KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **SecOps-Pro**

Title : Palo Alto Networks Security Operations Professional

Version : DEMO

1.Which incident should a responder prioritize based on overall functional and informational impact to the company?
A. A user in the accounting department receives a pop-up message after visiting a website.
B. A public-facing web server has multiple failed login attempts over a short period of time.
C. An external-facing company website is currently unavailable.
D. A large upload of user data from an internal file server to a public website occurs.
Answer: D

2.Which response action in Cortex XSIAM would be unavailable to a SOC analyst investigating an incident involving a Linux server?
A. File search and destroy
B. Live Terminal session initiation
C. Running a script
D. Halting network access
Answer: A

3.What is the role of content packs in Cortex XSOAR?
A. To provide rebuilt bundles for supporting security orchestration use cases
B. To support technical support teams with relevant information required to troubleshoot
C. To serve as a central location for installing, exchanging, and contributing content
D. To serve as a major software versioning update
Answer: A

4.Which action should an administrator take to create automated response actions when a user account is compromised, allowing attacker to upload data to an external IP address and infect a machine on the company network with malware?
A. Create automation rules in Cortex XDR that will trigger for each alert.
B. Create a script in Cortex XSOAR that will run a playbook based on the scenario.
C. Create playbook triggers in Cortex XSIAM and run playbooks for each alert.
D. Map the events as type of Cortex XSOAR incident, then run a playbook.
Answer: C

5.During a sophisticated cyber attack, a company experiences a stealthy, multivector intrusion that evades detection by traditional security tools.
The company requires a solution that will correlate and analyze the disparate attack indicators across its network, endpoints, and cloud environments to uncover the full scope of the breach and take immediate automated response actions.
Which solution should be recommended?
A. XDR
B. SIEM
C. EDR
D. XSOAR
Answer: A