ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

During an investigation of an alert with a completed playbook, it is determined that no indicators exist from the email "indicator@test.com" in the Key Assets & Artifacts tab of the parent incident. Which command will determine if Cortex XSIAM has been configured to extract indicators as expected?

A. IcreateNewIndicator value="indicator@test.com"

B. !extractIndicators text="indicator@test.com" auto-extract=inline

C. !checkIndicatorExtraction text="indicator@test.com"

D. Iemailvalue="indicator@test.com"

Answer: C

Explanation:

The correct answer is C, the !checkIndicatorExtraction text="indicator@test.com" command.

This command specifically verifies if Cortex XSIAM has been correctly configured to extract indicators from given text. It ensures that the text provided ("indicator@test.com") would indeed be recognized and extracted as an indicator under the current configuration of Cortex XSIAM.

Other provided commands do not directly verify the indicator extraction configuration:
Option A: IcreateNewIndicator manually creates an indicator; it does not validate extraction capability.

Option B: !extractIndicators attempts extraction immediately but does not verify existing configuration explicitly.

Option D: Iemailvalue command is generally for creating or querying email indicators, not verifying extraction configuration.

Therefore, the explicit functionality for checking if indicator extraction is configured correctly within Cortex XSIAM is precisely covered by !checkIndicatorExtraction.

Reference Extract from Official Document:

"Verify if Cortex XSIAM is correctly configured to extract indicators using the command !checkIndicatorExtraction text=<value>."

This exact description confirms that option C is the correct answer to validate the configuration explicitly.

Question: 2

A Cortex XSIAM analyst is reading a blog that references an unfamiliar critical zero-day vulnerability. This vulnerability has been weaponized, and there is evidence that it is being exploited by threat actors targeting a customer's industry. Where can the analyst go within Cortex XSIAM to learn more about this vulnerability and any potential impacts on the customer environment?

A. Threat Intel Management -> Sample Analysis

B. Threat Intel Management -> Indicators

C. Attack Surface -> Threat Response Center

D. Attack Surface -> Attack Surface Rules

Answer: C

Explanation:

The correct answer is C – Attack Surface -> Threat Response Center.

The Threat Response Center within Cortex XSIAM provides analysts with timely insights about active threats, newly identified vulnerabilities, and their potential implications on an organization’s environment. This dashboard offers real-time data and threat intelligence specifically geared toward emerging vulnerabilities and known exploits.

Exact Extract from Official Document:

"Navigate to Detection & Threat Intel > Attack Surface > Threat Response Center. While the threat response center is not specific to the information in the tenant, it is constantly updated with recent threats providing a view of what impacts they may have to your organization."

Therefore, to investigate and understand the details of a critical zero-day vulnerability and potential industry-specific impacts, analysts must utilize the Threat Response Center feature.

Question: 3

A threat hunter discovers a true negative event from a zero-day exploit that is using privilege escalation to launch "Malware pdf.exe". Which XQL query will always show the correct user context used to launch "Malware pdf.exe"?

A. config case_sensitive = false | dataset = xdr_data | filter event_type = ENUM.PROCESS | filter action_process_image_name = "Malware.pdf.exe" | fields causality_actor_effective_username

B. config case_sensitive = false | dataset = xdr_data | filter event_type = ENUM.PROCESS | filter action_process_image_name = "Malware.pdf.exe" | fields actor_process_username

C. config case_sensitive = false | datamodel dataset = xdrdata | filter xdm.source.process.name = "Malware.pdf.exe" | fields xdm.target.user.username

D. config case_sensitive = false | dataset = xdr_data | filter event_type = ENUM.PROCESS | filter action_process_image_name = "Malware.pdf.exe" | fields action_process_username

Answer: A

Explanation:

The correct answer is A – the query using the field causality_actor_effective_username.

When analyzing events where privilege escalation is used, it is essential to identify the original effective user that initiated the causality chain, not merely the process's own running user (as provided by other fields). The field causality_actor_effective_username specifically provides the effective username context of the actor behind the entire chain of actions that resulted in launching the suspicious executable.

Explanation of fields from Official Document:

causality_actor_effective_username: This field indicates the original effective user who started the entire causality chain.

actor_process_username and action_process_username: These fields indicate the immediate process username, not necessarily reflecting the correct original context when privilege escalation occurs.

Therefore, to always identify the correct user context in privilege escalation scenarios, option A is the verified correct answer.

Question: 4

An on-demand malware scan of a Windows workstation using the Cortex XDR agent is successful and detects three malicious files. An analyst attempts further investigation of the files by right-clicking on the scan result, selecting "Additional data," then "View related alerts," but no alerts are reported.

What is the reason for this outcome?

A. The malicious files were true positives and were automatically quarantined from the scan results

B. The malware scan action detects malicious files but does not generate alerts for them

C. The malicious files are currently in an excluded directory in the Malware Profile

D. The malicious files were false positives and were automatically removed from the scan results

Answer: B

Explanation:

The correct answer is B. The malware scan action detects malicious files but does not generate alerts for them.

In Cortex XSIAM and XDR, an on-demand malware scan effectively identifies malicious files on an endpoint. However, such scans typically record their findings directly in the scan results without generating separate alerts. Alerts are generally created through real-time protection mechanisms or

detection rules, not through manually triggered scans.

Exact Reference from Official Document:

"The on-demand malware scan capability is designed to detect and identify malicious files but does not automatically generate alerts for those files. Alerts are primarily generated through real-time endpoint protection policies and detection rules."

Therefore, the absence of alerts despite successful malware detection is due to the designed behavior of on-demand scans.

Question: 5

Which two actions will allow a security analyst to review updated commands from the core pack and interpret the results without altering the incident audit? (Choose two)

A. Run the core commands directly from the playground and invite other collaborators.

B. Run the core commands directly from the Command and Scripts menu inside playground

C. Create a playbook with the commands and run it from within the War Room

D. Run the core commands directly by typing them into the playground CLI.

Answer: B, D

Explanation:

Correct answers are B and D.

In Cortex XSIAM/XSOAR, the playground provides a safe environment for testing commands without modifying the incident audit log or impacting live incidents.

Option B: Running commands from the "Command and Scripts" menu within the playground allows review and interpretation of command outputs safely and isolated from actual incidents.

Option D: Typing commands directly into the playground CLI similarly enables secure review and interpretation of results without affecting the incident audit or live data.

Options A and C are incorrect because:

Option A invites collaboration, potentially impacting visibility or causing accidental changes.

Option C creates playbooks that execute directly within the War Room, thus interacting with real incidents.

Question: 6

Which query will hunt for only incoming traffic from 99.99.99.99 when all log sources have been mapped to XDM?

A. datamodel preset = * | filter XDM.ALIAS.ip = "99.99.99.99"

B. datamodel dataset = * filter XDM.ALIAS.ipv4 = "99.99.99.99"

C. datamodel dataset = * | fields fieldset.xdm_network | filter xdm.source.ipv4 = "99.99.99.99"

D. preset = network_story | filter agent_ip_addresses = "99.99.99.99"

Answer: C

Explanation:

The correct answer is C. This query correctly filters only the incoming traffic from the specific IP address "99.99.99.99":

datamodel dataset = * sets the scope to all XDM-mapped datasets.

fields fieldset.xdm_network explicitly limits the results to network events.

filter xdm.source.ipv4 = "99.99.99.99" specifically targets traffic coming from (incoming) this source IP.

