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.pass2lead.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

How many use cases should a POC success criteria document include?

A. only 1

B. 3 or more

C. no more than 5

D. no more than 2

Correct Answer: D

QUESTION 2

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 3

An adversary is attempting to communicate with malware running on your network for the purpose of controlling malware activities or for ex filtrating 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 4

Rearrange the steps into the correct order for modifying an incident layout.

Select and Place:

![Pass2Lead logo](https://Pass2Lead.com)
Edit the layout	
Select the Edit Layout option	
Navigate to Settings > Advanced > Incident Types	
Select the incident type you want to customize the layout view for	
Navigate to Settings > Layout Builder	

Correct Answer:

	Navigate to Settings > Advanced > Incident Types
	Select the incident type you want to customize the layout view for
	Edit the layout
	Select the Edit Layout option
	Navigate to Settings > Layout Builder

QUESTION 5

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

A. Regex

B. STIX

C. CSV

D. CIDR

Correct Answer: CD