



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.geekcert.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

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 2

An attacker tries to load dynamic libraries on macOS from an unsecure location. Which Cortex XDR module can prevent this attack?

- A. DDL Security
- B. Hot Patch Protection
- C. Kernel Integrity Monitor (KIM)
- D. Dylib Hijacking

Correct Answer: D

QUESTION 3

What kind of the threat typically encrypts user files?

- A. ransomware
- B. SQL injection attacks
- C. Zero-day exploits
- D. supply-chain attacks

Correct Answer: A

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

Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

A. NetBIOS over TCP

B. WebSocket

C. UDP and a random port

D. TCP, over port 80

Correct Answer: B

[PCDRA PDF Dumps](#)

[PCDRA Practice Test](#)

[PCDRA Study Guide](#)