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.pass2lead.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 regex should be used to capture only the domain name blackbox.computerfor all future machine names based on this example?

`Computer=3 8 9.blackbox.computer\\'

A. Computer= (. *?) \s

B. Computer=389. (.*?)\s

C. Computer=(389\..*?)\s

D. Computer=. *?\. (.*?)\s

Correct Answer: D

QUESTION 2

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

A. 1

B. 2

C. 5

D. 8

Correct Answer: C

QUESTION 3

A flow is a sequence of packets that have which common characteristics?

A. Same source, MAC address, flow source and destination IP address

B. Same source IP address, flow source and transport layer port information

C. Same source and destination IP address and transport layer port information

D. Same destination IP address, source bytes and transport layer port information

Correct Answer: C

QUESTION 4

What must be done in order to save a search criteria as a quick search?

A. Select Save Criteria and select My Dashboard

B. Select Save Criteria in the New/Edit Search dialog

C. Right-click on the filter and select Save as Quick Search

D. Select Save Criteria and select Include in my Quick Searches

Correct Answer: D

QUESTION 5

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 6

When working with rules, why do some rules specify QID values and some specify events?

A. Only low and high level categories can be specified within rules.

B. It is a matter of convention; QIDmap and event names are the same.

C. Event names are more precise; multiple events can be to the same QIDmap entry.

D. QID values are more precise; multiple QIDmap entries can be to same event name.

Correct Answer: D

QUESTION 7

A user is complaining of slow traffic on a specific network segment. An administrator is investigating the source of the congestion using the IBM Security QRadar V7.0 MR4 (QRadar) Dashboard workspace named Top Applications. The administrator has drilled down into the details of a traffic spike and is now on the Details tab.

What information is shown when double-clicking on the top application in the list?

A. A list of flows sorted by time for the selected application

B. A list of flows sorted by time for all of the top applications listed

C. A list of flows sorted by total byte count for the selected application

D. A list of flows sorted by total byte count for all of the top applications listed

Correct Answer: A

QUESTION 8

Where are QID values displayed?

A. In the Asset Properties of the asset

B. In the QID map menu of the Adrnin tab

C. In the detailed view of the Network Activity tab

D. In the Additional Information section of the event

Correct Answer: D

QUESTION 9

What are three time range options in the New/Edit search dialog box? (Choose three.)

A. Recent

B. Last Year

C. Real Time

D. Next Week

E. Last Month

F. Specific Interval

Correct Answer: ACF

QUESTION 10

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

QUESTION 11

How can a user pause live streaming events?

A. Action menu > Pause

B. Select the Pause icon

C. Display drop-down > Pause

D. Right-click on Events > Pause

Correct Answer: B

QUESTION 12

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 13

How can a user display Raw events?

A. View drop-down > Raw Events

B. Action menu > View Raw Events

C. Display drop-down > Raw Events

D. Right-click on the events > View Raw Events

Correct Answer: C

QUESTION 14

Which two components are only part of the IBM Security QRadar V7.0 MR4 (QRadar) SIEM and cannot be found in the QRadar Log Management? (Choose two.)

A. Console

B. Flow Collector

C. Event Collector

D. Event Processor

E. Offense Manager

Correct Answer: BE

QUESTION 15

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