C2150-612 Q&As

IBM Security QRadar SIEM V7.2.6 Associate Analyst

Pass IBM C2150-612 Exam with 100% Guarantee

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

https://www.pass2lead.com/c2150-612.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What are the various timestamps related to a flow?

A. First Packet Time, Storage Time, Log Source Time

B. First Packet Time, Storage Time, Last Packet Time

C. First Packet Time, Log Source Time, Last Packet Time

D. First Packet Time, Storage Time, Log Source Time, End Time

Correct Answer: B

Reference:

IBM Security QRadar SIEM Users Guide. Page: 101

QUESTION 2

While on the Offense Summary page, a specific Category of Events associated with the Offense can be investigated.

Where should a Security Analyst click to view them?

A. Click on Events, then filter on Flows

B. Highlight the Category and click the Events icon

C. Scroll down to Categories and view Top 10 Source IPs

D. Right Click on Categories and choose Filter on Network Activity

Correct Answer: B

Reference:

IBM Security QRadar SIEM Users Guide. Page: 42

QUESTION 3

What is the largest differentiator between a flow and event?

A. Events occur at a moment in time while flows have a duration.

B. Events can be forwarded to another destination, but flows cannot.

C. Events allow for the creation of custom properties, but flows cannot.

D. Flows only contribute to local correlated rules, while events are global.

Correct Answer: A

QUESTION 4

Which Anomaly Detection Rule type is designed to test event and flow traffic for changes in short term events when compared against a longer time frame?

A. Outlier Rule

B. Anomaly Rule

C. Threshold Rule

D. Behavioral Rule

Correct Answer: B

Reference: http://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_rul_anomaly_detection.html

QUESTION 5

What is the difference between an offense and a triggered rule?

A. Offenses are created every time a rule\\'s tests are satisfied, but a rule may only trigger if the response limiter allows.

B. The first time a rule triggers, it will create an offense, after than to new offense will be created for the same index type.

C. A rule will always trigger if its tests are satisfied, but an offense may only be created if the event magnitude is greater than 6.

D. An offense may be created or updated by a triggered rule, but a rule will always trigger when the tests are satisfied.

Correct Answer: C