

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

<https://www.2passeasy.com/dumps/PSE-Cortex/>



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

What is the result of creating an exception from an exploit security event?

- A. White lists the process from Wild Fire analysis
- B. exempts the user from generating events for 24 hours
- C. exempts administrators from generating alerts for 24 hours
- D. disables the triggered EPM for the host and process involve

Answer: D

NEW QUESTION 3

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

- A. file
- B. registry
- C. event log
- D. alert log

Answer: AB

Explanation:

<https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xd>

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

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

Answer: A

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

Given the exception thrown in the accompanying image by the Demisto REST API integration, which action would most likely solve the problem?

Which two playbook functionalities allow looping through a group of tasks during playbook execution? (Choose two.)

- A. Generic Polling Automation Playbook
- B. Playbook Tasks
- C. Sub-Play books
- D. Playbook Functions

Answer: AC

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

In the DBotScore context field, which context key would differentiate between multiple entries for the same indicator in a multi-TIP environment?

- A. Vendor
- B. Type
- C. Using
- D. Brand

Answer: A

NEW QUESTION 10

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

NEW QUESTION 11

Which three Demisto incident type features can be customized under Settings > Advanced > Incident Types? (Choose three.)

- A. Define whether a playbook runs automatically when an incident type is encountered
- B. Set reminders for an incident SLA
- C. Add new fields to an incident type
- D. Define the way that incidents of a specific type are displayed in the system
- E. Drop new incidents of the same type that contain similar information

Answer: ABD

NEW QUESTION 15

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

Answer: D

NEW QUESTION 16

The customer has indicated they need EDR data collection capabilities, which Cortex XDR license is required?

- A. Cortex XDR Pro per TB
- B. Cortex XDR Prevent
- C. Cortex XDR Endpoint
- D. Cortex XDR Pro Per Endpoint

Answer: D

Explanation:

<https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-licen>

NEW QUESTION 20

When a Demisto Engine is part of a Load-Balancing group it?

- A. Must be in a Load-Balancing group with at least another 3 members
- B. It must have port 443 open to allow the Demisto Server to establish a connection
- C. Can be used separately as an engine, only if connected to the Demisto Server directly
- D. Cannot be used separately and does not appear in the in the engines drop-down menu when configuring an integration instance

Answer: D

NEW QUESTION 24

An adversary is attempting to communicate with malware running on your network for the purpose of controlling malware activities or for exfiltrating 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

Answer: B

NEW QUESTION 28

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

- A. observed activity
- B. artifacts
- C. techniques
- D. error messages

Answer: C

NEW QUESTION 33

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

NEW QUESTION 38

"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

NEW QUESTION 40

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 45

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 48

Cortex XDR can schedule recurring scans of endpoints for malware. Identify two methods for initiating an on-demand malware scan (Choose two)

- A. Response > Action Center
- B. the local console
- C. Telnet
- D. Endpoint > Endpoint Management

Answer: AD

NEW QUESTION 49

An administrator of a Cortex XDR protected production environment would like to test its ability to protect users from a known flash player exploit. What is the safest way to do it?

- A. The administrator should attach a copy of the weaponized flash file to an email, send the email to a selected group of employees, and monitor the Events tab on the Cortex XDR console
- B. The administrator should use the Cortex XDR tray icon to confirm his corporate laptop is fully protected then open the weaponized flash file on his machine, and monitor the Events tab on the Cortex XDR console.
- C. The administrator should create a non-production Cortex XDR test environment that accurately represents the production environment, introduce the weaponized flash file, and monitor the Events tab on the Cortex XDR console.
- D. The administrator should place a copy of the weaponized flash file on several USB drives, scatter them around the office and monitor the Events tab on the Cortex XDR console

Answer: C

NEW QUESTION 51

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 52

If you have a playbook task that errors out. where could you see the output of the task?

- A. /var/log/messages
- B. War Room of the incident
- C. Demisto Audit log
- D. Playbook Editor

Answer: B

NEW QUESTION 54

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PSE-Cortex Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PSE-Cortex Product From:

<https://www.2passeasy.com/dumps/PSE-Cortex/>

Money Back Guarantee

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