



# 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.geekcert.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

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 2

What is the purpose of coalescing?

- A. To reduce the number of events which count against EPS licenses
- B. To reduce the amount of data received by QRadar event collectors
- C. To reduce the amount of data going through the pipeline and stored onto disk
- D. To reduce the number of offenses generated by QRadar as part of the tuning process

Correct Answer: A

Reference: <https://developer.ibm.com/answers/questions/438469/out-eps-licence-is-10k-im-attaching-twoscreenshot/>

---

#### QUESTION 3

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 4



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 5

What can be considered a log source type?

- A. ICMP
- B. SNMP
- C. Juniper IDP
- D. Microsoft SMBtail

Correct Answer: C

Reference: [https://www.ibm.com/support/knowledgecenter/SS42VS\\_DSM/c\\_LogSourceGuide\\_ExtDocs\\_typeIDs.html](https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_LogSourceGuide_ExtDocs_typeIDs.html)

[C2150-612 Practice Test](#)

[C2150-612 Exam Questions](#)

[C2150-612 Braindumps](#)