PCDRA Q&As

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

QUESTION 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

QUESTION 2

Which of the following is NOT a precanned script provided by Palo Alto Networks?

A. delete_file

B. quarantine_file

C. process_kill_name

D. list_directories

Correct Answer: B

QUESTION 3

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

Correct Answer: AC

QUESTION 4

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

A. DDL Security

B. Hot Patch Protection

C. Kernel Integrity Monitor (KIM)

D. Dylib Hijacking

Correct Answer: D

QUESTION 5

Which engine, of the following, in Cortex XDR determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident?

A. Sensor Engine

B. Causality Analysis Engine

C. Log Stitching Engine

D. Causality Chain Engine

Correct Answer: B