IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

http://www.it-dumps.com

Exam : PSE Cortex

Title : Palo Alto Networks System Engineer - Cortex Professional

Version : DEMO

1. A Cortex XSOAR customer wants to ingest from a single mailbox. The mailbox brings in reported phishing emails and email requests from human resources (HR) to onboard new users. The customer wants to run two separate workflows from this mailbox, one for phishing and one for onboarding.
What will allow Cortex XSOAR to accomplish this in the most efficient way?
A. Usee machine learning (ML) to determine incident type
B. Create two instances of the email integration and classily one instance as ingesting incidents of type phishing and the other as ingesting incidents of type boarding
C. Use an incident classifier based on field in each type of email to classify those containing “Phish Alert” in the subject as phishing and those containing “Onboard Request” as onboarding
D. Create a playbook to process and determine incident type based on content of the email
Answer: C

2. What allows the use of predetermined Palo Alto Networks roles to assign access rights to Cortex XDR users?
A. Restrictions security profile
B. Cloud identity engine (CIE)
C. Endpoint groups
D. role-based access control (RBAC)
Answer: D

3. What integration allows searching and displaying Splunk results within Cortex XSOAR?
A. Demisto App for Splunk integration
B. SplunkPY integration
C. Splunk integration
D. XSOAR REST API integration
Answer: B

4. How can Cortex XSOAR save time when a phishing incident occurs?
A. It can automatically identify every mailbox that received the phish and create corresponding cases for them
B. It can automatically email staff to warn them about the phishing attack and show them a copy of the email
C. It can automatically purge the email from user mailboxes in which it has not yet opened
D. It can automatically respond to the phishing email to unsubscribe from future emails
Answer: A

5. Which two types of Indicators of compromise (IOCs) are available for creation in Cortex XDR?
A. Internet Protocol (IP)
B. Endport hostname
C. registry entry
D. domain
Answer: A.D