



# C2150-612<sup>Q&As</sup>

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

When reviewing Network Activity, a flow shows a communication between a local server on port 443, and a random, remote port. The bytes from the local destination host are 2 GB, and the bytes from the remote, source host address are 40KB.

What is the flow bias of this session?

- A. Other
- B. Mostly in
- C. Near-same
- D. Mostly out

Correct Answer: D

---

### QUESTION 2

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](https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/b_qradar_users_guide.pdf)

---

### QUESTION 3

What is a common purpose for looking at flow data?

- A. To see which users logged into a remote system
- B. To see which users were accessing report data in QRadar
- C. To see application versions installed on a network endpoint
- D. To see how much information was sent from a desktop to a remote website



Correct Answer: D

---

#### QUESTION 4

Which three pages can be accessed from the Navigation menu on the Offenses tab? (Choose three.)

- A. Rules
- B. By Category
- C. My Offenses
- D. By Event Name
- E. Create Offense
- F. Closed Offenses

Correct Answer: ABC

---

#### QUESTION 5

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

[C2150-612 PDF Dumps](#)

[C2150-612 VCE Dumps](#)

[C2150-612 Braindumps](#)