DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Palo Alto Networks

Exam: XSIAM-Engineer Exam

Number of questions in the database: 137

Exam Version: NOV.2026

Question #1Topic 1

How will Cortex XSIAM help with raw log ingestion from third-party sources in an existing infrastructure?

A. Any structured logs coming into it are left completely unchanged, and only metadata is added to the raw data.

B. For structured logs, like CEF, LEEF, and JSON, it decouples the key-value pairs and saves them in table format.

C. Any unstructured logs coming into it are left completely unchanged, and metadata is not added to the raw data.

D. For unstructured logs, it decouples the key-value pairs and saves them in a table format.

Correct Answer: B

Question #2Topic 1

In which two locations can correlation rules be monitored for errors? (Choose two.)

A. XDR Collector audit logs (type = Rules, subtype = Error)

B. correlations_auditing dataset through XQL

C. Management audit logs (type = Rules, subtype = Error)

D. Alerts table as a health alert

Correct Answer: BC

Question #3Topic 1

Which option should be used when customizing a dashboard in Cortex XSIAM to include a widget that will display data filtered by more than one dynamic value?

A. Free text/number

B. Multi-select

C. Fixed filter

https://dbcloud.academy/

D. Single-select

Correct Answer: B

Question #4Topic 1

How must Cloud Identity Engine be deployed and activated on Cortex XSIAM?

A. In a different region than Cortex XSIAM; logs can be verified using pan_dss_raw dataset

B. In a different region than Cortex XSIAM; logs can be verified using endpoints dataset

C. In the same region as Cortex XSIAM; logs can be verified using pan_dss_raw dataset

D. In the same region as Cortex XSIAM; logs can be verified using endpoints dataset

Correct Answer: C

Question #5Topic 1

Which common issue can result in sudden data ingestion loss for a data source that was previously successful?

A. Data source is using an unsupported data format.

B. Data source has reached its maximum storage capacity.

C. Data source has reached its end of life for support.

D. API key used for the integration has expired.

Correct Answer: D

Question #6Topic 1

While using the remote repository on a Development XSIAM tenant, which two objects can be pushed or pulled to the remote repository? (Choose two.)

A. Scripts

B. Parsing rules

C. Lists

D. Layouts

Correct Answer: AD

https://dbcloud.academy/