



Paloalto-Networks

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

NEW QUESTION 1

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

Answer: D

NEW QUESTION 2

A prospect has agreed to do a 30-day POC and asked to integrate with a product that Demisto currently does not have an integration with. How should you respond?

- A. Extend the POC window to allow the solution architects to build it
- B. Tell them we can build it with Professional Services.
- C. Tell them custom integrations are not created as part of the POC
- D. Agree to build the integration as part of the POC

Answer: C

NEW QUESTION 3

Which CLI query would bring back Notable Events from Splunk?

- A)
- B)
- C)
- D)

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 4

What is the difference between an exception and an exclusion?

- A. An exception is based on rules and exclusions are on alerts
- B. An exclusion is based on rules and exceptions are based on alerts.
- C. An exception does not exist
- D. An exclusion does not exist

Answer: A

NEW QUESTION 5

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

Answer: C

NEW QUESTION 6

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

Answer: CD

NEW QUESTION 7

The certificate used for decryption was installed as a trusted root CA certificate to ensure communication between the Cortex XDR Agent and Cortex XDR Management Console. What action needs to be taken if the administrator determines the Cortex XDR Agents are not communicating with the Cortex XDR Management Console?

- A. add paloaltonetworks.com to the SSL Decryption Exclusion list
- B. enable SSL decryption
- C. disable SSL decryption
- D. reinstall the root CA certificate

Answer: D

NEW QUESTION 8

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

Answer: A

NEW QUESTION 9

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

Answer: BCD

NEW QUESTION 10

A test for a Microsoft exploit has been planned. After some research Internet Explorer 11 CVE-2016-0189 has been selected and a module in Metasploit has been identified

(exploit/windows/browser/ms16_051_vbscript)

The description and current configuration of the exploit are as follows;

What is the remaining configuration?

- A)
- B)
- C)
- D)

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

NEW QUESTION 10

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: BC

NEW QUESTION 11

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

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

NEW QUESTION 12

The images show two versions of the same automation script and the results they produce when executed in Demisto. What are two possible causes of the exception thrown in the second Image? (Choose two.)
SUCCESS

- A. The modified scnpt was run in the wrong Docker image
- B. The modified script required a different parameter to run successfully.
- C. The dictionary was defined incorrectly in the second script.
- D. The modified script attempted to access a dictionary key that did not exist in the dictionary named "data"

Answer: A

NEW QUESTION 13

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-conc>

NEW QUESTION 18

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: AB

NEW QUESTION 22

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

NEW QUESTION 26

What is the retention requirement for Cortex Data Lake sizing?

- A. number of endpoints
- B. number of VM-Series NGFW
- C. number of days
- D. logs per second

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-corte>

NEW QUESTION 28

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PSE-Cortex Practice Exam Features:

- * PSE-Cortex Questions and Answers Updated Frequently
- * PSE-Cortex Practice Questions Verified by Expert Senior Certified Staff
- * PSE-Cortex Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PSE-Cortex Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PSE-Cortex Practice Test Here](#)