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.leads4pass.com/c2150-612.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which information can be found under the Network Activity tab?

A. Flows

B. Events

C. Reports

D. Offenses

Correct Answer: A

QUESTION 2

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 3

An event is happening regularly and frequently; each event indicates the same target username. There is a rule configured to test for this event which has a rule action to create an offense indexed on the username. What will QRadar do with the triggered rule assuming no offenses exist for the username and no offenses are closed during this time?

A. Each matching event will be tagged with the Rule name, but only one Offense will be created.

B. Each matching event will cause a new Offense to be created and will be tagged with the Rule name.

C. Events will be tagged with the rule name as long as the Rule Response limiter is satisfied. Only one offense will be created.

D. Each matching event will be tagged with the Rule name, and an Offense will be created if the event magnitude is greater than 6.

Correct Answer: C

QUESTION 4

How is an event magnitude calculated?

A. As the sum of the three properties Severity, Credibility and Relevance of the Event

B. As the sum of the three properties Severity, Credibility and Importance of the Event

C. As a weighted mean of the three properties Severity, Credibility and Relevance of the Event

D. As a weighted mean of the three properties Severity, Credibility and Importance of the Event

Correct Answer: C

QUESTION 5

A Security Analyst found multiple connection attempts from suspicious remote IP addresses to a local host on the DMZ over port 80. After checking related events no successful exploits were detected. Upon checking international documentation, this activity was part of an expected penetration test which requires no immediate investigation. How can the Security Analyst ensure results of the penetration test are retained?

A. Hide the offense and add a note with a reference to the penetration test findings

B. Protect the offense to not allow it to delete automatically after the offense retention period has elapsed

C. Close the offense and mark the source IP for Follow-Up to check if there are future events from the host

D. Email the Offense Summary to the penetration team so they have the offense id, add a note, and close the Offense

Correct Answer: B

Reference: http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/c_qradar_Off_Retention.html