

IBM 000-195

IBM Security QRadar V7.0 MR4
Version: 4.0

QUESTION NO: 1

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

Explanation:

QUESTION NO: 2

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 networkobjects and log sources of alluser 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

Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 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

Explanation:

QUESTION NO: 5

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

Explanation:

QUESTION NO: 6

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

Explanation:

QUESTION NO: 7

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

- A. 1
- B. 2
- C. 5
- D. 8

Answer: C

Explanation:

QUESTION NO: 8

Which flow source is most often sampled?

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

Answer: B

Explanation:

QUESTION NO: 9

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, uncheck the 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

Explanation:

QUESTION NO: 10

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: A,B,F

Explanation:

QUESTION NO: 11

On the Offense summary page, which filter is executed when the Events icon or the link with the number of events is clicked?

- A. An event filter with all events matching the source IP address
- B. An event filter with all events matching the destination IP address
- C. An event filter with the Custom Rule Engine rule(s) for the last 24 hours
- D. An event filter with the Custom Rule Engine rule(s) for the duration of the offense

Answer: D

Explanation:

QUESTION NO: 12

What is a prerequisite to create a report that contains at least one bar chart?

- A. Have a color display and enable the JPanel
- B. Have the role assigned to create (graphical) reports
- C. Choose a search that has accumulated properties for the report

D. The search contained in the report must aggregate the results at least along one property

Answer: D

Explanation:

QUESTION NO: 13

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

Answer: A

Explanation:

QUESTION NO: 14

How does a user search for events by high/low level category?

- A. Actions menu > add a filter
- B. Display drop-down > select categories
- C. Add Filter icon > Category drop-down
- D. View drop-down > select By Category drop-down

Answer: C

Explanation:

QUESTION NO: 15

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

- A. RTF
- B. XML
- C. PDF
- D. CSV
- E. HTML

Answer: B,D

Explanation:

QUESTION NO: 16

In the All Offenses dialog box, which column are the offenses sorted by default?

- A. Start Date
- B. Magnitude
- C. Description
- D. Offense Type

Answer: B

Explanation:

QUESTION NO: 17

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

Answer: B

Explanation:

QUESTION NO: 18

Why is coalescing important to a non-admin user?

- A. It saves space on disk.
- B. It saves events per second.
- C. It makes it faster to parse the events.
- D. It makes events easier to read in the Log Activity screen.

Answer: D