user traffic and transactions to test availability, response time, and functionality. This approach allows analysts to proactively measure performance and detect issues without relying on real user activity.

NEW QUESTION: 24

During a security incident at a healthcare facility, an unauthorized user downloads multiple patients' PHI records. Which of the following is the best reason for the healthcare facility to communicate with the affected patients regarding the incident?

- A. To meet regulatory requirements
- B. To appease the stakeholders
- C. To avoid legal liability
- D. To get support from law enforcement

Answer: ([SHOW ANSWER](#))

Healthcare organizations are subject to regulatory requirements regarding the protection and disclosure of Protected Health Information (PHI). When a breach involving PHI occurs, regulations such as HIPAA require affected individuals to be notified so they can take appropriate actions to protect themselves and remain informed about the exposure of their personal information.

NEW QUESTION: 25

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: ([SHOW ANSWER](#))

Both XSS and SQL injection commonly occur when an application fails to properly validate, sanitize, and safely process untrusted user input.

NEW QUESTION: 26

A security analyst reviews the public-facing attack surface of a network that contains both Windows and Linux servers. Which of the following commands is the best way to identify the services running?

- A. `nmap -O -p- -iL hosts.txt`
- B. `nmap -sV -pl-1024 -iL hosts.txt`
- C. `nmap -sP -A -iL hosts.txt`
- D. `nmap -sn -vvvv -iL hosts.txt`

Answer: ([SHOW ANSWER](#))

Service version detection is required to identify which services are running on hosts. The command includes the service scan option and targets a range of ports, allowing the analyst to enumerate active services and their versions across the listed hosts.

NEW QUESTION: 27

Which of the following is a reason the false-positive rate is an important metric for incident response reporting and communication?

- A. A high false-positive rate indicates that the alerting rules are not sensitive enough.
- B. A high false-positive rate can help the response team prioritize critical events.
- C. A high false-positive rate validates that the incident response plan is working well.
- D. A high false-positive rate can result in wasted time and resources.

Answer: ([SHOW ANSWER](#))

A high false-positive rate leads to unnecessary investigation of benign alerts, consuming analyst time and resources, which reduces overall efficiency and can delay response to actual threats.

NEW QUESTION: 28

An analyst receives the following output:

```
Initiating SYN Stealth Scan
Scanning 16 hosts [3 ports / host]
Discovered open port 22/tcp on 10.203.20.15
Discovered open port 22/tcp on 10.203.20.10
Discovered open port 80/tcp on 10.203.20.15
Discovered open port 22/tcp on 10.203.20.13
Discovered open port 22/tcp on 10.203.20.11
Discovered open port 22/tcp on 10.203.20.14
Discovered open port 80/tcp on 10.203.20.10
Discovered open port 443/tcp on 10.203.20.14
```

Which of the following is the correct number of discovered systems that are allowing unencrypted traffic?

- A. 1
- B. 2
- C. 3
- D. 5

Answer: ([SHOW ANSWER](#))

TCP port 80 carries unencrypted HTTP traffic and is open on 10.203.20.15 and 10.203.20.10.
SSH on port 22 and HTTPS on port 443 are encrypted.

NEW QUESTION: 29

Which of the following helps identify the attack surface area of a new environment?

- A. Incident response process
- B. Software development life cycle (SDLC)
- C. Open Systems Interconnection (OSI) model
- D. Cyber Kill Chain

Answer: ([SHOW ANSWER](#))

The Cyber Kill Chain provides a structured model of the stages of a cyberattack, from reconnaissance through exploitation and data exfiltration. By mapping potential attack paths across these stages, analysts can identify where an attacker could interact with systems and services in the environment. This helps reveal exposed entry points and weaknesses, effectively identifying the environment's attack surface area.

NEW QUESTION: 30

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: ([SHOW ANSWER](#))

An after-action report provides the complete post-incident record, including the timeline, response activities, outcomes, root cause, lessons learned, and recommendations.

NEW QUESTION: 31

A security analyst is implementing a process to perform vulnerability management on an OT environment:

- Systems must remain on an isolated network.

- The process should focus on external threats.
- No additional software can be deployed on the systems.
- Transmitted packets cannot be modified or dropped.
- Additional processing delays are not tolerated.

Which of the following is the best way to securely meet the requirements?

- A. Implement agentless sensors at the network edge.
- B. Use reverse engineering to detect flaws on the in-scope systems.
- C. Deploy an IPS In-line with the network traffic.
- D. Check the compatibility of an EDR agent with the OSs used on the OT environment.

Answer: (SHOW ANSWER)

Agentless sensors placed at the network edge allow the analyst to observe traffic passively without installing software, modifying packets, or introducing latency. This approach fits OT requirements while enabling detection of external threats in an isolated network.

Valid CS0-004 Dumps shared by EduDump.com for Helping Passing CS0-004 Exam! EduDump.com now offer the **newest CS0-004 exam dumps**, the EduDump.com CS0-004 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-004 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-004/premium/> (190 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 32

Two organizations are assessing a partnership to exchange security information and share resources in case an incident occurs. The assessment is in the pre-contract stage, and no detailed definitions have been made by management. Which of the following is the best artifact to formalize the agreement at the current stage?

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

Answer: (SHOW ANSWER)

A Memorandum of Understanding (MOU) is used during the early stages of a partnership to document the intent of the parties to cooperate and outline high-level roles, expectations, and objectives. It is appropriate when detailed contractual terms, service commitments, and operational definitions have not yet been established.

NEW QUESTION: 33

A systems administrator reviews a ticket from a third-party SOC regarding a recent security event. The SOC provided the following table:

Time	Username	Hostname	Success/failure	Source location
13:48:12	jdoe	app-01	Success	United States
13:57:18	jdoe	app-02	Success	United States
14:02:26	jroe	app-01	Failure	United Kingdom
14:19:08	jroe	app-02	Failure	United Kingdom
14:44:26	jroe	web-04	Failure	United Kingdom
15:49:02	jroe	web-06	Failure	United Kingdom
16:31:44	jdoe	app-01	Success	India

Which of the following is most likely the reason for the SOC ticket?

