DUMPSARENA

Performing CyberOps Using Core Security Technologies (CBRCOR)

Cisco 350-201

Version Demo

Total Demo Questions: 22

Total Premium Questions: 228

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Security Concepts	89
Topic 2, Security Monitoring	32
Topic 3, Host-Based Analysis	29
Topic 4, Network Intrusion Analysis	33
Topic 5, Incident Response	45
Total	228

QUESTION NO: 1

A company recently started accepting credit card payments in their local warehouses and is undergoing a PCI audit. Based on business requirements, the company needs to store sensitive authentication data for 45 days. How must data be stored for compliance?

A. post-authorization by non-issuing entities if there is a documented business justification

B. by entities that issue payment cards or perform support issuing services, when there is a legitimate business need and the data is stored securely

C. post-authorization by non-issuing entities if the data is encrypted and securely stored

D. by issuers and issuer processors if there is a legitimate reason

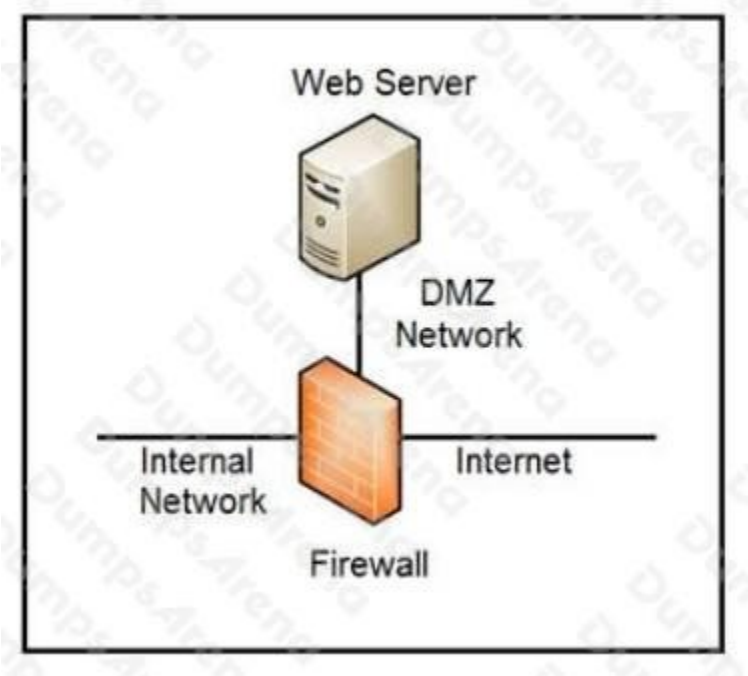
ANSWER: B

Explanation:

Sensitive authentication data includes information such as full track data, card verification values, and PIN-related data. For a merchant accepting card payments, this information must not be retained after authorization, even where encryption or another protective control is used. The narrowly defined exception applies to card issuers and organizations that provide issuing-support services. Those entities may retain sensitive authentication data after authorization only when a legitimate business need exists and the data is stored securely.

Therefore, the applicable compliance condition is that the organization must be an issuer or provide support for issuing services, must have a legitimate business need for the retention period, and must protect the retained data securely. A stated 45-day retention period does not itself establish permission; the retention must be justified by the issuer-related business function and secured in accordance with the applicable PCI DSS controls. PCI SSC states that sensitive authentication data cannot be stored after authorization, with this limited issuer and issuing-support exception. See the PCI Security Standards Council merchant guidance and the PCI DSS document library.

QUESTION NO: 2



Refer to the exhibit. Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

A. Create an ACL on the firewall to allow only TLS 1.3

B. Implement a reverse server in the DMZ network

C. Create an ACL on the firewall to allow only external connections

D. Move the webserver to the internal network

E. Move the webserver to the external network

ANSWER: B D

Explanation:

Implementing a reverse server in the DMZ network and moving the webserver to the internal network provide layered protection for an Internet-facing application. A reverse server, commonly deployed as a reverse proxy, is placed in the DMZ as the only system directly reachable from untrusted Internet clients. It accepts inbound web requests and proxies only permitted traffic to the application server. This creates a controlled security boundary where inspection, rate limiting, web-application firewall functions, TLS termination, request filtering, and logging can be applied before traffic reaches the protected server.

Moving the actual webserver to the internal network ensures that it does not have a directly Internet-routable exposure. Firewall policy can then permit only the specific flows required between the reverse proxy in the DMZ and the internal webserver, typically limited to the necessary application ports and source addresses. This segmentation reduces the reachable attack surface and helps contain an intrusion of the public-facing proxy tier so that it does not automatically provide direct access to the application host. Cisco's security architecture guidance emphasizes segmentation and controlled traffic enforcement between network zones, while OWASP identifies reverse proxies as a useful control point for protecting web applications. See Cisco Secure Firewall and OWASP Reverse Proxy.

QUESTION NO: 3

An engineer is analyzing a possible compromise that happened a week ago when the company? (Choose two.)

A. firewall

B. Wireshark

C. autopsy

D. SHA512

E. IPS

ANSWER: B C

Explanation:

Wireshark and **autopsy** are appropriate tools for retrospective compromise analysis because they support two complementary areas of digital forensics: network evidence and endpoint/storage evidence. Wireshark can inspect saved packet-capture files, allowing an analyst to reconstruct observed network conversations and identify useful artifacts such as protocol activity, DNS requests, HTTP exchanges, suspicious connections, transferred files, and indicators of command-and-control behavior. Its value for an event from a week earlier depends on packet captures having been retained, but it is the standard analysis tool for available PCAP evidence. Wireshark's documentation describes its ability to capture and interactively browse packet data: Wireshark User's Guide.

Autopsy is a forensic analysis platform used to examine acquired disk images and other storage evidence. It helps investigators identify and correlate artifacts such as file-system metadata, deleted files, browser history, downloads, operating-system events, executables, hashes, and timeline data. These artifacts can establish what executed, changed, or persisted on an affected host during the suspected compromise window. The Autopsy project documents its forensic-analysis capabilities at Autopsy Digital Forensics Platform. Together, retained network traffic analyzed with Wireshark and endpoint evidence examined with Autopsy provide the relevant evidence sources for investigating a past compromise.

