Practice Exam Questions

Palo Alto Networks Certified Detection and Remediation Analyst

EXAMKILLER

Help Pass Your Exam At First Try

Paloalto Networks

Exam PCDRA

Palo Alto Networks Certified Detection and Remediation Analyst

Version: 3.0

[Total Questions: 60]

Question No : 1

While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires anexclusion. What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?

A. mark the incident as Unresolved
B. create a BIOC rule excluding this behavior
C. create an exception to prevent future false positives
D. mark the incident as Resolved – False Positive

Answer: D
Reference:https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/alert-exclusions/add-an-alert-exclusion.html

Question No : 2

To create a BIOC rule with XQL query you must at a minimum filter on which field inorder for it to be a valid BIOC rule?

A. causality_chain
B. endpoint_name
C. threat_event
D. event_type

Answer: D
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs/create-a-bioc-rule.html

Question No : 3

After scan, how does file quarantine function work on an endpoint?

A. Quarantine takes ownership of the files and folders and prevents execution through access control.
B. Quarantine disables the network adapters and locks down access preventing any

communications with the endpoint.
C. Quarantine removes a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.
D. Quarantine prevents an endpoint from communicating with anything besides the listed exceptions in the agent profile and Cortex XDR.

Answer: C
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/investigation-and-response/investigate-files/manage-quarantined-files

Question No : 4

Which statement is true for Application Exploits and Kernel Exploits?

A. The ultimate goal of any exploit is to reach the application.
B. Kernel exploits are easier to prevent then application exploits.
C. The ultimate goal of any exploit is to reach the kernel.
D. Application exploits leverage kernel vulnerability.

Answer: A
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/about-cortex-xdr-protection.html

Question No : 5

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

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
Reference: https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users

Question No : 6

What kind of the threat typically encrypts userfiles?

A. ransomware
B. SQL injection attacks
C. Zero-day exploits
D. supply-chain attacks

Answer: A
Reference: https://www.proofpoint.com/us/threat-reference/ransomware#:~:text=Ransomware%20is%20a%20type%20of,ransom%20fee%20to%20the%20attacker

Question No : 7

A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

A. It is true positive.
B. It is false positive.
C. It is a false negative.
D. It is true negative.

Answer: B
Reference: https://live.paloaltonetworks.com/t5/cortex-xdr-discussions/cortex-xdr-false-positive-cloud2model-manager-1-005/td-p/391391

Question No : 8

LiveTerminal uses which type of protocol to communicate with the agent on the endpoint?

A. NetBIOS over TCP
B. WebSocket
C. UDP and a random port

D. TCP, over port 80

Answer: B

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/communication-between-cortex-xdr-and-agents.html

Question No : 9

What are two purposes of “Respond to Malicious Causality Chains” in a Cortex XDR Windows Malware profile? (Choose two.)

A. Automatically close the connections involved in malicious traffic.
B. Automatically kill the processes involved in malicious activity.
C. Automatically terminate the threads involved in malicious activity.
D. Automaticallyblock the IP addresses involved in malicious traffic.

Answer: A,D

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/endpoint-security-profiles/add-malware-security-profile.html#:~:text=With%20Behavioral

%20threat%20protection%2C%20the,appear%20legitimate%20if%20inspected%20individually

Question No : 10

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

‘An exception allowing specific PHP files’

A. Support exception
B. Local file threat examination exception
C. Behavioral threat protection rule exception
D. Process exception

Answer: B

Question No : 11

Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

A. Security Manager Dashboard
B. Data Ingestion Dashboard
C. Security Admin Dashboard
D. Incident Management Dashboard

Answer: A
Reference:https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-release-notes/release-information/features-introduced/features-introduced-in-2021.html

Question No : 12

When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

A. Assign incidents to an analyst in bulk.
B. Change the status of multiple incidents.
C. Investigate several Incidents at once.
D. Delete the selected Incidents.

Answer: A,B
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-release-notes/release-information/features-introduced/features-introduced-in-2021.html

Question No : 13

Which of the following represents the correct relation of alerts to incidents?

A. Only alerts with thesame host are grouped together into one Incident in a given time frame.
B. Alerts that occur within a three hour time frame are grouped together into one Incident.
C. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.
D. Every alert creates a new Incident.

Answer: A
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-incidents/cortex-xdr-incidents.html

Question No : 14

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

A. Broker VM Pathfinder
B. Local Agent Proxy
C. Local Agent Installer and Content Caching
D. Broker VM Syslog Collector

Answer: C
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/broker-vm/set-up-broker-vm/activate-the-agent-proxy-for-closed-networks.html

Question No : 15

When creating a custom XQL query in a dashboard, how would a user save that XQL query to the Widget Library?

A. Click the three dots on the widget andthen choose “Save” and this will link the query to the Widget Library.
B. This isn’t supported, you have to exit the dashboard and go into the Widget Library first to create it.
C. Click on “Save to Action Center” in the dashboard and you will be promptedto give the query a name and description.
D. Click on “Save to Widget Library” in the dashboard and you will be prompted to give the query a name and description.

Answer: D
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/monitoring/cortex-xdr-dashboard/widget-library.html