

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.leads4pass.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

Which Cortex XDR Agent capability prevents loading malicious files from USB-connected removable equipment?

- A. Agent Configuration
- B. Device Control
- C. Device Customization
- D. Agent Management

Correct Answer: B

<https://live.paloaltonetworks.com/t5/blogs/cortex-xdr-features-introduced-in-december-2019/ba-p/302231>

QUESTION 2

The prospect is deciding whether to go with a phishing or a ServiceNow use case as part of their POC We have integrations for both but a playbook for phishing only Which use case should be used for the POC?

- A. phishing
- B. either
- C. ServiceNow
- D. neither

Correct Answer: A

QUESTION 3

An administrator has a critical group of systems running Windows XP SP3 that cannot be upgraded The administrator wants to evaluate the ability of Traps to protect these systems and the word processing applications running on them

How should an administrator perform this evaluation?

- A. Gather information about the word processing applications and run them on a Windows XP SP3 VM Determine if any of the applications are vulnerable and run the exploit with an exploitation tool
- B. Run word processing exploits in a latest version of Windows VM in a controlled and isolated environment. Document indicators of compromise and compare to Traps protection capabilities
- C. Run a known 2015 flash exploit on a Windows XP SP3 VM. and run an exploitation tool that acts as a listener Use the results to demonstrate Traps capabilities
- D. Prepare the latest version of Windows VM Gather information about the word processing applications, determine if some of them are vulnerable and prepare a working exploit for at least one of them Execute with an exploitation tool

Correct Answer: C

QUESTION 4

Which two log types should be configured for firewall forwarding to the Cortex Data Lake for use by Cortex XDR?(Choose two)

- A. Security Event
- B. HIP
- C. Correlation
- D. Analytics

Correct Answer: AD

QUESTION 5

A General Purpose Dynamic Section can be added to which two layouts for incident types? (Choose two)

- A. "Close" Incident Form
- B. Incident Summary
- C. Incident Quick View
- D. "New"/"Edit" Incident Form

Correct Answer: BC

[PSE-CORTEX PDF Dumps](#) [PSE-CORTEX VCE Dumps](#) [PSE-CORTEX Braindumps](#)