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

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

QUESTION 2

What is the reason for this system notification?

A. Deny ntpdate communication on port 423.

B. Deny ntpdate communication on port 223.

C. Deny ntpdate communication on port 323.

D. Deny ntpdate communication on port 123.

Correct Answer: D

Explanation:

38750129 - Time synchronization to primary or Console has failed.

The managed host cannot synchronize with the console or the secondary HA appliance

cannotsynchronize with the primary appliance.

Administrators must allow ntpdatecommunication on port 123.

Reference: https://www.coursehero.com/file/p35nlom9/Process-exceeds-allowed-run-time-38750122Process-takes-too-long-to-execute-The/

QUESTION 3

What is a valid offense naming mechanism? This information should:

A. set the naming of the associated offense(s).

B. set or replace the naming of the associated offense(s).

C. replace the naming of the associated offense(s).

D. be included in the naming of the associated offense(s).

Correct Answer: A

Explanation:

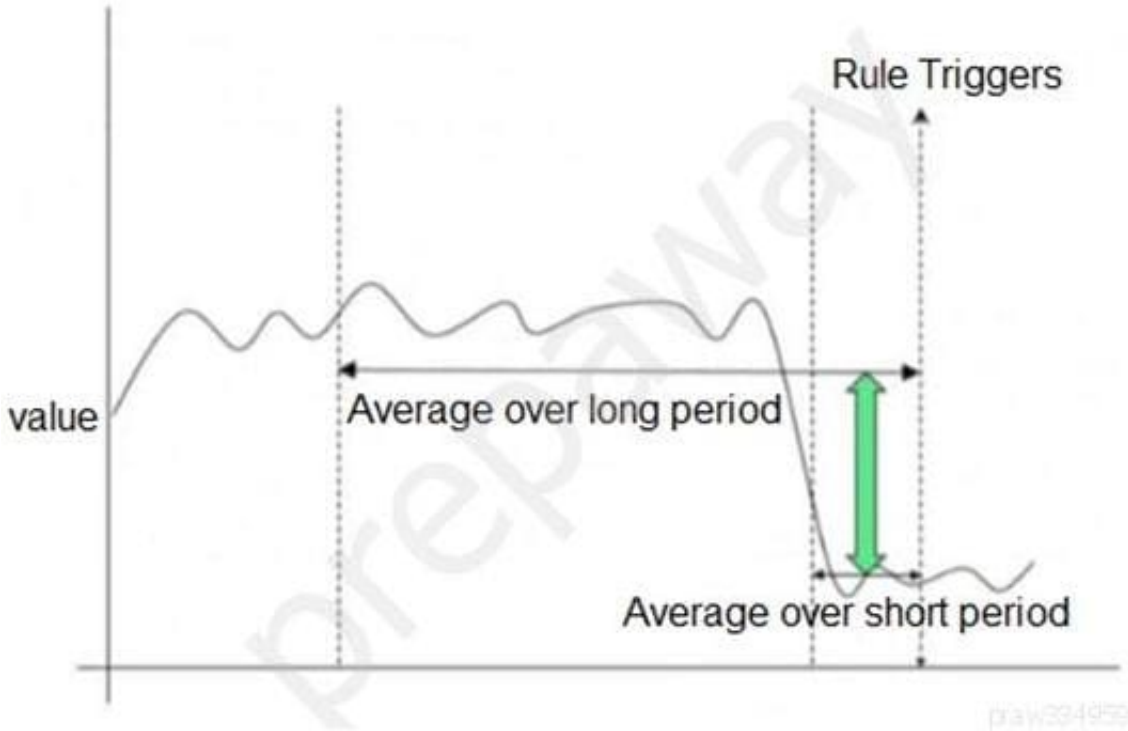
Under "Offense Naming", check "This information should

contribute to the name of the associated offense(s)".

Reference: https://www.ibm.com/support/pages/apar/IJ27086

QUESTION 4

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 5

What are the different flow types in QRadar?

A. L2L, L2R, R2R, R2L

B. Standard, Type A, Type B, Type C

C. Standard, Type 1, Type2, Type 3

D. Type 1, Type 2, Type 3, Type 4

Correct Answer: B

Reference: https://docplayer.net/19071559-Qradar-siem-7-2-flows-overview.html