Vendor: Palo Alto Networks

Exam Code: XSOAR-Engineer

Exam Name: Palo Alto Networks XSOAR Engineer

Version: 26.011

QUESTION 1
A breakpoint is added to a saved playbook to ensure that it pauses before running the task "ad-delete-user." However, it is later discovered that an Active Directory account was deleted by this playbook, and the playbook did not pause at the breakpoint. What is the cause of this issue?

A. The playbook does not stop at the breakpoint when run from an incident.
B. The task was not set to "skip."
C. The task was not configured to override input.
D. The playbook was not set to "quiet mode."

Answer: A
Explanation:
Breakpoints in XSOAR are only effective when running the playbook in the playbook debugger. If the playbook is executed directly from an incident, it will not pause at the breakpoint, which is why the "ad-delete-user" task still ran and deleted the account.

QUESTION 2
What is the result of an indicator being marked as expired?

A. It still exists and can be searched.
B. It is immediately deleted from the database.
C. It still exists but is not searchable.
D. It is deleted from the database after seven days.

Answer: A
Explanation:
When an indicator is marked as expired in XSOAR, it remains in the system and can still be searched, but it is considered inactive for enrichment, correlation, or automation unless specifically configured otherwise.

QUESTION 3
When the "Only allow these dashboards" checkbox is selected for a user role, what is the primary effect on users assigned this role?

A. They are prompted to select their preferred dashboards upon login and can only modify these chosen dashboards.
B. They can only view specified dashboards and make minor modifications.
C. They will automatically have all dashboards that are shared with them added to their view.
D. They will be restricted to viewing only the specified default dashboards and cannot make any modifications.

Answer: D
Explanation:
When the "Only allow these dashboards" checkbox is enabled for a user role in XSOAR, it enforces strict control - users with that role can view only the specified dashboards and cannot create, modify, or access other dashboards beyond those explicitly allowed.

QUESTION 4
What must happen before a pre-process rule can be applied to a potential incident?

A. Mapping
B. Playbook execution
C. Ingestion
D. Classification

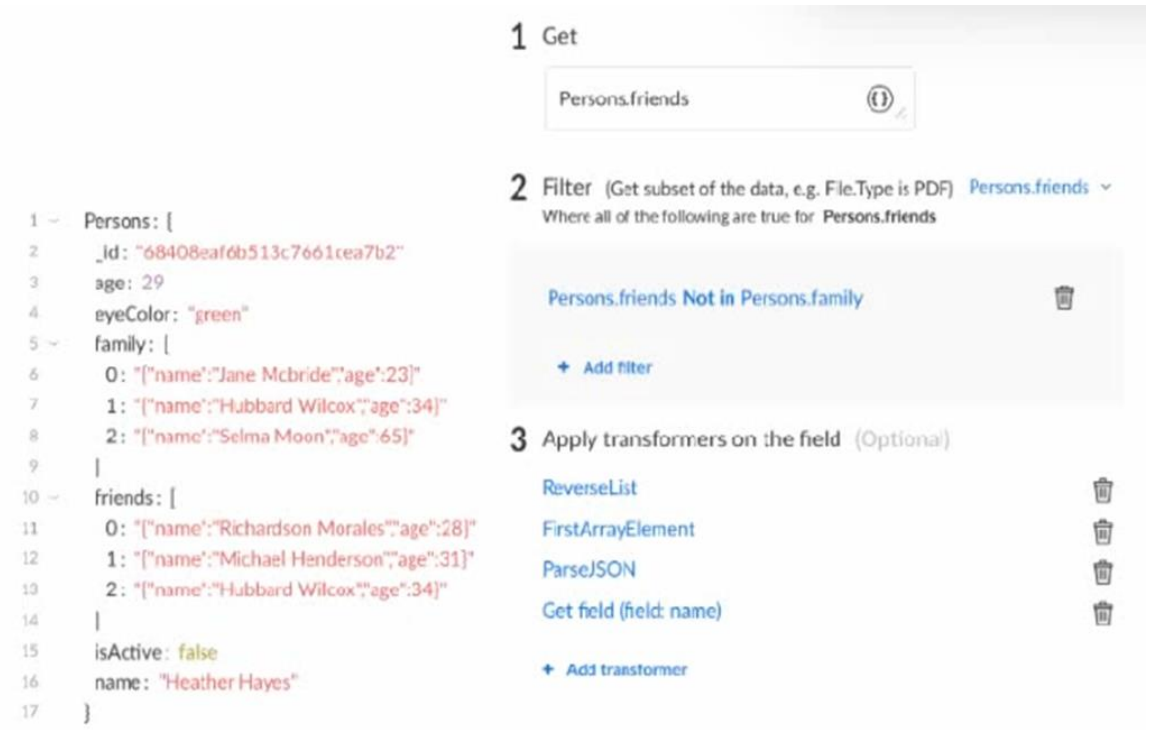
Answer: D
Explanation:
Before a pre-process rule can be applied, the incoming event must go through classification, which determines the incident type. Pre-process rules are tied to incident types and are applied immediately after classification but before ingestion, allowing actions like dropping, merging, or modifying incidents based on their type.

QUESTION 5
Which set of trigger options is available to start a job when a new instance is created?

A. "Mapping" and "Classification"
B. "Time" and "By delta in feed"
C. "Cron View" and "Human View"
D. "Script Start" and "CLI"

Answer: B
Explanation:
Jobs in XSOAR can be triggered based on scheduled time intervals ("Time") or changes in feed content ("By delta in feed"). These options are available when configuring jobs to start automatically, such as when a new feed instance is created.

QUESTION 6
Based on the images below, what will be the result of the Filters and Transformers?



A. Selma Moon
B. Richardson Morales
C. Hubbard Wilcox
D. Michael Henderson

Answer: D
Explanation:
The filter keeps only friends not in the family list → ["Richardson Morales", "Michael Henderson"].

ReverseList → ["Michael Henderson", "Richardson Morales"].

FirstArrayElement selects "Michael Henderson".

ParseJSON and Get field(name) output the name Michael Henderson.

QUESTION 7
Which feature is used to convert event data values into incident fields when an integration fetches an event?

A. Classification
B. Mapping
C. Field configuration
D. Layout configuration

Answer: B
Explanation:
When an integration fetches events, XSOAR uses mapping to convert event data values into incident fields. Classification determines the incident type, but mapping is the step that assigns

specific event data to the corresponding incident fields.

QUESTION 8
A SOC team must send a notification email to specific teams based on the severity of an incident. Which feature will accomplish this task each time the severity escalates?

A. SLA script
B. Post-processing rule
C. Field-change trigger script
D. Server config

Answer: C
Explanation:
A field-change trigger script in XSOAR can monitor when a field, such as incident severity, changes. Each time severity escalates, the script executes automatically and can send targeted notification emails to the appropriate teams.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: ASTR14