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.leads4pass.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

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 2

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 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

Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

A. Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list.

B. From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.

C. Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.

D. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the

list, and apply it.

Correct Answer: B

QUESTION 5

Which of the following best defines the Windows Registry as used by the Cortex XDR agent?

A. a hierarchical database that stores settings for the operating system and for applications

B. a system of files used by the operating system to commit memory that exceeds the available hardware resources. Also known as the "swap"

C. a central system, available via the internet, for registering officially licensed versions of software to prove ownership

D. a ledger for maintaining accurate and up-to-date information on total disk usage and disk space remaining available to the operating system

Correct Answer: A

[PCDRA Study Guide](#)   [PCDRA Exam Questions](#)   [PCDRA Braindumps](#)