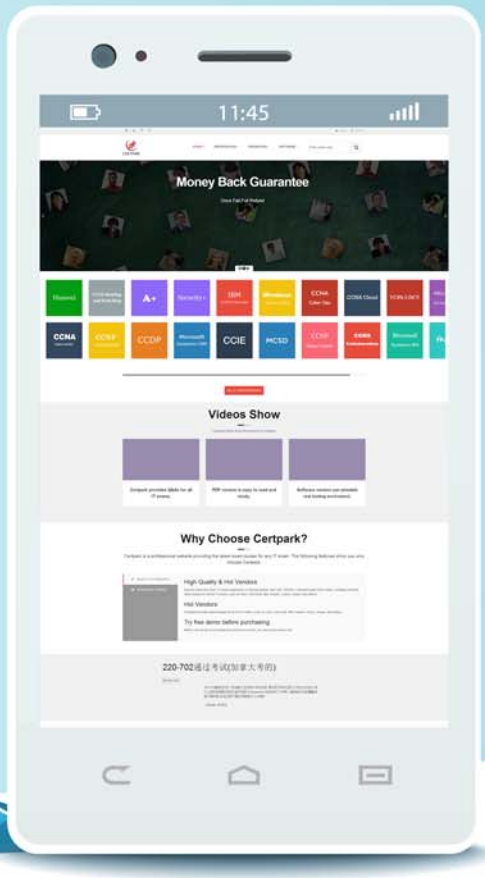
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **PCDRA**

Title : Palo Alto Networks Certified Detection and Remediation Analyst

Version : DEMO

1.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
Answer: D
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/investigate-endpoint-alerts/alert-exclusions/add-an-alert-exclusion.html

2.To create a BIOC rule with XQL query you must at a minimum filter on which field inorder for it to be a valid BIOC rule?
A. causality_chain
B. endpoint_name
C. threat_event
D. event_type
Answer: D
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xdr-indicators/working-with-biocs/create-a-bioc-rule.html

3.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.
Answer: C
Explanation:
Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/investigation-and-response/investigate-files/manage-quarantined-files

4.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.
Answer: A
Explanation:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/about-cortex-xdr-protection.html

5.Which of the following best defines the Windows Registry as used by the Cortex XDRagent?
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
Answer: A
Explanation:
Reference: https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users