DUMPSQUEEN

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://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

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

QUESTION NO: 2

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: 3

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: 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.

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: 5

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: 6

What functionality of the Broker VM would you use to ingest third-party firewall logs to the Cortex Data Lake?

A. Netflow Collector

B. Syslog Collector

C. DB Collector

D. Pathfinder

ANSWER: B

Explanation:

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

QUESTION NO: 7

While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion. What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?

A. mark the incident as Unresolved

B. create a BIOC rule excluding this behavior

C. create an exception to prevent future false positives

D. mark the incident as Resolved – False Positive

ANSWER: D

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/alert-exclusions/add-an-alert-exclusion.html

QUESTION NO: 8

When using the “File Search and Destroy” feature, which of the following search hash type is supported?

A. SHA256 hash of the file

B. AES256 hash of the file

C. MD5 hash of the file

D. SHA1 hash of the file

ANSWER: A

Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/response-actions/search-file-and-destroy.html

QUESTION NO: 9

What is the purpose of targeting software vendors in a supply-chain attack?

A. to take advantage of a trusted software delivery method.

B. to steal users' login credentials.

C. to access source code.

D. to report Zero-day vulnerabilities.

ANSWER: B

Explanation:

Reference: https://unit42.paloaltonetworks.com/solarstorm-supply-chain-attack-timeline/