# 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.certbus.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**

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

A. alert root cause

B. hostname

C. domain/workgroup membership

D. OS

E. presence of Flash executable

Correct Answer: ACE

**QUESTION 2**

What are two manual actions allowed on War Room entries? (Choose two.)

A. Mark as artifact

B. Mark as scheduled entry

C. Mark as note

D. Mark as evidence

Correct Answer: A

**QUESTION 3**

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

**QUESTION 4**

Which two formats are supported by Whitelist? (Choose two)

A. Regex

B. STIX

C. CSV

D. CIDR

Correct Answer: CD

**QUESTION 5**

How can you view all the relevant incidents for an indicator?

A. Linked Incidents column in Indicator Screen

B. Linked Indicators column in Incident Screen

C. Related Indicators column in Incident Screen D. Related Incidents column in Indicator Screen

Correct Answer: B

**QUESTION 6**

In an Air-Gapped environment where the Docker package was manually installed after the Cortex XSOAR installation which action allows Cortex XSOAR to access Docker?

A. create a "docker" group and add the "Cortex XSOAR" or "demisto" user to this group

B. create a "Cortex XSOAR\\' or "demisto" group and add the "docker" user to this group

C. disable the Cortex XSOAR service

D. enable the docker service

Correct Answer: B

**QUESTION 7**

An adversary is attempting to communicate with malware running on your network for the purpose of controlling malware activities or for ex filtrating 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 8**

When integrating with Splunk, what will allow you to push alerts into Cortex XSOAR via the REST API?

A. splunk-get-alerts integration command

B. Cortex XSOAR TA App for Splunk

C. SplunkSearch automation

D. SplunkGO integration

Correct Answer: A

**QUESTION 9**

What are process exceptions used for?

A. whitelist programs from WildFire analysis

B. permit processes to load specific DLLs

C. change the WildFire verdict for a given executable

D. disable an EPM for a particular process

Correct Answer: A

**QUESTION 10**

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

PSE-CORTEX PDF Dumps PSE-CORTEX VCE Dumps PSE-CORTEX Practice Test