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

What license would be required for ingesting external logs from various vendors?

A. Cortex XDR Pro per Endpoint

B. Cortex XDR Vendor Agnostic Pro

C. Cortex XDR Pro per TB

D. Cortex XDR Cloud per Host

Correct Answer: C

QUESTION 2

What is the function of WildFire for Cortex XDR?

A. WildFire runs in the cloud and analyses alert data from the XDR agent to check for behavioural threats.

B. WildFire is the engine that runs on the local agent and determines whether behavioural threats are occurring on the endpoint.

C. WildFire accepts and analyses a sample to provide a verdict.

D. WildFire runs entirely on the agent to quickly analyse samples and provide a verdict.

Correct Answer: C

QUESTION 3

What is the purpose of the Unit 42 team?

A. Unit 42 is responsible for automation and orchestration of products

B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server

C. Unit 42 is responsible for threat research, malware analysis and threat hunting

D. Unit 42 is responsible for the rapid deployment of Cortex XDR agents

Correct Answer: C

QUESTION 4

When viewing the incident directly, what is the "assigned to" field value of a new Incident that was just reported to Cortex?

A. Pending

B. It is blank

C. Unassigned

D. New

Correct Answer: D

QUESTION 5

As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to download Cobalt Strike on one of your servers. Days later, you learn about a massive ongoing supply chain attack. Using Cortex XDR you recognize that your server was compromised by the attack and that Cortex XDR prevented it. What steps can you take to ensure that the same protection is extended to all your servers?

A. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.

B. Enable DLL Protection on all servers but there might be some false positives.

C. Create IOCs of the malicious files you have found to prevent their execution.

D. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.

Correct Answer: A