- A. Impossible travel
- B. Geoblocking policy

- C. Time-of-day restrictions
- D. Brute-force authentication

Answer: ([SHOW ANSWER](#))

The log entries show successful logins for the same user account from the United States and later from India within a relatively short period. Traveling between those locations in the elapsed time would be unrealistic, which is a classic indicator of impossible travel. This type of alert is commonly generated when authentication events occur from geographically distant locations in a timeframe that is physically impossible for a legitimate user.

NEW QUESTION: 34

An analyst executes the top command on a Linux system for an unresponsive application and observes the following output:

PID	USER	%CPU	%MEM	COMMAND
6651	xrdp	6.3	0.2	xrdp
7316	comptia	0.3	0.1	top
7583	root	91.2	96	python
6680	comptia	0.7	0.1	kworker

Which of the following is the most likely cause of this issue?

- A. Service disruption
- B. Unauthorized software
- C. Resource exhaustion
- D. Filesystem changes

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

The python process is consuming 91.2% CPU and 96% memory, exhausting system resources and causing the application to become unresponsive.

NEW QUESTION: 35

A security operations center analyst must determine which threat actor is targeting their industry based on similar attack vectors. Which of the following provides the best intelligence for attribution?

- A. AbuseIPDB
- B. Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege
- C. Tactics, techniques, and procedures
- D. Internet Protocols

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

Tactics, techniques, and procedures describe the behavioral patterns, methods, and operational approaches used by threat actors during attacks. These patterns are often consistent across campaigns and are widely used in threat intelligence to associate activity with specific threat groups, making them highly effective for attribution and identifying which actors are targeting a particular industry.

NEW QUESTION: 36

During a recent security event, log files were being sent to a stand-alone console that was not being checked on a daily basis. As a result, the stated SLA for detection was exceeded. Which of the following is a way to prevent this delay in the future?

- A. Decreasing the interval for sending logs from endpoints
- B. Using a centralized dashboard for monitoring
- C. Automating the process for ingesting logs into the stand-alone console
- D. Reevaluating the SLA for detection to reflect current operations

Answer: ([SHOW ANSWER](#))

The issue was not that logs were unavailable, but that they were being sent to a stand-alone console that was not routinely monitored. A centralized dashboard improves visibility by aggregating logs and alerts into a single monitoring platform, making it more likely that security events are detected within the required SLA.

NEW QUESTION: 37

A security analyst reruns infrastructure as code (IaC) to tear down and rebuild a new environment after a ransomware attack. Which of the following describes this phase?

- A. Analysis
- B. Post-incident
- C. Detection
- D. Containment
- E. Recovery

Answer: ([SHOW ANSWER](#))

Rebuilding the environment from trusted IaC configurations restores systems and services to normal operation after the ransomware attack.

NEW QUESTION: 38

An analyst reviews alerts that indicate a number of different users had a spike in login attempts from the same IP. Using the security information and event management (SIEM) system, the analyst finds that a number of users received the following email:

```
Sender: HR-Department@gmail.com
Recipient: xxxxxx
Subject: Student Loan Forgiveness Benefits
Body:

Greetings,

We are pleased to announce a new company student loan forgiveness benefit for all eligible employees. To ensure your eligibility, please visit the
Student Loan Forgiveness page.

Sincerely,
HR
```

Which of the following best describes this activity?

- A. URL shortening
- B. Whaling
- C. Spoofing
- D. Social engineering

Answer: ([SHOW ANSWER](#))

The email uses a forged sender address that appears to come from an internal HR department while actually originating from an external domain, indicating impersonation intended to deceive recipients.

NEW QUESTION: 39

A security analyst responds to an incident and finds the attacker embedded in the critical infrastructure. There is no evidence of lateral movement in the past 30 days. Which of the following is the most likely type of threat actor in the system?

- A. Script kiddie
- B. Organized crime
- C. Hacktivist

D. Nation-state

Answer: ([SHOW ANSWER](#))

A nation-state threat actor is the most likely candidate because these actors are known for establishing long-term, persistent access to critical infrastructure targets. Their objectives often involve espionage, strategic positioning, or preparation for future operations, allowing them to remain embedded within systems for extended periods while minimizing detectable activity such as lateral movement.

NEW QUESTION: 40

An analyst reviews the following web server log entries:

%2E%2E/%2E%2E/%2E%2E/%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](#))

The log entry shows URL-encoded sequences (%2E%2E) representing "..", which is characteristic of a directory traversal attempt. This technique is used to access files such as /etc/passwd for reconnaissance. Even if unsuccessful, the pattern clearly indicates a traversal attempt.

NEW QUESTION: 41

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: ([SHOW ANSWER](#))

A recurring team call supports information sharing, workflow alignment, role awareness, and coordination among the cybersecurity engineers.

NEW QUESTION: 42

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](#))

-Pn skips host discovery and treats the target as online, which is necessary when ping probes are blocked. -p- scans all TCP ports.

NEW QUESTION: 43

A security director at a remote company is concerned about recent threat intelligence reports regarding threat actors who are hired by the company and steal intellectual property. Which of the following solutions are the best ways to identify the tactics, techniques, and procedures (TTPs) used by these threat actors? (Choose two.)

- A. Installing and configuring a data loss prevention tool
- B. Subscribing to an identity proofing service for all employees
- C. Conducting thorough background checks on all incoming employees
- D. Utilizing user behavioral analytics-based detections implemented in the security information and event management (SIEM)
- E. Deploying a fully featured endpoint detection and response (EDR)
- F. Validating identification information manually

Answer: ([SHOW ANSWER](#))

User behavioral analytics in a SIEM helps detect insider threat patterns by analyzing deviations from normal user activity, which reveals how malicious insiders operate and exposes their techniques and behaviors.

Endpoint detection and response provides deep visibility into endpoint activities, enabling monitoring and investigation of attacker actions on systems, which helps identify the specific techniques and procedures used to exfiltrate data or misuse access.

