Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

https://www.2passeasy.com/dumps/PSE-Cortex/

NEW QUESTION 1
What are process exceptions used for?

A. whitelist programs from WildFire analysis
B. permit processes to load specific DLLs
C. change the WildFire verdict for a given executable
D. disable an EPM for a particular process

Answer: D

NEW QUESTION 2
Which option describes a Load-Balancing Engine Group?

A. A group of engines that use an algorithm to efficiently share the workload for integrations
B. A group of engines that ensure High Availability of Demisto backend databases.
C. A group of engines that use an algorithm to efficiently share the workload for automation scripts
D. A group of D2 agents that share processing power across multiple endpoints

Answer: C

NEW QUESTION 3
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

Answer: A

NEW QUESTION 4
In Cortex XDR Prevent, which three matching criteria can be used to dynamically group endpoints? (Choose three.)

A. Domain/workgroup membership
B. quarantine status
C. hostname
D. OS
E. attack threat intelligence tag

Answer: BCD

NEW QUESTION 5
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

Answer: A

NEW QUESTION 6
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. ste
D. Wait until the indicators are enriched but doesn't populate context data before executing the next step.
E. Wait until the indicators are enriched and populate context data before executing the next step.

Answer: D

NEW QUESTION 7
The prospect is deciding whether to go with a phishing or a ServiceNow use case as part of their POC We have integrations for both but a playbook for phishing only Which use case should be used for the POC?

A. phishing
B. either
C. ServiceNow
D. neither

Answer: A

NEW QUESTION 8
Which two formats are supported by Whitelist? (Choose two)

A. Regex
B. STIX
C. CSV
D. CIDR

Answer: AD

NEW QUESTION 9
Which Cortex XDR Agent capability prevents loading malicious files from USB-connected removable equipment?

A. Agent Configuration
B. Device Control
C. Device Customization
D. Agent Management

Answer: B

Explanation:
https://live.paloaltonetworks.com/t5/blogs/cortex-xdr-features-introduced-in-december-2019/ba-p/302231

NEW QUESTION 10
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

Answer: BC

NEW QUESTION 10
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

Answer: A

NEW QUESTION 11
"Bob" is a Demisto user. Which command is used to add 'Bob" to an investigation from the War Room CLI?

A. #Bob
B. /invite Bob
C. @Bob
D. !invite Bob

Answer: C

NEW QUESTION 16
An antivirus refresh project was initiated by the IT operations executive. Who is the best source for discussion about the project's operational considerations'?

A. endpoint manager
B. SOC manager
C. SOC analyst
D. desktop engineer

Answer: C

NEW QUESTION 19
Which two items are stitched to the Cortex XDR causality chain'' (Choose two)

A. firewall alert
B. SIEM alert
C. full URL
D. registry set value

Answer: AC

NEW QUESTION 23
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

Answer: B

NEW QUESTION 26
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PSE-Cortex Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PSE-Cortex Product From:

https://www.2passeasy.com/dumps/PSE-Cortex/

Money Back Guarantee

PSE-Cortex Practice Exam Features:

* PSE-Cortex Questions and Answers Updated Frequently

* PSE-Cortex Practice Questions Verified by Expert Senior Certified Staff

* PSE-Cortex Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PSE-Cortex Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year