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

QUESTION 1

Which colored icon must be selected in the chart to change the chart type when viewing a grouped search?

A. The red X

B. The green star

C. The yellow gear

D. The blue question mark (?)

Correct Answer: C

QUESTION 2

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 3

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 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

Correct Answer: A

QUESTION 5

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 6

Which two pages or tabs are added to the IBM Security QRadar V7.0 MR4 (QRadar) Log Management product after it has been upgraded to QRadar SIEM? (Choose two.)

A. Admin

B. Reports

C. Offenses

D. Dashboard

E. Network Activity

Correct Answer: CE

QUESTION 7

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 8

How can a user clear all filters and return to the default search in the Log Activity user interface?

A. Search > Default Search

B. Action menu > Clear All Filters

C. Double-click the Log Activity tab

D. Right-click on the filter and select Clear Filter

Correct Answer: C

QUESTION 9

Using Quick Filter, what is a correct search term to find Blocked related activities in the payload?

A. Blocked

B. "payload includes Blocked"

C. payload includes "Blocked"

D. (payload includes) Blocked

Correct Answer: A

QUESTION 10

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 11

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 12

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.

Correct Answer: B

QUESTION 13

If an IBM Security QRadar V7.0 MR4 operator wants to detect a specific data string in the flow content, which search parameter should be used as a filter?

A. Source IP

B. Event Name

C. Remote Network

D. Source Payload Contains

Correct Answer: D

QUESTION 14

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 15

Which four fields are used when importing assets from a CSV file?

A. IP, Name, Weight. Description

B. IP. Port, MAC Address, Weight

C. IP, Port. MAC Address. Description

D. IP, User, Host Name, Service Version

Correct Answer: A