QUESTION NO: 4



Refer to the exhibit. At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?

A. exploitation

B. actions on objectives

C. delivery

D. reconnaissance

ANSWER: D

Explanation:

reconnaissance is correct because requests from known malicious Internet scanners to a range of web URIs indicate information gathering and target discovery. At this point, the attacker is attempting to learn which web server paths, applications, frameworks, administrative interfaces, or potentially vulnerable resources are exposed. Requests for common paths can reveal software characteristics through response codes, page content, headers, redirects, and timing behavior. This information helps an attacker identify viable targets and select a later intrusion technique.

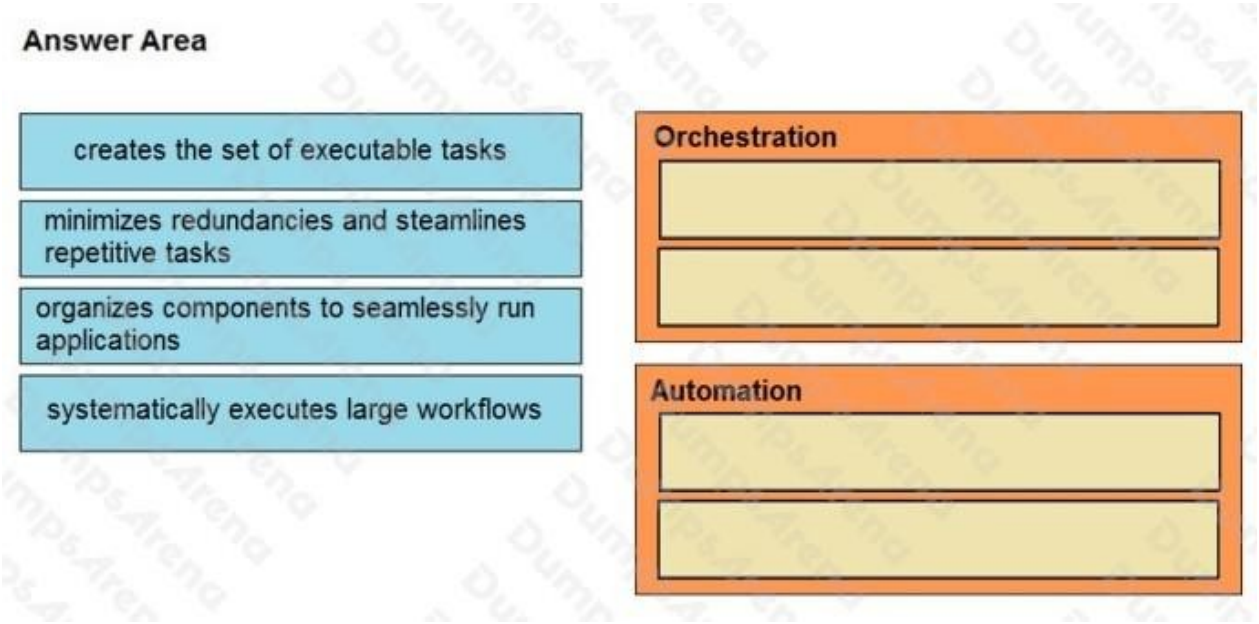
In the Cyber Kill Chain model, reconnaissance encompasses collecting information about a prospective target before attempting to compromise it. Web scanning is a common reconnaissance activity because it maps the externally visible attack surface without necessarily requiring successful access to the application or host. The observation that the requests are inbound and originate from malicious scanners supports classifying the behavior as pre-compromise discovery rather than a completed intrusion action. Cisco security operations workflows similarly treat repeated requests for sensitive, unusual, or widely known URI paths as indicators that should be investigated for web application enumeration and exposure. See the Lockheed Martin Cyber Kill Chain and Cisco's Secure Firewall documentation for relevant threat-detection context.

QUESTION NO: 5 - (DRAG DROP)

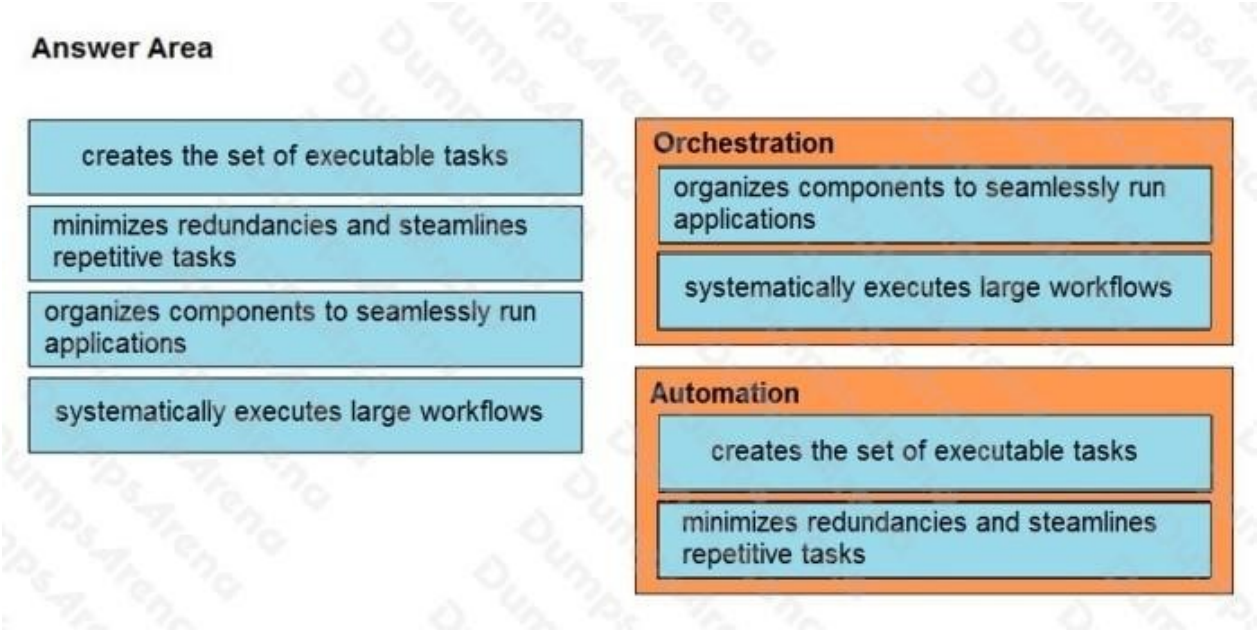
DRAG DROP

Drag and drop the function on the left onto the mechanism on the right.

