C1000-018 Q&As

IBM QRadar SIEM V7.3.2 Fundamental Analysis

Pass IBM C1000-018 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/c1000-018.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

QUESTION 1

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

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

Which consideration should be given to the position of rule tests that evaluate regular expressions (Regex tests)?

A. They can only be used in Building Blocks to ensure they are evaluated as infrequently as possible.

B. They are usually the most specific. As such, they should appear first in the order.

C. They are usually the most expensive. As such, they should appear last in the order.

D. They are stateful tests. As such QRadar automatically evaluates them last.

Correct Answer: A

Reference: https://towardsdatascience.com/everything-you-need-to-know-about-regular-expressions8f622fe10b03

QUESTION 4

Which are the supported protocol configurations for Check Point integration with QRadar? (Choose two.)

A. CHECKPOINT REST API

B. SYSLOG

C. JDBC

D. SFTP

E. OPSEC/LEA

Correct Answer: BE

QUESTION 5

While creating a new custom property, which is a valid property type selection?

A. Flow Based

B. Event Based

C. AQL Based

D. Regular Expressions Based

Correct Answer: D