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

QUESTION 1

How do sub-playbooks affect the Incident Context Data?

A. When set to private, task outputs do not automatically get written to the root context

B. When set to private, task outputs automatically get written to the root context

C. When set to global, allows parallel task execution.

D. When set to global, sub-playbook tasks do not have access to the root context

Correct Answer: D

QUESTION 2

When analyzing logs for indicators, which are used for only BIOC identification\\'?

A. observed activity

B. artifacts

C. techniques

D. error messages

Correct Answer: A

QUESTION 3

If a customer activates a TMS tenant and has not purchased a Cortex Data Lake instance.

Palo Alto Networks will provide the customer with a free instance

What size is this free Cortex Data Lake instance?

A. 1 TB

B. 10 GB

C. 100 GB

D. 10 TB

Correct Answer: A

QUESTION 4

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 5

In Cortex XDR Prevent, which three matching criteria can be used to dynamically group endpoints? (Choose three.)

A. Domain/workgroup membership

B. quarantine status

C. hostname

D. OS

E. attack threat intelligence tag

Correct Answer: ACD