DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Palo Alto Networks

Exam: XSIAM-Analyst Exam

Number of questions in the database: 50

Exam Version: NOV.2026

Question #1Topic 1

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

A. dataset = pan_dss_raw

B. dataset = ngfw_threat_panw_raw

C. dataset = panw_ngfw_traffic_raw

D. dataset = ngfw*

Correct Answer: C

Question #2Topic 1

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

A. Feed Integration settings

B. Indicator Configuration in Object Setup

C. STIX parser code

D. Classification & Mapping tab

Correct Answer: B

Question #3Topic 1

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 this 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.

https://dbcloud.academy/

C. The endpoint agents were in offline 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.

Correct Answer: B

Question #4Topic 1

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

A. Activation period

B. Deduplication period

C. Training period

D. Test period

Correct Answer: A

Question #5Topic 1

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 BIOC rule exception.

B. Implement a global exception in the prevention profile.

C. Implement an alert exclusion rule.

D. Implement a shunt in a BIOC bypass rule.

Correct Answer: C

Question #6Topic 1

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

Why were the playbooks not executed?

A. Playbook triggers were not configured for those alerts.

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

C. Misconfiguration of the connector instance has occurred.

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

Correct Answer: A

https://dbcloud.academy/