



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.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

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

Correct Answer: B

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

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 4

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 5

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

Correct Answer: A

[PSE-CORTEX PDF Dumps](#) [PSE-CORTEX Practice Test](#) [PSE-CORTEX Study Guide](#)