PCDRA$^{\text{Q\&As}}$

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.geekcert.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

QUESTION 1

Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

A. Hash Verdict Determination

B. Behavioral Threat Protection

C. Restriction Policy

D. Child Process Protection

Correct Answer: B

QUESTION 2

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 3

When is the wss (WebSocket Secure) protocol used?

A. when the Cortex XDR agent downloads new security content

B. when the Cortex XDR agent uploads alert data

C. when the Cortex XDR agent connects to WildFire to upload files for analysis

D. when the Cortex XDR agent establishes a bidirectional communication channel

Correct Answer: D

QUESTION 4

What is the purpose of the Unit 42 team?

A. Unit 42 is responsible for automation and orchestration of products

B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server

C. Unit 42 is responsible for threat research, malware analysis and threat hunting

D. Unit 42 is responsible for the rapid deployment of Cortex XDR agents

Correct Answer: C

QUESTION 5

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

PCDRA Study Guide PCDRA Exam Questions PCDRA Braindumps