IBM

C1000-018 Exam

IBM QRadar SIEM V7.3.2 Fundamental Analysis

Questions & Answers
Demo

Version: 5.0

Question: 1

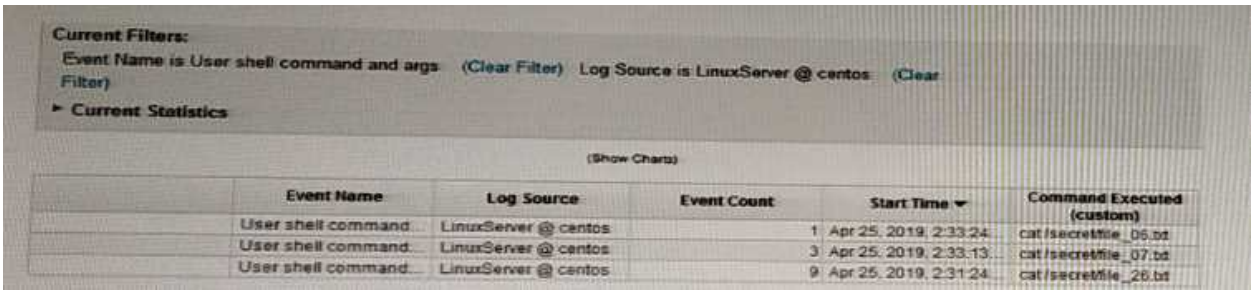
An analyst is noticing false positives from a single IP on a specific offense. How can the analyst tune the event rule to eliminate these false positives?

A. Add the rule test "AND when IP address equals" to the bottom of the test list of the rule.
B. Add the rule test "AND NOT when the offense is indexed by one of the following IP addresses".
C. Add the rule test "AND NOT when IP address equals" to the bottom of the test list of the rule,
D. Add the rule test "AND when IP address equals" to the top of the test list of the rule.

Answer: C

Question: 2

An analyst is investigating access to sensitive data on a Linux system. Data is accessible from the /secret directory and can be viewed using the 'sudo oaf command. The specific file /secret/file_08-txt was known to be accessed in this way. After searching in the Log Activity Tab, the following results are shown.



When interpreting this, the analyst is having trouble locating events which show when the file was accessed. Why could this be?

A. The 'LinuxServer @ cantos' log source has boon configured as a Faise Positive and the specific event for that file has been dropped.
B. The 'LinuxServer @ centos' log source has not been configured to send the relevant events to QRadar.
C. The 'LinuxServer @ centos' log source has coalescing configured and the specific event for that file can only be accessed by clicking on the 'Event Count' value.
D. The ;LinuxServer @ centos; log source has coalesscing conigured and the specific event for that file has been discardedd.

Answer: C

Question: 3

The SOC team complained that they have can only see one Offense in the Offenses tab.
space of 10 minutes, but the analyst How can the analyst ensure only one email is sent in this circumstance?

A. Configure the postfix mail server on the Console to suppress duplicate items
B. Ensure that the Rule Action Limiter is configured the same way as the Rule Response Limiter.
C. Add a Response Limiter to the Rule, configured to execute only once every 30 minutes.
D. Disable Automated Offense Notification - by email, in Advanced System Settings.

Answer: A

Question: 4

An analyst has been assigned a number of Offenses to review and a new event occurs, review and manage. While reviewing an inactive offense, a new event occurs.
Which statement applies to the Offense?

A. The event is added in a new Offense that is created.
B. The event is added to the Offense and the status is changed to Dormant.
C. The rule that created the Offense is temporarily halted.
D. The event is added to the Offense and the status is changed to Active.

Answer: B

Question: 5

An analyst has been assigned a task to modify a rule in such a manner that Source IP of the triggered Offense from this rule should be stored in a Reference set.
Under which section of the rule wizard can the analyst achieve this?

A. Rule Response
B. Rule Action
C. Rule Test Stack Editor
D. Rule Response Limiter

Answer: C