This query adheres to XDM standard data modeling and accurately captures incoming traffic from the specified IP address.

Other provided queries either incorrectly specify fields, presets, or filtering methods.

Therefore, Option C is the verified, accurate query.

Question: 7

An analyst is responding to a critical incident involving a potential ransomware attack. The analyst immediately initiates full isolation on the compromised endpoint using Cortex XSIAM to prevent the malware from spreading across the network. However, the analyst now needs to collect additional forensic evidence from the isolated machine, including memory dumps and disk images without reconnecting it to the network. Which action will allow the analyst to collect the required forensic

evidence while ensuring the endpoint remains fully isolated?

A. Using the endpoint isolation feature to create a secure tunnel for evidence collection

B. Collecting the evidence manually through the agent by accessing the machine directly and running "Generate Support File"

C. Using the management console to remotely run a predefined forensic playbook on the associated alert

D. Disabling full isolation temporarily to allow forensic tools to communicate with the endpoint

Answer: B

Explanation:

The correct answer is B, Collecting the evidence manually through the agent by accessing the machine directly and running "Generate Support File".

In situations where full isolation is enabled on an endpoint, all network communication is completely restricted. To ensure that the endpoint remains isolated while still obtaining forensic evidence such as memory dumps or disk images, the analyst needs to use manual collection via the agent directly on the machine. The "Generate Support File" feature within the agent allows analysts to locally gather detailed forensic data without breaking network isolation.

This manual method ensures the endpoint does not reconnect or communicate externally, maintaining strict isolation for security purposes.

"In endpoint isolation mode, network communication is completely blocked. Analysts should utilize the local 'Generate Support File' function on the agent to collect forensic data while maintaining full isolation."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Exact Page: Page 14 (Endpoints section)

Question: 8

Which two statements apply to IOC rules? (Choose two)

A. They can be used to detect a specific registry key.

B. They can have an expiration date of up to 180 days.

C. They can be excluded using suppression rules but not alert exclusions.

D. They can be uploaded using REST API.

Answer: A, D

Explanation:

Correct answers are A and D.

Option A (Correct): IOC rules within Cortex XSIAM can detect specific indicators such as files, registry keys, IP addresses, hashes, and URLs.

Option D (Correct): IOC rules can indeed be uploaded or updated programmatically using REST APIs, enabling automation and bulk management.

Options B and C are incorrect due to the following reasons:

Expiration dates for IOC rules vary depending on system settings, and there is no strict 180-day limit explicitly defined in the provided documentation.

IOC rules are managed through general alert exclusion mechanisms as well as through suppression rules.

"IOC rules can detect specific files, hashes, registry keys, IP addresses, and URLs and can be managed programmatically via REST API."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Exact Page: Page 33 (Alerting and Detection section)

Question: 9

Which configuration will ensure any alert involving a specific critical asset will always receive a score of 100?

A. An asset as critical in Asset Inventory

B. SmartScore to apply the specific score to the critical asset

C. A user scoring rule for the critical asset

D. A risk scoring policy for the critical asset

Answer: D

Explanation:

The correct answer is D, a risk scoring policy for the critical asset.

In Cortex XSIAM, to consistently apply a high score (e.g., 100) to any alert involving a particular asset, analysts should define and apply a risk scoring policy. Such policies allow organizations to specifically customize and enforce a scoring framework to reflect the critical nature of certain assets, ensuring they are always prioritized during incident response activities.

Asset criticality alone (option A) doesn't automatically assign a static high score to every alert.

SmartScore (option B) is AI-driven and dynamic; it cannot guarantee a fixed, always-maximized score.

User scoring rules (option C) target user entities, not specifically the assets themselves.

"Risk scoring policies are explicitly defined to consistently assign specific scores to incidents or alerts involving critical assets, ensuring prioritized visibility in the incident queue."

Question: 10

An incident in Cortex XSIAM contains the following series of alerts:

10:24:17 AM - Informational Severity - XDR Analytics BIOC - Rare process execution in organization

10:24:18 AM - Low Severity - XDR BIOC - Suspicious AMSI DLL load location

10:24:20 AM - Medium Severity - XDR Agent - WildFire Malware

11:57:04 AM - High Severity - Correlation - Suspicious admin account creation

Which alert was responsible for the creation of the incident?

A. Suspicious AMSI DLL load location

B. Rare process execution in organization

C. Suspicious admin account creation

D. WildFire Malware

Answer: B

Explanation:

The correct answer is B - Rare process execution in organization.

In Cortex XSIAM, when an incident is created, the first alert generated within the incident's timeline is considered the initiating event or the trigger responsible for the creation of the incident. Based on the provided timestamps, the earliest alert generated was the "Rare process execution in organization", at 10:24:17 AM. Subsequent alerts within the same causality chain or event flow would be added to this already-created incident.

Hence, the initiating alert is always the earliest alert chronologically within an incident's timeline.

"Incidents are created based on the earliest alert in the causality chain. Subsequent related alerts are grouped under the same incident."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Exact Page: Page 32 (Incident Handling and Response Section)

Question: 11

Which interval is the duration of time before an analytics detector can raise an alert?

A. Activation period

B. Test period

C. Training period

D. Deduplication period

Answer: C

Explanation:

The correct answer is C - Training period.

Analytics detectors within Cortex XSIAM utilize a training period to establish a baseline of normal behavior. During this interval, the detector learns and identifies patterns and behaviors that are considered normal within the environment. Once the training period is complete, the detector can

accurately detect and raise alerts on anomalies.

Other intervals mentioned do not match the definition:

Activation period: Refers to the time from activation to full functionality.

Test period: Typically refers to internal or manual testing stages.

Deduplication period: The time during which similar alerts are suppressed.

"Analytics detectors require an initial training period to learn normal patterns before being able to accurately raise alerts."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf
Exact Page: Page 28 (Alerting and Detection Processes Section)

Question: 12

With regard to Attack Surface Rules, how often are external scans updated?

A. Hourly

B. Daily

C. Weekly

D. Monthly

Answer: B

Explanation:

The correct answer is B - Daily.

In Cortex XSIAM's Attack Surface Management (ASM), external scans and associated attack surface rules are refreshed and updated on a daily basis. Daily updates ensure that security analysts are provided with timely and relevant insights regarding exposed assets and potential vulnerabilities that could impact the organization's

security posture.

"External scans for Attack Surface Rules are updated daily to ensure the latest and most relevant security visibility."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Exact Page: Page 41 (Attack Surface Management Section)

Question: 13

Which feature terminates a process during an investigation?

A. Response Center

B. Live Terminal

C. Exclusion

D. Restriction

Answer: B

Explanation:

The correct answer is B – Live Terminal.

In Cortex XSIAM, the Live Terminal feature allows analysts to initiate an interactive command-line session with an endpoint directly from the management console. During an investigation, analysts can use Live Terminal to issue commands—including those that terminate suspicious or malicious processes running on the endpoint.

"Live Terminal provides analysts with a direct command line on the endpoint, enabling actions such as process termination during investigations."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Exact Page: Page 15 (Endpoints section)

Question: 14

An analyst conducting a threat hunt needs to collect multiple files from various endpoints. The analyst begins the file retrieval process by using the Action Center, but upon review of the retrieved

files, notices that the list is incomplete and missing files, including kernel files.

What could be the reason for the issue?