Select and Place:



ANSWER:



Explanation:

Automation and orchestration work together to reduce manual operational effort, but they operate at different levels. Automation creates executable tasks that perform a defined action without requiring a person to carry out every step. This can include actions such as collecting data, applying a configuration, opening a case, enriching an alert, or running a script. Because these actions are repeatable, automation also minimizes redundant effort and streamlines routine tasks. Cisco describes security automation as using technology to perform tasks with reduced human intervention, allowing teams to execute recurring operational work consistently.

Orchestration is the higher-level coordination of multiple automated tasks, tools, systems, and decision points into an end-to-end process. It organizes those components so that they operate together seamlessly in support of an application or security process. A workflow may require information from several security products, conditional logic, approvals, and a sequence of response actions. Orchestration systematically executes that larger workflow in the intended order, connecting the individual executable tasks into one coordinated outcome. This is especially relevant in security operations, where incident-response workflows commonly span detection, enrichment, containment, ticketing, and notification activities.

Accordingly, Orchestration maps to “organizes components to seamlessly run applications” and “systematically executes large workflows.” Automation maps to “creates the set of executable tasks” and “minimizes redundancies and streamlines repetitive tasks.” Cisco’s overview of security orchestration and automation and the NIST automation glossary definition support this distinction between executing individual repeatable tasks and coordinating them as a broader process.

QUESTION NO: 6

Which action should be taken when the HTTP response code 301 is received from a web application?

A. Update the cached header metadata.

B. Confirm the resource's new location specified in the Location header.

C. Increase the allowed user limit.

D. Modify the session timeout setting.

ANSWER: B

Explanation:

"Confirm the resource's new location specified in the Location header" is correct because a 301 response means that the requested resource has been assigned a new permanent URI. The web application communicates the destination URI through the `Location` response header. A client, browser, proxy, or security analyst validating application behavior should inspect that header, confirm that it points to the intended destination, and use the new URI for subsequent requests or references. Since this is a permanent redirect, clients can also retain the redirect mapping according to applicable caching rules, reducing future requests to the original URI. Confirming the destination is particularly important during troubleshooting and security review: it verifies that the application's redirect behavior is expected and that users are not being sent to an unintended endpoint. The HTTP Semantics specification defines 301 as "Moved Permanently" and specifies the use of the `Location` field value as the preferred URI reference for the resource. Cisco security operations work commonly includes interpreting web-server status codes and validating redirect behavior during web-application monitoring and incident investigation. See RFC 9110, 301 Moved Permanently and MDN: 301 Moved Permanently.

QUESTION NO: 7

A security analyst confirms that an employee entered corporate credentials into a fraudulent website. The employee has not reported any other suspicious activity. Which two actions should the incident response team take immediately to contain the potential account compromise? (Choose two.)

A. Reset the employee password.

B. Revoke active authentication sessions.

C. Delete all email from the employee mailbox.

D. Disable centralized authentication logging.

E. Remove the employee from all business applications permanently.

ANSWER: A B

Explanation:

Reset the employee password and **revoke active authentication sessions** are correct. Resetting the password prevents continued use of the credential that may have been captured by the fraudulent site. Revoking active sessions and refresh tokens invalidates authentication artifacts that an attacker may already have obtained, reducing the opportunity to access cloud services without using the newly reset password.

These containment actions should be followed by review of authentication, email, endpoint, and cloud audit logs to determine whether the account was used maliciously. The response team should also assess whether mailbox rules, OAuth grants, or multifactor-authentication methods were altered. NIST incident-handling guidance identifies containment as an activity intended to limit an incident's scope and damage. See NIST SP 800-61 Rev. 2.

QUESTION NO: 8

An engineer is hardening a Linux server that hosts a business application. The application service must read a configuration file that contains database credentials, but no other local users should be able to read or modify the file. Which two actions should be taken? (Choose two.)

A. Set the file owner to the application service account.

B. Set permissions to 600.

C. Set permissions to 644.

D. Set permissions to 777.

E. Make the file executable for all local users.

ANSWER: A B

Explanation:

Set the file owner to the application service account and **set permissions to 600** are correct. Assigning ownership to the account under which the service runs allows that account to access the configuration file without granting access to unrelated users. Permission mode 600 grants read and write permissions to the owner and no permissions to group or other users.

The database credentials should also be protected by appropriate secrets-management practices, but restrictive file ownership and permissions provide necessary operating-system enforcement. Granting read access to all users or making the file executable would unnecessarily expand the attack surface. See the chmod manual page and the GNU Coreutils mode structure documentation.

QUESTION NO: 9

A security incident affected an organization's critical business services, and the customer-side web API became unresponsive and crashed. An investigation revealed a spike of API call requests and a high number of inactive sessions during the incident. Which two recommendations should the engineers make to prevent similar incidents in the future? (Choose two.)

