Palo Alto Networks
XSIAM-Analyst
Palo Alto Networks XSIAM Analyst

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

Latest Version: 6.0

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.
==========

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/