



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 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 2

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 3

Which statement is true for Application Exploits and Kernel Exploits?

- A. The ultimate goal of any exploit is to reach the application.
- B. Kernel exploits are easier to prevent than application exploits.
- C. The ultimate goal of any exploit is to reach the kernel.
- D. Application exploits leverage kernel vulnerability.

Correct Answer: A

QUESTION 4

Which statement regarding scripts in Cortex XDR is true?

- A. Any version of Python script can be run.



- B. The level of risk is assigned to the script upon import.
- C. Any script can be imported including Visual Basic (VB) scripts.
- D. The script is run on the machine uploading the script to ensure that it is operational.

Correct Answer: A

QUESTION 5

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

[PCDRA VCE Dumps](#)

[PCDRA Exam Questions](#)

[PCDRA Braindumps](#)