PCDRA Q&As

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/pcdra.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

QUESTION 1

Phishing belongs which of the following MITRE ATTandCK tactics?

A. Initial Access, Persistence

B. Persistence, Command and Control

C. Reconnaissance, Persistence

D. Reconnaissance, Initial Access

Correct Answer: D

QUESTION 2

You can star security events in which two ways? (Choose two.)

A. Create an alert-starring configuration.

B. Create an Incident-starring configuration.

C. Manually star an alert.

D. Manually star an Incident.

Correct Answer: BD

QUESTION 3

What functionality of the Broker VM would you use to ingest third-party firewall logs to the Cortex Data Lake?

A. Netflow Collector

B. Syslog Collector

C. DB Collector

D. Pathfinder

Correct Answer: B

QUESTION 4

Which Type of IOC can you define in Cortex XDR?

A. destination port

B. e-mail address

C. full path

D. App-ID

Correct Answer: C

QUESTION 5

While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion. 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

Correct Answer: D

QUESTION 6

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

Correct Answer: D

QUESTION 7

Which statement best describes how Behavioral Threat Protection (BTP) works?

A. BTP injects into known vulnerable processes to detect malicious activity.

B. BTP runs on the Cortex XDR and distributes behavioral signatures to all agents.

C. BTP matches EDR data with rules provided by Cortex XDR.

D. BTP uses machine Learning to recognize malicious activity even if it is not known.

Correct Answer: D

QUESTION 8

Live Terminal 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

Correct Answer: B

QUESTION 9

When is the wss (WebSocket Secure) protocol used?

A. when the Cortex XDR agent downloads new security content

B. when the Cortex XDR agent uploads alert data

C. when the Cortex XDR agent connects to WildFire to upload files for analysis

D. when the Cortex XDR agent establishes a bidirectional communication channel

Correct Answer: D

QUESTION 10

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.

Correct Answer: AB