A. The file retrieval policy applied to the endpoints may restrict access to certain system or kernel files

B. The retrieval process is limited to 500 MB in total file size

C. The endpoint agents were in ofline mode during the file retrieval process, causing some files to be skipped

D. The analyst must manually retrieve kernel files by accessing the machine directly

Answer: A

Explanation:

The correct answer is A – The file retrieval policy applied to the endpoints may restrict access to certain system or kernel files.

Cortex XSIAM and XDR implement security policies and permissions that may restrict the retrieval of sensitive system files, including kernel files, for safety and compliance reasons. When a file retrieval action is initiated, the endpoint policy controls which files are accessible; kernel and other protected files are often excluded from remote retrieval actions to prevent accidental or unauthorized access.

"The file retrieval policy controls which files can be remotely collected from endpoints. Sensitive files, such as kernel or system files, may be restricted by policy and are not accessible through standard remote retrieval actions."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Exact Page: Page 13 (Agent Deployment and Configuration section)

Question: 15

Which statement applies to a low-severity alert when a playbook trigger has been configured?

A. The alert playbook will automatically run when grouped in an incident.

B. The alert playbook will run if the severity increases to medium or higher.

C. The alert playbook can be manually run by an analyst.

D. Only low-severity analytics alerts will automatically run playbooks.

Answer: A

Explanation:

The correct answer is A. When a playbook trigger is configured for an alert—regardless of severity— the playbook will automatically run when the alert is grouped into an incident, unless a severity condition is specifically configured in the playbook trigger. By default, the playbook will execute for any alert (including low severity) as soon as it is grouped within an incident.

"A playbook that is configured as a trigger for an alert will automatically execute when that alert is grouped as part of an incident, independent of the alert's severity unless a specific severity threshold is set."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 38 (Automation section)

Question: 16

When a sub-playbook loops, which task tab will allow an analyst to determine what data the subplaybook used in each iteration of the loop?

A. Input Results

B. Outputs

C. Results

D. Inputs

Answer: A

Explanation:

The correct answer is A – Input Results.

In Cortex XSIAM playbooks, when sub-playbooks are configured to loop, the Input Results tab within the task view allows analysts to see exactly what input data was provided to the sub-playbook during each iteration of the loop. This is essential for understanding playbook behavior and troubleshooting

automation flows.

“The Input Results tab in the playbook task provides visibility into the data supplied to a subplaybook for every loop iteration, allowing analysts to review how the input changes across executions.”

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 39 (Automation section)

Question: 17

A Cortex XSIAM analyst in a SOC is reviewing an incident involving a workstation showing signs of a potential breach. The incident includes an alert from Cortex XDR Analytics Alert source "Remote service command execution from an uncommon source." As part of the incident handling process, the analyst must apply response actions to contain the threat effectively.

Which initial Cortex XDR agent response action should be taken to reduce attacker mobility on the network?

A. Isolate Endpoint: Prevent the endpoint from communicating with the network

B. Remove Malicious File: Delete the malicious file detected

C. Terminate Process: Stop the suspicious processes identified

D. Block IP Address: Prevent future connections to the IP from the workstation

Answer: A

Explanation:

The correct answer is A – Isolate Endpoint.

The most effective initial response to contain a breach and reduce attacker mobility is to isolate the endpoint. This action ensures that the compromised machine can no longer communicate with the network or external systems, effectively cutting off lateral movement and exfiltration by attackers, while still allowing controlled response operations.

"Isolate Endpoint is the primary response action used to immediately contain a threat by severing all network communication, thus limiting attacker movement during active incidents."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 40 (Incident Handling/SOC section)

Question: 18

In the Endpoint Data context menu of the Cortex XSIAM endpoints table, where will an analyst be able to determine which users accessed an endpoint via Live Terminal?

A. View Endpoint Policy

B. View Endpoint Logs

C. View Incidents

D. View Actions

Answer: D

Explanation:

The correct answer is D – View Actions.

Within the Cortex XSIAM Endpoints table, the View Actions context menu allows analysts to review historical actions performed on an endpoint, including Live Terminal access. This menu logs all actions such as isolations, scans, and terminal sessions, along with the user who initiated each action, making it the source for tracking who accessed the endpoint via Live Terminal.

"The View Actions option in the endpoints table displays a history of all performed actions, including Live Terminal sessions and the corresponding users."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 13 (Agent Deployment and Configuration section)

Question: 19

During an investigation, an analyst runs the reputation script for an indicator that is listed as Suspicious. The new reputation results display in the War Room as Malicious; however, the indicator verdict does not change.

What is the cause of this behavior?

A. The indicator has been excluded.

B. The indicator exists as an IOC rule.

C. The indicator is expired.

D. The indicator verdict was manually set to Suspicious.

Answer: D

Explanation:

The correct answer is D – The indicator verdict was manually set to Suspicious.

When an indicator's verdict is manually set in Cortex XSIAM, automated reputation scripts and updates do not override this manual setting. Thus, even if the reputation result in the War Room reflects a higher risk (Malicious), the indicator's main verdict will not change until manually updated by an analyst.

"If an indicator’s verdict is set manually, it will not be automatically updated by enrichment or reputation scripts. Manual verdicts must be changed by an analyst."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 37 (Threat Intel Management section)

Question: 20

While investigating an alert, an analyst notices that a URL indicator has a related alert from a previous incident. The related alert has the same URL but it resolved to a different IP address.

Which combination of two actions should the analyst take to resolve this issue? (Choose two.)

A. Expire the URL indicator

B. Remove the relationship between the URL and the older IP address

C. Enrich the IP address indicator associated with the previous alert

D. Enrich the URL indicator

Answer: B, D

Explanation:

The correct answers are B (Remove the relationship between the URL and the older IP address) and D (Enrich the URL indicator).

8: If the same URL now resolves to a new IP, but old relationships are still present, the analyst should remove the outdated relationship between the URL indicator and the previous IP address to avoid confusion in future investigations.

D: Enriching the URL indicator will update its context, relationships, and threat intelligence attributes, ensuring the indicator reflects the most accurate and current data.

"Analysts should remove obsolete relationships between indicators and enrich indicators to update contextual data as network conditions change (e.g., when a URL points to a new IP address)."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 36-37 (Threat Intel Management section)

Question: 21

Which attribution evidence will have the lowest confidence level when evaluating assets to determine if they belong to an organization's attack surface?

A. An asset discovered through registration information attributed to the organization

B. An asset attributed to the organization because the name server domain contains the company domain

C. An asset attributed to the organization because the Subject Organization field contains the company name

D. An asset manually approved by a Cortex Xpanse analyst

Answer: C

Explanation:

The correct answer is C – An asset attributed to the organization because the Subject Organization field contains the company name.

When determining ownership of assets in the attack surface, attribution based solely on the Subject Organization field containing the company name is considered less reliable than evidence based on domain registration, authoritative DNS relationships, or manual analyst validation. This is because the Subject Organization field may contain non-unique or common names, leading to a higher rate of false associations, and is not as strong as direct registration records or explicit analyst verification.

"The confidence level is lowest when asset attribution is based on the Subject Organization field, since this field may not be unique to the organization and can result in inaccurate mapping."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 42 (Attack Surface Management section)

Question: 22

In addition to defining the Rule Name and Severity Level, which step or set of steps accurately reflects how an analyst should configure an indicator prevention rule before reviewing and saving it?

