Vendor: Palo Alto Networks

Exam Code: PSE-Cortex

Exam Name: Palo Alto Networks System Engineer - Cortex Professional

Version: DEMO

QUESTION 1
Which option is required to prepare the VDI Golden Image?

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 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

Answer: C

QUESTION 3
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 4
Which four types of Traps logs are stored within Cortex Data Lake?

A. Threat, Config, System, Data
B. Threat, Config, System, Analytic
C. Threat, Monitor. System, Analytic
D. Threat, Config, Authentication, Analytic

Answer: B

QUESTION 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: ACF

QUESTION 6
Which Cortex XDR Agent capability prevents loading malicious files from USB-connected removable equipment?

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 7
An Administrator is alerted to a Suspicious Process Creation security event from multiple users. The users believe that these events are false positives Which two steps should the administrator take to confirm the false positives and create an exception? (Choose two)

A. With the Malware Security profile, disable the "Prevent Malicious Child Process Execution" module
B. Within the Malware Security profile add the specific parent process, child process, and command

line argument to the child process whitelist
C. In the Cortex XDR security event, review the specific parent process, child process, and command line arguments
D. Contact support and ask for a security exception.

Answer: BC

QUESTION 8
Which Cortex XDR capability extends investigations to an endpoint?

A. Log Stitching
B. Causality Chain
C. Sensors
D. Live Terminal

Answer: A
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-concepts

QUESTION 9
Which two types of IOCs are available for creation in Cortex XDR? (Choose two.)

A. IP
B. endpoint hostname
C. domain
D. registry entry

Answer: AC

QUESTION 10
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

Answer: C

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**