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

QUESTION 1

What is the outcome of creating and implementing an alert exclusion?

A. The Cortex XDR agent will allow the process that was blocked to run on the endpoint.

B. The Cortex XDR console will hide those alerts.

C. The Cortex XDR agent will not create an alert for this event in the future.

D. The Cortex XDR console will delete those alerts and block ingestion of them in the future.

Correct Answer: B

QUESTION 2

Where would you view the WildFire report in an incident?

A. next to relevant Key Artifacts in the incidents details page

B. under Response --> Action Center

C. under the gear icon --> Agent Audit Logs

D. on the HUB page at apps.paloaltonetworks.com

Correct Answer: B

QUESTION 3

Which type of BIOC rule is currently available in Cortex XDR?

A. Threat Actor

B. Discovery

C. Network

D. Dropper

Correct Answer: D

QUESTION 4

Which of the following represents the correct relation of alerts to incidents?

A. Only alerts with the same host are grouped together into one Incident in a given time frame.

B. Alerts that occur within a three hour time frame are grouped together into one Incident.

C. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.

D. Every alert creates a new Incident.

Correct Answer: A

QUESTION 5

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATTandCKTM techniques.

A. Exfiltration, Command and Control, Collection

B. Exfiltration, Command and Control, Privilege Escalation

C. Exfiltration, Command and Control, Impact

D. Exfiltration, Command and Control, Lateral Movement

Correct Answer: D