Paloalto Networks
XSOAR-Engineer
Palo Alto Networks XSOAR Engineer

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: 8.1

Question: 1

Which two behaviors occur while an incident is closed? (Choose two.).

A. Playbook is marked as complete.
B. Commands cannot be executed in the War Room.
C. Timers can no longer run.
D. Running timers are in a paused state.

Answer: A, C

Explanation:
The XSOAR Timers/SLA documentation states that when an incident reaches the Closed state, all timers automatically stop and cannot continue unless manually reset. Timers do not pause — they terminate.
Additionally, when an incident is closed, its associated playbook completes, because closure marks the end of the investigation lifecycle.

Question: 2

An engineer must create a playbook task which asks a user a single question to determine the next step in the playbook flow.
Which type of task will accomplish this goal?.

A. Standard task using manual task settings.
B. Data collection task using the task option.
C. Conditional task using the ask option.
D. Data collection task using the generated link option.

Answer: C

Explanation:
The XSOAR Admin Guide explains that the Ask task is created inside a Conditional Task, and is specifically used when the system needs to prompt the analyst with a single question to determine the playbook path.
Data collection tasks are used for multi-question forms, not conditional branching.

Question: 3

What determines the current verdict for an indicator when multiple sources provide different reliability scores and verdicts?.

A. Verdict provided by the most recently updated source.
B. Average verdict score from all sources.
C. Verdict provided by the source with the highest reliability score.
D. Highest severity verdict from all sources.

Answer: C

Explanation:
The Threat Intelligence section specifies that XSOAR determines an indicator's verdict by selecting the verdict from the source that has the highest reliability score.
Only when two sources have equal reliability does XSOAR choose the most severe (worst) verdict between them.

Question: 4

The code snippet below is from the fetch command of an integration instance configured to run on the server.
demisto.debug(f"(len(incidents)} events fetched")
Where is the output from the snippet located when the instance runs an automatic fetch?.

A. Incident label.
B. Platform Log bundle.
C. Integration Logs table.
D. War Room entry.

Answer: C

Explanation:
Integration debug messages (generated using demisto.debug) are stored in the Integration Logs table, not in the War Room or incident labels.
The Admin Guide states that all logs generated by integration code are visible through the Integration Logs section for troubleshooting.

Question: 5

Which action will resolve the issue when an analyst upgrades a content pack from the Marketplace, and the new version has a code error?.

A. Revert the content pack to a previous version.
B. Uninstall and reinstall the content pack.

C. Upgrade the dependencies of the content pack.
D. Export and manually upload the content pack.

Answer: A

Explanation:
The Marketplace section states that administrators can revert any installed content pack to a previous version via the Version History → Revert to this version option.
This is the recommended method when a new release introduces a bug.
Reinstalling the same version does not fix the code error.

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/