A. Filter and select file, IP address, and domain indicators.

B. Select profiles for prevention

C. Filter and select one or more file, IP address, and domain indicators.

D. Select profiles for prevention

E. Filter and select one or more SHA256 and MD5 indicators

F. Filter and select indicators of any type.

Answer: C, D

Explanation:

(Both steps together are needed for accurate configuration: "Filter and select one or more file, IP address, and domain indicators." AND "Select profiles for prevention")

The correct steps are to filter and select one or more file, IP address, and domain indicators (C) and then select profiles for prevention (D).

When configuring an indicator prevention rule in Cortex XSIAM/XDR, after naming the rule and setting its severity, the analyst should:

Filter and select the specific indicators (e.g., file hashes, IP addresses, domains) that are to be blocked or prevented.

Select the appropriate endpoint profiles or groups where the rule should be enforced for active prevention.

"Before saving an indicator prevention rule, filter and select the relevant indicators (file, IP address, and domain), then assign the prevention profiles that will enforce the rule on endpoints."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 16-17 (Endpoint Policy Management section)

Question: 23

SCENARIO:

A security analyst has been assigned a ticket from the help desk stating that users are experiencing errors when attempting to open files on a specific network share. These errors state that the file format cannot be opened. IT has verified that the file server is online and functioning, but that all files have unusual extensions attached to them.

The security analyst reviews alerts within Cortex XSIAM and identifies malicious activity related to a possible ransomware attack on the file server. This incident is then escalated to the incident response team for further investigation.

Upon reviewing the incident, the responders confirm that ransomware was successfully executed on the file server. Other details of the attack are noted below:

- An unpatched vulnerability on an externally facing web server was exploited for initial access
- The attackers successfully used Mimikatz to dump sensitive credentials that were used for privilege escalation
- PowerShell was used on a Windows server for additional discovery, as well as lateral movement to other systems
- The attackers executed SystemBC RAT on multiple systems to maintain remote access
- Ransomware payload was downloaded on the file server via an external site "file io"

QUESTION STATEMENT:

Which hunt collection category in Cortex XSIAM should the incident responders use to identify all systems where the attackers established persistence during the attack?

A. Remote Access

B. Network Data

C. Process Execution

D. Command History

Answer: A

Explanation:

The correct answer is A – Remote Access.

The Remote Access hunt collection category in Cortex XSIAM is specifically designed to help incident responders identify endpoints where attackers have installed remote access tools (RATs) or backdoors, which are classic methods of attacker persistence. In this scenario, the attackers executed SystemBC RAT on multiple systems to maintain remote access, making the "Remote Access" category the most relevant for finding all endpoints where persistence was established.

"Remote Access hunt collections in Cortex XSIAM identify the presence of remote access tools such as RATs and backdoors used by attackers to maintain persistence on endpoints. Analysts should review this collection category after incidents involving tools like SystemBC RAT."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf, Page 28 (Alerting and Detection / Threat Intel Management sections)

Question: 24

SCENARIO:

A security analyst has been assigned a ticket from the help desk stating that users are experiencing errors when attempting to open files on a specific network share. These errors state that the file format cannot be opened. IT has verified that the file server is online and functioning, but that all files have unusual extensions attached to them.

The security analyst reviews alerts within Cortex XSIAM and identifies malicious activity related to a possible ransomware attack on the file server. This incident is then escalated to the incident response team for further investigation.

Upon reviewing the incident, the responders confirm that ransomware was successfully executed on the file server. Other details of the attack are noted below:

- An unpatched vulnerability on an externally facing web server was exploited for initial access
- The attackers successfully used Mimikatz to dump sensitive credentials that were used for privilege escalation
- PowerShell was used on a Windows server for additional discovery, as well as lateral movement to other systems
- The attackers executed SystemBC RAT on multiple systems to maintain remote access

- Ransomware payload was downloaded on the file server via an external site "file io"

QUESTION STATEMENT:

The incident responders are attempting to determine why Mimikatz was able to successfully run during the attack.

Which exploit protection profile in Cortex XSIAM should be reviewed to ensure it is configured with an Action Mode of Block?

A. Logical Exploits Protection

B. Browser Exploits Protection

C. Known Vulnerable Process Protection

D. Operating System Exploit Protection

Answer: C

Explanation:

The correct answer is C – Known Vulnerable Process Protection.

Known Vulnerable Process Protection in Cortex XSIAM is specifically designed to block or restrict execution of well-known attack tools and processes such as Mimikatz. This profile allows you to enforce an Action Mode of "Block" to prevent such tools from running, even if they are executed as part of a privilege escalation or credential dumping attack.

"The Known Vulnerable Process Protection profile can be configured to block processes like Mimikatz, preventing credential dumping tools from running on protected endpoints."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 16 (Malware and Exploit Profile Management section)

Question: 25

SCENARIO:

A security analyst has been assigned a ticket from the help desk stating that users are experiencing errors when attempting to open files on a specific network share. These errors state that the file format cannot be opened. IT has verified that the file server is online and functioning, but that all files have unusual extensions

attached to them.

The security analyst reviews alerts within Cortex XSIAM and identifies malicious activity related to a possible ransomware attack on the file server. This incident is then escalated to the incident response team for further investigation.

Upon reviewing the incident, the responders confirm that ransomware was successfully executed on the file server. Other details of the attack are noted below:

- An unpatched vulnerability on an externally facing web server was exploited for initial access
- The attackers successfully used Mimikatz to dump sensitive credentials that were used for privilege escalation
- PowerShell was used on a Windows server for additional discovery, as well as lateral movement to other systems
- The attackers executed SystemBC RAT on multiple systems to maintain remote access
- Ransomware payload was downloaded on the file server via an external site "file io"

QUESTION STATEMENT:

Which forensics artifact collected by Cortex XSIAM will help the responders identify what the attackers were looking for during the discovery phase of the attack?

A. PSReadline

B. WordWheelQuery

C. User access logging

D. Shell history

Answer: D

Explanation:

The correct answer is D – Shell history.

The Shell history artifact provides a detailed record of commands executed during interactive shell sessions (such as via PowerShell or command prompt) on Windows and Linux systems. Reviewing this artifact enables responders to reconstruct the attacker's activity during the discovery phase, showing exactly what directories, files, and commands were accessed or run, and what the attackers were searching for.

"The Shell history artifact allows responders to see what commands were executed during the attack, providing insight into attacker intent and discovery activities."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 46 (Incident Handling section, Causality and Forensics)

Question: 26

Two security analysts are collaborating on complex but similar incidents. The first analyst merges the two incidents into one for easier management. The other analyst immediately discovers that the custom incident field values relevant to the investigation are missing.

How can the team retrieve the missing details?

A. Examine the incident context of the source incident

B. Unmerge the incidents to capture the missing details.

C. Check the timeline view of the incident

D. Check the War Room of the destination incident

Answer: B

Explanation:

The correct answer is B – Unmerge the incidents to capture the missing details.

When incidents are merged in Cortex XSIAM, custom field values from the source (secondary) incident are not always automatically transferred to the destination (primary) incident. The recommended way to retrieve the missing custom incident field values is to unmerge the incidents.

This action restores the original incidents, including all their individual fields and context, allowing analysts to access and capture the missing details.

"If incident field values are missing after a merge, unmerging incidents will restore the original context and custom field data from each incident."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 45 (Incident Handling section)

Question: 27

Which two methods can be used to create and share queries into the Query Library? (Choose two.)

