PSE-CORTEX$^{Q\&As}$

Palo Alto Networks System Engineer - Cortex Professional

Pass Palo Alto Networks PSE-CORTEX Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/pse-cortex.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

An Administrator is alerted to a Suspicious Process Creation security event from multiple users.

The users believe that these events are false positives Which two steps should the administrator take to confirm the false positives and create an exception? (Choose two)

A. With the Malware Security profile, disable the "Prevent Malicious Child Process Execution" module

B. Within the Malware Security profile add the specific parent process, child process, and command line argument to the child process whitelist

C. In the Cortex XDR security event, review the specific parent process, child process, and command line arguments

D. Contact support and ask for a security exception.

Correct Answer: D

QUESTION 2

Which option is required to prepare the VDI Golden Image?

A. Configure the Golden Image as a persistent VDI

B. Use the Cortex XDR VDI tool to obtain verdicts for all PE files

C. Install the Cortex XOR Agent on the local machine

D. Run the Cortex VDI conversion tool

Correct Answer: D

QUESTION 3

The customer has indicated they need EDR data collection capabilities, which Cortex XDR license is required?

A. Cortex XDR Pro per TB

B. Cortex XDR Prevent

C. Cortex XDR Endpoint

D. Cortex XDR Pro Per Endpoint

Correct Answer: C

https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-licenses/migrate-your-cortex-xdr-license

QUESTION 4

Which process in the causality chain does the Cortex XDR agent identify as triggering an event sequence?

A. the relevant shell

B. The causality group owner

C. the adversary\\'s remote process

D. the chain\\'s alert initiator

Correct Answer: B

QUESTION 5

Which two filter operators are available in Cortex XDR? (Choose two.)

A.

B. Contains

C. =

D. Is Contained By

Correct Answer: BC