Palo Alto Networks

PCDRA

Palo Alto Networks Certified Detection and Remediation Analyst

QUESTION & ANSWERS

Question: 1

In incident-related widgets, how would you filter the display to only show incidents that were “starred”?

A. Create a custom XQL widget

B. This is not currently supported

C. Create a custom report and filter on starred incidents

D. Click the star in the widget

Answer: D

Explanation/Reference:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/monitoring/cortexxdr-dashboard/predefined-dashboards.html#:~:text=To filter a widget to,until you clear the star

To filter a widget to display only incidents that match incident starring policies, select the star in the right corner. A purple star indicates that the widget is displaying only starred incidents. The starring filter is persistent and will continue to show the filtered results until you clear the star.

Question: 2

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

Answer: B

Explanation/Reference:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/ cortex-xdr-concepts.html

XDR

With Endpoint Detection and Response (EDR), enterprises rely on endpoint data as a means to trigger cybersecurity incidents. As cybercriminals and their tactics have become more sophisticated, the time to identify and contain breaches has only increased. Extended Detection and Response (XDR) goes beyond the traditional EDR approach of using only endpoint data to identify and respond to threats by applying machine learning across all your enterprise, network, cloud, and endpoint data. This approach enables you to quickly find and stop targeted attacks and insider abuse and remediate compromised endpoints.

Question: 3

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

Answer: D

Explanation/Reference:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-andresponse/response-actions/remediate-endpoints.html

When investigating suspicious incidents and causality chains you often need to restore and revert changes made to your endpoints as result of a malicious activity. To avoid manually searching for the affected files and registry keys on your endpoints, you can request Cortex XDR for remediation suggestions.

Cortex XDR investigates suspicious causality process chains and incidents on your endpoints and displays a list of suggested actions to remediate processes, files and registry keys on your endpoint.

To initiate remediation suggestions, you must meet the following requirements:

- Cortex XDR Pro per Endpoint license
- An `App Administrator`, `Privileged Responder`, or `Privileged Security Admin` role permissions which include the remediation permissions
- EDR data collection enabled
- Cortex XDR agent version 7.2 and above on Windows endpoints

Question: 4

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATT&CKTM 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

Answer: D

Question: 5

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

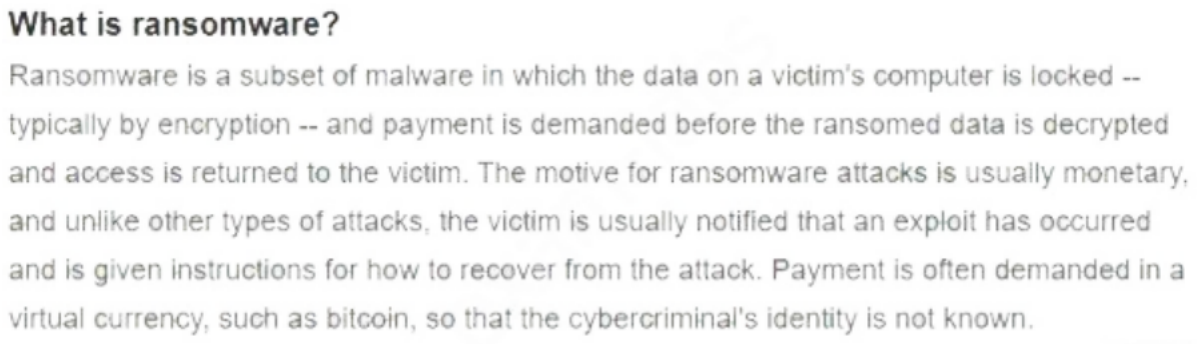
C. restricting access to administrative accounts to the victim

D. encrypting certain files to prevent access by the victim

Answer: D

Explanation/Reference:

Reference: https://www.techtarget.com/searchsecurity/definition/ransomware



What is ransomware?

Ransomware is a subset of malware in which the data on a victim's computer is locked -- typically by encryption -- and payment is demanded before the ransomed data is decrypted and access is returned to the victim. The motive for ransomware attacks is usually monetary, and unlike other types of attacks, the victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in a virtual currency, such as bitcoin, so that the cybercriminal's identity is not known.

Question: 6

What license would be required for ingesting external logs from various vendors?

A. Cortex XDR Pro per Endpoint

B. Cortex XDR Vendor Agnostic Pro

C. Cortex XDR Pro per TB

D. Cortex XDR Cloud per Host

Answer: C

Explanation/Reference:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/external-data-ingestion/ about-external-data-ingestion.html