



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

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

QUESTION 2

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 3

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATTandCKTM techniques.

- A. Exfiltration, Command and Control, Collection
- B. Exfiltration, Command and Control, Privilege Escalation
- C. Exfiltration, Command and Control, Impact
- D. Exfiltration, Command and Control, Lateral Movement

Correct Answer: D

QUESTION 4

Which module provides the best visibility to view vulnerabilities?

- A. Live Terminal module



B. Device Control Violations module

C. Host Insights module

D. Forensics module

Correct Answer: C

QUESTION 5

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

[PCDRA PDF Dumps](#)

[PCDRA VCE Dumps](#)

[PCDRA Study Guide](#)