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.geekcert.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 two pieces of information can be found under the Log Activity tab? (Choose two.)

A. Offenses

B. Vulnerabilities

C. Firewall events

D. Destination Bytes

E. Internal QRadar messages

Correct Answer: AD

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

Which device uses signatures for traffic analysis when deployed in a network environment to detect, allow, block, or simulated-block traffic?

A. Proxy

B. QRadar

C. Switch

D. IDS/IPS

Correct Answer: D

QUESTION 4

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 5

What is a primary benefit of building blocks?

A. They can notify users of strange behavior.

B. They allow the execution of its test within all rules.

C. They generate new events into the pipeline before rules fire.

D. They allow for report result to be used in custom rules tests.

Correct Answer: C

Reference:
https://www.ibm.com/developerworks/community/forums/html/topic?id=77777777-0000-00000000-000014969067