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

IBM QRadar SIEM V7.3.2 Fundamental Analysis

Pass IBM C1000-018 Exam with 100% Guarantee

QUESTION 1

What is the intent of the magnitude of an offense?

A. It measures the age of the event attached to the offense.

B. It measures the age of the offense.

C. It measures the importance of the offense.

D. It measures the importance of the event attached to the offense.

Correct Answer: B

Explanation:

The age of the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.3.3?topic=management-offense-prioritization

QUESTION 2

What is displayed in the status bar of the Log Activity tab when streaming events?

A. Average number of results that are received per second.

B. Average number of results that are received per minute.

C. Accumulated number of results that are received per second.

D. Accumulated number of results that are received per minute.

Correct Answer: A

Explanation:

Status bar

When streaming events, the status bar displays the average number of results that are received per second.

Reference: https://www.ibm.com/docs/en/qradar-on-cloud?topic=investigation-log-activity-tab-overview

QUESTION 3

An analyst needs to use a new custom property in a rule.

What must be the mandatory characteristic of the custom property?

A. It must be shared.

B. It must be boolean.

C. It must be stored.

D. It must be extracted.

Correct Answer: B

QUESTION 4

An analyst is performing an investigation regarding an Offense. The analyst is uncertain to whom some of the external destination IP addresses in List of Events are registered.

How can the analyst verify to whom the IP addresses are registered?

A. Right-click on the destination address, More Options, then Navigate, and then Destination Summary

B. Right-click on the destination address, More Options, then IP Owner

C. Right-click on the destination address, More Options, then Information, and then WHOIS Lookup

D. Right-click on the destination address, More Options, then Information, and then DNS Lookup

Correct Answer: A

Explanation:

Navigate > View Destination Summary Displays the offenses that are associated with the selected

destination IP address.

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

QUESTION 5

An analyst noticed that from a particular subnet (203.0.113.0/24), all IP addresses are simultaneously

trying to reach out to the company\\'s publicly hosted FTP server.

The analyst also noticed that this activity has resulted in a Type B Superflow on the Network Activity tab.

Under which category, should the analyst report this issue to the security administrator?

A. Syn Flood

B. Port Scan

C. Network Scan

D. DDoS

Correct Answer: A