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.pass2lead.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

When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

A. Remediation Automation

B. Machine Remediation

C. Automatic Remediation

D. Remediation Suggestions

Correct Answer: D

QUESTION 2

How does Cortex XDR agent for Windows prevent ransomware attacks from compromising the file system?

A. by encrypting the disk first.

B. by utilizing decoy Files.

C. by retrieving the encryption key.

D. by patching vulnerable applications.

Correct Answer: B

QUESTION 3

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 4

Network attacks follow predictable patterns. If you interfere with any portion of this pattern, the attack will be neutralized. Which of the following statements is correct?

A. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the firewall.

B. Cortex XDR Analytics does not interfere with the pattern as soon as it is observed on the endpoint.

C. Cortex XDR Analytics does not have to interfere with the pattern as soon as it is observed on the endpoint in order to prevent the attack.

D. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the endpoint.

Correct Answer: A

QUESTION 5

A Linux endpoint with a Cortex XDR Pro per Endpoint license and Enhanced Endpoint Data enabled has reported malicious activity, resulting in the creation of a file that you wish to delete. Which action could you take to delete the file?

A. Manually remediate the problem on the endpoint in question.

B. Open X2go from the Cortex XDR console and delete the file via X2go.

C. Initiate Remediate Suggestions to automatically delete the file.

D. Open an NFS connection from the Cortex XDR console and delete the file.

Correct Answer: A