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.leads4pass.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

Which statement best describes how Behavioral Threat Protection (BTP) works?

A. BTP injects into known vulnerable processes to detect malicious activity.

B. BTP runs on the Cortex XDR and distributes behavioral signatures to all agents.

C. BTP matches EDR data with rules provided by Cortex XDR.

D. BTP uses machine Learning to recognize malicious activity even if it is not known.

Correct Answer: D

QUESTION 2

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

QUESTION 3

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

QUESTION 4

When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

A. Assign incidents to an analyst in bulk.

B. Change the status of multiple incidents.

C. Investigate several Incidents at once.

D. Delete the selected Incidents.

Correct Answer: AB

QUESTION 5

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