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

QUESTION 1

Which two pages or tabs are added to the IBM Security QRadar V7.0 MR4 (QRadar) Log Management product after it has been upgraded to QRadar SIEM? (Choose two.)

A. Admin

B. Reports

C. Offenses

D. Dashboard

E. Network Activity

Correct Answer: CE

QUESTION 2

How does a user search for events by high/low level category?

A. Actions menu > add a filter

B. Display drop-down > select categories

C. Add Filter icon > Category drop-down

D. View drop-down > select By Category drop-down

Correct Answer: C

QUESTION 3

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, uncheckthe 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 4

Click the Exhibit button.

What is the appropriate regex to extract the TirneWritten field value from the payload?

A. Written=.*\s

B. TimeWritten=.*\s

C. (TimeWritten=. *?\s)

D. TimeWritten=(. *?)\s

Correct Answer: D

QUESTION 5

What two tasks can be performed from the Assets tab? (Choose two.)

A. Edit asset severity

B. Clear vulnerabilities

C. Manually add asset profiles

D. Search assets that match specific attributes

E. Show which offenses an asset has been involved with

Correct Answer: CD