KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **XSIAM-Analyst**

Title : Palo Alto Networks XSIAM Analyst

Version : DEMO

1.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)

2.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)

3.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)

4.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 fieldcausality_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 fieldcausality_actor_effective_usernamespecifically 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_usernameandaction_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, optionAis the verified correct answer.

5.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 toisolate 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)