NEW QUESTION: 44

Customers are unable to upload files to an SFTP server. Firewall logs show the following activity sourced from multiple IP addresses in one geographic region:

```
Time: 2024-10-11 15:05:21
Src_IP: 103.1.114.26
Dest_IP: 199.52.99.11
Src_port: 45678
Dest_port: 22
Action: Allow
Application: TCP
Src_zone: untrust
Dest_zone: trust
Session_end_reason: aged-out/incomplete
```

The analyst reviewing the logs notices that the session_end_reason does not change for any of the log entries. Which of the following is the next step the analyst should take to determine what is occurring?

- A. Submit a request to the engineering team to restart SFTP services on the host due to the session limit being reached.
- B. Take a packet capture of all traffic to or from dest_IP 199.52.99.11 to see whether it is responding to SYN-ACK with an ACK.
- C. Correct the misconfigured firewall by blocking dest_port 22 to prevent further credential brute-force attacks from src_IP 103.1.114.26.
- D. Review endpoint detection logs on the SFTP server for any malware running on dest_port 22 that may be intercepting client communications.

Answer: ([SHOW ANSWER](#))

The firewall log shows TCP traffic to port 22 is being allowed, but the sessions consistently end with an "aged-out/incomplete" status. This commonly indicates that the TCP three-way handshake is not completing. Capturing packets to determine whether the server is responding properly and whether clients are completing the handshake is the appropriate next step to identify where the connection process is failing.

NEW QUESTION: 45

A security analyst investigates a malware alert from a critical system. The following information is present in the ticket:

Services running: (2)	Apache; sendmail
Suspicious/unknown files: (2)	rust_scan; sssh
Suspicious running processes: (1)	sssh
Suspicious IP addresses: (1)	128.210.175.23

Which of the following should the analyst do first?

- A. Block the suspicious IP address 128.210.175.23.
- B. Determine whether sssh is a malicious program.
- C. Delete the suspicious files.
- D. Review the Apache logs.

Answer: ([SHOW ANSWER](#))

The presence of an unknown running process on a critical system is a strong indicator of compromise. Before taking any containment actions, the analyst must confirm whether the process is malicious. Identifying and validating the nature of the suspicious process provides the foundation for correct next steps in containment and eradication.

NEW QUESTION: 46

A security analyst detects that a large amount of data is being exfiltrated. The data contains confidential customer information. Which of the following should be done first in this situation?

- A. Contact public relations so they can communicate with customers.
- B. Identify stakeholders and communicate with them.
- C. Inform law enforcement about the activities.
- D. Declare an incident and contain the affected servers.

Answer: ([SHOW ANSWER](#))

When active data exfiltration involving confidential customer information is detected, the immediate priority is to initiate incident response procedures and contain the affected systems to stop further data loss. Containment helps limit the impact of the breach before moving on to stakeholder notifications, external communications, or law enforcement involvement.

Valid CS0-004 Dumps shared by EduDump.com for Helping Passing CS0-004 Exam! EduDump.com now offer the **newest CS0-004 exam dumps**, the EduDump.com CS0-004 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-004 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-004/premium/> (190 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 47

A compliance analyst works with a management team to develop remediation plans following a recent red-team assessment of the organization's operational technology (OT) networks within an industrial facility. While the backbone of the OT network is based on modern, fully supported infrastructure, the OT components are outdated and vulnerable to a variety of attacks. Further mitigation is not possible from a logical controls perspective. Which of the following approaches is best for the organization to consider for ongoing risk mitigation efforts?

- A. Reduced patching requirements for OT systems
- B. Deployment of token-based multifactor authentication (MFA) for all access to industrial systems
- C. Increased use of network segmentation
- D. Expansion of cyber insurance coverage

E. Enhanced usage of AI to augment existing endpoint detection and response (EDR) solutions

Answer: ([SHOW ANSWER](#))

Network segmentation isolates vulnerable systems from other parts of the network, reducing the ability of attackers to move laterally or reach critical systems. In environments where outdated operational technology cannot be easily patched or protected with additional logical controls, segmentation is an effective mitigation strategy because it limits exposure and confines potential compromises to smaller, controlled network zones.

NEW QUESTION: 48

Which of the following is the best strategy for prioritizing vulnerabilities for remediation?

- A. Remediate from the beginning to the end of the report.
- B. Remediate the findings based on the description of the vulnerabilities.
- C. Remediate the vulnerabilities based on the CVE score only.
- D. Remediate based on the organization's timeframe in the procedures.

Answer: ([SHOW ANSWER](#))

Organizations establish vulnerability management procedures that define remediation timeframes based on risk levels, asset criticality, and business requirements. Prioritizing remediation according to these documented procedures ensures vulnerabilities are addressed consistently and in alignment with the organization's risk management strategy rather than relying solely on report order, descriptions, or CVE scores.

NEW QUESTION: 49

An employee submits a ticket that contains the following information to a cybersecurity analyst:

Ticket Body: Please review this file received via email as it is coming from an unknown sender and let me know if it is safe to open.

Ticket Attachment: Invoice-0123456789.pdf

Which of the following is the best way to help the analyst determine the impact of opening the attachment if the file has been customized for the specific recipient?

- A. Execute cuckoo submit Invoice-0123456789.pdf.
- B. Run strings Invoice-0123456789.pdf.
- C. Submit the sender IP address to AbuseIPDB and review the report.
- D. Send the IP address found on the email header to VirusTotal.

Answer: ([SHOW ANSWER](#))

If the file has been customized specifically for the recipient, static reputation-based checks may not reveal its behavior. Executing the PDF in a sandbox such as Cuckoo allows the analyst to observe its actual behavior, including any malicious actions, network communications, process creation, or exploitation attempts. This provides the best assessment of the impact of opening the attachment.

NEW QUESTION: 50

The Chief Information Officer (CIO) is requiring users to phase out a legacy system that no longer receives security updates because the system will be decommissioned soon. Which of the following risk management strategies is the CIO using?

- A. Avoidance
- B. Mitigation
- C. Acceptance
- D. Transference

Answer: ([SHOW ANSWER](#))

Decommissioning the legacy system eliminates the activity and asset creating the risk, which is risk avoidance.

