A2150-195 Q&As

Assess: IBM Security QRadar V7.0 MR4 Fundamentals

Pass IBM A2150-195 Exam with 100% Guarantee

QUESTION 1

How does a user access the Extract a Custom Property section from a paused event screen in the Log Activity tab?

A. Actions menu > Extract Property

B. Double-click the event > Extract Property

C. Actions menu > Show All > Extract Custom Property

D. Right-click on the event > Properties > Extract Property

Correct Answer: B

QUESTION 2

Which search property is required for a user to create a Time Series chart?

A. Have a saved search filtered by an IP/CIDR

B. Have a saved search using an Order By option

C. Have a saved search displaying only two columns

D. Have a saved search with a Grouped By option enabled

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

If a report author shares a report with another IBM Security QRadar V7 0 MR4 user, what type of report access is granted to the other user?

A. The other user can only access the report if they are an administrator.

B. The other user can use the original report as if it were created by that person.

C. The report output will be defined by the intersection of networkobjects and log sources of alluser with whom the report is shared.

D. The other user will not have any access to the original report definition but can do as they please with the report definition of the shared copy.

Correct Answer: D

QUESTION 5

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 anoffense 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

Latest A2150-195 Dumps   A2150-195 Practice Test   A2150-195 Exam Questions