A. Configure shorter timeout periods.

B. Determine API rate-limiting requirements.

C. Implement API key maintenance.

D. Automate server-side error reporting for customers.

E. Decrease simultaneous API responses.

ANSWER: A B

Explanation:

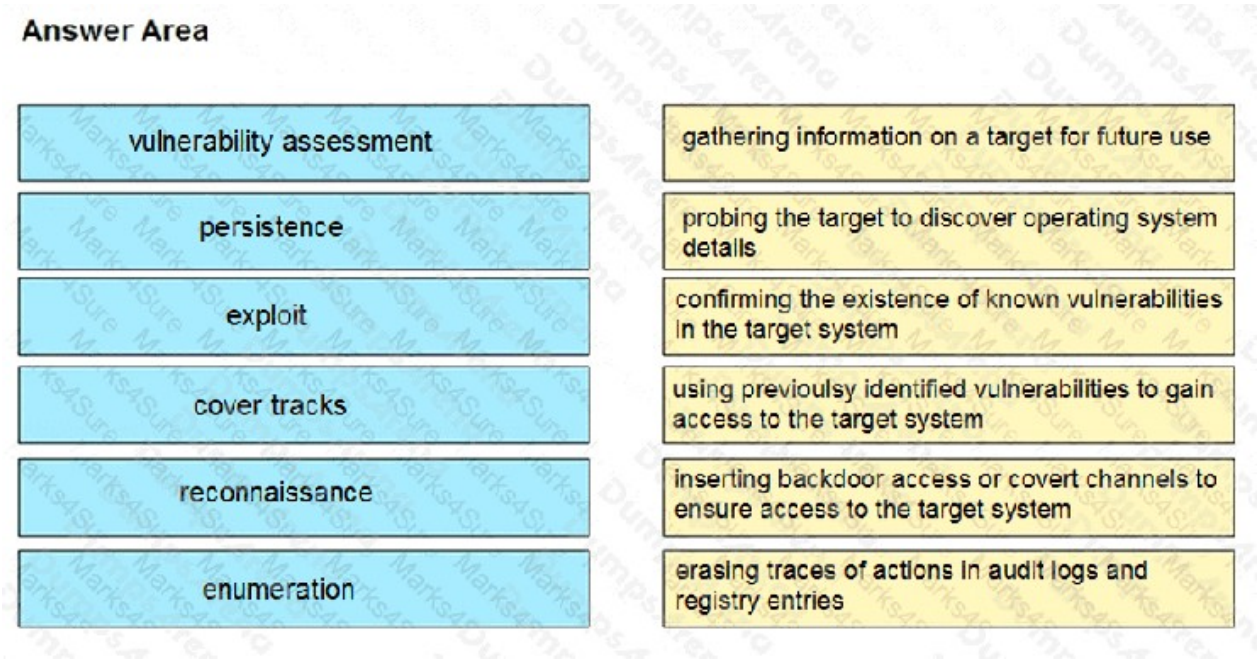
Determine API rate-limiting requirements is appropriate because request spikes can consume API processing capacity, connection pools, memory, and downstream-service resources. Engineers should establish limits based on normal client behavior and service capacity, then enforce them per client identity, API key, source, or endpoint as appropriate. Rate limiting helps ensure that a sudden burst—whether accidental, abusive, or malicious—cannot monopolize resources needed by critical business functions. OWASP identifies unrestricted resource consumption, including excessive API requests, as an API security risk and recommends limits on requests and resource-intensive operations: OWASP API Security Top 10: Unrestricted Resource Consumption.

Configure shorter timeout periods is also appropriate because the incident involved many inactive sessions. Idle or stalled sessions retain finite server-side resources, such as worker threads, sockets, session state, and memory. A suitably short idle-session timeout automatically releases those resources when clients stop interacting with the API, reducing the likelihood that abandoned sessions contribute to capacity exhaustion during a traffic spike. Timeout values should be chosen from measured application behavior so legitimate long-running operations are accommodated while idle connections are

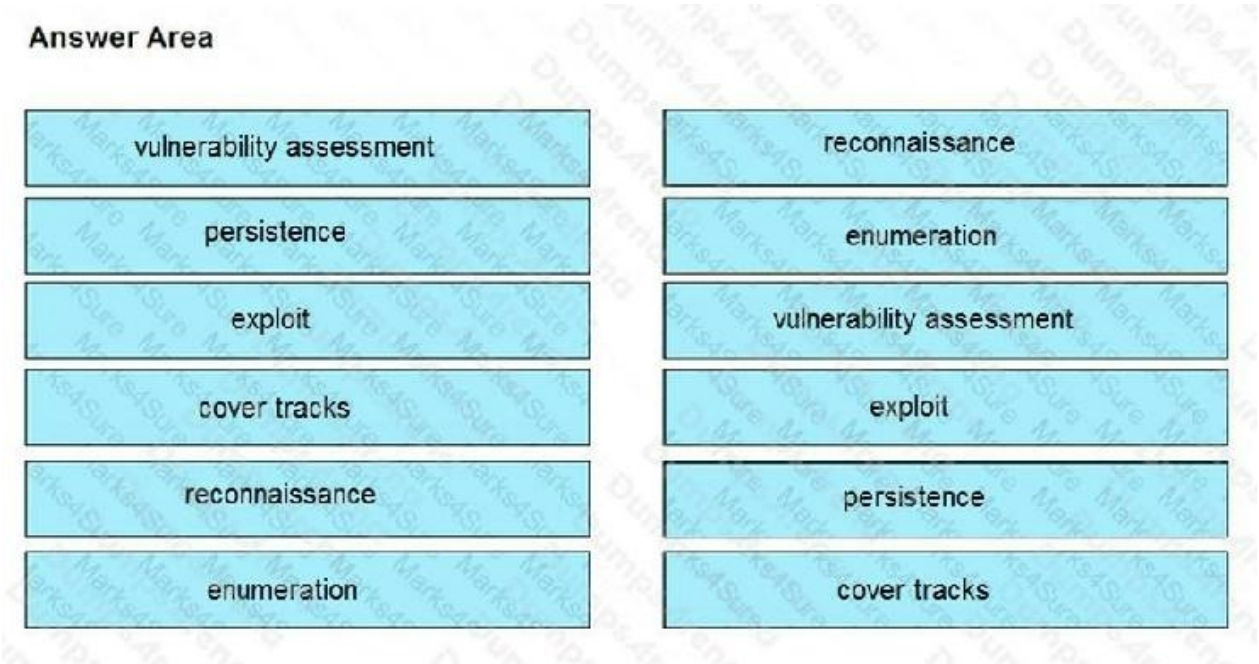
cleaned up promptly. Cisco guidance on protecting web applications includes using controls that mitigate denial-of-service conditions and preserve service availability: Cisco Web Application Firewall.