NEW QUESTION: 51

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: ([SHOW ANSWER](#))

YARA scans files locally for patterns and signatures associated with known malware. It is appropriate for an isolated system, whereas VirusTotal requires uploading or querying the file online.

NEW QUESTION: 52

A security analyst discovers several vulnerabilities on a critical legacy system. The analyst must recommend a solution with the following limitations:

- No downtime is permitted due to criticality.
- Patches for the vulnerabilities do not exist.
- No redundancy systems are in place.

Which of the following is the best risk management strategy to implement?

- A. Transference
- B. Mitigation
- C. Avoidance
- D. Acceptance

Answer: ([SHOW ANSWER](#))

When vulnerabilities cannot be patched and the system must remain operational, implementing compensating controls reduces the likelihood or impact of exploitation. This approach lowers risk without requiring downtime or system replacement, aligning with mitigation as the appropriate strategy.

NEW QUESTION: 53

A DevOps analyst must include code scanning in the current CI/CD pipeline. The company decided not to invest in a different system, so the analyst has found a lightweight scanning module in the CI/CD tool to utilize. Which of the following best describes the analyst's approach?

- A. They activated a threat feed combination.
- B. They defined a new webhook.
- C. They configured an available API.
- D. They leveraged an existing plug-in.

Answer: ([SHOW ANSWER](#))

The analyst is adding code-scanning functionality to the existing CI/CD platform by using a lightweight module already available within the tool. This is an example of leveraging an existing plug-in, which extends the capabilities of the current system without requiring the purchase and integration of a separate solution.

NEW QUESTION: 54

Hotspot Question

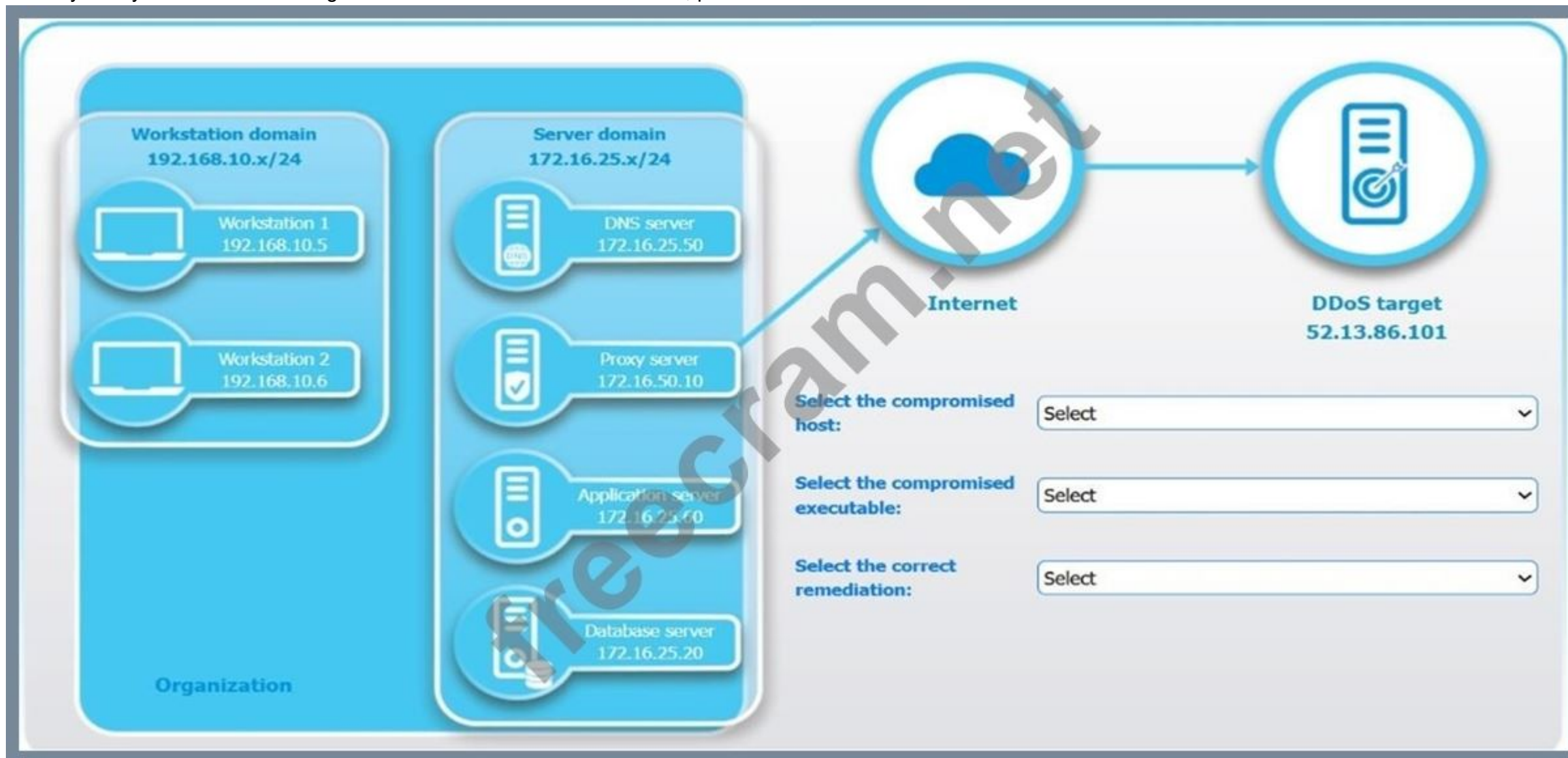
An organization receives an indication that one of its hosts is part of a DDoS attack against a victim. The proxy server is supposed to handle all web page requests from all internal hosts.

INSTRUCTIONS

Click on each workstation and server to review outputs and a log file.

Identify the compromised host and executable, and determine an appropriate remediation for the issue.

