Vendor: Palo Alto Networks

Exam Code:PCDRA

Exam Name: Palo Alto Networks Certified Detection and Remediation Analyst

Version: Demo

QUESTION 1

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

Correct Answer: C

QUESTION 2

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

Correct Answer: D

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

How does Cortex XDR agent for Windows prevent ransomware attacks from compromising the file system?

A. by encrypting the disk first.

B. by utilizing decoy Files.

C. by retrieving the encryption key.

D. by patching vulnerable applications.

Correct Answer: B

QUESTION 5

What is the purpose of targeting software vendors in a supply-chain attack?

A. to take advantage of a trusted software delivery method.

B. to steal users\\' login credentials.

C. to access source code.

D. to report Zero-day vulnerabilities.

Correct Answer: B

QUESTION 6

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

Correct Answer: B

QUESTION 7

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

Correct Answer: C

QUESTION 8

Which profiles can the user use to configure malware protection in the Cortex XDR console?

A. Malware Protection profile

B. Malware profile

C. Malware Detection profile

D. Anti-Malware profile

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

Which statement regarding scripts in Cortex XDR is true?

A. Any version of Python script can be run.

B. The level of risk is assigned to the script upon import.

C. Any script can be imported including Visual Basic (VB) scripts.

D. The script is run on the machine uploading the script to ensure that it is operational.

Correct Answer: A

QUESTION 11

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 12

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