C1000-018$^{Q\&As}$

IBM QRadar SIEM V7.3.2 Fundamental Analysis

QUESTION 1

Where can an analyst working with Offenses add a regular expression test into an existing rule?

A. Left

B. Top

C. Bottom

D. Right

Correct Answer: B

QUESTION 2

An analyst wants to view information about repeated offenders and IP addresses that generate many attacks or are subject to many attacks.

What should the analyst choose from the navigation options in the Offense tab?

A. By Event Category or By Event Source

B. By Source IP or By Destination IP

C. By Log Source IP or By Event Source

D. By Event or By Flows

Correct Answer: B

Explanation:

Use the navigation options on the left to view the offenses from different perspectives. For example, select

By Source IP or By Destination IP.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_users_guide.pdf

QUESTION 3

An analyst is investigating a series of events that triggered an Offense. The analyst wants to get more detailed information about the IP address from the reference set.

How can the analyst accomplish this?

A. Click on Searches tab then perform an Advanced Search

B. Click on Log Activity tab then perform a Quick Search

C. Click on Searches tab then perform a Quick Search

D. Click on Log Activity tab then perform an Advanced Search

Correct Answer: A

QUESTION 4

What is the maximum time period for 3 subsequent events to be coalesced?

A. 10 minutes

B. 10 seconds

C. 5 minutes

D. 60 seconds

Correct Answer: B

Explanation:

Event coalescing starts after three events have been found with matching properties within a 10 second

window.

Reference: https://www.ibm.com/support/pages/qradar-how-does-coalescing-work-qradar

QUESTION 5

An analyst is investigating a user\\'s activities and sees that they have repeatedly executed an action which triggers a rule that emails the SOC team and creates an Offense, indexed on Username.

The SOC team complained that they have received 15 emails in the space of 10 minutes, but the analyst can only see one Offense in the Offenses tab.

How is this explained?

A. There is a Rule Limiter on the Rule Action which creates the Offense, this should also be applied to the Rule Responses.

B. This is expected behavior, the offense will contain the information about all 15 events.

C. An Offense rule has been configured to send multiple emails upon Offense creation.

D. The Custom Rules Engine (CRE) has fallen behind and the additional Offenses will be created shortly.

Correct Answer: C