



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.passapply.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

What is the purpose of the Cortex Data Lake?

- A. a local storage facility where your logs and alert data can be aggregated
- B. a cloud-based storage facility where your firewall logs are stored
- C. the interface between firewalls and the Cortex XDR agents
- D. the workspace for your Cortex XDR agents to detonate potential malware files

Correct Answer: B

QUESTION 2

A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

- A. It is true positive.
- B. It is false positive.
- C. It is a false negative.
- D. It is true negative.

Correct Answer: B

QUESTION 3

When creating a custom XQL query in a dashboard, how would a user save that XQL query to the Widget Library?

- A. Click the three dots on the widget and then choose "Save" and this will link the query to the Widget Library.
- B. This isn't supported, you have to exit the dashboard and go into the Widget Library first to create it.
- C. Click on "Save to Action Center" in the dashboard and you will be prompted to give the query a name and description.
- D. Click on "Save to Widget Library" in the dashboard and you will be prompted to give the query a name and description.

Correct Answer: D

QUESTION 4

Which statement best describes how Behavioral Threat Protection (BTP) works?



- A. BTP injects into known vulnerable processes to detect malicious activity.
- B. BTP runs on the Cortex XDR and distributes behavioral signatures to all agents.
- C. BTP matches EDR data with rules provided by Cortex XDR.
- D. BTP uses machine Learning to recognize malicious activity even if it is not known.

Correct Answer: D

QUESTION 5

Which Type of IOC can you define in Cortex XDR?

- A. destination port
- B. e-mail address
- C. full path
- D. App-ID

Correct Answer: C

[Latest PCDRA Dumps](#)

[PCDRA PDF Dumps](#)

[PCDRA Study Guide](#)