QUESTION NO: 10 - (DRAG DROP)

Drag and drop the phases to evaluate the security posture of an asset from the left onto the activity that happens during the phases on the right.



ANSWER:



Explanation:

Evaluating an asset's security posture commonly follows a structured workflow that moves from collecting intelligence to validating weaknesses, demonstrating impact, and documenting how access could be maintained or concealed. Reconnaissance is the information-gathering phase. Its purpose is to build a useful profile of the target for subsequent testing, using information such as domains, addresses, personnel details, technologies, and publicly exposed resources.

Enumeration then involves more direct probing to identify technical characteristics of the target, including operating-system details, services, users, shares, and other exposed resources.

Once the target has been characterized, vulnerability assessment confirms whether known weaknesses exist in the discovered software, configuration, services, or operating system. This is more than simply collecting a scan result: it establishes that a vulnerability is relevant to the target and may be usable. Exploitation is the phase in which an identified vulnerability is used to gain access or otherwise demonstrate its security impact. After access is gained, persistence represents the ability to retain access, such as by installing a backdoor or establishing a covert access channel. Finally, covering tracks refers to removing or altering evidence of activity, including traces in audit logs and registry entries. These terms are widely used in penetration-testing and adversary-behavior models; see the NIST Technical Guide to Information Security Testing and Assessment and the MITRE ATT&CK Persistence tactic for related security-testing and post-compromise concepts.

QUESTION NO: 11

A new malware variant is discovered hidden in pirated software that is distributed on the Internet. Executives have asked for an organizational risk assessment. The security officer is given a list of all assets. According to NIST, which two elements are missing to calculate the risk assessment? (Choose two.)

A. incident response playbooks

B. asset vulnerability assessment

C. report of staff members with asset relations

D. key assets and executives

E. malware analysis report

ANSWER: B E

Explanation:

asset vulnerability assessment and **malware analysis report** provide the missing information needed to assess risk from the identified malware scenario. NIST risk assessment methodology considers threat sources and threat events, vulnerabilities and predisposing conditions, likelihood that a threat event will exploit a vulnerability, and the resulting adverse impact. An inventory of assets establishes what the organization must protect, but it does not establish whether those assets have exploitable weaknesses or how the newly discovered malware operates and could affect them.

An asset vulnerability assessment identifies relevant weaknesses in systems, applications, configurations, controls, and user exposure that could allow the pirated-software malware to execute, persist, spread, or access organizational resources. A malware analysis report characterizes the threat event by providing technical evidence such as delivery behavior, execution requirements, capabilities, indicators of compromise, command-and-control behavior, and potential effects. Together, these inputs allow analysts to determine applicable threat-vulnerability pairs and estimate likelihood and impact for the listed assets. This supports a defensible organizational risk determination and prioritization of treatment actions. NIST describes these required assessment elements in SP 800-30 Rev. 1, Guide for Conducting Risk Assessments; related cybersecurity risk-management guidance is available in the NIST Cybersecurity Framework.

QUESTION NO: 12

An organization is implementing centralized log collection for security investigations. The security team must ensure that collected logs can be correlated accurately across firewalls, endpoints, and identity services and that unauthorized changes to retained records can be detected. Which two controls should be implemented? (Choose two.)

A. Synchronize system clocks using a trusted time source.

B. Restrict write access to the centralized log repository.

C. Allow each system administrator to delete local events after forwarding logs.

D. Configure all log sources to use different timestamp formats.

E. Disable auditing after logs have been forwarded to reduce storage use.

ANSWER: A B

Explanation:

Synchronize system clocks using a trusted time source and **restrict write access to the centralized log repository** are correct. Accurate and synchronized timestamps allow analysts to correlate events from separate sources into a reliable incident timeline. Without consistent time, authentication events, network connections, and endpoint actions can appear in the wrong order.

Restricting write access protects retained logs from unauthorized modification or deletion. Centralized log storage should use role-based access controls and retain administrative audit records so that analysts can trust the evidence used during an investigation. NIST recommends time synchronization, centralized log management, and protection of log data in NIST SP 800-92, Guide to Computer Security Log Management.

QUESTION NO: 13

A security engineer discovers that a spreadsheet containing confidential information for nine of their employees was fraudulently posted on a competitor's website. The spreadsheet contains names, salaries, and social security numbers. What is the next step the engineer should take in this investigation?

A. Determine if there is internal knowledge of this incident.

B. Check incoming and outgoing communications to identify spoofed emails.

C. Disconnect the network from Internet access to stop the phishing threats and regain control.

D. Engage the legal department to explore action against the competitor that posted the spreadsheet.

ANSWER: D

Explanation:

Engage the legal department to explore action against the competitor that posted the spreadsheet. The confirmed public exposure of employee names, salary information, and Social Security numbers is a sensitive-data incident with potentially significant legal, privacy, contractual, and regulatory consequences. Legal counsel should be involved immediately to direct the organization's response, including preserving evidence of the posting, assessing notification and reporting duties, coordinating communications, and determining whether a takedown demand or other legal action is appropriate. Counsel can also help ensure that investigative actions, records, and external communications are handled in a way that supports potential litigation and protects applicable legal privileges. The public website hosting the data may be outside the security team's direct administrative control, so a legal-led approach is essential for pursuing removal and addressing the competitor's role while the technical investigation continues to identify the source and scope of the disclosure. NIST's incident-response guidance recognizes that incident handling requires coordination with organizational stakeholders, including legal counsel, especially when an incident can create legal or regulatory exposure. Cisco likewise identifies legal and communications coordination as important elements of incident response. See NIST SP 800-61 Rev. 2 and Cisco Incident Response Services.

QUESTION NO: 14

An analyst is reviewing a packet capture after receiving reports that internal clients are contacting an unauthorized DNS resolver. The analyst must display only DNS requests and exclude DNS responses. Which Wireshark display filter should be used?

