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

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 2

Which two high level Event Categories are used by QRadar? (Choose two.)

A. Policy

B. Direction

C. Localization

D. Justification

E. Authentication

Correct Answer: AE

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_adm_h_level_evt_categories.html

QUESTION 3

What is the primary goal of data categorization and normalization in QRadar?

A. It allows data from different kinds of devices to be compared.

B. It preserves original data allowing for forensic investigations.

C. It allows for users to export data and import it into other system.

D. It allows for full-text indexing of data to improve search performance.

Correct Answer: A

QUESTION 4

Where can event data be exported from for external analysis?

A. From the Offenses Tab, select the offense and right click, select export event data

B. From the list of events page, select actions and click export to XML or export to CSV

C. From the offense summary page, select actions and click on export to XML or export to CSV.

D. From the Offenses Tab, select the offense, click on actions, select export to XML or export to CSV

Correct Answer: B

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