



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.geekcert.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 adversary is attempting to communicate with malware running on your network for the purpose of controlling malware activities or for exfiltrating data from your network. Which Cortex XDR Analytics alert is this activity most likely to trigger?

- A. Uncommon Local Scheduled Task Creation
- B. Malware
- C. New Administrative Behavior
- D. DNS Tunneling

Correct Answer: B

QUESTION 2

Which two types of IOCs are available for creation in Cortex XDR? (Choose two.)

- A. IP
- B. endpoint hostname
- C. domain
- D. registry entry

Correct Answer: BD

QUESTION 3

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

- A.
- B. Contains
- C. =
- D. Is Contained By

Correct Answer: BC

QUESTION 4

Which step is required to prepare the VDI Golden Image?

- A. Review any PE files that WildFire determined to be malicious



- B. Ensure the latest content updates are installed
- C. Run the VDI conversion tool
- D. Set the memory dumps to manual setting

Correct Answer: D

QUESTION 5

Which four types of Traps logs are stored within Cortex Data Lake?

- A. Threat, Config, System, Data
- B. Threat, Config, System, Analytic
- C. Threat, Monitor, System, Analytic
- D. Threat, Config, Authentication, Analytic

Correct Answer: A

[Latest PSE-CORTEX Dumps](#)

[PSE-CORTEX VCE Dumps](#) [PSE-CORTEX Practice Test](#)