Free Questions for PSE-Cortex by ebraindumps

Shared by Carpenter on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

A- 1 TB

B- 10 GB

C- 100 GB

D- 10 TB

Answer:

C

Question 2

Question Type: **MultipleChoice**

What are process exceptions used for?

Options:

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

Question 3

Question Type: **MultipleChoice**

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'?

Options:

A- Uncommon Local Scheduled Task Creation

B- Malware

C- New Administrative Behavior

D- DNS Tunneling

Answer:

B

Question 4

Question Type: **MultipleChoice**

A customer wants to modify the retention periods of their Threat logs in Cortex Data Lake.

Where would the user configure the ratio of storage for each log type?

Options:

A- Within the TMS, create an agent settings profile and modify the Disk Quota value

B- It is not possible to configure Cortex Data Lake quota for specific log types.

C- Go to the Cortex Data Lake App in Cloud Services, then choose Configuration and modify the Threat Quota

D- Write a GPO for each endpoint agent to check in less often

Answer:

C

Question 5

Question Type: **MultipleChoice**

Which two types of IOCs are available for creation in Cortex XDR? (Choose two.)

Options:

A- IP

B- endpoint hostname

C- domain

D- registry entry

Answer:

A, C

Question 6

Question Type: MultipleChoice

Which Cortex XDR capability extends investigations to an endpoint?

Options:

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-concepts

Question 7

Question Type: MultipleChoice

An Administrator is alerted to a Suspicious Process Creation security event from multiple users.

The users believe that these events are false positives Which two steps should the administrator take to confirm the false positives and create an exception? (Choose two)

Options:

A- With the Malware Security profile, disable the 'Prevent Malicious Child Process Execution' module

B- Within the Malware Security profile add the specific parent process, child process, and command line argument to the child process whitelist

C- In the Cortex XDR security event, review the specific parent process, child process, and command line arguments

D- Contact support and ask for a security exception.

Answer:

B, C