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

What is indicated by an event on an existing log in QRadar that has a Low Level Category of "Unknown"?

A. That event could not be parsed

B. That event arrived out of order from the original device

C. That event was from a device that is not supported by QRadar

D. That the event was parsed, but not mapped to an existing QRadar category

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.dsm.doc/c_DSM_guide_UniversalLEEF_eventmap.html#c_dsm_guide_universalleef_eventmap

QUESTION 3

Which flow fields should be used to determine how long a session has been active on a network?

A. Start time and end time

B. Start time and storage time

C. Start time and last packet time

D. Last packet time and storage time

Correct Answer: C

Flow timestamps are created as traffic are detected and recored by the QRadar Flow Collector. Some flows can last seconds, ie, an email message, file upload, etc, while others may far longer - minutes, hours, or even days, such as an interactive remote session, audio/video stream (Netflix, voip call), or database application connection. As these sessions/flows continue over time, they are reported into the system. The original "start time" for each session remains

the same, when first detected, while the "last packet time" will update as time passes. The best way to see this is to search for the two ip addresses involved in the session/flow, then search over a longer time window ?you should see multiple records, one that ends for each minute that the session was active. Each minute will also have the byte and packet count, for each minute the flow was active. Reference: https://developer.ibm.com/qradar/2018/01/09/qradar-flow-faq/

QUESTION 4

What are two common uses for a SIEM? (Choose two.)

A. Managing and normalizing log source data

B. Identifying viruses based on payload MD5s

C. Blocking network traffic based on rules matched

D. Enforcing governmental compliance auditing and remediation

E. Performing near real-time analysis and observation of a network and its devices

Correct Answer: AB

QUESTION 5

Which three could be considered a log source type? (Choose three.)

A. Red Hat Network

B. IBM ISS Proventia

C. QRadar Event Processor

D. Check Point Firewall-1

E. Sourcefire Flow Injector

F. McAfee ePolicy Orchestrator

Correct Answer: BDF