



# PSE-CORTEX<sup>Q&As</sup>

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.passapply.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

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

Correct Answer: B

---

#### QUESTION 2

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

Correct Answer: BC

---

#### QUESTION 3

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 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 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

Correct Answer: A

---

#### QUESTION 5

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

Correct Answer: B

[PSE-CORTEX Study Guide](#)

[PSE-CORTEX Exam Questions](#)

[PSE-CORTEX Braindumps](#)