



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

Which information can be found under the Network Activity tab?

- A. Flows
- B. Events
- C. Reports
- D. Offenses

Correct Answer: A

QUESTION 2

Which browser is officially supported for QRadar?

- A. Safari version 9.0.3
- B. Chromium version 33
- C. 32-bit Internet Explorer 9
- D. Firefox version 38.0 ESR

Correct Answer: D

Reference: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.1/com.ibm.qradar.doc/c_shi_browser_support.html

QUESTION 3

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

QUESTION 4

Which QRadar rule could detect a possible potential data loss?



- A. Apply "Potential data loss" on event of flows which are detected by the local system and when any IP is part of any of the following XForce premium Premium_Malware
- B. Apply "Potential data loss" on flows which are detected by the local system and when at least 1000 flows are seen with the same Destination IP and different Source IP in 2 minutes
- C. Apply "Potential data loss" on events which are detected by the local system and when the event category for the event is one of the following Authentication and when any of Username are contained in any of Terminated_User
- D. Apply "Potential data loss" on flows which are detected by the local system and when the source bytes is greater than 200000 and when at least 5 flows are seen with the same Source IP, Destination IP, Destination Port in 12 minutes

Correct Answer: D

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

[Latest C2150-612 Dumps](#)

[C2150-612 Practice Test](#)

[C2150-612 Study Guide](#)