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 is required to prepare the VDI Golden Image?

A. Configure the Golden Image as a persistent VDI
B. Use the Cortex XDR VDI tool to obtain verdicts for all PE files
C. Install the Cortex XOR Agent on the local machine
D. Run the Cortex VDI conversion tool

Answer: B

NEW QUESTION 3
What method does the Traps agent use to identify malware during a scheduled scan?

A. Heuristic analysis
B. Local analysis
C. Signature comparison
D. WildFire hash comparison and dynamic analysis

Answer: D

NEW QUESTION 4
Which two entities can be created as a BIOC? (Choose two.)

A. file
B. registry
C. event log
D. alert log

Answer: AB

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xd

NEW QUESTION 5
If a customer activates a TMS tenant and has not purchased a Cortex Data Lake instance. Palo Alto Networks will provide the customer with a free instance
What size is this free Cortex Data Lake instance?

A. 1 TB
B. 10 GB
C. 100 GB
D. 10 TB

Answer: C

NEW QUESTION 6
In Cortex XDR Prevent, which three matching criteria can be used to dynamically group endpoints? (Choose three)

A. alert root cause
B. hostname
C. domain/workgroup membership
D. OS
E. presence of Flash executable

Answer: BCD

NEW QUESTION 7
Given the exception thrown in the accompanying image by the Demisto REST API integration, which action would most likely solve the problem?

Which two playbook functionalities allow looping through a group of tasks during playbook execution? (Choose two.)

A. Generic Polling Automation Playbook
B. Playbook Tasks
C. Sub-Play books
D. Playbook Functions

Answer: AC

NEW QUESTION 8
How do sub-playbooks affect the Incident Context Data?

A. When set to private, task outputs do not automatically get written to the root context
B. When set to private, task outputs automatically get written to the root context
C. When set to global, allows parallel task execution.
D. When set to global, sub-playbook tasks do not have access to the root context

Answer: A

NEW QUESTION 9
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 10
An EDR project was initiated by a CISO. Which resource will likely have the most heavy influence on the project?

A. desktop engineer
B. SOC manager
C. SOC analyst IT
D. operations manager

Answer: B

NEW QUESTION 10
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 11
Which two types of lOCs are available for creation in Cortex XDR? (Choose two.)

A. IP
B. endpoint hostname
C. domain
D. registry entry

Answer: AC

NEW QUESTION 16
Which three Demisto incident type features can be customized under Settings > Advanced > Incident Types? (Choose three.)

A. Define whether a playbook runs automatically when an incident type is encountered
B. Set reminders for an incident SLA
C. Add new fields to an incident type
D. Define the way that incidents of a specific type are displayed in the system
E. Drop new incidents of the same type that contain similar information

Answer: ABD

NEW QUESTION 19
Which deployment type supports installation of an engine on Windows, Mac OS. and Linux?

A. RPM
B. SH
C. DEB
D. ZIP

Answer: D

Explanation:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/engines/install-deploy-and-confi

NEW QUESTION 20
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

Answer: B

NEW QUESTION 23
Which two filter operators are available in Cortex XDR? (Choose two.)

A. not Contains
B. !*
C. =>
D. < >

Answer: AB

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/get-started-with-cortex-xdr-pro/use-c

NEW QUESTION 25
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

Answer: B

NEW QUESTION 30
During the TMS instance activation, a tenant (Customer) provides the following information for the fields in the Activation - Step 2 of 2 window.

During the service instance provisioning which three DNS host names are created? (Choose three.)

A. cc-xnet50.traps.paloaltonetworks.com
B. hc-xnet50.traps.paloaltonetworks.com
C. cc-xnet.traps.paloaltonetworks.com
D. cc.xnet50traps.paloaltonetworks.com
E. xnettraps.paloaltonetworks.com
F. ch-xnet.traps.paloaltonetworks.com

Answer: ACF

NEW QUESTION 35
The images show two versions of the same automation script and the results they produce when executed in Demisto. What are two possible causes of the exception thrown in the second Image? (Choose two.)
SUCCESS

A. The modified scnpt was run in the wrong Docker image
B. The modified script required a different parameter to run successfully.
C. The dictionary was defined incorrectly in the second script.

D. The modified script attempted to access a dictionary key that did not exist in the dictionary named "data"

Answer: A

NEW QUESTION 40
Which Cortex XDR capability extends investigations to an endpoint?

A. Log Stitching
B. Causality Chain
C. Sensors
D. Live Terminal

Answer: A

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-conc

NEW QUESTION 42
Which two log types should be configured for firewall forwarding to the Cortex Data Lake for use by Cortex XDR? (Choose two)

A. Security Event
B. HIP
C. Correlation
D. Analytics

Answer: AB

NEW QUESTION 45
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

Answer: C

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-corte

NEW QUESTION 50
.....

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