



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

What is the Identity Information section used for?

- A. To show which rules match an event
- B. To show which log source an event belongs to
- C. To show the High/Low level category of an event
- D. To show the user information relative to an event

Correct Answer: D

QUESTION 2

Which regex should be used to capture only the domain name blackbox.computer for all future machine names based on this example?

``Computer=3 8 9.blackbox.computer\``

- A. `Computer= (. *) \s`
- B. `Computer=389. (.*)\s`
- C. `Computer=(389\..*)\s`
- D. `Computer=. *?. (.*)\s`

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

On the Offense Summary page, which filter is executed when the Flows icon or the link with the number of flows is clicked on?

- A. A flow filter with all flows matching the source IP address
- B. A flow filter with all flows matching the destination IP address
- C. A flow filter with the Custom Rule Engine rule(s) for the last 24 hours
- D. A flow filter with the Custom Rule Engine rule(s) for the duration of the offense

Correct Answer: D

QUESTION 5

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

[A2150-195 VCE Dumps](#)

[A2150-195 Study Guide](#)

[A2150-195 Brindumps](#)