C2150-612$^{\text{Q\&As}}$

IBM Security QRadar SIEM V7.2.6 Associate Analyst

Pass IBM C2150-612 Exam with 100% Guarantee

QUESTION 1

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

QUESTION 2

Where are events related to a specific offense found?

A. Offenses Tab and Event List window

B. Dashboard and List of Events window

C. Offense Summary Page and List of Events window

D. Under Log Activity, search for Events associated with an Offense

Correct Answer: A

QUESTION 3

Which type of search uses a structured query language to retrieve specified fields from the events, flows, and simarc tables?

A. Add Filter

B. Asset Search

C. Quick Search

D. Advanced Search

Correct Answer: D

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

c_qradar_ug_search_bar.html

QUESTION 4

What are the two available formats for exporting event and flow data for external analysis? (Choose two.)

A. XML

B. DOC

C. PDF

D. CSV

E. HTML

Correct Answer: AD

QUESTION 5

Which type of rule requires a saved search that must be grouped around a common parameter?

A. Flow Rule

B. Event Rule

C. Common Rule

D. Anomaly Rule

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/
c_qradar_rul_anomaly_detection.html