PCDRA$^{\text{Q\&As}}$

Palo Alto Networks Certified Detection and Remediation Analyst

Pass Palo Alto Networks PCDRA Exam with 100% Guarantee

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

QUESTION 1

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

A. Broker VM Pathfinder

B. Local Agent Proxy

C. Local Agent Installer and Content Caching

D. Broker VM Syslog Collector

Correct Answer: C

QUESTION 2

What is the function of WildFire for Cortex XDR?

A. WildFire runs in the cloud and analyses alert data from the XDR agent to check for behavioural threats.

B. WildFire is the engine that runs on the local agent and determines whether behavioural threats are occurring on the endpoint.

C. WildFire accepts and analyses a sample to provide a verdict.

D. WildFire runs entirely on the agent to quickly analyse samples and provide a verdict.

Correct Answer: C

QUESTION 3

With a Cortex XDR Prevent license, which objects are considered to be sensors?

A. Syslog servers

B. Third-Party security devices

C. Cortex XDR agents

D. Palo Alto Networks Next-Generation Firewalls

Correct Answer: C

QUESTION 4

Which of the following best defines the Windows Registry as used by the Cortex XDR agent?

A. a hierarchical database that stores settings for the operating system and for applications

B. a system of files used by the operating system to commit memory that exceeds the available hardware resources. Also known as the "swap"

C. a central system, available via the internet, for registering officially licensed versions of software to prove ownership

D. a ledger for maintaining accurate and up-to-date information on total disk usage and disk space remaining available to the operating system

Correct Answer: A

QUESTION 5

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

Correct Answer: D

QUESTION 6

Which statement is true for Application Exploits and Kernel Exploits?

A. The ultimate goal of any exploit is to reach the application.

B. Kernel exploits are easier to prevent then application exploits.

C. The ultimate goal of any exploit is to reach the kernel.

D. Application exploits leverage kernel vulnerability.

Correct Answer: A

QUESTION 7

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 8

When creating a scheduled report which is not an option?

A. Run weekly on a certain day and time.

B. Run quarterly on a certain day and time.

C. Run monthly on a certain day and time.

D. Run daily at a certain time (selectable hours and minutes).

Correct Answer: B

QUESTION 9

What kind of the threat typically encrypts user files?

A. ransomware

B. SQL injection attacks

C. Zero-day exploits

D. supply-chain attacks

Correct Answer: A

QUESTION 10

After scan, how does file quarantine function work on an endpoint?

A. Quarantine takes ownership of the files and folders and prevents execution through access control.

B. Quarantine disables the network adapters and locks down access preventing any communications with the endpoint.

C. Quarantine removes a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.

D. Quarantine prevents an endpoint from communicating with anything besides the listed exceptions in the agent profile and Cortex XDR.

Correct Answer: C