PCDRA Q&As

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

QUESTION 1

In Windows and macOS you need to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. What is one way to add an exception for the singer?

A. In the Restrictions Profile, add the file name and path to the Executable Files allow list.

B. Create a new rule exception and use the singer as the characteristic.

C. Add the signer to the allow list in the malware profile.

D. Add the signer to the allow list under the action center page.

Correct Answer: C

QUESTION 2

Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

A. Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list.

B. From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.

C. Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.

D. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the

list, and apply it.

Correct Answer: B

QUESTION 3

What is by far the most common tactic used by ransomware to shut down a victim\\'s operation?

A. preventing the victim from being able to access APIs to cripple infrastructure

B. denying traffic out of the victims network until payment is received

C. restricting access to administrative accounts to the victim

D. encrypting certain files to prevent access by the victim

Correct Answer: D

QUESTION 4

With a Cortex XDR Prevent license, which objects are considered to be sensors?

A. Syslog servers

B. Third-Party security devices

C. Cortex XDR agents

D. Palo Alto Networks Next-Generation Firewalls

Correct Answer: C

QUESTION 5

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

A. Remediation Automation

B. Machine Remediation

C. Automatic Remediation

D. Remediation Suggestions

Correct Answer: D

QUESTION 6

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATTandCKTM techniques.

A. Exfiltration, Command and Control, Collection

B. Exfiltration, Command and Control, Privilege Escalation

C. Exfiltration, Command and Control, Impact

D. Exfiltration, Command and Control, Lateral Movement

Correct Answer: D

QUESTION 7

Which engine, of the following, in Cortex XDR determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident?

A. Sensor Engine

B. Causality Analysis Engine

C. Log Stitching Engine

D. Causality Chain Engine

Correct Answer: B

QUESTION 8

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?

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.

Correct Answer: A

QUESTION 9

What is the purpose of the Unit 42 team?

A. Unit 42 is responsible for automation and orchestration of products

B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server

C. Unit 42 is responsible for threat research, malware analysis and threat hunting

D. Unit 42 is responsible for the rapid deployment of Cortex XDR agents

Correct Answer: C

QUESTION 10

What is the purpose of the Cortex Data Lake?

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

Correct Answer: B