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

IBM QRadar SIEM V7.3.2 Fundamental Analysis

Pass IBM C1000-018 Exam with 100% Guarantee

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

QUESTION 1

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

QUESTION 2

What could be a possible reason that events are routed directly to storage by the custom rule engine (CRE)?

A. System is under high load

B. A rule is processing 20,000 EPS

C. Event normalization issue

D. Event Parsing issue

Correct Answer: A

QUESTION 3

What is the procedure to re-open a closed Offense?

A. A closed Offense cannot be re-opened.

B. Wait for new events/flows that will re-open the closed Offense.

C. Activate the Offense in the action/re-open drop down menu of the Offense tab.

D. Activate the Offense in action/re-open drop down menu in the Admin tab.

Correct Answer: A

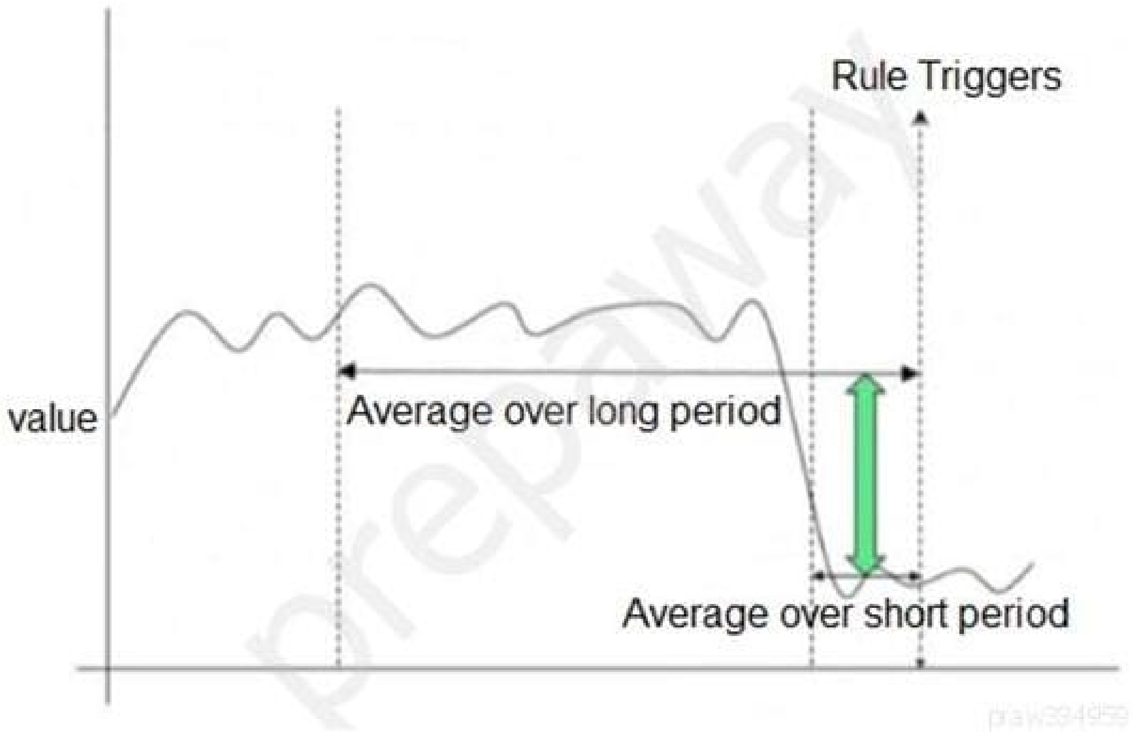
Explanation:

Not possible to reopen a closed offense.

Reference: https://www.ibm.com/support/pages/qradar-closed-offense-information

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

An analyst had been researching an Offense that has now disappeared from the active Offense list.

What is the period of time that has to pass before an active Offense that receives no new contributing events or flows become inactive?

A. 5 days

B. 3 days

C. 24 hours

D. 1 hour

Correct Answer: A

Explanation:

An offense remains in a dormant state for 5 days. If an event is added while an offense is dormant, the

five-day counter is reset.

Reference: https://www.ibm.com/docs/en/SS42VS_7.3.2/com.ibm.qradar.doc/b_qradar_users_guide.pdf

C1000-018 VCE Dumps   C1000-018 Practice Test   C1000-018 Braindumps