PCDRA Q&As

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/pcdra.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

When creating a BIOC rule, which XQL query can be used?

A. dataset = xdr_data | filter event_sub_type = PROCESS_START and action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

B. dataset = xdr_data | filter event_type = PROCESS and event_sub_type = PROCESS_START and action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

C. dataset = xdr_data | filter action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe" | fields action_process_image

D. dataset = xdr_data | filter event_behavior = true event_sub_type = PROCESS_START and action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

Correct Answer: B

QUESTION 2

Which engine, of the following, in Cortex XDR determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident?

A. Sensor Engine

B. Causality Analysis Engine

C. Log Stitching Engine

D. Causality Chain Engine

Correct Answer: B

QUESTION 3

In incident-related widgets, how would you filter the display to only show incidents that were "starred"?

A. Create a custom XQL widget

B. This is not currently supported

C. Create a custom report and filter on starred incidents

D. Click the star in the widget

Correct Answer: D

QUESTION 4

How does Cortex XDR agent for Windows prevent ransomware attacks from compromising the file system?

A. by encrypting the disk first.

B. by utilizing decoy Files.

C. by retrieving the encryption key.

D. by patching vulnerable applications.

Correct Answer: B

QUESTION 5

While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion. What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?

A. mark the incident as Unresolved

B. create a BIOC rule excluding this behavior

C. create an exception to prevent future false positives

D. mark the incident as Resolved ?False Positive

Correct Answer: D