C2150-612 Q&As

IBM Security QRadar SIEM V7.2.6 Associate Analyst

QUESTION 1

An event is happening regularly and frequently; each event indicates the same target username. There is a rule configured to test for this event which has a rule action to create an offense indexed on the username. What will QRadar do with the triggered rule assuming no offenses exist for the username and no offenses are closed during this time?

A. Each matching event will be tagged with the Rule name, but only one Offense will be created.

B. Each matching event will cause a new Offense to be created and will be tagged with the Rule name.

C. Events will be tagged with the rule name as long as the Rule Response limiter is satisfied. Only one offense will be created.

D. Each matching event will be tagged with the Rule name, and an Offense will be created if the event magnitude is greater than 6.

Correct Answer: C

QUESTION 2

What is accessible from the Offenses Tab but is not used to present a sorted list of offenses?

A. Rules

B. Category

C. Source IP

D. Destination IP

Correct Answer: A

QUESTION 3

Which three options are available on the New Search on the My Offenses and All Offenses pages? (Choose three.)

A. Notes

B. Source IP

C. Magnitude

D. Attack Name

E. Malware Name

F. Specific Interval

Correct Answer: BDF

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/

t_qradar_search_my_all_off_pages.html

QUESTION 4

What is a common purpose for looking at flow data?

A. To see which users logged into a remote system

B. To see which users were accessing report data in QRadar

C. To see application versions installed on a network endpoint

D. To see how much information was sent from a desktop to a remote website

Correct Answer: D

QUESTION 5

Which approach allows a rule to test for Active Directory (AD) group membership?

A. Import the AD membership information into the Asset Database using AXIS and use an asset rule test

B. Use the build-in LDAP integration to execute a search for each event as it is received by the Event Processor to test for group membership

C. Maintain reference data for the AD group(s) of interest containing lists of usernames and then add rule tests to see if the normalized username is in the reference data

D. Export the AD group membership information to a CSV file and place it in the /store/AD_mapping.csv

file on the console, then use the `is a member of AD group\\' test in the rule

Correct Answer: A