Palo Alto Networks
XDR-Analyst
Palo Alto Networks XDR Analyst

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: 6.0

Question: 1

What does the 'Disconnected' state of a Cortex XDR agent indicate?

A. It has been removed by the admin
B. The agent is unlicensed
C. The agent is offline or unable to connect to Cortex XDR
D. The agent is in quarantine

Answer: C

Question: 2

What is the primary purpose of Host Insights in Cortex XDR?

A. To scan file attachments in email
B. To visualize firewall configuration changes
C. To automate policy updates across tenants
D. To provide deep visibility into endpoint health and risk indicators

Answer: D

Question: 3

Which Cortex XDR component generates alerts based on correlated logs and endpoint behavior?

A. BIOC Engine
B. XQL Query Builder
C. Asset Inventory
D. Live Terminal

Answer: A

Question: 4

Which of the following components is part of the schema in an XQL query?

A. schedule
B. xdr_data
C. hostname
D. timeline

Answer: C

Question: 5

Which two benefits does the timeline feature provide in alert investigation?
(Choose two)

A. Execution timestamps of related alerts
B. Automatic endpoint isolation
C. Overview of causality-based incident links
D. Network topology visualization

Answer: A,C

Question: 6

What benefits does configuring custom prioritization provide?
(Choose two)

A. Ensures all alerts trigger endpoint isolation
B. Reduces analyst time by pre-filtering irrelevant alerts
C. Suppresses alerts from internal systems
D. Aligns alert relevance to business context

Answer: B,D

Question: 7

What is a "field" in the context of an XQL query's schema?

A. A pre-built response action
B. A type of agent event
C. A named attribute within a dataset
D. A dashboard panel widget

Answer: C

Question: 8

Which Cortex XDR capability isolates an infected host from the network?

A. Host Insights
B. Endpoint Isolation
C. IOC Analysis
D. Agent Profiles

Answer: B

Question: 9

Which issues could cause a Cortex XDR agent to report an 'Error' status?
(Choose three)

A. Agent service crash
B. Tamper protection disabled
C. DNS resolution failure
D. Operating system incompatibility

Answer: A,C,D

Question: 10

Which syntax snippet will correctly extract the user_name field from the alerts dataset?

A. dataset = alerts | select user_name
B. xdr_data.alerts | filter user_name == "*"
C. dataset = xdr_data.alerts | fields user_name
D. select xdr_data.alerts where user_name=*

Answer: C

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/