

Latest Version: 6.0

Question: 1

Phishing belongs which of the following MITRE ATT&CK tactics?

- A. Initial Access, Persistence
- B. Persistence, Command and Control
- C. Reconnaissance, Persistence
- D. Reconnaissance, Initial Access

Answer: D

Explanation:

Reference: <https://attack.mitre.org/techniques/T1566/>

Question: 2

When creating a BIOC rule, which XQL query can be used?

- A.
dataset = xdr_data
| filter event_sub_type = PROCESS_START and
action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
- B.
dataset = xdr_data
| filter event_type = PROCESS and
event_sub_type = PROCESS_START and
action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
- C.
dataset = xdr_data
| filter action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"
| fields action_process_image
- D.
dataset = xdr_data
| filter event_behavior = true
event_sub_type = PROCESS_START and
action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

Answer: B

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigationand->

Question: 3

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

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-release-notes/releaseinformation/features-introduced/features-introduced-in-2021.html>

Question: 4

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. Automatically block the IP addresses involved in malicious traffic.

Answer: A, D

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpointsecurity/>
<https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpointsecurity-profiles/add-malware-security-profile.html#:~:text=With%20Behavioral%20threat%20protection%2C%20the,appear%20legitimate%20if%20inspected%20individually>

Question: 5

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 and then 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 prompted to 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

Explanation:

Reference: <https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-proadmin/monitoring/cortex-xdr-dashboard/widget-library.html>