DUMPSARENA

Palo Alto Networks Certified Detection and Remediation Analyst

Palo Alto Networks PCDRA

Version Demo

Total Demo Questions: 9

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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.

ANSWER: A B

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-release-notes/release-information/features-introduced/features-introduced-in-2021.html

QUESTION NO: 2

You can star security events in which two ways? (Choose two.)

A. Create an alert-starring configuration.

B. Create an Incident-starring configuration.

C. Manually star an alert.

D. Manually star an Incident.

ANSWER: B D

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-incidents/create-a-starred-incident-policy

QUESTION NO: 3

A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

A. It is true positive.

B. It is false positive.

C. It is a false negative.

D. It is true negative.

ANSWER: B

Explanation:

Reference: https://live.paloaltonetworks.com/t5/cortex-xdr-discussions/cortex-xdr-false-positive-cloud2model-manager-1-005/td-p/391391

QUESTION NO: 4

What are two purposes of “Respond to Malicious Causality Chains” in a Cortex XDR Windows Malware profile? (Choose two.)

A. Automatically close the connections involved in malicious traffic.

B. Automatically kill the processes involved in malicious activity.

C. Automatically terminate the threads involved in malicious activity.

D. Automatically block the IP addresses involved in malicious traffic.

ANSWER: A D

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/endpoint-security-profiles/add-malware-security-profile.html#:~:text=With%20Behavioral

%20threat%20protection%2C%20the,appear%20legitimate%20if%20inspected%20individually

QUESTION NO: 5

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

ANSWER: C

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/external-data-ingestion/about-external-data-ingestion.html

QUESTION NO: 6

Which two types of exception profiles you can create in Cortex XDR? (Choose two.)

A. exception profiles that apply to specific endpoints

B. agent exception profiles that apply to specific endpoints

C. global exception profiles that apply to all endpoints

D. role-based profiles that apply to specific endpoints

ANSWER: A C

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/endpoint-security/exceptions-security-profiles.html

QUESTION NO: 7

A Linux endpoint with a Cortex XDR Pro per Endpoint license and Enhanced Endpoint Data enabled has reported malicious activity, resulting in the creation of a file that you wish to delete. Which action could you take to delete the file?

A. Manually remediate the problem on the endpoint in question.

B. Open X2go from the Cortex XDR console and delete the file via X2go.

C. Initiate Remediate Suggestions to automatically delete the file.

D. Open an NFS connection from the Cortex XDR console and delete the file.

ANSWER: A

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-release-notes/release-information/features-introduced/features-introduced-in-2020.html

QUESTION NO: 8

Which Type of IOC can you define in Cortex XDR?

A. destination port

B. e-mail address

C. full path

D. App-ID

ANSWER: C

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-iocs.html

QUESTION NO: 9

Which of the following represents the correct relation of alerts to incidents?

A. Only alerts with the same host are grouped together into one Incident in a given time frame.

B. Alerts that occur within a three hour time frame are grouped together into one Incident.

C. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.

D. Every alert creates a new Incident.

ANSWER: A

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-incidents/cortex-xdr-incidents.html