Palo Alto Networks

XSIAM-ENGINEER Exam

Palo Alto Networks XSIAM Engineer

Questions & Answers
Demo

Version: 4.0

Question: 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.

Answer: B

Explanation:

Cortex XSIAM ingests structured third-party logs (such as CEF, LEEF, and JSON) by breaking down the key-value pairs and saving them in a normalized table format. This enables efficient correlation, analytics, and query performance across diverse log sources while preserving data fidelity.

Question: 2

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

Answer: A, B

Explanation:

Correlation rule errors can be tracked in XDR Collector audit logs (type = Rules, subtype = Error) and by querying the correlations_auditing dataset through XQL. These provide visibility into execution issues and failures for correlation rules.

Question: 3

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

D. Single-select

Answer: B

Explanation:

The Multi-select option allows a dashboard widget in Cortex XSIAM to be filtered by more than one dynamic value, enabling flexible data exploration and visualization across multiple selected criteria.

Question: 4

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

Answer: C

Explanation:

Cloud Identity Engine must be deployed in the same region as Cortex XSIAM to ensure compliance and proper data handling. Once integrated, the ingestion can be verified by checking the pan_dss_raw dataset, which records the raw directory synchronization logs.

Question: 5

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.

Answer: D

Explanation:

A sudden data ingestion loss for a previously successful data source commonly occurs when the API key used for the integration has expired, breaking authentication and preventing further log collection.