DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified



Technology Provider: Palo Alto Networks

Exam: Palo Alto Networks Certified Detection and Remediation Analyst

Number of questions in the database: 96

Exam Version: NOV.2026

Question #1Topic 1

Phishing belongs which of the following MITRE ATT&CK tactics?

A. Initial Access, Persistence

B. Persistence, Command and Control

C. Reconnaissance, Persistence

D. Reconnaissance, Initial Access

Correct Answer: D

Respuesta por mayor votación de la comunidad

D (100%)

Question #2Topic 1

When creating a BIOC rule, which XQL query can be used?

A. dataset = xdr_data

| filter event_sub_type = PROCESS_START and

action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

B. dataset = xdr_data

| filter event_type = PROCESS and

event_sub_type = PROCESS_START and

action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

C. dataset = xdr_data

| filter action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

| fields action_process_image

D. dataset = xdr_data

| filter event_behavior = true

https://dbcloud.academy/

event_sub_type = PROCESS_START and

action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

Correct Answer: B

Respuesta por mayor votación de la comunidad

B (100%)

Question #3Topic 1

Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

A. Security Manager Dashboard

B. Data Ingestion Dashboard

C. Security Admin Dashboard

D. Incident Management Dashboard

Correct Answer: D

Respuesta por mayor votación de la comunidad

D (100%)

Question #4Topic 1

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. Most Voted

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. Most Voted

Correct Answer: AD

Respuesta por mayor votación de la comunidad

AD (100%)

https://dbcloud.academy/

Question #5Topic 1

When creating a custom XQL query in a dashboard, how would a user save that XQL query to the Widget Library?

A. Click the three dots on the widget and then choose “Save” and this will link the query to the Widget Library.

B. This isn’t supported, you have to exit the dashboard and go into the Widget Library first to create it.

C. Click on “Save to Action Center” in the dashboard and you will be prompted to give the query a name and description.

D. Click on “Save to Widget Library” in the dashboard and you will be prompted to give the query a name and description.

Correct Answer: D

Respuesta por mayor votación de la comunidad

D (100%)

Question #6Topic 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

Respuesta por mayor votación de la comunidad

C (100%)

Question #7Topic 1

An attacker tries to load dynamic libraries on macOS from an unsecure location. Which Cortex XDR module can prevent this attack?

https://dbcloud.academy/