

PCDRA^{Q&As}

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

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

<https://www.pass2lead.com/pcdra.html>

100% Passing Guarantee
100% Money Back Assurance

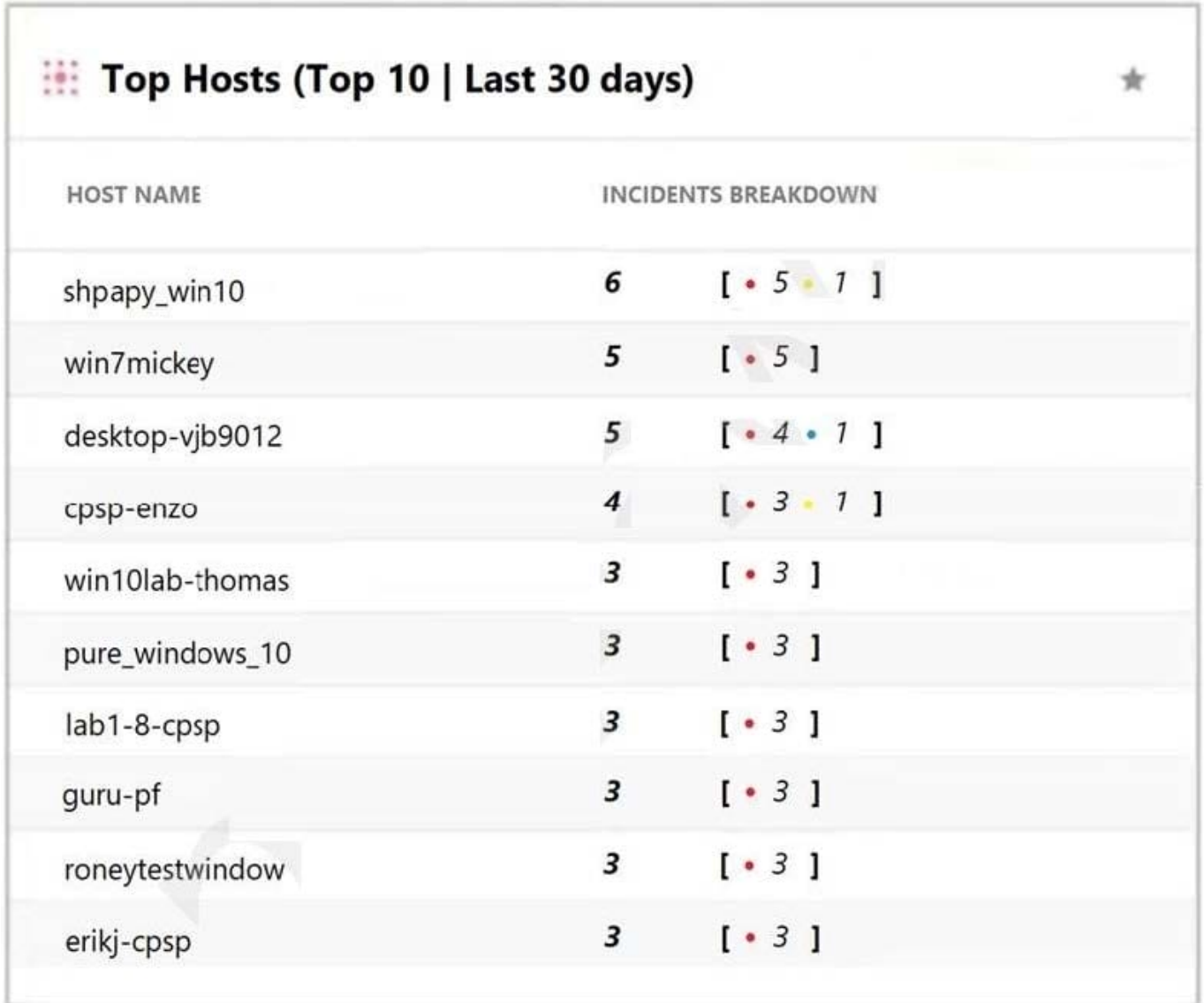
Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

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



QUESTION 1

What does the following output tell us?



HOST NAME	INCIDENTS BREAKDOWN
shpapy_win10	6 [5 1]
win7mickey	5 [5]
desktop-vjb9012	5 [4 1]
cpsp-enzo	4 [3 1]
win10lab-thomas	3 [3]
pure_windows_10	3 [3]
lab1-8-cpsp	3 [3]
guru-pf	3 [3]
roneytestwindow	3 [3]
erikj-cpsp	3 [3]

- A. There is one low severity incident.
- B. Host shpapy_win10 had the most vulnerabilities.
- C. There is one informational severity alert.
- D. This is an actual output of the Top 10 hosts with the most malware.

Correct Answer: D

QUESTION 2

In incident-related widgets, how would you filter the display to only show incidents that were "starred"?

- A. Create a custom XQL widget
- B. This is not currently supported
- C. Create a custom report and filter on starred incidents
- D. Click the star in the widget

Correct Answer: D

QUESTION 3

What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

- A. Automatically close the connections involved in malicious traffic.
- B. Automatically kill the processes involved in malicious activity.
- C. Automatically terminate the threads involved in malicious activity.
- D. Automatically block the IP addresses involved in malicious traffic.

Correct Answer: AD

QUESTION 4

Which module provides the best visibility to view vulnerabilities?

- A. Live Terminal module
- B. Device Control Violations module
- C. Host Insights module
- D. Forensics module

Correct Answer: C

QUESTION 5

What license would be required for ingesting external logs from various vendors?

- A. Cortex XDR Pro per Endpoint
- B. Cortex XDR Vendor Agnostic Pro
- C. Cortex XDR Pro per TB

D. Cortex XDR Cloud per Host

Correct Answer: C

[PCDRA PDF Dumps](#)

[PCDRA VCE Dumps](#)

[PCDRA Practice Test](#)