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.pass4itsure.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 two formats are supported by Whitelist? (Choose two)

A. Regex

B. STIX

C. CSV

D. CIDR

Correct Answer: CD

QUESTION 2

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 3

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 4

A customer wants to modify the retention periods of their Threat logs in Cortex Data Lake.

Where would the user configure the ratio of storage for each log type?

A. Within the TMS, create an agent settings profile and modify the Disk Quota value

B. It is not possible to configure Cortex Data Lake quota for specific log types.

C. Go to the Cortex Data Lake App in Cloud Services, then choose Configuration and modify the Threat Quota

D. Write a GPO for each endpoint agent to check in less often

Correct Answer: C

QUESTION 5

Which two log types should be configuredfor 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

PSE-CORTEX VCE Dumps PSE-CORTEX Study Guide PSE-CORTEX Exam Questions