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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which profiles can the user use to configure malware protection in the Cortex XDR console?

A. Malware Protection profile

B. Malware profile

C. Malware Detection profile

D. Anti-Malware profile

Correct Answer: B

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

Which license is required when deploying Cortex XDR agent on Kubernetes Clusters as a DaemonSet?

A. Cortex XDR Pro per TB

B. Host Insights

C. Cortex XDR Pro per Endpoint

D. Cortex XDR Cloud per Host

Correct Answer: D

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

To create a BIOC rule with XQL query you must at a minimum filter on which field in order for it to be a valid BIOC rule?

A. causality_chain

B. endpoint_name

C. threat_event

D. event_type

Correct Answer: D