Palo Alto Networks
XDR-Analyst
Palo Alto Networks XDR Analyst

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**



Latest Version: 6.0

Question: 1

Phishing belongs to 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:
Phishing is a technique that belongs to two MITRE ATT&CK tactics: Reconnaissance and Initial Access. Reconnaissance is the process of gathering information about a target before launching an attack. Phishing for information is a sub-technique of Reconnaissance that involves sending phishing messages to elicit sensitive information that can be used during targeting. Initial Access is the process of gaining a foothold in a network or system. Phishing is a sub-technique of Initial Access that involves sending phishing messages to execute malicious code on victim systems. Phishing can be used for both Reconnaissance and Initial Access depending on the objective and content of the phishing message. Reference:
Phishing, Technique T1566 - Enterprise | MITRE ATT&CK® 1
Phishing for Information, Technique T1598 - Enterprise | MITRE ATT&CK® 2
Phishing for information, Part 2: Tactics and techniques 3
PHISHING AND THE MITREATT&CK FRAMEWORK - EnterpriseTalk 4
Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK® 5

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:
A BIOC rule is a custom detection rule that uses the Cortex Query Language (XQL) to define the behavior or actions that indicate a potential threat. A BIOC rule can use the xdr_data and cloud_audit_log datasets and presets for these datasets. A BIOC rule can also use the filter stage, alter stage, and functions without any aggregations in the XQL query. The query must return a single field named action_process_image, which is the process image name of the suspicious process. The query must also include the event_type and event_sub_type fields in the filter stage to specify the type and sub-type of the event that triggers the rule.
Option B is the correct answer because it meets all the requirements for a valid BIOC rule query. It uses the xdr_data dataset, the filter stage, the event_type and event_sub_type fields, and the action_process_image_name field with a regular expression to match any process image name that ends with .pdf.exe or .docx.exe, which are common indicators of malicious files.
Option A is incorrect because it does not include the event_type field in the filter stage, which is mandatory for a BIOC rule query.
Option C is incorrect because it does not include the event_type and event_sub_type fields in the filter stage, and it uses the fields stage, which is not supported for a BIOC rule query. It also returns the action_process_image field instead of the action_process_image_name field, which is the expected output for a BIOC rule query.
Option D is incorrect because it uses the event_behavior field, which is not supported for a BIOC rule query. It also does not include the event_type field in the filter stage, and it uses the event_sub_type field incorrectly. The event_sub_type field should be equal to PROCESS_START, not true.
Reference:
Working with BIOCs
Cortex Query Language (XQL) Reference

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: D

Explanation:
The Incident Management Dashboard provides a high-level overview of the incident response process,

including the Mean Time to Resolution (MTTR) metric. This metric measures the average time it takes to resolve an incident from the moment it is created to the moment it is closed. The dashboard also shows the number of incidents by status, severity, and assigned analyst, as well as the top alerts by category, source, and destination. The Incident Management Dashboard is designed for executives and managers who want to monitor the performance and efficiency of their security teams. Reference: [PCDRA Study Guide], page 18.

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: B, D

Explanation:
The “Respond to Malicious Causality Chains” feature in a Cortex XDR Windows Malware profile allows the agent to take automatic actions against network connections and processes that are involved in malicious activity on the endpoint. The feature has two modes: Block IP Address and Kill Process1.
The two purposes of “Respond to Malicious Causality Chains” in a Cortex XDR Windows Malware profile are:
Automatically kill the processes involved in malicious activity. This can help to stop the malware from spreading or doing any further damage.
Automatically block the IP addresses involved in malicious traffic. This can help to prevent the malware from communicating with its command and control server or other malicious hosts.
The other two options, automatically close the connections involved in malicious traffic and automatically terminate the threads involved in malicious activity, are not specific to “Respond to Malicious Causality Chains”. They are general security measures that the agent can perform regardless of the feature.
Reference:
Cortex XDR Agent Security Profiles
Cortex XDR Agent 7.5 Release Notes
PCDRA: What are purposes of “Respond to Malicious Causality Chains” in …

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:
To save a custom XQL query to the Widget Library, you need to click on "Save to Widget Library" in the dashboard and you will be prompted to give the query a name and description. This will allow you to reuse the query in other dashboards or reports. You cannot save a query to the Widget Library by clicking the three dots on the widget, as this will only give you options to edit, delete, or clone the widget. You also cannot save a query to the Action Center, as this is a different feature that allows you to create alerts or remediation actions based on the query results. You do not have to exit the dashboard and go into the Widget Library first to create a query, as you can do it directly from the dashboard. Reference:
Cortex XDR Pro Admin Guide: Save a Custom Query to the Widget Library
Cortex XDR Pro Admin Guide: Create a Dashboard

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/