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.passapply.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 three log sources are supported by QRadar? (Choose three.)

A. Log files via SFTP

B. Barracuda Web Filter

C. TLS multiline Syslog

D. Oracle Database Listener

E. Sourcefire Defense Center

F. Java Database Connectivity (JDBC)

Correct Answer: DEF

QUESTION 2

Which QRadar rule could detect a possible potential data loss?

A. Apply "Potential data loss" on event of flows which are detected by the local system and when any IP is part of any of the following XForce premium Premium_Malware

B. Apply "Potential data loss" on flows which are detected by the local system and when at least 1000 flows are seen with the same Destination IP and different Source IP in 2 minutes

C. Apply "Potential data loss" on events which are detected by the local system and when the event category for the event is one of the following Authentication and when any of Username are contained in any of Terminated_User

D. Apply "Potential data loss" on flows which are detected by the local system and when the source bytes is greater than 200000 and when at least 5 flows are seen with the same Source IP, Destination IP, Destination Port in 12 minutes

Correct Answer: D

QUESTION 3

A Security Analyst is looking on the Assets Tab at an asset with offenses associated to it.

With a "Right Click" on the IP address, where could the Security Analyst go to obtain all offenses associated with it?

A. Information > Asset Profile

B. Navigate > View by Network

C. Run Vulnerability Scan > Source offenses

D. Navigate > View Source Summary or Destination Summary

Correct Answer: A

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/b_qradar_users_guide.pdf

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 the maximum number of supported dashboards for a single user?

A. 10

B. 25

C. 255

D. 1023

Correct Answer: C

Reference: http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_custom_dboard.html