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



Workstation 1



Active Connections

Proto	Local address	Foreign Address	State	PID	
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000	
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1033	
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1400	
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	1989	
TCP	127.0.0.1:1960	172.16.25.50:22	ESTABLISHED	2230	sftp.exe
TCP	127.0.0.1:8447	172.16.50.10:https	ESTABLISHED	2480	mozilla.exe
UDP	127.0.0.1:9211	172.16.25.50:53	ESTABLISHED	3100	
TCP	127.0.0.1:55357	32.111.16.37:22	TIME_WAIT	4800	sftp.exe

DNS server



Active Connections

Proto	Local Address	Foreign Address	State	PID	
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000	
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1200	
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1480	
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	2122	
TCP	127.0.0.1	172.16.25.20:3306	ESTABLISHED	2480	mysql.exe
UDP	127.0.0.1:53	192.168.10.5	ESTABLISHED	2722	dns.exe

Workstation 2



Active Connections

Proto	Local address	Foreign Address	State	PID	
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000	
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1235	
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1466	
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	1566	
TCP	127.0.0.1:1960	172.16.25.20:3306	ESTABLISHED	2001	mysql.exe
TCP	127.0.0.1:8447	52.13.86.101:https	ESTABLISHED	2277	mozilla.exe
UDP	127.0.0.1:9211	172.16.25.50:53	ESTABLISHED	3245	

Proxy server



Netstat output

Proxy logs

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1200
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1480
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	2122
TCP	127.0.0.1:8100	43.104.133.18:https	ESTABLISHED	2699
TCP	127.0.0.1:8100	16.14.111.8:https	ESTABLISHED	2722
TCP	127.0.0.1:8100	203.4.3.7:https	ESTABLISHED	2782
TCP	127.0.0.1:8100	43.104.133.19:https	ESTABLISHED	2900
UDP	127.0.0.1:9211	172.16.25.50:53	ESTABLISHED	9145

Proxy server



Netstat output

Proxy logs

Host	Destination	Protocol	Request
192.168.10.5	8.8.8.8	https	"GET https://google.com"
192.168.10.5	8.8.8.8	https	"GET https://google.com/search?q=current+stoc+price"
192.168.10.5	8.8.8.8	https	"GET https://google.com/search?q=current+stock+price"
172.16.25.20	43.104.133.18	https	"GET https://sourceforge/search?'default sql login'"
192.168.10.5	8.8.8.8	https	"GET https://google.com/search?q=last+stock+price"
172.16.25.20	16.14.111.8	https	"POST https://oracle.com/patch=%version%"
192.168.10.5	52.13.86.101	https	"GET https://bank.com/mylogin"
192.168.10.5	203.4.3.7	https	"GET https://newsource.com/latest.html"
172.16.25.20	43.104.133.19	https	"GET https://sourceforge/search?'default sql login command syntax'"
192.168.10.5	52.13.86.101	https	"GET https://bank.com/mylogin"

Application server



Active Connections

Proto	Local Address	Foreign Address	State	PID	
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000	
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1322	
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1577	
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	2189	
TCP	127.0.0.1	172.16.25.20:3306	ESTABLISHED	2440	mysql.exe
TCP	127.0.0.1:7001	192.168.10.5	ESTABLISHED	6200	weblogic.exe
TCP	127.0.0.1:7002	192.168.10.6	ESTABLISHED	6234	weblogic.exe
UDP	127.0.0.1	172.16.25.50:53	ESTABLISHED	6844	

Database server



Active Connections

Proto	Local Address	Foreign Address	State	PID	
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000	
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1200	
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1480	
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	2122	
TCP	192.16.25.20:3306	192.168.10.6	ESTABLISHED	2480	
TCP	127.0.0.1:8100	172.16.50.10:https	ESTABLISHED	2722	mozilla.exe
UDP	127.0.0.1:9211	172.16.25.50:53	ESTABLISHED	9145	



Internet

DDoS target
52.13.86.101

Select the compromised host:

Select
Select
172.16.25.60
192.168.10.5
192.168.10.6
172.16.25.20
172.16.50.10
172.16.25.50

Select the compromised executable:

Select
Select
sftp.exe
mozilla.exe
weblogic.exe
dns.exe
mysql.exe

Select the correct remediation:

Select
Select
Block all HTTP requests to the target IP address.
Bypass the proxy server for all HTTP requests.
Reimage the host workstation 2.
Disable web browsing from the server domain.

Answer:

Internet

DDoS target
52.13.86.101

Select the compromised host:

Select
Select
172.16.25.60
192.168.10.5
192.168.10.6
172.16.25.20
172.16.50.10
172.16.25.50

Select the compromised executable:

Select
Select
sftp.exe
mozilla.exe
weblogic.exe
dns.exe
mysql.exe

Select the correct remediation:

Select
Select
Block all HTTP requests to the target IP address.
Bypass the proxy server for all HTTP requests.
Reimage the host workstation 2.
Disable web browsing from the server domain.

Explanation:

Workstation 2 has a direct HTTPS connection from mozilla.exe to the DDoS target 52.13.86.101, bypassing the required proxy server. Reimaging the compromised workstation removes the malicious software and restores the system to a trusted state.

NEW QUESTION: 55

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: (SHOW ANSWER)

SASE delivers networking and security controls through cloud-based services, protecting users and resources regardless of location instead of relying on a traditional network perimeter.

NEW QUESTION: 56

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 define approved tools, permitted data, acceptable use, and security requirements, enabling AI adoption while protecting organizational information and objectives.

NEW QUESTION: 57

An analyst reviews code for a sensitive application for their company and uploads it to an AI platform.

This application is critical to the company's business operations. Which of the following risks is most important for the analyst to consider?

- A. Hallucinations
- B. Malicious prompts
- C. Data exposure
- D. Model poisoning

Answer: (SHOW ANSWER)

Uploading sensitive application code to an AI platform creates a significant risk that proprietary or confidential information could be exposed, stored, or used beyond the organization's control.

NEW QUESTION: 58

An organization's security operations center (SOC) team prioritizes confidentiality and integrity over monetary considerations. The SOC team contains a quickly progressing ransomware incident.

Which of the following factors motivated the SOC team to take this action? (Choose two.)

- A. Attack vector
- B. Risk appetite
- C. Scope
- D. Impact
- E. Common Vulnerability Scoring System (CVSS) score
- F. Asset value

Answer: (SHOW ANSWER)

Risk appetite defines the organization's tolerance for risk and reflects the prioritization of confidentiality and integrity over financial considerations.

