Free Questions for PCDRA by ebraindumps

Shared by Hester on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following policy exceptions applies to the following description?

'An exception allowing specific PHP files'

Options:

A- Support exception

B- Local file threat examination exception

C- Behavioral threat protection rule exception

D- Process exception

Answer:

B

Question 2

Question Type: **MultipleChoice**

Which statement best describes how Behavioral Threat Protection (BTP) works?

Options:

A- BTP injects into known vulnerable processes to detect malicious activity.

B- BTP runs on the Cortex XDR and distributes behavioral signatures to all agents.

C- BTP matches EDR data with rules provided by Cortex XDR.

D- BTP uses machine Learning to recognize malicious activity even if it is not known.

Answer:

D

Question 3

Question Type: **MultipleChoice**

Which of the following best defines the Windows Registry as used by the Cortex XDR agent?

Options:

A- a hierarchical database that stores settings for the operating system and for applications

B- a system of files used by the operating system to commit memory that exceeds the available hardware resources. Also known as the "swap"

C- a central system, available via the internet, for registering officially licensed versions of software to prove ownership

D- a ledger for maintaining accurate and up-to-date information on total disk usage and disk space remaining available to the operating system

Answer:

A

Question 4

Question Type: **MultipleChoice**

A Linux endpoint with a Cortex XDR Pro per Endpoint license and Enhanced Endpoint Data enabled has reported malicious activity, resulting in the creation of a file that you wish to delete. Which action could you take to delete the file?

Options:

A- Manually remediate the problem on the endpoint in question.

B- Open X2go from the Cortex XDR console and delete the file via X2go.

C- Initiate Remediate Suggestions to automatically delete the file.

D- Open an NFS connection from the Cortex XDR console and delete the file.

Answer:

A

Question 5

Question Type: **MultipleChoice**

What is the function of WildFire for Cortex XDR?

Options:

A- WildFire runs in the cloud and analyses alert data from the XDR agent to check for behavioural threats.

B- WildFire is the engine that runs on the local agent and determines whether behavioural threats are occurring on the endpoint.

C- WildFire accepts and analyses a sample to provide a verdict.

D- WildFire runs entirely on the agent to quickly analyse samples and provide a verdict.

Answer:

C

Question 6

Question Type: **MultipleChoice**

Which statement regarding scripts in Cortex XDR is true?

Options:

A- Any version of Python script can be run.

B- The level of risk is assigned to the script upon import.

C- Any script can be imported including Visual Basic (VB) scripts.

D- The script is run on the machine uploading the script to ensure that it is operational.

Answer:

A

Question 7

Question Type: **MultipleChoice**

When creating a scheduled report which is not an option?

Options:

A- Run weekly on a certain day and time.

B- Run quarterly on a certain day and time.

C- Run monthly on a certain day and time.

D- Run daily at a certain time (selectable hours and minutes).

Answer:

B

Question 8

Question Type: MultipleChoice

What is the purpose of the Cortex Data Lake?

Options:

A- a local storage facility where your logs and alert data can be aggregated

B- a cloud-based storage facility where your firewall logs are stored

C- the interface between firewalls and the Cortex XDR agents

D- the workspace for your Cortex XDR agents to detonate potential malware files

Answer:

B

Question 9

Question Type: MultipleChoice

When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

Options:

A- Remediation Automation

B- Machine Remediation

C- Automatic Remediation

D- Remediation Suggestions

Answer:

D

Question 10

Question Type: **MultipleChoice**

As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to open a malicious Word document. You learn from the WildFire report and AutoFocus that this document is known to have been used in Phishing campaigns since 2018. What steps can you take to ensure that the same document is not opened by other users in your organization protected by the Cortex XDR agent?

Options:

A- Enable DLL Protection on all endpoints but there might be some false positives.

B- Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.

C- No step is required because Cortex shares IOCs with our fellow Cyber Threat Alliance members.

D- No step is required because the malicious document is already stopped.

Answer:

B

20%
DISCOUNT