Free Questions for PSE-Cortex by dumpssheet

Shared by Boone on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Agent Configuration

B- Device Control

C- Device Customization

D- Agent Management

Answer:

B

Explanation:

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

Question 2

Question Type: MultipleChoice

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.)

Options:

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 3

Question Type: MultipleChoice

Which four types of Traps logs are stored within Cortex Data Lake?

Options:

A- Threat, Config, System, Data

B- Threat, Config, System, Analytic

C- Threat, Monitor. System, Analytic

D- Threat, Config, Authentication, Analytic

Answer:

B

Question 4

Question Type: MultipleChoice

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?

Options:

A- Live Sensors

B- File Explorer

C- Log Stitching

D- Live Terminal

Answer:

D

Question 5

Question Type: MultipleChoice

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?

Options:

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 6

Question Type: MultipleChoice

Which option is required to prepare the VDI Golden Image?

Options:

A- Configure the Golden Image as a persistent VDI

B- Use the Cortex XDR VDI tool to obtain verdicts for all PE files

C- Install the Cortex XOR Agent on the local machine

D- Run the Cortex VDI conversion tool

Answer:

B

Question 7

Question Type: MultipleChoice

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

Options:

A- observed activity

B- artifacts

C- techniques

D- error messages

Answer:

C

Question 8

Question Type: MultipleChoice

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

Options:

A- Domain/workgroup membership

B- quarantine status

C- hostname

D- OS

E- attack threat intelligence tag

Answer:

B, C, D

Question 9

Question Type: MultipleChoice

Which process in the causality chain does the Cortex XDR agent identify as triggering an event sequence?

Options:

A- the relevant shell

B- The causality group owner

C- the adversary's remote process

D- the chain's alert initiator

Answer:

B

Question 10

Question Type: **MultipleChoice**

Which two items are stitched to the Cortex XDR causality chain" (Choose two)

Options:

A- firewall alert

B- SIEM alert

C- full URL

D- registry set value

Answer:

A, C

Question 11

Question Type: MultipleChoice

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

Options:

A- Security Event

B- HIP

C- Correlation

D- Analytics

Answer:

A, B