



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

A Security Analyst, looking at a Log Activity search result, wants to limit the results to one Log Source.

Which right-click method would be the fastest way for the Security Analyst to ensure this?

- A. Right click on a Log Source name, then select Filter on Log Source is
- B. Right click on a Source IP Address, then select Filter on Log Source is
- C. Right click on the Log Source Type name, then select Filter on Log Source Group is
- D. Right click on the Log Source Group name, then select Filter on Log Source Group is

Correct Answer: A

QUESTION 2

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 3

What is the default view when a user first logs in to QRadar?

- A. Report Tab
- B. Offense Tab
- C. Dashboard tab
- D. Messages menu

Correct Answer: C

Reference: http://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/c_qradar_dash_tab.html



QUESTION 4

What is a key difference between the magnitude of an event and the magnitude of an offense?

- A. The magnitude of an event is derived when the event is received and does not vary, the magnitude of an offense can only increase.
- B. The magnitude of an event is derived when the event is received and does not vary, the magnitude of an offense can increase or decrease over time.
- C. The magnitude of an event is derived from the current magnitude of the offense it creates, the magnitude of an offense can increase or decrease over time.
- D. The magnitude of an event is derived when the event is received and does not vary, the magnitude of an offense is derived when the offense is created and does not vary.

Correct Answer: B

QUESTION 5

How is an event magnitude calculated?

- A. As the sum of the three properties Severity, Credibility and Relevance of the Event
- B. As the sum of the three properties Severity, Credibility and Importance of the Event
- C. As a weighted mean of the three properties Severity, Credibility and Relevance of the Event
- D. As a weighted mean of the three properties Severity, Credibility and Importance of the Event

Correct Answer: C

[C2150-612 VCE Dumps](#)

[C2150-612 Study Guide](#)

[C2150-612 Exam Questions](#)