Vendor:IBM

Exam Code:A2150-195

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

Version: Demo

QUESTION 1

Offenses can be exported to which two file formats? (Choose two.)

A. RTF

B. XML

C. PDF

D. CSV

E. HTML

Correct Answer: BD

QUESTION 2

What is used to parse an event (log record) in IBM Security QRadar V7.0 MR4?

A. CRE

B. DSMs

C. Qidmaps

D. Protocols

Correct Answer: B

QUESTION 3

What are two examples of an exact search phrase for finding Firewall deny events using the Quick Filter? (Choose two.)

A. Firewall deny

B. Firewall*deny

C. Firewall.*deny

D. Firewall + deny

E. "Firewall" + "deny"

Correct Answer: AD

QUESTION 4

On the Offense Summary page, which filter is executed when the Flows icon or the link with the number of flows is clicked on?

A. A flow filter with all flows matching the source IP address

B. A flow filter with all flows matching the destination IP address

C. A flow filter with the Custom Rule Engine rule(s) for the last 24 hours

D. A flow filter with the Custom Rule Engine rule(s) for the duration of the offense

Correct Answer: D

QUESTION 5

What is the Identity Information section used for?

A. To show which rules match an event

B. To show which log source an event belongs to

C. To show the High/Low level category of an event

D. To show the user information relative to an event

Correct Answer: D

QUESTION 6

Where would a user set a searched view as the default view?

A. Under Save Criteria

B. Under the Admin tab

C. Select the View drop-down list

D. Select Default under the Actions menu

Correct Answer: A

QUESTION 7

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 8

Which statement is most accurate regarding the information that NetFlow provides?

A. The start time of the conversation, the source and destination IP address, and the total bytes transferred.

B. The start time and the duration of the conversation, application ID, the source and the destination IP address.

C. The start time and duration of the conversation, the source and destination IP address, payload information, and the IP port number the data was sent to and received over.

D. The start time and duration of the conversation, the source and destination IP address, the IP port number the data was sent to and received over, and the total bytes transferred.

Correct Answer: D

QUESTION 9

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 10

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 11

A user is complaining about slow traffic on a specific network segment, and an administrator has been asked to investigate the source of the congestion using an IBM Security QRadar V7.0 MR4 (QRadar) Dashboard workspace named Top Applications.

From the Top Applications dashboard workspace, which tab is displayed when View Details is clicked?

A. Assets

B. Offenses

C. Log Activity

D. Network Activity

Correct Answer: D

QUESTION 12

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