A. dns.flags.response == 0

B. dns.flags.response == 1

C. dns.query == 1

D. dns.request == true

ANSWER: A

Explanation:

dns.flags.response == 0 is correct because the DNS response flag is set to 0 for a query and to 1 for a response. Applying this display filter limits the packet list to DNS queries, allowing the analyst to review requested domain names, query types, source hosts, and the destination resolver without response traffic obscuring the analysis.

Wireshark display filters affect only how captured traffic is shown; they do not alter the packet capture. The DNS protocol field can be combined with other conditions, such as an IP address or query-name filter, when additional scoping is needed. See the Wireshark DNS display-filter reference.

QUESTION NO: 15

A security incident affected an organizationâ€™s critical business services, and the customer-side web API became unresponsive and crashed. An investigation revealed a spike of API call requests and a high number of inactive sessions during the incident. Which two recommendations should the engineers make to prevent similar incidents in the future? (Choose two.)

A. Configure shorter timeout periods.

B. Determine API rate-limiting requirements.

C. Implement API key maintenance.

D. Automate server-side error reporting for customers.

E. Decrease simultaneous API responses.

ANSWER: A B

Explanation:

Configure shorter timeout periods. is appropriate because idle or inactive sessions consume server-side resources, including memory, connection pools, and session-state capacity. Enforcing an appropriately short idle-session timeout ensures that abandoned sessions are expired and their associated resources are released promptly. This reduces the likelihood that a buildup of inactive sessions will exhaust capacity during periods of heavy use. Timeout values should be selected according to the application's normal user workflow and the sensitivity of the session.

Determine API rate-limiting requirements. directly addresses the observed surge in API requests. Rate limiting establishes enforceable thresholds for requests per client, identity, token, IP address, or time interval. These limits protect finite API and backend resources from burst traffic, accidental client retry loops, and deliberate resource-exhaustion activity, while allowing the organization to define suitable quotas for legitimate users and business processes. API resource-consumption controls, including rate limiting, are a recognized API-security practice; see the OWASP API Security guidance on unrestricted resource consumption. Session expiration is also a core session-management safeguard described in the OWASP Session Management Cheat Sheet.

QUESTION NO: 16

```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com, realm-0, isRealm=0, realmDomain=0, shortrealm=0
x-xss-protection: 1; mode=block
```

Refer to the exhibit. Where does it signify that a page will be stopped from loading when a scripting attack is detected?

A. x-frame-options

B. x-content-type-options

C. x-xss-protection

D. x-test-debug

ANSWER: C

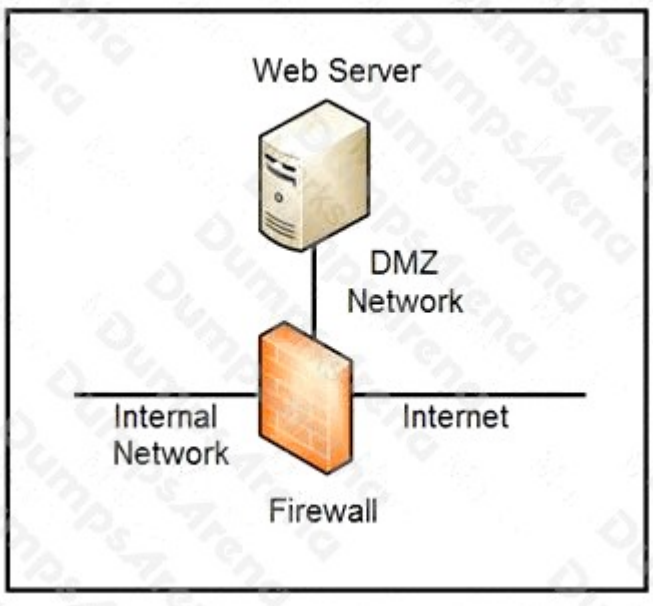
Explanation:

The correct header is **x-xss-protection**. In browsers that implement the legacy XSS filter, this response header controls the filter's behavior. Its blocking directive, commonly expressed as `1; mode=block`, instructs the browser to prevent rendering the page when the filter detects a reflected cross-site-scripting attack. Rather than attempting to sanitize and display the suspected response, the browser stops the document from loading, which is the behavior described in the question.

This header is associated with older browser-based reflected-XSS filtering and is identifiable in an HTTP security-header configuration by its explicit XSS-protection name and block mode. Modern web applications should primarily mitigate XSS through context-aware output encoding, safe DOM APIs, input handling, and a well-designed Content Security Policy. However, when interpreting the exhibited header configuration and the stated page-blocking behavior, **x-xss-protection** is the header that signifies it. MDN documents the header and its legacy browser behavior at MDN Web Docs. Microsoft also documents HTTP security-header configuration, including this header, at Microsoft Learn.

QUESTION NO: 17

Refer to the exhibit.



Which two steps mitigate attacks on the webserver from the Internet? (Choose two.)

A. Create an ACL on the firewall to allow only TLS 1.3

B. Implement a proxy server in the DMZ network

C. Create an ACL on the firewall to allow only external connections

D. Move the webserver to the internal network

ANSWER: B D

Explanation:

Implementing a proxy server in the DMZ network and moving the webserver to the internal network provide a layered, screened architecture for an Internet-facing application. The proxy, functioning as a reverse proxy, is the only component directly exposed to requests from Internet clients. It can terminate client sessions, enforce request-validation and security policies, normalize traffic, and forward only permitted requests to the origin server. This reduces direct exposure of the webserver and creates a controlled enforcement point in the DMZ.

Moving the webserver to the internal network places the application's origin server behind an additional security boundary. The firewall policy between the DMZ and internal network can be tightly restricted so that only the proxy is allowed to initiate the specific required connections to the webserver. Internet clients therefore cannot establish a direct session with the origin server. This separation also helps contain an incident involving the exposed proxy tier and limits an attacker's ability to reach internal systems. Cisco describes the DMZ as a buffer network used to isolate Internet-facing services from the trusted internal network in its DMZ configuration guidance. OWASP likewise recommends reverse proxies and network segmentation as defensive controls for web applications in its Web Security Testing Guide.

QUESTION NO: 18

Refer to the exhibit. A security analyst needs to investigate a security incident involving several suspicious connections with a possible attacker. Which tool should the analyst use to identify the source IP of the offender?

