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 three optional items can be added to the Default and Custom Dashboards without requiring additional licensing? (Choose three.)

A. Offenses

B. Log Activity

C. Risk change

D. Flow Search

E. Risk Monitoring

F. Asset Management

Correct Answer: ABF

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

QUESTION 2

What is an example of the use of a flow data that provides more information than an event data?

A. Represents a single event on the network

B. Automatically identifies and better classifies new assets found on a network

C. Performs near real-time comparisons of application data with logs sent from security devices

D. Represents network activity by normalizing IP addresses ports, byte and packet counts, as well as other details

Correct Answer: D

Reference: http://www-01.ibm.com/support/docview.wss?uid=swg21682445

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 a user add a note to an offense in the user interface?

A. Dashboard and Offenses Tab

B. Offenses Tab and Offense Detail Window

C. Offenses Detail Window, Dashboard, and Admin Tab

D. Dashboard, Offenses Tab, and Offense Detail Window

Correct Answer: B

Reference:

IBM Security QRadar SIEM Users Guide. Page: 34

QUESTION 5

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