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.pass2lead.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 needs to investigate an Offense and navigates to the attached rule(s).

Where in the rule details would the analyst investigate the reason for why the rule was triggered?

A. Rule response limiter

B. List of test conditions

C. Rule actions

D. Rule responses

Correct Answer: A

QUESTION 2

How many normalized timestamp field(s) does an event contain?

A. 2

B. 3

C. 4

D. 1

Correct Answer: B

Explanation:

There are 3 timestamp fields on events in Qradar.

Reference: https://www.ibm.com/mysupport/s/question/0D50z00006PEG2mCAH/why-do-i-see-differenttime-stamps-for-qradar-events?language=en_US

QUESTION 3

Which statement about False Positive Building Blocks applies?

Using False Positive Building Blocks:

A. helps to prevent unwanted alerts, but there is no effect on performance.

B. helps to prevent unwanted alerts, and reduces the performance impact of testing rules that do not need to be tested.

C. has no impact on unwanted alerts, but it does reduce the performance impact of testing rules that do not need to be tested.

D. has no impact on unwanted alerts, or performance.

Correct Answer: A

Reference: https://community.carbonblack.com/t5/Knowledge-Base/Cb-Defense-UnderstandingEliminating-Unwanted-Alerts/ta-p/44924

QUESTION 4

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 5

The administrator had set up several scheduled reports that can be executed by analysts every Monday, and the first day of each month. On Thursday, an executive requests one of the weekly reports.

If the analyst executes the report on Thursday, what information will the report contain?

A. Data from Monday to Sunday from the previous week.

B. Data from Thursday from the previous week to Wednesday from the current week.

C. Data from Monday to Thursday from the current week.

D. Data from Monday to Wednesday from the current week.

Correct Answer: C