# 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.leads4pass.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**

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.)

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"

Correct Answer: A

**QUESTION 2**

How does DBot score an indicator that has multiple reputation scores?

A. uses the most severe score scores

B. the reputation as undefined

C. uses the average score

D. uses the least severe score

Correct Answer: A

**QUESTION 3**

Which two formats are supported by Whitelist? (Choose two)

A. Regex

B. STIX

C. CSV

D. CIDR

Correct Answer: CD

**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

Correct Answer: A

**QUESTION 5**

Which Cortex XDR capability extends investigations to an endpoint?

A. Log Stitching

B. Causality Chain

C. Sensors

D. Live Terminal

Correct Answer: A

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

**QUESTION 6**

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

Correct Answer: C

https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-cortex-data-lake/set-log-storage-quota

**QUESTION 7**

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

A. Security Event

B. HIP

C. Correlation

D. Analytics

Correct Answer: AD

**QUESTION 8**

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

Correct Answer: D

**QUESTION 9**

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 10**

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

Correct Answer: D