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.pass4itsure.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

Which log source and protocol combination delivers events to QRadar in real time?

A. Sophos Enterprise console via JDBC

B. McAfee ePolicy Orchestrator via JDBC

C. McAfee ePolicy Orchestrator via SNMP

D. Solaris Basic Security Mode (BSM) via Log File Protocol

Correct Answer: C

QUESTION 2

Which feature of a Next Generation Firewall is not available on previous firewalls?

A. VPN Support

B. Layer 3 based firewall rules

C. Integrated signature based IPS engine

D. Network and Port-Address Translation (NAT)

Correct Answer: C

QUESTION 3

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 4

Events and Flows both have multiple different timestamps available to them. Which timestamp is available to both events and flows?

A. End Time

B. Storage Time

C. First Activity Time

D. Last Activity Time

Correct Answer: B

Reference: https://developer.ibm.com/answers/questions/292620/why-do-i-see-different-time-stamps-forqradar-even/

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