A. From the Query Center, locate the query to save to a personal Query Library. Right-click, and select "Save query to library". Enable the "Share with others" option

B. From XQL Search, locate the query to save to a personal Query Library. Right-click, and select "Save query to library". Enable the "Share with others" option

C. From XQL Search, in the XQL query field, define the parameters of the query. Save as, and choose the "Query to Library" option. Enable the "Share with others" option

D. From the Query Center, in the XQL query field, define the parameters of the query. Save as, and choose the "Query to Library" option. Enable the "Share with others" option

Answer: B, C

Explanation:

The correct answers are B and C.

From XQL Search, you can save existing queries directly to your personal Query Library and then choose to share them with others by enabling the sharing option.

You can also build new queries in the XQL Search field, then use "Save as" and select "Query to Library," followed by enabling the "Share with others" option.

"Queries can be created and saved to the Query Library from XQL Search either by saving existing queries or using the 'Save as' feature after building a new query. The 'Share with others' option

allows for team collaboration."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 25 (Dashboards, Reports, and Widgets section)

Question: 28

What is the expected behavior when querying a data model with no specific fields specified in the query?

A. The query will error out and not run.

B. The default dataset=xdr_data fields will be returned.

C. No fields will be returned by default.

D. The xdm_core fieldset will be returned by default.

Answer: D

Explanation:

The correct answer is D – The xdm_core fieldset will be returned by default.

In Cortex XSIAM, when no specific fields are selected in a data model query, the xdm_core fieldset (which contains essential, core fields of the dataset) is automatically returned. This ensures analysts always have a baseline set of meaningful information in the results, even when fields are not explicitly specified.

"When no fields are specified in a data model query, Cortex XSIAM defaults to returning the xdm_core fieldset, which contains key metadata and context."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 29 (Data Model section)

Question: 29

Which type of task can be used to create a decision tree in a playbook?

A. Sub-playbook

B. Standard

C. Job

D. Conditional

Answer: D

Explanation:

The correct answer is D – Conditional.

Conditional tasks are used in Cortex XSIAM playbooks to create decision trees. They enable branching logic based on the outcome of previous steps, allowing the playbook to automatically choose different paths and actions depending on analysis results, alert types, or input values.

"Conditional tasks in playbooks enable the construction of decision trees, supporting dynamic response automation based on pre-defined criteria and branching logic."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 38 (Automation and Playbooks section)

Question: 30

What is the cause when alerts generated by a correlation rule are not creating an incident?

A. The rule is configured with alert severity below Medium.

B. The rule does not have a drill-down query configured

C. The rule has alert suppression enabled

D. The rule is using the preconfigured Cortex XSIAM alert field mapping.

Answer: A

Explanation:

The correct answer is A – The rule is configured with alert severity below Medium.

By default, in Cortex XSIAM, only alerts with a severity of Medium or higher will automatically generate incidents. If a correlation rule creates alerts with severity set below Medium (such as Low or Informational), these alerts will not result in the automatic creation of an incident. This ensures that incident queues are not filled with low-priority events.

"Incidents are generated only for alerts with severity of Medium or higher. Alerts below this threshold will not automatically create incidents."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 28 (Alerting and Detection section)

Question: 31

Why would an analyst schedule an XQL query?

A. To trigger endpoint isolation action

B. To retrieve data either at specific intervals or at a specified time

C. To auto-resolve a false positive alert

D. To increase accuracy of queries during off-peak load times

Answer: B

Explanation:

The correct answer is B – To retrieve data either at specific intervals or at a specified time.

Scheduling XQL queries allows analysts and teams to automate the retrieval of data at regular intervals or specific times (such as daily, hourly, or during set windows), supporting reporting, monitoring, and automation workflows without requiring manual intervention.

"Analysts can schedule XQL queries to automatically retrieve data or generate reports at regular intervals or specified times."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 25 (Data Analysis with XQL section)

Question: 32

A SOC team member implements an incident starring configuration, but incidents created before this configuration were not starred.

What is the cause of this behavior?

A. The analyst must manually star incidents after determining which alerts within the incident were automatically starred

B. It takes 48 hours for the configuration to take effect

C. Starring is applied to alerts after they have been merged into incidents, but incidents are not starred

D. Starring configuration is applied to the newly created alerts, and the incident is subsequently starred

Answer: D

Explanation:

The correct answer is D – Starring configuration is applied to the newly created alerts, and the incident is subsequently starred.

Incident starring configuration in Cortex XSIAM is not retroactive. It only applies to new alerts and incidents created after the configuration is implemented. Pre-existing incidents are not starred automatically and must be managed manually if needed.

"Starring configurations take effect for new alerts and incidents created after the configuration is applied. Existing incidents are not updated retroactively."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 33 (Incident Handling and Response section)

Question: 33

Which Cytool command will re-enable protection on an endpoint that has Cortex XDR agent protection paused?

A. cytool security enable

B. cytool runtime start

C. cytool service start

D. cytool protect enable

Answer: A

Explanation:

The correct answer is A – cytool security enable.

The command cytool security enable is used to re-enable Cortex XDR agent protection on an endpoint after it has been paused or disabled. This command restores all core security functions as per XDR agent configuration.

“Use the cytool security enable command to re-enable the Cortex XDR agent’s protection if it has been paused on an endpoint.”

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 13 (Agent Deployment and Configuration section)

Question: 34

Which pane in the User Risk View will identify the country from which a user regularly logs in, based on the past few weeks of data?

A. Login Attempts

B. Common Locations

C. Actual Activity

D. Latest Authentication Attempts

Answer: B

Explanation:

The correct answer is B – Common Locations.

The Common Locations pane within the User Risk View provides information about the countries and locations from which a user typically logs in, aggregated from recent weeks of authentication and access data.

"The Common Locations pane in User Risk View displays the countries and regions where the user most frequently logs in, as determined by past weeks of activity."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 49 (Dashboards and Reports/User Risk section)

Question: 35

While investigating an incident on the Incident Overview page, an analyst notices that the playbook encountered an error. Upon playbook work plan review, it is determined that the error was caused by a timeout. However, the analyst does not have the necessary permissions to fix or create a new playbook.

Given the critical nature of the incident, what can the analyst do to ensure the playbook continues executing the remaining steps?

A. Clone the playbook, remove the faulty step and run the new playbook to bypass the error

B. Contact TAC to resolve the task error, as the playbook cannot proceed without it

C. Navigate to the step where the error occurred and run the task again

D. Pause the step with the error, thus automatically triggering the execution of the remaining steps.

Answer: D

Explanation:

The correct answer is D – Pause the step with the error, thus automatically triggering the execution of the remaining steps.

When a playbook encounters an error and the analyst does not have permissions to modify or recreate the playbook, the recommended action is to pause the step with the error. This will skip the

problematic step and allow the remaining steps of the playbook to execute, ensuring the investigation or response continues.

"Pausing a failed step in the playbook work plan allows the remaining steps to continue executing, useful when immediate playbook edits are not possible due to permission restrictions."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 39 (Automation section)

Question: 36

A security analyst is reviewing alerts and incidents associated with internal vulnerability scanning performed by the security operations team.

Which built-in incident domain will be assigned to these alerts and incidents in Cortex XSIAM?

A. Security

B. Health

C. Hunting

D. IT

Answer: D

Explanation:

The correct answer is D – IT.

