Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

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

NEW QUESTION 1
Which two filter operators are available in Cortex XDR? (Choose two.)

A. < >
B. Contains
C. =
D. Is Contained By

Answer: BC

NEW QUESTION 2
Which four types of Traps logs are stored within Cortex Data Lake?

A. Threat, Config, System, Data
B. Threat, Config, System, Analytic
C. Threat, Monito
D. System, Analytic
E. Threat, Config, Authentication, Analytic

Answer: B

NEW QUESTION 3
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 4
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

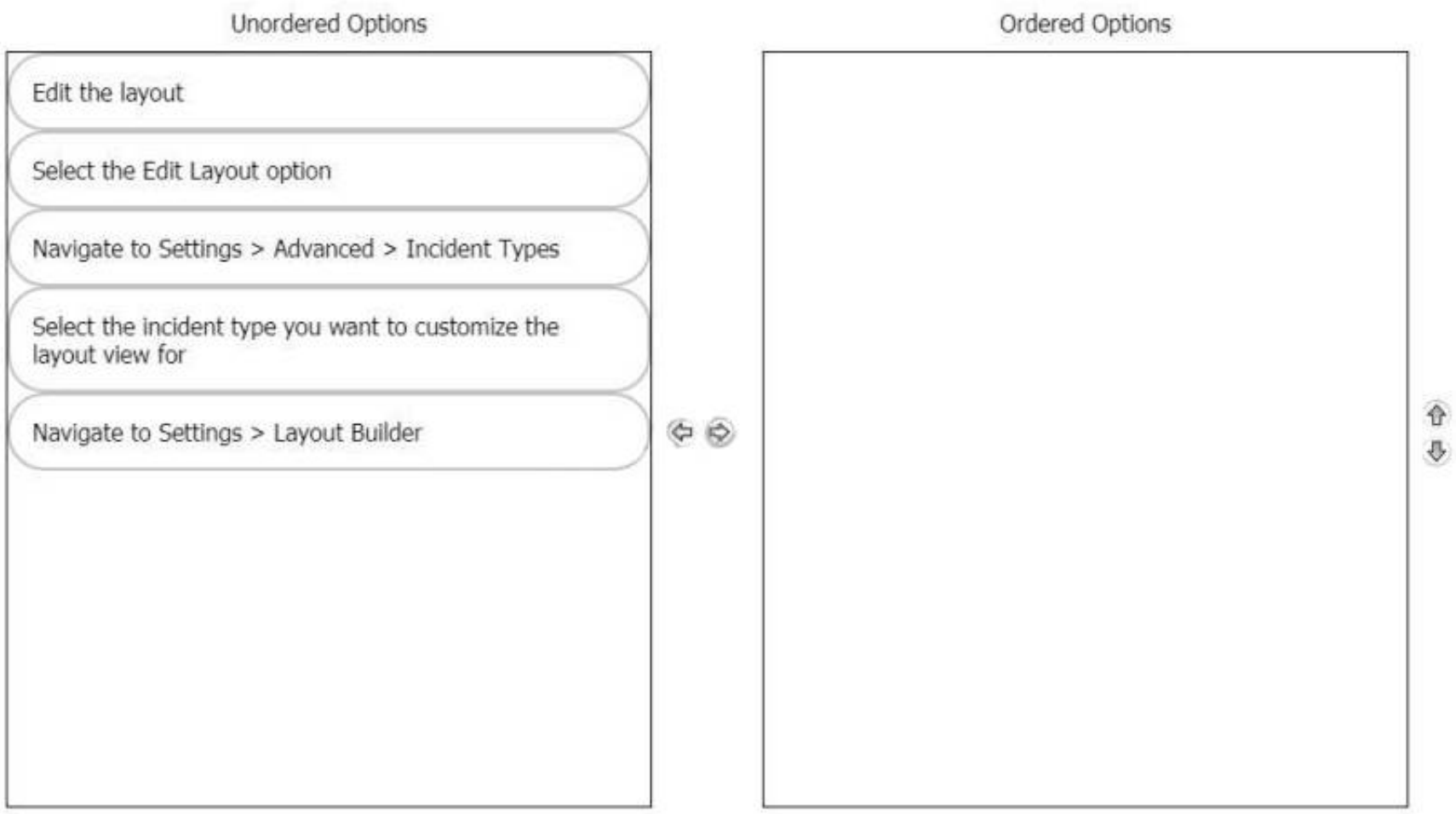
Answer: C

NEW QUESTION 5
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 6
Rearrange the steps into the correct order for modifying an incident layout.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 7
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 8
In the DBotScore context field, which context key would differentiate between multiple entries for the same indicator in a multi-TIP environment?

A. Vendor
B. Type
C. Using
D. Brand

Answer: A

NEW QUESTION 9
How can you view all the relevant incidents for an indicator?

A. Linked Incidents column in Indicator Screen
B. Linked Indicators column in Incident Screen
C. Related Indicators column in Incident Screen

D. Related Incidents column in Indicator Screen

Answer: D

NEW QUESTION 10
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 10
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 11
When analyzing logs for indicators, which are used for only BIOC identification'?

A. observed activity
B. artifacts
C. techniques
D. error messages

Answer: C

NEW QUESTION 16
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 21
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 22
An administrator of a Cortex XDR protected production environment would like to test its ability to protect users from a known flash player exploit.
What is the safest way to do it?

A. The administrator should attach a copy of the weapomzed flash file to an email, send the email to a selected group of employees, and monitor the Events tab on the Cortex XDR console
B. The administrator should use the Cortex XDR tray icon to confirm his corporate laptop is fully protected then open the weaponized flash file on his machine, and monitor the Events tab on the Cortex XDR console.
C. The administrator should create a non-production Cortex XDR test environment that accurately represents the production environment, introduce the weaponized flash file, and monitor the Events tab on the Cortex XDR console.
D. The administrator should place a copy of the weaponized flash file on several USB drives, scatter them around the office and monitor the Events tab on the Cortex XDR console

Answer: C

NEW QUESTION 24
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 26
If you have a playbook task that errors out. where could you see the output of the task?

A. /var/log/messages
B. War Room of the incident
C. Demisto Audit log
D. Playbook Editor

Answer: B

NEW QUESTION 28
.....

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