DUMPSARENA

Palo Alto Networks System Engineer - Cortex Professional

Palo Alto Networks PSE-Cortex

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

"Bob" is a Demisto user. Which command is used to add 'Bob" to an investigation from the

War Room CLI?

A. #Bob

B. /invite Bob

C. @Bob

D. !invite Bob

ANSWER: C

QUESTION NO: 2

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

ANSWER: B

QUESTION NO: 3

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

ANSWER: B

QUESTION NO: 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

ANSWER: C

QUESTION NO: 5

During the TMS instance activation, a tenant (Customer) provides the following information for the fields in the Activation - Step 2 of 2 window.

Field	Value
Company Name	XNet Education Systems
Instance Name	xnet50
Subdomain	xnet
Region	EU

During the service instance provisioning which three DNS host names are created?

(Choose three.)

A. cc-xnet50.traps.paloaltonetworks.com

B. hc-xnet50.traps.paloaltonetworks.com

C. cc-xnet.traps.paloaltonetworks.com

D. cc.xnet50traps.paloaltonetworks.com

E. xnettraps.paloaltonetworks.com

F. ch-xnet.traps.paloaltonetworks.com

ANSWER: A C F

QUESTION NO: 6

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

ANSWER: B C

QUESTION NO: 7

Which two entities can be created as a BIOC? (Choose two.)

A. file

B. registry

C. event log

D. alert log

ANSWER: A B

Explanation:

: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-proadmin/investigation-and-response/cortex-xdr-indicators/working-with-biocs/create-a-biocrule.html

QUESTION NO: 8

If an anomalous process is discovered while investigating the cause of a security event, you can take immediate action to terminate the process or the whole process tree, and block processes from running by initiating which Cortex XDR capability?

A. Live Sensors

B. File Explorer

C. Log Stitching

D. Live Terminal

ANSWER: D

QUESTION NO: 9

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

A. < >

B. Contains

C. =

D. Is Contained By

ANSWER: B C

QUESTION NO: 10

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

ANSWER: A B