TCP	192.168.1.8:54580	vk-in-f108:imaps	ESTABLISHED
TCP	192.168.1.8:54583	132.245.61.50:https	ESTABLISHED
TCP	192.168.1.8:54916	bay405-m:https	ESTABLISHED
TCP	192.168.1.8:54978	vu-in-f188:5228	ESTABLISHED
TCP	192.168.1.8:55094	72.21.194.109:https	ESTABLISHED
TCP	192.168.1.8:55401	wonderhowto:http	ESTABLISHED
TCP	192.168.1.8:55730	mia07s34-in-f78:https	TIME WAIT
TCP	192.168.1.8:55824	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55825	a23-40-191-15:https	CLOSE_WAIT
TCP	192.168.1.8:55846	mia07s25-in-f14:https	TIME_WAIT
TCP	192.168.1.8:55847	a184-51-150-89:http	CLOSE_WAIT
TCP	192.168.1.8:55853	157.55.56.154:40028	ESTABLISHED
TCP	192.168.1.8:55879	atl14s38-in-f4:https	ESTABLISHED
TCP	192.168.1.8:55884	208-46-117-174:https	ESTABLISHED
TCP	192.168.1.8:55893	vx-in-f95:https	TIME_WAIT
TCP	192.168.1.8:55947	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55966	stackoverflow:https	ESTABLISHED
TCP	192.168.1.8:55970	mia07s34-in-f78:https	TIME_WAIT
TCP	192.168.1.8:55972	191.238.241.80:https	TIME_WAIT
TCP	192.168.1.8:55976	54.239.26.242:https	ESTABLISHED
TCP	192.168.1.8:55979	mia07s35-in-f14:https	ESTABLISHED
TCP	192.168.1.8:55986	server11:https	TIME_WAIT
TCP	192.168.1.8:55988	104.16.118.182:http	ESTABLISHED

A. packet sniffer

B. malware analysis

C. SIEM

D. firewall manager

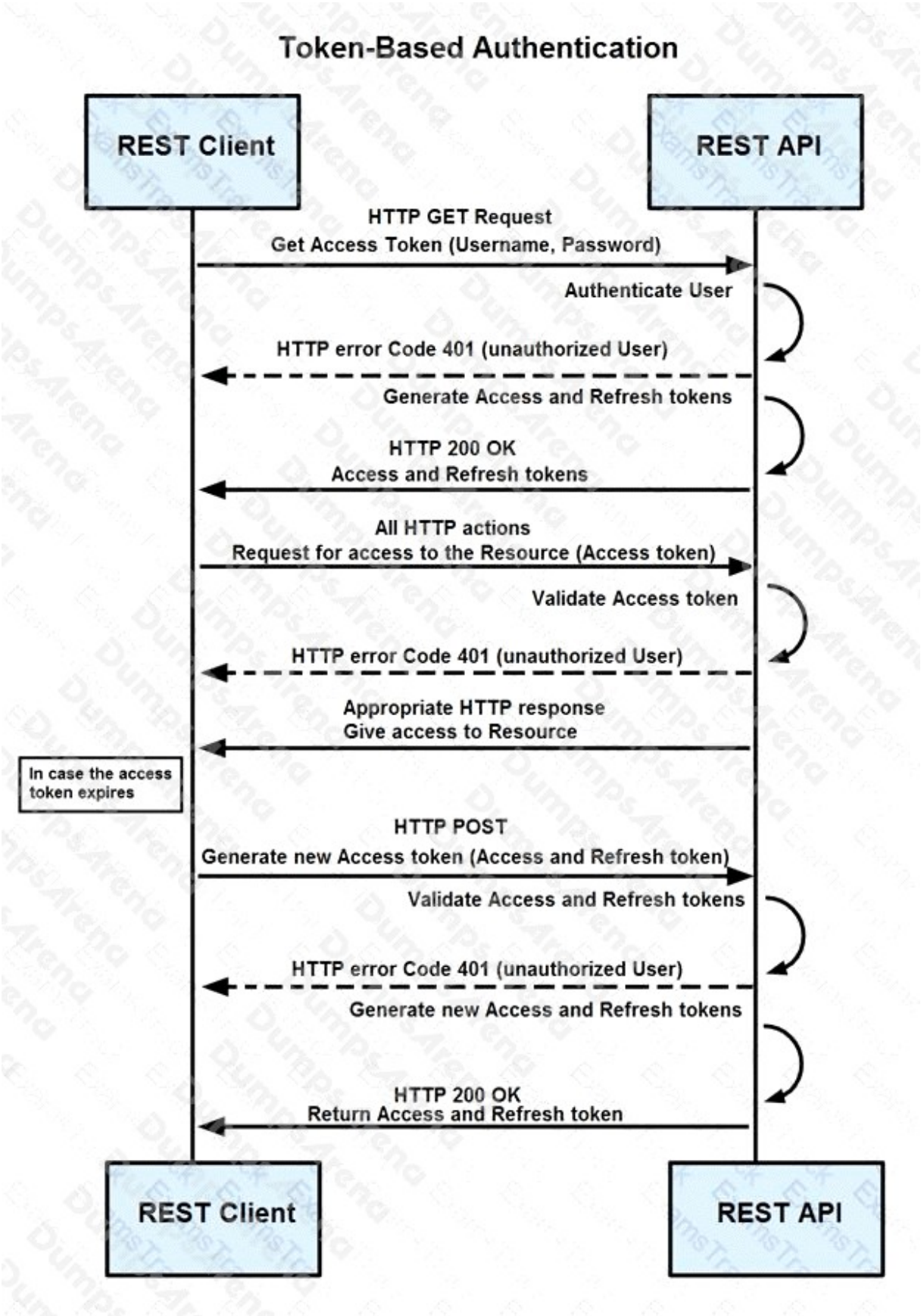
ANSWER: A

Explanation:

A packet sniffer is the appropriate tool because it captures and decodes the network packets associated with the suspicious connections. Each captured IP packet includes a source IP address and a destination IP address in its IP header, allowing the analyst to determine the address from which the observed traffic originated. The analyst can apply capture or display filters for the relevant protocol, port, time range, target host, or suspicious session, then inspect the matching packets' source-address fields. Packet-level evidence also provides useful context for incident investigation, including transport ports, TCP flags, payload characteristics when visible, timestamps, and the sequence of communication. This enables the analyst to correlate the suspected attacker address with the specific connections shown in the exhibit and preserve detailed evidence of the activity. Wireshark documentation describes filtering captured traffic and inspecting packet details, including protocol-header fields: Wireshark User's Guide: Building Display Filter Expressions. Cisco also documents packet capture as a method for collecting traffic for analysis: Cisco ASA Command Reference: packet-capture commands.

