PSE-CORTEX Q&As

Palo Alto Networks System Engineer - Cortex Professional

Pass Palo Alto Networks PSE-CORTEX Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/pse-cortex.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: C

QUESTION 2

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

A. file

B. registry

C. event log

D. alert log

Correct Answer: AB

https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs/create-a-bioc-rule.html

QUESTION 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

Correct Answer: A

QUESTION 4

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 weapomzed 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

Correct Answer: A

QUESTION 5

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

Correct Answer: A

QUESTION 6

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

Correct Answer: ADE

QUESTION 7

Which deployment type supports installation of an engine on Windows, Mac OS. and Linux?

A. RPM

B. SH

C. DEB

D. ZIP

Correct Answer: D

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/engines/install-deploy-and-configure-demisto-engines/create-a-new-engine.html

QUESTION 8

How does an "inline" auto-extract task affect playbook execution?

A. Doesn\\'t wait until the indicators are enriched and continues executing the next step

B. Doesn\\'t wait until the indicators are enriched but populate context data before executing the next

C. step. Wait until the indicators are enriched but doesn\\'t populate context data before executing the next step.

D. Wait until the indicators are enriched and populate context data before executing the next step.

Correct Answer: D

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

Correct Answer: BD

QUESTION 10

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

A.

B. Contains

C. =

D. Is Contained By

Correct Answer: BC