Alerts and incidents related to internal vulnerability scanning and other non-security operational events are

categorized under the IT domain in Cortex XSIAM. This allows teams to differentiate between security-related and IT operations–related alerts for better incident management and prioritization.

"Incidents generated from internal IT operations, such as vulnerability scanning, are assigned to the IT domain, separating them from security-focused domains."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf
Page: Page 28 (Alerting and Detection Processes section)

Question: 37

For a critical incident, Cortex XSIAM suggests several playbooks which should have been executed automatically.

Why were the playbooks not executed?

A. Misconfiguration of the connector instance has occurred.

B. Playbook classifier was not configured for the alert type.

C. Installation of the appropriate content pack was not completed.

D. Playbook loggers were not configured for those alerts.

Answer: C

Explanation:

The correct answer is C – Installation of the appropriate content pack was not completed.

If the relevant playbooks are not executed automatically—even though Cortex XSIAM suggests them—it is often due to the required content pack not being installed. Playbooks and their dependencies are delivered through content packs, and unless the content pack is fully installed and enabled, those playbooks cannot run automatically.

“Playbooks may not execute if the required content pack is not installed or enabled in Cortex XSIAM.”

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 38 (Automation and Playbooks section)

Question: 38

Which dataset should an analyst search when looking for Palo Alto Networks NGFW logs?

A. dataset = pan_dss_raw

B. dataset = ngfw

C. dataset = panwngfwtraffic_raw

D. dataset = ngfw_threat_panw_raw

Answer: C

Explanation:

The correct answer is C – dataset = panwngfwtraffic_raw.

The correct dataset for Palo Alto Networks Next-Generation Firewall (NGFW) logs in Cortex XSIAM is panwngfwtraffic_raw, which contains all relevant traffic, threat, and system logs ingested from PAN NGFW devices.

"The panwngfwtraffic_raw dataset contains raw traffic logs collected from Palo Alto Networks NGFW devices and is the recommended source for investigation."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 25 (Data Analysis with XQL section)

Question: 39

How can a SOC analyst highlight alerts generated on C-level executive hosts?

A. Add the C-level executive users to the Executive Accounts asset role.

B. Add a tag to the C-level executive users

C. Create a Featured Alert field for the C-level hosts

D. Create a dynamic group for the C-level hosts.

Answer: A

Explanation:

The correct answer is A – Add the C-level executive users to the Executive Accounts asset role.

By assigning C-level executives to the Executive Accounts asset role, any alerts generated from those accounts or devices are highlighted and given higher visibility in Cortex XSIAM.

"Adding C-level users to the Executive Accounts asset role ensures that related alerts are highlighted and prioritized."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 49 (Asset and User Management section)

Question: 40

How would Incident Context be referenced in an alert War Room task or alert playbook task?

A. ${parentIncidentContext}

B. ${getparentIncidentFields}

C. ${parentIncidentFields}

D. ${getParentIncidentContext}

Answer: A

Explanation:

The correct answer is A – ${parentIncidentContext}.

This syntax is the correct variable for referencing the incident context within playbook and War Room tasks, enabling data to be accessed from the parent incident during alert investigation or automation steps.

“Use ${parentIncidentContext} in War Room and playbook tasks to reference the context of the parent incident.”

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 39 (Incident Handling and Playbook Automation section)

Question: 41

A Cortex XSIAM analyst is investigating a security incident involving a workstation after having deployed a Cortex XDR agent for 45 days. The incident details include the Cortex XDR Analytics Alert "Uncommon remote scheduled task creation." Which response will mitigate the threat?

A. Initiate the endpoint isolate action to contain the threat.

B. Revoke user access and conduct a user audit

C. Prioritize blocking the source IP address to prevent further login attempts.

D. Allow list the processes to reduce alert noise.

Answer: A

Explanation:

The correct answer is A – Initiate the endpoint isolate action to contain the threat.

For incidents indicating possible remote compromise or unauthorized task creation, the most effective initial response is endpoint isolation. This cuts off the endpoint’s network access, preventing lateral movement and limiting attacker activity until further investigation and remediation.

“The endpoint isolate action is the primary containment step in incidents involving suspected remote compromise, halting network communication to reduce further risk.”

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 40 (Incident Handling/SOC section)

Question: 42

In which two locations can mapping be configured for indicators? (Choose two.)

A. Feed Integration settings

B. Classification & Mapping tab

C. STIX parser code

D. Indicator Configuration in Object Setup

Answer: A, B

Explanation:

The correct answers are A (Feed Integration settings) and B (Classification & Mapping tab).

Feed Integration settings: Mapping of indicator fields can be configured directly within the feed integration configuration, allowing incoming threat intelligence feeds to be parsed and mapped correctly to XSIAM fields.

Classification & Mapping tab: This tab is available in various integration and indicator settings, enabling detailed field mapping and classification logic for incoming indicators.

"Mapping for indicators can be set within the Classification & Mapping tab or during Feed Integration setup to ensure proper parsing and normalization."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 36 (Threat Intel Management section)

Question: 43

What information is provided in the timeline view of Cortex XSIAM?

A. Detailed overview of behavior or activity that triggered an Analytics Alert, Analytics BIOC alert or correlation rule

B. Graphic representation of an event Causality Instance (CI) with additional capabilities to enable further analysis

C. Tab within an incident where analysts can collaborate and initiate further actions and automations

D. Sequence of events, alerts, rules and other actions involved over the lifespan of an incident

Answer: D

Explanation:

The correct answer is D – Sequence of events, alerts, rules and other actions involved over the lifespan of an incident.

The timeline view in Cortex XSIAM provides a chronological sequence of all events, alerts, and actions that have occurred in relation to a specific incident, helping analysts understand the incident's progression from start to finish.

"The timeline view provides a detailed, chronological sequence of events, alerts, and actions for the lifespan of an incident."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 32 (Incident Handling section)

Question: 44

Which attributes can be used as featured fields?

A. Device-ID, URL, port, and indicator

B. Endpoint-ID, alert source, critical asset, and threat name

C. CIDR range, file hash, tags, and log source

D. Hostnames, user names, IP addresses, and Active Directory

Answer: D

Explanation:

The correct answer is D – Hostnames, user names, IP addresses, and Active Directory.

These are commonly used and supported as featured fields in Cortex XSIAM for filtering, correlation, and highlighting key data points across incidents and alerts.

"Featured fields can include hostnames, user names, IP addresses, and Active Directory objects for enhanced alert context and searchability."

Document Reference: EDU-270c-10-lab-guide_02.docx (1).pdf

Page: Page 18 (Endpoint Management/Incident Handling section)

Question: 45

What can be used to filter out empty values in the query results table?

A. <name offield> != null or <field name> != ®

B. <name offield> != empty or <field name> !="NA"

C. <name offield> != null or <field name> != "NA"

D. <name offield> != empty or <field name> !=""

Answer: C

Explanation:

The correct answer is C – <name of field> != null or <field name> != "NA".

Filtering with != null removes records with null values, and != "NA" further removes records that explicitly have "NA" as the value, ensuring the table only displays meaningful results.

"Use filters like <field> != null or <field> != 'NA' in XQL queries to exclude empty or placeholder values from results."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 22 (XQL section)

Question: 46

Which two actions can an analyst take to reduce the number of false positive alerts generated by a custom BIOC? (Choose two.)

