



**Vendor:** Palo Alto Networks

**Exam Code:** PCDDRA

**Exam Name:** Palo Alto Networks Certified Detection and Remediation Analyst

**Version:** DEMO

### 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:

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.

### 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.

### 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:**

Mean Time to Resolution (MTTR) metric are inside Security Admin Dashboard.

#### 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:** AD

**Explanation:**

When the Cortex XDR agent identifies a remote network connection that attempts to perform malicious activity - such as encrypting endpoint files - the agent can automatically block the IP address to close all existing communication and block new connections from this IP address to the endpoint. When Cortex XDR blocks an IP address per endpoint, that address remains blocked throughout all agent profiles and policies, including any host-firewall policy rules. You can view the list of all blocked IP addresses per endpoint from the Action Center, as well as unblock them to re-enable communication as appropriate.

#### 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.

#### 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:**

Ingesting Logs and Data from external sources requires a Cortex XDR Pro per GB license. To receive Syslog data from an external source, you must first set up the Syslog Collector applet on a Broker VM within your network.

#### QUESTION 7

An attacker tries to load dynamic libraries on macOS from an unsecure location. Which Cortex XDR module can prevent this attack?

- A. DDL Security
- B. Hot Patch Protection
- C. Kernel Integrity Monitor (KIM)
- D. Dylib Hijacking

**Answer: D**

**Explanation:**

Prevents Dylib-hijacking attacks where the attacker attempts to load dynamic libraries on Mac operating systems from unsecured locations to gain control of a process.

<https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Prevent-Administrator-Guide/Endpoint-Protection-Modules>

#### QUESTION 8

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

**Answer: C**

**Explanation:**

Unit 42 is the threat intelligence and response team of Palo Alto Networks. The purpose of Unit 42 is to collect and analyze the most up-to-date threat intelligence and apply it to respond to cyberattacks. Unit 42 is composed of world-renowned threat researchers, incident responders and security consultants who help organizations proactively manage cyber risk. Unit 42 is responsible for threat research, malware analysis and threat hunting, among other activities.

#### QUESTION 9

Which Type of IOC can you define in Cortex XDR?

- A. destination port
- B. e-mail address
- C. full path
- D. App-ID

**Answer: C**

**Explanation:**

Explain the purpose and use of the IOC technique

Indicators of compromise (IOCs) are the artifacts that are considered malicious or suspicious.

IOCs are static and based on criteria such as:

- Full path
- File name
- Domain
- Destination IP address
- MD5 hash
- SHA-256

**QUESTION 10**

When viewing the incident directly, what is the "assigned to" field value of a new Incident that was just reported to Cortex?

- A. Pending
- B. It is blank
- C. Unassigned
- D. New

**Answer: C**

**Explanation:**

Assigned To: The user to which the incident is assigned. The assignee tracks which analyst is responsible for investigating the threat. Incidents that have not been assigned have a status of Unassigned.

<https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Incidents>

**QUESTION 11**

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:**

To filter the display to only show incidents that were "starred", you need to click the star in the widget. This will apply a filter that shows only the incidents that contain a starred alert, which is an alert that matches a specific condition that you define in the incident starring configuration. You can use the incident starring feature to prioritize and focus on the most important or relevant incidents in your environment.

### QUESTION 12

Where would you view the WildFire report in an incident?

- A. next to relevant Key Artifacts in the incidents details page
- B. under Response --> Action Center
- C. under the gear icon --> Agent Audit Logs
- D. on the HUB page at apps.paloaltonetworks.com



**Answer: A**

#### Explanation:

The WildFire verdict displays next to relevant Key Artifacts in the incidents details page, the causality view, and within the Live Terminal view of processes.

### QUESTION 13

What does the following output tell us?

 <b>Top Hosts (Top 10   Last 30 days)</b> 		
HOST NAME	INCIDENTS BREAKDOWN	
shpapy_win10	6	[ 5 1 ]
win7mickey	5	[ 5 ]
desktop-vjb9012	5	[ 4 1 ]
cpasp-enzo	4	[ 3 1 ]
win10lab-thomas	3	[ 3 ]
pure_windows_10	3	[ 3 ]
lab1-8-cpasp	3	[ 3 ]
guru-pf	3	[ 3 ]
roneytestwindow	3	[ 3 ]
erikj-cpasp	3	[ 3 ]

- A. There is one low severity incident.
- B. Host shpapy\_win10 had the most vulnerabilities.

- C. There is one informational severity alert.
- D. This is an actual output of the Top 10 hosts with the most malware.

**Answer: A**

**Explanation:**

The blue color codes for low severity incidents.

#### QUESTION 14

What is the standard installation disk space recommended to install a Broker VM?

- A. 1GB disk space
- B. 2GB disk space
- C. 512GB disk space
- D. 256GB disk space

**Answer: C**

**Explanation:**

Before you set up the broker VM, verify you meet the following requirements.

Hardware: For standard installation, use a minimum of a 4-core processor, 8GB RAM, and 512GB disk. If you only intend to use the broker VM for agent proxy, you can use a 2-core processor. If you intend to use the broker VM for agent installer and content caching, you must use an 8-core processor.

#### QUESTION 15

Where can SHA256 hash values be used in Cortex XDR Malware Protection Profiles?

- A. in the macOS Malware Protection Profile to indicate allowed signers
- B. in the Linux Malware Protection Profile to indicate allowed Java libraries
- C. SHA256 hashes cannot be used in Cortex XDR Malware Protection Profiles
- D. in the Windows Malware Protection Profile to indicate allowed executables

**Answer: D**

**Explanation:**

Create a Rule Exception based on the PROCESS SHA256 field for IO rules that hit more than 100 endpoints over a 72-hour period.

[https://www.paloaltonetworks.com/content/dam/pan/en\\_US/assets/pdf/datasheets/education/pcdra-study-guide.pdf](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcdra-study-guide.pdf)

## Thank You for Trying Our Product

### Braindump2go Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.braindump2go.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER  
NETWORKS



EMC<sup>2</sup>  
where information lives

**10% Discount Coupon Code: ASTR14**