

Vendor: IBM

Exam Code: A2150-195

Exam Name: Assess: IBM Security QRadar V7.0 MR4 Fundamentals

Version: DEMO

QUESTION 1
What is the rule for using the Quick Filter to group terms using logical expressions such as AND, OR, and NOT?

A. The syntax is not case sensitive.
B. The syntax is case sensitive and the operators must be upper case to be recognized as logical expressions and not as search terms.
C. The syntax is case sensitive and the operators must be placed between square brackets to be recognized as logical expressions and not as search terms.
D. The syntax is case sensitive and the operators must be lower case and placed between square brackets to be recognized as logical expressions and not as search terms.

Answer: B

QUESTION 2
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

Answer: C

QUESTION 3
What is a QID identifier?

A. A mapping of a single device to a Q1 Labs unique identifier.
B. A mapping of a single event of an external device to a Q1 Labs unique identifier.
C. A mapping of multiple events of a single external device to a Q1 Labs unique identifier.
D. A mapping of a single event to multiple external devices to a Q1 Labs unique identifier.

Answer: B

QUESTION 4
Which event search group contains default PCI searches?

A. Compliance
B. System Monitoring
C. Network Monitoring and Management
D. Authentication, Identity, and User Activity

Answer: A

QUESTION 5
How many default dashboards are included in IBM Security QRadar V7.0 MR4?

A. 1
B. 2

C. 5
D. 8

Answer: C

QUESTION 6
Which flow source is most often sampled?

A. vFlow
B. sFlow
C. QFlow
D. netflow

Answer: B

QUESTION 7
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.

Answer: B

QUESTION 8
If the IBM Security QRadar V7.0 MR4 operator wants to graph the flow data in the Network Activity tab, which three chart types can be presented? (Choose three.)

A. Pie Chart
B. Bar Chart
C. Line Chart
D. Area Chart
E. Gant Chart
F. Time Series Chart

Answer: ABF

QUESTION 9
What does it mean if events are coming in as stored?

A. The events are not mapped to an existing QID map.
B. The events are being captured and parsed by a DSM.
C. The events are being captured but not being parsed by a DSM.

D. The events are being stored on disk and will be parsed by a DSM later.

Answer: C

QUESTION 10
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 network objects and log sources of all user 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.

Answer: D

Thank You for Trying Our Product

Lead2pass Certification Exam Features:



★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.



★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**