Impact represents the effect of the incident on critical security objectives such as confidentiality and integrity, which motivated rapid containment of the ransomware incident.

NEW QUESTION: 59

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

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

Prowler assesses cloud environments against security benchmarks and best practices, helping establish and validate cloud security baselines.

NEW QUESTION: 60

Cybersecurity analysts determine that SIEM alerts are true positives and an internal application is being attacked. Which of the following is a critical step to understanding the impact on the business at this stage?

- A. Notification of the legal team
- B. Knowledge of any regulatory requirements
- C. Root cause analysis
- D. Identification of stakeholders

Answer: (SHOW ANSWER)

Identifying stakeholders is critical for understanding the business impact of an attack because stakeholders can provide information about the application's role, the business processes it supports, the data it handles, and the operational consequences of disruption. This information helps determine the severity and scope of the incident and guides response priorities.

NEW QUESTION: 61

Which of the following is the main concept behind the use of an attack methodology framework?

- A. Implementing continuous monitoring and rapid deployment of system fixes over the traditional patch, test, and deploy approach
- B. Prioritizing vulnerabilities that can be exploited based on risk calculations and using the consequences and likelihood of the exploits to determine where resources should be allocated
- C. Approaching cybersecurity from the perspective of a threat actor and using their common behaviors and motivations to identify secure solutions
- D. Applying a Zero Trust environment by assuming networks and systems are vulnerable to malicious actions by both external, hostile adversaries and insider threats

Answer: (SHOW ANSWER)

Attack methodology frameworks model how adversaries think and operate, helping defenders anticipate attack behaviors and design effective detections and controls.

Valid CS0-004 Dumps shared by EduDump.com for Helping Passing CS0-004 Exam! EduDump.com now offer the **newest CS0-004 exam dumps**, the EduDump.com CS0-004 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-004 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-004/premium/> (190 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 62

Which of the following best describes the action a technical team should take during the containment phase of a security breach?

- A. Make vulnerability scan reports available to the appropriate teams.
- B. Create automation scripts for immediate isolation.
- C. Maintain a reliable patch management solution.
- D. Specify clear and defined incident response roles.

Answer: (SHOW ANSWER)

During the containment phase, the primary objective is to limit the spread and impact of the security incident by isolating affected systems or segments of the network. Creating automation scripts that can immediately isolate compromised hosts or block malicious activity helps rapidly contain the breach and prevent further damage.

NEW QUESTION: 63

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

Metric	Value	Notes
Alerts	3701	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: (SHOW ANSWER)

The large number of alerts and investigations compared with only five confirmed incidents indicates excessive non-actionable alerts. Tuning detection rules reduces false positives and unnecessary analyst workload.

NEW QUESTION: 64

Which of the following best describes the main objective of the exploitation phase according to the Cyber Kill Chain methodology?

- A. To actively scan for vulnerabilities
- B. To send a malicious payload
- C. To gain access to a target
- D. To destroy logs

Answer: (SHOW ANSWER)

In the Cyber Kill Chain, the exploitation phase is where the attacker takes advantage of a vulnerability to execute malicious code and gain unauthorized access to the target system. This step follows delivery and represents the point at which the attack successfully compromises the target.

NEW QUESTION: 65

A red-team exercise identifies the following string that was entered in a username field on a web application and caused data exposure:

' or 1=1; select * from users; --

Which of the following is the best strategy to remediate this issue?

- A. Attack surface management
- B. Secure coding best practices
- C. Compensating controls
- D. Patching and configuration management

Answer: ([SHOW ANSWER](#))

The input string demonstrates a SQL injection attack, where malicious input is used to manipulate database queries and expose sensitive data. The most effective remediation is implementing secure coding practices such as input validation, parameterized queries, and proper sanitization of user inputs to prevent injection vulnerabilities in the application code.

NEW QUESTION: 66

Which of the following is a reason an executive summary is important for incident response communication?

- A. It uses quantifiable metrics to identify the root cause.
- B. It is a concise way for the leadership team to understand the event.
- C. It is included as part of privacy disclosure statements.
- D. It provides a detailed explanation of the incident.

Answer: ([SHOW ANSWER](#))

An executive summary provides a brief, high-level overview of the incident so leadership and nontechnical stakeholders can quickly understand what happened, the impact on the organization, and the current status of the response without needing to review detailed technical information.

NEW QUESTION: 67

A spillage incident results in the access of controlled information across multiple unauthorized business units. Which of the following response techniques should be implemented first?

- A. Analysis and triage
- B. Containment and isolation
- C. Evidence and legal hold
- D. Escalation and monitoring

Answer: ([SHOW ANSWER](#))

Containment and isolation must be implemented first to immediately stop further unauthorized access and prevent additional spread of controlled information across business units.

NEW QUESTION: 68

Which of the following describes the importance of an organization understanding SLOs when outsourcing IR to a third party?

- A. To track the performance of specific KPIs
- B. To understand the hidden costs of an SLA
- C. To ensure that an objective risk score can be calculated
- D. To quantify the risk appetite in an MOU

Answer: ([SHOW ANSWER](#))

Service Level Objectives (SLOs) define specific performance targets for services provided by a third party, such as incident detection, response, or resolution times. Understanding these objectives allows an organization to measure and track the provider's performance through relevant KPIs and determine whether the outsourced incident response service is meeting expectations.

NEW QUESTION: 69

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: ([SHOW ANSWER](#))

Correlating the logs chronologically identifies which system showed the earliest evidence of compromise, helping determine patient zero.

NEW QUESTION: 70

A recent security audit found that RCE was possible for a specific application server that requires public access for HTTP and HTTPS traffic. Which of the following controls should a security analyst recommend?

- A. Modifying the rules on the WAF to sanitize user input
- B. Only allowing one application server to be publicly accessible
- C. Creating an IAM policy so that only administrators can access the server
- D. Configuring a firewall rule to deny all inbound external traffic

Answer: ([SHOW ANSWER](#))

A Web Application Firewall (WAF) can help mitigate Remote Code Execution (RCE) attacks by inspecting and filtering HTTP/HTTPS traffic and sanitizing malicious user input before it reaches the application. Since the server must remain publicly accessible for web traffic, modifying WAF rules is the most appropriate control to reduce the risk while preserving required functionality.

