



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.passapply.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**

Everyone involved in a forensic analysis is now convinced that account management events involving promotion of accounts to AD administrator groups must be reported on daily. What is the most efficient method to accomplish this in IBM Security QRadar V7.0 MR4 (QRadar)?

- A. Such a report requires additional parsing of events using extra custom properties and then including these properties in a manual report.
- B. A new rule must be created which triggers an offense every time an account is assigned to an AD administrator group. By examining the event in detail it can be determined if this was really an offense or not.
- C. The detailed search that the user has used to identify the relevant events must be saved first. Once it is saved, then it can be reused on demand, and it can also be used to build a custom report which can then be scheduled.
- D. Automation or scripting is out of the question. The user has to repeat the analysis manually every time a similar incident occurs. The best the user can do is document the steps so that it is repeatable by anyone with access to the QRadar interface.

Correct Answer: C

QUESTION 2

Which item in the IBM Security QRadar V7.0 MR4 interface provides a context sensitive help page which is available for any page, window, or section?

- A. Help > Documentation
- B. type Help in the Search field
- C. Help drop-down list > Category
- D. The question mark in the far right corner

Correct Answer: D

QUESTION 3

What action must be taken to view reports related to PCI specifically?

- A. Right-click on Compliance and select PCI group.
- B. There are no filtering or grouping capabilities for reports.
- C. Click on the Group drop-down menu and select the category.
- D. SSH to the Console and execute a GREP command to find PCI report options.

Correct Answer: C



QUESTION 4

In the All Offenses dialog box, which column are the offenses sorted by default?

- A. Start Date
- B. Magnitude
- C. Description
- D. Offense Type

Correct Answer: B

QUESTION 5

An IBM Security QRadar V7.0 MR4 report can be generated into which three formats? (Choose three.)

- A. XLS
- B. PDF
- C. CSV
- D. DOC
- E. JPEG
- F. HTML

Correct Answer: ABF

[Latest A2150-195 Dumps](#)

[A2150-195 PDF Dumps](#)

[A2150-195 Study Guide](#)