

A2150-195^{Q&As}

Assess: IBM Security QRadar V7.0 MR4 Fundamentals

Pass IBM A2150-195 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/a2150-195.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 flow is a sequence of packets that have which common characteristics?

- A. Same source, MAC address, flow source and destination IP address
- B. Same source IP address, flow source and transport layer port information
- C. Same source and destination IP address and transport layer port information
- D. Same destination IP address, source bytes and transport layer port information

Correct Answer: C

QUESTION 2

What is the main difference between a QFlow record versus a netflow capable router or switch?

- A. QFlow can be used to trigger an alert.
- B. QFlow cannot capture the communication payload.
- C. QFlow can also be viewed in the Event Viewer window.
- D. QFlow and vFlow can capture the communication payload.

Correct Answer: D

QUESTION 3

How can a user cancel a running report in IBM Security QRadar V7.0 MR4?

- A. A running report cannot be canceled
- B. Select the report > Actions > Cancel Report
- C. Right-click on the report > select Cancel Report
- D. Look at the report queue, select the report to be canceled, select Delete

Correct Answer: A

QUESTION 4

A user is complaining of slow traffic on a specific network segment. An administrator is investigating the source of the

congestion using the IBM Security QRadar V7.0 MR4 (QRadar) Dashboard workspace named Top Applications. The administrator has drilled down into the details of a traffic spike and is now on the Details tab.

What information is shown when double-clicking on the top application in the list?

- A. A list of flows sorted by time for the selected application
- B. A list of flows sorted by time for all of the top applications listed
- C. A list of flows sorted by total byte count for the selected application
- D. A list of flows sorted by total byte count for all of the top applications listed

Correct Answer: A

QUESTION 5

In the Offense Summary page, which field indicates if an attack was sudden or if the attack occurred over a long period of time?

- A. Duration
- B. Total Time
- C. Attack Length
- D. Offense Period

Correct Answer: A

[Latest A2150-195 Dumps](#)

[A2150-195 PDF Dumps](#)

[A2150-195 Brindumps](#)