NEW QUESTION: 71

A critical server hosting final exams for an educational institution fails while students are taking their exams. The final exam deadline is in 16 hours. Which of the following is the best source for guidance on remediation for the IT team?

- A. MOU
- B. KPI
- C. SLA
- D. BCP

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

A business continuity plan provides documented procedures and guidance for restoring critical services and operations after a disruption, especially when time-sensitive activities like exams are impacted.

NEW QUESTION: 72

Which of the following can a software provider use to implement secure authentication and authorization mechanisms that leverage existing controls in-place on their customers' environments?

- A. SSO
- B. SASE
- C. PAM
- D. CASB

Answer: ([SHOW ANSWER](#))

Single sign-on enables integration with a customer's existing identity and access management systems, allowing the provider to rely on established authentication and authorization controls already in place within the customer environment.

NEW QUESTION: 73

Users frequently get disconnected from the company's internal wireless network. The wireless system and clients are healthy. Once disconnected, the wireless clients reconnect automatically. Which of the following is the best way for a security analyst to determine the source of the wireless disconnection?

- A. Looking at authentication logs for impossible travel
- B. Collecting the RADIUS logs and investigating the IP addresses of failed user authentications
- C. Utilizing aireplay-ng to disconnect the malicious wireless station and capture its handshake
- D. Using a client with kismet to analyze the airspace for potential deauthentication attacks

Answer: ([SHOW ANSWER](#))

Deauthentication attacks force wireless clients to disconnect from an access point by sending forged deauthentication frames. Since the clients automatically reconnect and the wireless infrastructure appears healthy, analyzing the wireless airspace with Kismet is the best way to detect unauthorized deauthentication frames and determine whether a wireless attack is causing the disconnects.

NEW QUESTION: 74

During a routine review of DNS logs, a security analyst observes that Host X has been making frequent DNS requests to domains with random alphanumeric strings (e.g.. atd8ekthj.xyz). IPS anomaly rules are blocking these domains. This behavior started shortly after a new software installation on the host. Which of the following should the analyst do first to determine whether Host X has been compromised?

- A. Allow the domains because the DNS requests are part of a misconfigured software update.
- B. Check the software installation logs for errors and reinstall the software.
- C. Block all outbound connections from the host to prevent further DNS queries.
- D. Use threat intelligence to check if the queried domains are associated with legitimate sites.

Answer: ([SHOW ANSWER](#))

Random, algorithmically generated domain names are a common indicator of malware using domain generation algorithms (DGAs). Checking the queried domains against threat intelligence is the fastest way to confirm whether they are malicious and whether the host is likely compromised.

NEW QUESTION: 75

Current playbooks for incident response mention resources that have been decommissioned. Which of the following actions should an analyst take?

- A. Schedule a meeting with the responsible team for a policy review
- B. Create an automation script to archive unused playbooks.
- C. Begin an asset inventory review with the appropriate team.
- D. Rewrite all threat response playbooks.

Answer: ([SHOW ANSWER](#))

Playbooks are part of formal incident response procedures and must remain aligned with current policies, infrastructure, and available resources. When they reference decommissioned resources, the appropriate action is to coordinate with the responsible stakeholders to review and update the policy and procedures so the playbooks accurately reflect the current environment.

NEW QUESTION: 76

A security analyst is handling vulnerability management tasks and reviewing the following output from Recon-ng's Shodan-IP module:

```

...
[*] Country: United States of America
[*] Host: domaincontroller.comptia.org
[*] Ip_Address: 177.511.10.10
...
[*] Region: US-East
[*]-----

[*]-----
[*] Country: United States of America
[*] Host: vpn.comptia.org
[*] Ip_Address: 177.511.10.20
...
[*] Region: US-East
[*]-----

[*]-----
[*] Country: United States of America
[*] Host: hrdb.comptia.org
[*] Ip_Address: 177.511.10.30
...
[*] Region: US-East
[*]-----

[*]-----
[*] Country: United States of America
[*] Host: payroll.comptia.org
[*] Ip_Address: 177.511.10.40
...
[*] Region: US-East
[*]-----

[*]-----
[*] Country: United States of America
[*] Host: comptia.org
[*] Ip_Address: 177.511.10.80
...
[*] Region: US-East
[*]-----

```

Which of the following are the greatest vulnerabilities? (Choose two.)

- A. Critical data is on the same subnet
- B. IP addresses are in a small range
- C. Systems fail to comply with PCI DSS
- D. The hosts have a high CVSS score
- E. Sensitive systems are exposed to WAN
- F. The OSSTMM evaluation failed

Answer: (SHOW ANSWER)

The output reveals sensitive systems such as a domain controller, VPN server, HR database, and payroll server. Exposing these systems to the WAN increases the attack surface and makes critical infrastructure directly discoverable by external attackers.

The systems are also located within the same subnet range (177.511.10.x), indicating that critical data and sensitive services are concentrated on the same network segment. This can facilitate lateral movement and increase the impact of a compromise.

Valid CS0-004 Dumps shared by EduDump.com for Helping Passing CS0-004 Exam! EduDump.com now offer the **newest CS0-004 exam dumps**, the EduDump.com CS0-004 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-004 dumps with Test Engine here:
<https://www.edudump.com/exams/CuramSoftware/CS0-004/premium/> (**190** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 77

Which of the following is best suited for determining the methods of an adversary?

- A. OWASP
- B. Penetration Test Framework
- C. OSSTMM
- D. Diamond Model of Intrusion Analysis

Answer: (SHOW ANSWER)

The Diamond Model of Intrusion Analysis is specifically designed to analyze adversary activity by examining the relationships among the adversary, infrastructure, capabilities, and victims. It helps security analysts understand how attackers operate, identify their methods and behaviors, and develop intelligence about their tactics, techniques, and procedures (TTPs).

NEW QUESTION: 78

Which of the following best explains the importance of communicating unusual alert findings?

