



# 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**

Which QRadar component provides Layer 7 visibility within a physical network infrastructure?

- A. QRadar Data Node
- B. QRadar Flow Analyzer
- C. QRadar Flow Collector
- D. QRadar VFlow Collector

Correct Answer: D

Reference: <https://www.robertrojek.pl/2017/11/09/qradar-appliances-types/>

---

**QUESTION 2**

An event is happening regularly and frequently; each event indicates the same target username. There is a rule configured to test for this event which has a rule action to create an offense indexed on the username. What will QRadar do with the triggered rule assuming no offenses exist for the username and no offenses are closed during this time?

- A. Each matching event will be tagged with the Rule name, but only one Offense will be created.
- B. Each matching event will cause a new Offense to be created and will be tagged with the Rule name.
- C. Events will be tagged with the rule name as long as the Rule Response limiter is satisfied. Only one offense will be created.
- D. Each matching event will be tagged with the Rule name, and an Offense will be created if the event magnitude is greater than 6.

Correct Answer: C

---

**QUESTION 3**

What is a main function of a Cisco Adaptive Security Appliance (ASA)?

- A. A Proxy
- B. A Switch
- C. A Firewall
- D. An Authentication device

Correct Answer: C

---

**QUESTION 4**



What are the various timestamps related to a flow?

- A. First Packet Time, Storage Time, Log Source Time
- B. First Packet Time, Storage Time, Last Packet Time
- C. First Packet Time, Log Source Time, Last Packet Time
- D. First Packet Time, Storage Time, Log Source Time, End Time

Correct Answer: B

Reference:

IBM Security QRadar SIEM Users Guide. Page: 101

---

#### QUESTION 5

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/>

[C2150-612 PDF Dumps](#)

[C2150-612 VCE Dumps](#)

[C2150-612 Braindumps](#)