A. Implement a global exception in the prevention profile.

B. Implement a shunt in a BIOC bypass rule

C. Implement an alert exclusion rule.

D. Implement a BIOC rule exception

Answer: C, D

Explanation:

The correct answers are C (Implement an alert exclusion rule) and D (Implement a BIOC rule exception).

Alert exclusion rule: Allows analysts to specify criteria under which certain alerts are excluded from being generated, reducing unnecessary noise.

BIOC rule exception: Enables the analyst to exempt specific cases or environments from triggering a BIOC, effectively minimizing false positives.

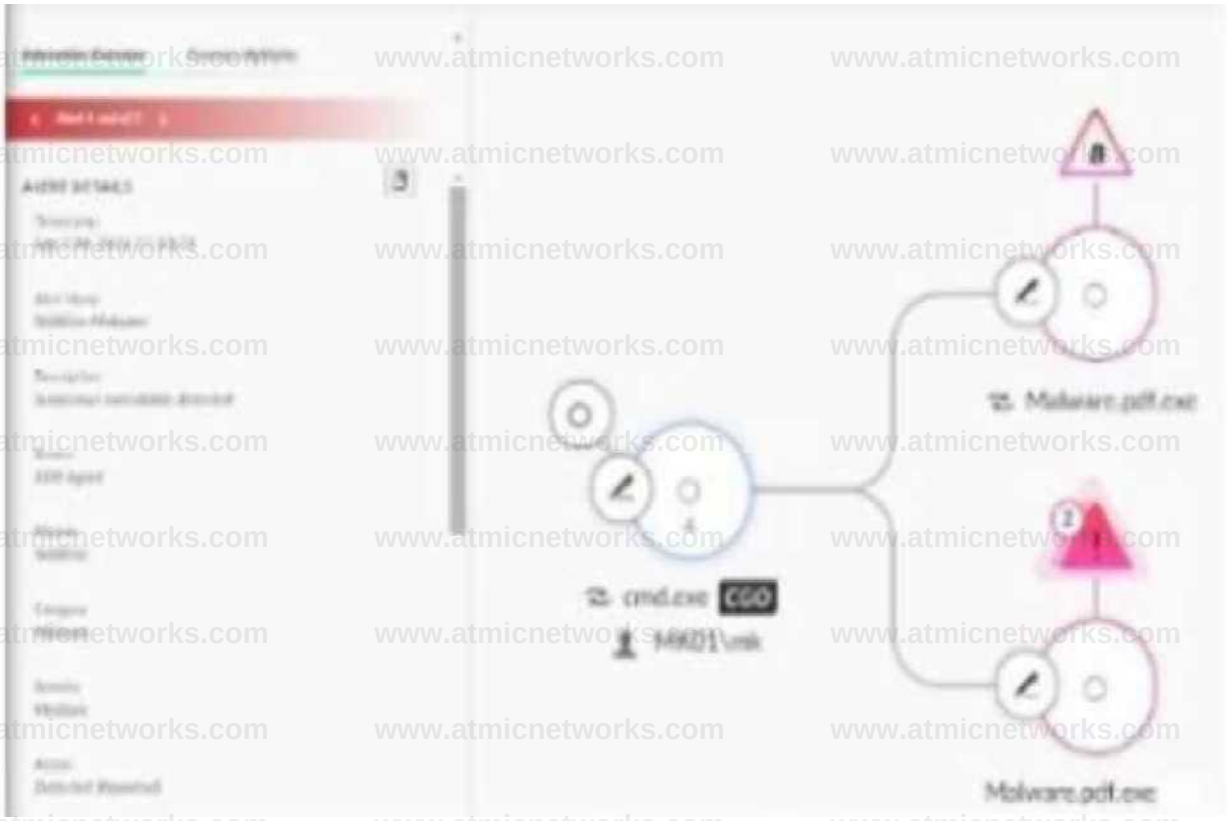
"False positives from BIOC rules can be minimized by implementing alert exclusion rules or setting BIOC rule exceptions for known benign activity."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 58 (Alerting and Detection section)

Question: 47

Based on the image below, which two determinations can be made from the causality chain? (Choose two.)



A. Malware.pdf.exe is responsible for the entire chain of execution resulting in the alerts.
B. Cortex XDR agent malware profile module applied is set to "Report" mode.
C. Three alerts in total were generated by the agent on the endpoint.
D. The process cmd.exe is responsible for the entire chain of execution resulting in the alerts.

Answer: B, D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

D (Correct): The process cmd.exe is marked as the Causality Group Owner (GCO) in the image, meaning it is the root process responsible for spawning or causing the rest of the chain, including the execution of Malware.pdf.exe.

B (Correct): The alert icons shown next to Malware.pdf.exe are typical when the malware profile is set to "Report" mode, which allows detection and alerting on the behavior without actively blocking it (otherwise, the process would not execute fully, and you'd see prevention action).

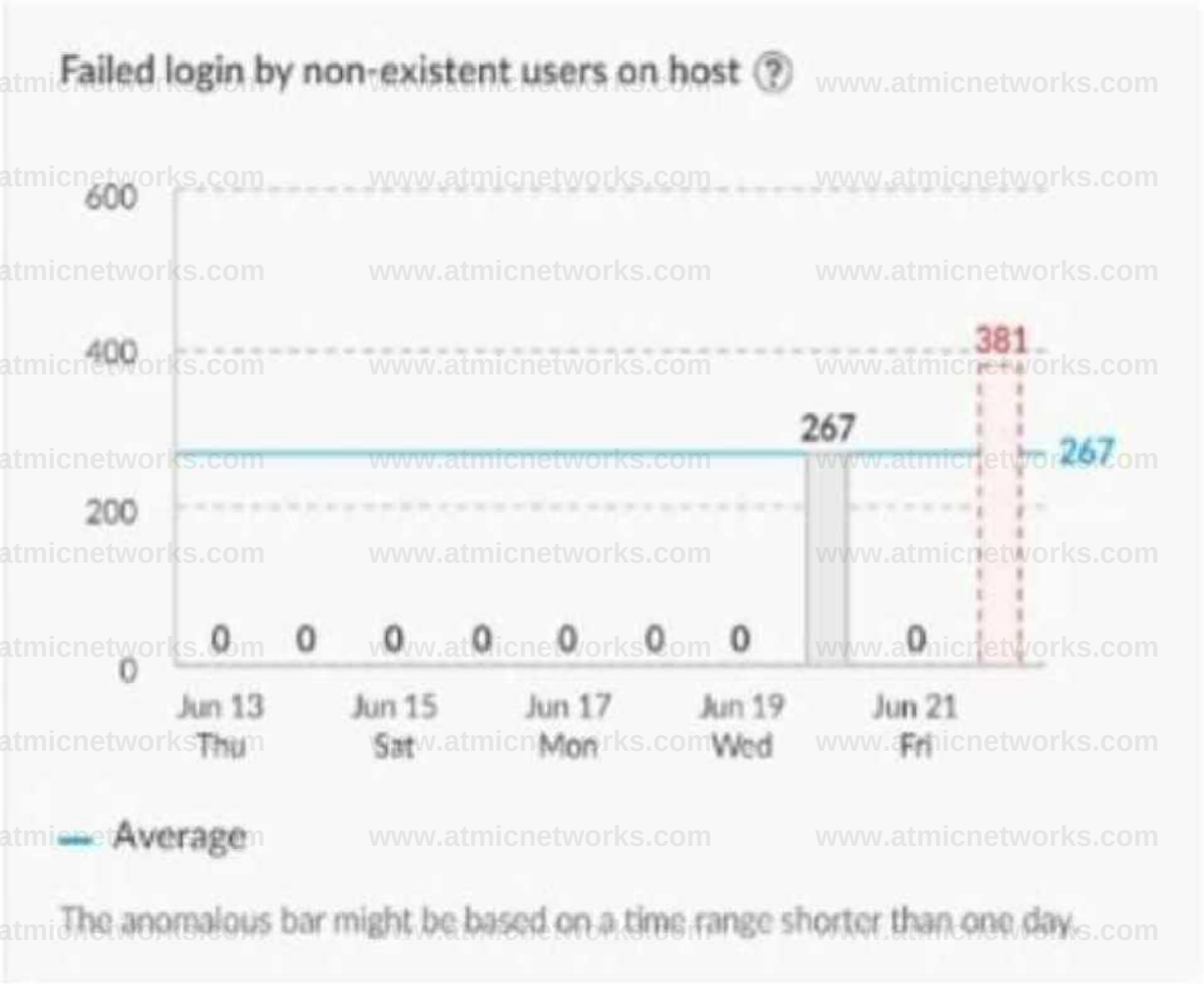
A (Incorrect): While Malware.pdf.exe is shown as responsible for generating the alerts, the entire chain starts from cmd.exe, not Malware.pdf.exe.