- A. To provide better metrics related to activities
- B. To identify who found the activity
- C. To ensure activities are properly investigated
- D. To define how each activity is triaged

Answer: (SHOW ANSWER)

Communicating unusual alert findings ensures that potentially significant security activities receive appropriate attention and investigation. What initially appears unusual may indicate a developing threat, compromise, or control failure, and timely communication helps analysts validate, investigate, and respond before the issue escalates.

NEW QUESTION: 79

Which of the following phases of the incident response process will permanently remove an attacker's access to corporate resources?

- A. Eradication
- B. Containment
- C. Denial of service
- D. Detection

Answer: A (LEAVE A REPLY)

Eradication removes the attacker's foothold, malware, compromised accounts, and persistence mechanisms. Containment only limits or temporarily blocks the attacker's activity.

NEW QUESTION: 80

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	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 attacker used sudo, su, and linpeas.sh to move from lower-privileged accounts to the root account, demonstrating privilege escalation.

NEW QUESTION: 81

Which of the following security controls should be classified as operational?

- A. An IDS alerting upon suspicious packet fragmentation
- B. Denying remote VPN connections based on country of origin
- C. Encrypting sensitive data traversing an untrusted network
- D. Conducting a penetration test of data center servers

Answer: ([SHOW ANSWER](#))

Operational controls are implemented through people and processes rather than technology alone. Conducting a penetration test is an operational control because it is a security activity performed by personnel to assess the effectiveness of security measures and identify vulnerabilities in the environment.

NEW QUESTION: 82

Which of the following explains how MTTD can affect IR 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. The 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](#))

Mean Time to Detect (MTTD) measures how quickly an organization identifies security incidents.

A shorter MTTD means threats are discovered sooner, allowing responders to contain and remediate them before they cause greater damage. This directly reduces the potential impact of an incident and is an important metric in incident response reporting.

NEW QUESTION: 83

A security analyst performs a vulnerability scan on the corporate assets and finds the following vulnerabilities:

System	Vulnerability	CVSS severity score
System A	Buffer overflow	9.5
System B	Remote code execution	9.8
System C	DDoS	8.2
System D	XSS	8.6

The vulnerability manager reviews the analyst's recommendations and asks the analyst to add more information in order to confirm prioritization. Which of the following best explains the reason the manager requests more information?

- A. Host critically is unknown
- B. SLA information is missing
- C. Existing KPIs were not measured
- D. Zero-day vulnerabilities were excluded

Answer: ([SHOW ANSWER](#))

CVSS scores alone are not sufficient to prioritize remediation efforts. The criticality of the affected host or asset must also be considered. A vulnerability with a lower CVSS score on a mission-critical system may present a greater business risk than a higher-scoring vulnerability on a less important system. The manager is requesting additional information to perform proper risk-based prioritization.

NEW QUESTION: 84

Which of the following best describes the reason a root cause analysis is an important part of the incident response process?

- A. Compliance teams can be legally required to conduct a post-incident root cause analysis to satisfy regulatory requirements.
- B. Response teams can use the analysis to isolate a system while the incident is ongoing to prevent further contamination.
- C. The organization can use the results of the analysis to provide stakeholders with assurances that customer data was not disclosed.
- D. The leadership team can better allocate resources to address systemic issues that span multiple groups in an organization.

Answer: ([SHOW ANSWER](#))

Root cause analysis identifies the underlying systemic issues that allowed the incident to occur, enabling leadership to address weaknesses across processes, technology, or teams and allocate resources effectively to prevent recurrence.

NEW QUESTION: 85

Which of the following should be configured in a WAF to mitigate an RCE attack?

- A. Rate control in deny mode
- B. Rule to detect and block OS commands
- C. Parameterized queries
- D. Stored procedure in the database

Answer: ([SHOW ANSWER](#))

Remote Code Execution (RCE) attacks often attempt to execute operating system commands through user-supplied input. A WAF can mitigate these attacks by using rules that detect and block malicious command patterns and payloads before they reach the application. This provides protection at the web application layer against command execution attempts.

NEW QUESTION: 86

An analyst reviews the following log entries:

Time (UTC)	Source Internet Protocol (IP)	Source hostname	Source port/protocol	Destination IP	Destination port/protocol
16:44:53	192.168.1.57	ws-57	49571/client	192.168.1.2	22/ssh
16:44:54	192.168.1.57	ws-57	44236/client	192.168.1.2	23/telnet
16:44:55	192.168.1.57	ws-57	46871/client	192.168.1.2	80/http
16:44:56	192.168.1.57	ws-57	43664/client	192.168.1.2	139/netbios
16:44:57	192.168.1.57	ws-57	50127/client	192.168.1.2	443/https
16:44:58	192.168.1.57	ws-57	48741/client	192.168.1.2	445/smb
16:44:59	192.168.1.57	ws-57	50111/client	192.168.1.2	3389/rdp
16:46:33	192.168.1.2	dc-1	445/smb	192.168.1.57	48741/client
16:52:12	192.168.1.57	ws-57	49853/client	185.167.3.24	53/https
16:59:31	192.168.1.57	ws-57	49953/client	192.168.1.25	25/smtp

Which of the following conclusions should the analyst reach? (Choose two.)

- A. Host ws-57 is performing a network scan against dc-1.
- B. Domain Controller dc-1 is performing a network scan against ws-57.
- C. Host ws-57 delivered a phishing email via Simple Mail Transfer Protocol.
- D. Host ws-57 is communicating on a service using a non-standard port.
- E. Domain Controller dc-1 is infected with ransomware and initiating connections with ws-57.
- F. Domain Controller dc-1 is communicating using a non-standard port.

Answer: (SHOW ANSWER)

ws-57 connects to many common service ports on dc-1 within seconds, indicating a port scan. It also uses HTTPS over port 53, which is a non-standard port for HTTPS.

Valid CS0-004 Dumps shared by EduDump.com for Helping Passing CS0-004 Exam! EduDump.com now offer the **newest CS0-004 exam dumps**, the EduDump.com CS0-004 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com CS0-004 dumps with Test Engine here:

<https://www.edudump.com/exams/CuramSoftware/CS0-004/premium/> (190 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)