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

Where would a user look to see the entire payload of an event?

A. The Raw Event tab

B. View > Show Payload

C. Right-click > Show Payload

D. The Payload Information section

Correct Answer: D

QUESTION 2

Which event search group contains default PCI searches?

A. Compliance

B. System Monitoring

C. Network Monitoring and Management

D. Authentication, Identity, and User Activity

Correct Answer: A

QUESTION 3

Using the regex * (RecordNumber) = (. *?)\s\\', which capture group should be used to capture the digits?

A. 0

B. 1

C. 2

D. 3

Correct Answer: C

QUESTION 4

How can a report be set up with restricted user access?

A. Click Reports > Restrict Users

B. Click on Manage Groups and add the user to the Restricted Reports group

C. Select the appropriate users on the Report Editing wizard to access the reports

D. Click Admin > Users, edit each user, and create lists of report filters users are allowed to see

Correct Answer: C

QUESTION 5

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

A2150-195 Practice Test   A2150-195 Study Guide   A2150-195 Braindumps