QUESTION NO: 19

Refer to the exhibit.



How are tokens authenticated when the REST API on a device is accessed from a REST API client?

A. The token is obtained by providing a password. The REST client requests access to a resource using the access token. The REST API validates the access token and gives access to the resource.

B. The token is obtained by providing a password. The REST API requests access to a resource using the access token, validates the access token, and gives access to the resource.

C. The token is obtained before providing a password. The REST API provides resource access, refreshestokens, and returns them to the REST client. The REST client requests access to a resource using the access token.

D. The token is obtained before providing a password. The REST client provides access to a resource using the access token. The REST API encrypts the access token and gives access to the resource.

ANSWER: A

Explanation:

The token is obtained by providing a password. The REST client requests access to a resource using the access token. The REST API validates the access token and gives access to the resource. This describes the expected token-based REST API workflow: the client first authenticates to the device or authorization service with its credentials, such as a username and password, and receives an access token. The access token represents the authenticated client session and is subsequently included with requests for protected API resources, commonly in an HTTP `Authorization` header. When the device receives the resource request, its REST API validates that token, including its integrity, validity period, and associated authorization context. After successful validation, the API permits access to the requested resource according to the permissions associated with the authenticated identity. This approach avoids sending the password with every individual API request while still allowing the device to authenticate and authorize each request. Cisco API platforms commonly use this initial credential exchange followed by token presentation for subsequent calls. See Cisco's Cisco DNA Center authentication documentation and the OAuth 2.0 Bearer Token Usage RFC for the standard use of access tokens in protected HTTP API requests.

QUESTION NO: 20

Refer to the exhibit.



An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior. Which type of compromise is occurring?

A. compromised insider

B. compromised root access

C. compromised database tables

D. compromised network

ANSWER: D

Explanation:

compromised network is correct because the evidence links unauthorized privileged Active Directory account creation to suspicious traffic that originated inside the organization's network. Creating privileged accounts is a high-impact persistence and privilege-escalation action: an attacker who has obtained a foothold in the environment can establish additional identities, grant elevated rights, and use those accounts to maintain access or move through internal resources. The temporal correlation is especially significant. Network activity occurring first, followed by the creation of privileged accounts, supports an incident narrative in which a compromise enabled an attacker to perform identity-management actions within the domain. Correlating directory events with network telemetry is a core investigation practice because it connects a control-plane change—new privileged users—with the communications and potential access path that preceded it. Cisco describes network security monitoring as using telemetry and event data to detect malicious activity and investigate incidents across the environment. Cisco's guidance on identity security also emphasizes protecting privileged access because privileged identities can provide broad control of enterprise systems. See Cisco Secure Network Analytics and Cisco Identity Services Engine.

QUESTION NO: 21

An organization is developing a post-incident report after a confirmed compromise of an internal server. Leadership requires information that supports future prevention and response improvement. Which two items should be included in the lessons-learned activity? (Choose two.)

A. Document the root cause and attack timeline.

B. Identify corrective actions with assigned owners.

C. Delete incident evidence after service restoration.

D. Disable monitoring rules that generated alerts during the incident.

E. Exclude business stakeholders from reviewing operational impact.

ANSWER: A B

Explanation:

Document the root cause and attack timeline and **identify corrective actions with assigned owners** are correct. A root-cause analysis and timeline establish how the incident occurred, how it progressed, and which controls succeeded or failed. This evidence enables the organization to make informed improvements rather than relying on assumptions.

Corrective actions should be specific, tracked, and assigned to accountable owners. Examples include improving detections, patching affected systems, revising access-control policies, updating playbooks, and addressing training or process gaps. NIST describes post-incident activity as an opportunity to document lessons learned and identify actions that improve future incident handling. See NIST SP 800-61 Rev. 2.

QUESTION NO: 22

An engineer notices that every Sunday night, there is a two-hour period with a large load of network activity. Upon further investigation, the engineer finds that the activity is from locations around the globe outside the organization's service area. What are the next steps the engineer must take?

A. Assign the issue to the incident handling provider because no suspicious activity has been observed during business hours.

B. Review the SIEM and FirePower logs, block all traffic, and document the results of calling the call center.

C. Define the access points using StealthWatch or SIEM logs, understand services being offered during the hours in question, and cross-correlate other source events.

D. Treat it as a false positive, and accept the SIEM issue as valid to avoid alerts from triggering on weekends.

ANSWER: C

Explanation:

Define the access points using StealthWatch or SIEM logs, understand services being offered during the hours in question, and cross-correlate other source events. This is the appropriate next step because unusual, recurring traffic from geographically unexpected sources requires investigation and scoping before containment or escalation decisions are made. The engineer should identify the affected internal hosts, external peers, protocols, ports, traffic volumes, and connection direction to determine the actual exposure and whether the activity reaches an unauthorized service. Establishing which services are available during the recurring time window helps distinguish legitimate scheduled activity from an exposed application, command-and-control communications, scanning, or attempted exploitation. Correlating network telemetry with firewall, authentication, endpoint, DNS, and other event sources provides the context needed to validate the alert, assess impact, and build an evidence-based incident record. Cisco Secure Network Analytics, formerly Stealthwatch, is designed to use network telemetry to identify anomalous behavior and support investigation through contextual analysis. Cisco also describes correlation and investigation as essential security-operations functions for determining the scope and priority of a potential incident. See Cisco Secure Network Analytics and Cisco Security Operations Center.