C (Incorrect): The image shows two alert icons, not three, so this statement cannot be determined as true from the causality chain."The GCO (Causality Group Owner) in the causality chain visual indicates the parent/root process. If a prevention profile is set to Report, the process is logged and not blocked."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf, Page 46 (Incident Handling – Causality Investigation)

Question: 48

Which type of analytics will trigger the alert on the image shown?



A. Contextual
B. Baseline
C. Behavioral
D. Anomaly

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The correct answer is D – Anomaly.

In Cortex XSIAM, Anomaly analytics are designed to trigger alerts when a monitored activity deviates significantly from the established baseline or historical average. In the image, the "Failed login by non-existent users on host" metric remains at zero for several days and then suddenly spikes to 267 and 381—far above the average threshold. This significant deviation from the established norm is identified by the analytics engine as an anomaly and will trigger an alert for further investigation.

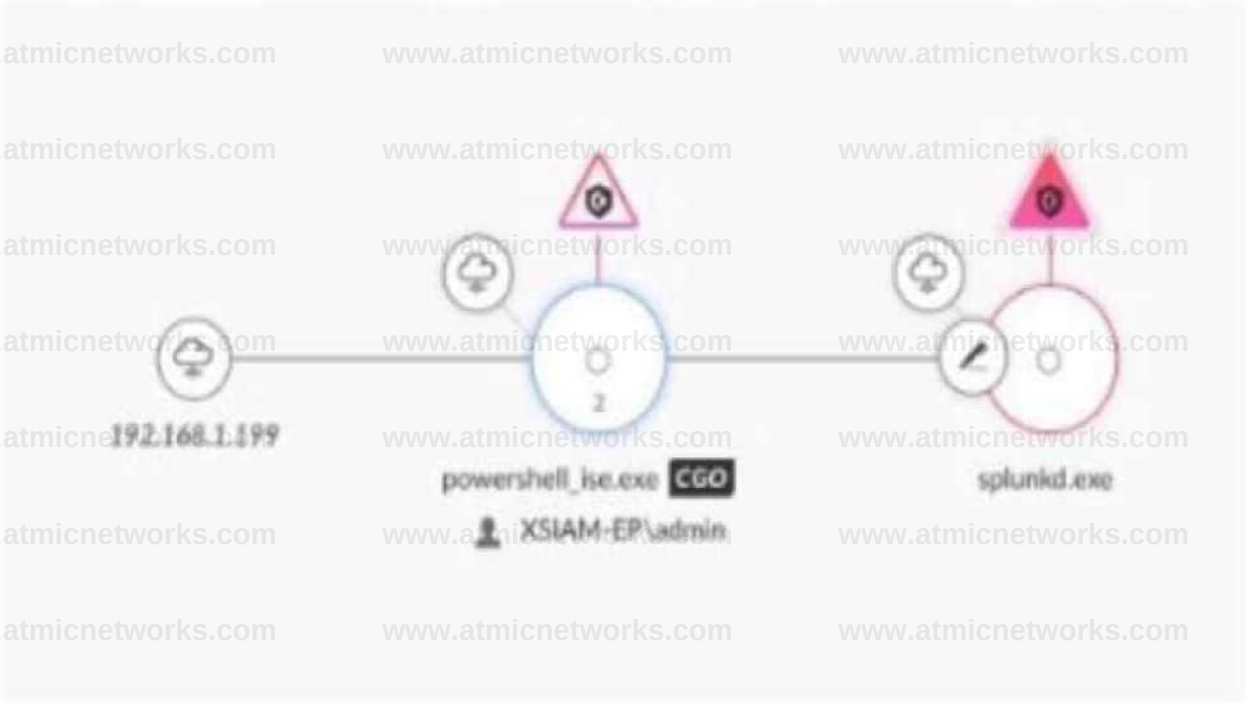
“Anomaly analytics identify significant deviations from established baselines or averages, such as unusual spikes in failed login attempts or other behavioral outliers, and trigger alerts for potential threats.”

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 28 (Alerting and Detection section)

Question: 49

Based on the image below, which two additional steps should a SOC analyst take to secure the endpoint? (Choose two.)



A. Live Terminal into the workstation to verify.

B. Reboot the machine.

C. Block 192.168.1.199.

D. Isolate the affected workstation.

Answer: C, D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The correct answers are C – Block 192.168.1.199 and D – Isolate the affected workstation.

Block 192.168.1.199: The image shows that the suspicious or malicious activity originated from this source IP address, making it a potential threat actor or compromised system on the network.

Blocking this IP helps prevent further communication or lateral movement from the suspected attacker.

Isolate the affected workstation: Since suspicious activities (like powershell_ise.exe running as an admin and launching splunkd.exe) are detected, isolating the workstation is a critical containment measure. This action disconnects the endpoint from the network, stopping any ongoing attack, lateral movement, or command-and-control activity, while allowing for forensic investigation.

"Isolating an endpoint and blocking the source IP address are best practices for immediate containment in the event of detected compromise or suspicious activity."

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 40 (Incident Handling section)

Question: 50

Based on the artifact details in the image below, what can an analyst infer from the hexagon-shaped object with the exclamation mark (!) at the center?

A. The WildFire verdict returned is "Low Confidence."
B. The artifact verdict has changed from a previous state to "Malware."
C. The malicious artifact was injected.
D. The malware requires further analysis.

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

The correct answer is B – The artifact verdict has changed from a previous state to "Malware."

The hexagon-shaped object with an exclamation mark in Cortex XSIAM artifact analysis indicates a change or escalation in verdict—typically from "Unknown" or another previous state to "Malware." This symbol is a visual cue for analysts to pay attention to the updated status, as the system has reclassified the file/object to "Malware" based on new intelligence or analysis.

“The exclamation mark in a hexagon is used to signal that the verdict of the artifact has changed, most commonly to indicate a new classification as 'Malware.'”

Document Reference: XSIAM Analyst ILT Lab Guide.pdf

Page: Page 37 (Threat Intel Management section, Artifact verdict/status changes)