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

QUESTION 1

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

QUESTION 2

A Security Analyst was asked to search for an offense on a specific day. The requester was not sure of the time frame, but had Source Host information to use as well as networks involved, Destination IP and username.

Which filters can the Security Analyst use to search for the information requested?

A. Offense ID, Source IP, Username

B. Magnitude, Source IP, Destination IP

C. Description, Destination IP, Host Name

D. Specific Interval, Username, Destination IP

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/
t_qradar_search_my_all_off_pages.html

QUESTION 3

When might a Security Analyst want to review the payload of an event?

A. When immediately after login, the dashboard notifies the analyst of payloads that must be investigated

B. When "Review payload" is added to the offense description automatically by the "System: Notification" rule

C. When the event is associated with an active offense, the payload may contain information that is not normalized or extracted fields

D. When the event is associated with an active offense with a magnitude greater than 5, the payload should be reviewed, otherwise it is not necessary

Correct Answer: C

QUESTION 4

A Security Analyst has noticed that an offense has been marked inactive.

How long had the offense been open since it had last been updated with new events or flows?

A. 1 day + 30 minutes

B. 5 days + 30 minutes

C. 10 days + 30 minutes

D. 30 days + 30 minutes

Correct Answer: B

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.0/com.ibm.qradar.doc/
c_qradar_Off_Retention.html

QUESTION 5

What is accessible from the Offenses Tab but is not used to present a sorted list of offenses?

A. Rules

B. Category

C. Source IP

D. Destination IP

Correct Answer: A