# 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.leads4pass.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**

What are three regulatory reports standard in IBM Security QRadar V7.0 MR4? (Choose three.)

A. SOX

B. NERC

C. HIPAA

D. BASEL

E. GPG13

F. ISO-9001

Correct Answer: ABC

**QUESTION 2**

When investigating an offense, how can a user gather information about the source IP address within IBM Security QRadarV7.0MR4?

A. Ping the IP address

B. Perform a NMap scan

C. Perform a Google search

D. Mouse over the source IP address

Correct Answer: D

**QUESTION 3**

What are three types of time options available to search on from the View pull-down menu under Network Activity and Log Activity? (Choose three.)

A. Last Year

B. Real Time

C. Last Month

D. Date Range

E. Last Interval

F. Last 45 Minutes

Correct Answer: BEF

**QUESTION 4**

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 5**

When using the Quick Filter feature in the Network Activity tab, which character must be used in front of special characters to indicate that the character is part of the search term?

A. +(plus)

B. -(minus)

C. \ (backslash)

D. ? (question mark)

Correct Answer: C

**QUESTION 6**

If an IBM Security QRadar V7.0 MR4 operator wants to make the log data view/search available as a Dashboard item, what specifically must be done with the saved log search?

A. The search must be assigned to a Group.

B. The search must be saved as a Quick Search.

C. The search results must be exported as an XML document.

D. The search must be grouped around a parameter such as Source IP, Destination IP, etc.

Correct Answer: D

**QUESTION 7**

For any Dashboard workspace, which two methods can be used to zoom into any of the spikes in traffic? (Choose two.)

A. Right-click on the peak of the spike

B. Double left-click on the peak of the spike

C. Hold the Shift key, left-click the mouse, drag to the right past the spike, and release the mouse button

D. Hold the Ctrl key. right-click the mouse, drag to the right past the spike, and release the mouse button

E. Hold the Shift key, right-click the mouse, drag to the right past the spike, and release the mouse button

Correct Answer: BC

**QUESTION 8**

IBM Security QRadar V7.0 MR4 (QRadar) events that match a particular QRadar event rule are given a magnitude. This magnitude is a combination of which three factors?

A. Severity. Relevance, Weight

B. Severity, Frequency, Weight

C. Severity, Quantity, Credibility

D. Severity, Relevance, Credibility

Correct Answer: D

**QUESTION 9**

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 10**

Which function queries for offenses using specific criteria and displays those offenses that match the criteria?

A. Find

B. Search

C. Offense Lookup

D. Right-click > Navigate

Correct Answer: B

**QUESTION 11**

By default how often is the information on the Dashboard refreshed?

A. Every 30 seconds

B. Every 60 seconds

C. Every 90 seconds

D. Every 120 seconds

Correct Answer: B

**QUESTION 12**

What is required for a custom report to be generated?

A. A saved search

B. Administrative access

C. A custom report group

D. Access to the Custom Reporting module

Correct Answer: A

**QUESTION 13**

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 14**

How can a user search to show only hosts with vulnerabilities?

A. Change the risk level to a value greater than five

B. From the Assets tab click on VA Scan and view results

C. From the Assets tab select Actions > Show Vulnerabilities

D. Check the Show Only Hosts with Vulnerabilities checkbox

Correct Answer: D

**QUESTION 15**

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

Correct Answer: ABF

A2150-195 Practice Test A2150-195 Exam Questions A2150-195 Braindumps