



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.geekcert.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

Which steps are required to see hidden offenses in IBM Security QRadar V7.0 MR4 (QRadar)?

- A. Contact the QRadar administrator to select Hidden Offenses and then choose the Show option from the Action menu.
- B. From the Offenses page, navigate to All Offenses and open the Search menu. Select Edit Search and in the Search Parameters section, uncheck the box Exclude Hidden Offenses.
- C. From the Offenses page, navigate to the Offenses by Category, and click on Show Inactive Categories to display all hidden offenses. Click Hide Inactive Categories to hide them again.
- D. Hidden Offenses are no longer associated with Offenses so a custom report and a search should be created that uses a search parameter where Associated with Offense equals False. To create a custom report, navigate to Reports and from the Actions menu select Create.

Correct Answer: B

QUESTION 2

A flow is always based on what?

- A. unicast and any cast traffic
- B. unicast and broadcast traffic
- C. unicast, multicast, and anycast traffic
- D. unicast, broadcast, and multicast traffic

Correct Answer: C

QUESTION 3

Which column in the log activity displays the coalesced value?

- A. Count
- B. Raw Count
- C. Event Count
- D. Roll-up Count

Correct Answer: C



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

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.

If the administrator double-clicks on the top application in the list, and then sorts by the Total Bytes column, what information is displayed regarding the source and destination IPs of the devices?

- A. The devices causing the least traffic for all applications
- B. The devices causing the most traffic for all applications
- C. The devices causing the least traffic for the selected application
- D. The devices causing the most traffic for the selected application

Correct Answer: D

[A2150-195 PDF Dumps](#)

[A2150-195 VCE Dumps](#)

[A2150-195 Brindumps](#)