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:

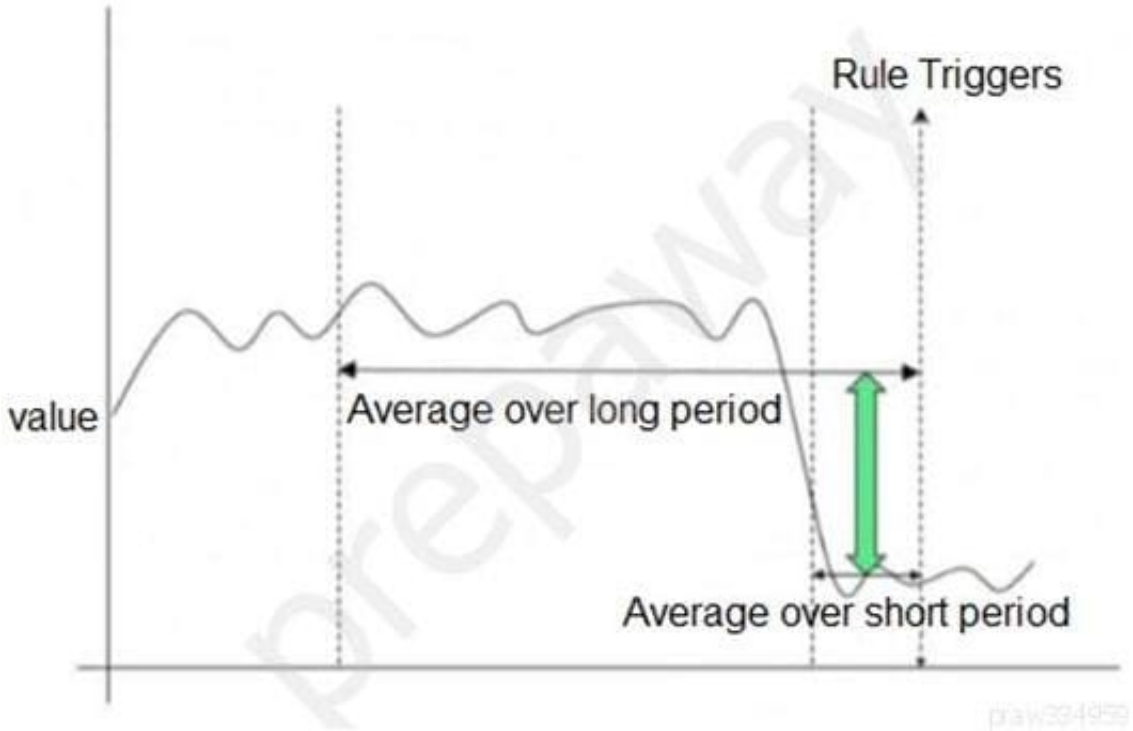
https://www.pass4itsure.com/c1000-018.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

The graph below shows a time series of a value. A rule has been created which will trigger at the indicated point.



Which type of QRadar rule has been used?

A. Common Rule

B. Threshold Rule

C. Behavioral Rule

D. Anomaly Rule

Correct Answer: B

QUESTION 2

An analyst needs to perform a Quick search to find events under the Log Activity tab that contains an ‘exe’ file during a certain time period.

How can the analyst do this?

A. On the Search bar select Quick Filter, then insert filter criteria for ‘/*.exe/’ and then select a time interval from the view option\\'s drop down.

B. Select Search – New Search from the menu bar, then select all the search criteria required from the UI options provided.

C. Select Quick Searches on the menu bar, then go through the list of saved searches available to see if one already exists, that can be altered.

D. On the Search bar select Quick Filter, insert: 'exe, last 1 hour' into the filter criteria, then click Search.

Correct Answer: A

Reference: https://www.ibm.com/support/pages/searching-your-qradar-data-efficiently-part-1-quick-filters

QUESTION 3

When ordering these tests in an event rule, which of them is the best test to place at the top of the list for rule performance?

A. When the source is [local or remote]

B. When the destination is [local or remote]

C. When the event(s) were detected by one or more of [these log sources]

D. When an event matches all of the following [Rules or Building Blocks]

Correct Answer: A

QUESTION 4

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 5

An analyst needs to review additional information about the Offense top contributors, including notes and annotations that are collected about the Offense.

Where can the analyst review this information?

A. In the top portion of the Offense Summary window

B. In the bottom portion of the Offense main view

C. In the bottom portion of the Offense Summary window

D. In the top portion of the Offense main view

Correct Answer: C

Explanation:

In the bottom portion of the Offense Summary window, review additional information about the offense top contributors, including notes and annotations that are collected about the offense.

Reference: https://www.ibm.com/docs/en/qsip/7.4?topic=investigations-investigating-offense-by-using summary-information