Vendor: IBM

Exam Code: C2150-195

Exam Name: IBM Security QRadar V7.0 MR4

Version: Demo

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, uncheckthe 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

Explanation:

QUESTION NO: 19

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

Answer: A,B,F
Explanation:

QUESTION NO: 20

How would a user navigate to the Help menu in the IBM Security QRadar V7.0 MR4 (QRadar) interface?

A. Press Ctrl+H
B. Right-click on Item > Help
C. Help > QRadar Help Content
D. Select from the Action drop-down list

Answer: C
Explanation:

QUESTION NO: 21

Which statement about log source identifiers is true for the same log source identifier to be used more than once?

A. It must always be unique.
B. It must be unique amongst the same protocol.
C. It must be unique amongst the same log source group.

D. It must be unique amongst log sources of the same type

Answer: D
Explanation:

QUESTION NO: 22

What is an Offense Type?

A. The offense response
B. A scoring priority of Set by Event
C. The destination of the e-mail notification sent
D. The index option chosen in the rule that created the offense

Answer: D
Explanation:

QUESTION NO: 23

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.

Answer: D
Explanation:

QUESTION NO: 24

How can a user quickly add a filter?

A. Actions > Add Filter

B. Click the Add Filter menu icon
C. Search > Edit Search, and add the filter
D. Right-click the column header > Add Filter

Answer: B
Explanation:

QUESTION NO: 25

In the default Log Activity screen the right-click > False Positive menu is available in which column?

A. In every column
B. In every column header
C. In every column except time
D. In only the source and destination IP addresses columns

Answer: C
Explanation:

QUESTION NO: 26

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

Answer: D
Explanation:

QUESTION NO: 27

What are two IT Security Frameworks? (Choose two.)

A. ITIL

B. SLA
C. COBIT
D. ISO 27001
E. Common Criteria

Answer: C,D
Explanation:

QUESTION NO: 28

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 (?)

Answer: C
Explanation:

QUESTION NO: 29

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

Answer: A
Explanation:

QUESTION NO: 30

What effect does the Offense Retention period have on closed offenses and who can modify this period?

A. The Offense Retention period determines how long a closed offense will be kept in the database before it is deleted. The only person who can modify this period is an IBM Security QRadar V7.0 MR4 (QRadar) admin.
B. Once an offense is closed, any other QRadar user will be able to open it again for the time given by the Offense Retention period. The person who closes an offense is also the person who determines the offense retention period of the closed offense.
C. The offense retention period has no effect on closed offenses. A closed offense is the same as a deleted offense, and offenses that are deleted do not have a retention time. Only QRadar admins can change the offense retention period because it is found in the Admin tab.
D. The offense retention period has no effect on the closed offenses but only on offenses under evaluation. While the QRadar magistrate evaluates and correlates offenses, it may rely on the life span of an offense. Everyone who can create QRadar rules can modify the offense retention period.

Answer: A
Explanation:

QUESTION NO: 31

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

Answer: D
Explanation:

QUESTION NO: 32

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

Answer: D
Explanation:

QUESTION NO: 33

What are the three common fields on the Asset tab > VA Scan section? (Choose three.)

A. Potts
B. Status
C. Host Name **D.**
Asset Name **E.**
MAC Address
F. Next Run Time

Answer: A,B,F
Explanation:

QUESTION NO: 34

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

Answer: B,C
Explanation:

QUESTION NO: 35

How does IBM Security QRadar V7.0 MR4 (QRadar) use the information from vulnerability scanners?

A. The internal QRadar vulnerability scanner provides reports for auditors.
B. The results are used by QRadar to automatically patch and update the asset.
C. The information can be used to determine if an asset is vulnerable to an exploit.
D. Systems on which vulnerabilities are found are automatically monitored more closely.

Answer: C
Explanation:

QUESTION NO: 36

How can the time zone be changed for an existing report?

A. From the Report tab > Actions > select Time Zone
B. Right-click on the Report template > Change Time Zone
C. Select the report from the Reports tab > Options > Change Time Zone
D. Modify the template, under Chart Type select Define > select Time Zone

Answer: D
Explanation:

QUESTION NO: 37

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

Answer: D
Explanation:

QUESTION NO: 38

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

Answer: B,E
Explanation:

QUESTION NO: 39

Which search parameter in the Log Activity tab must be used to filter events by activity (e.g. SSH Login Succeeded)?

A. Category **B.**
Magnitude **C.**
User Name **D.**
Log Source

Answer: A
Explanation:

QUESTION NO: 40

What two tasks can be performed from the Assets tab? (Choose two.)

A. Edit asset severity
B. Clear vulnerabilities
C. Manually add asset profiles
D. Search assets that match specific attributes
E. Show which offenses an asset has been involved with

Answer: C,D
Explanation:

QUESTION NO: 41

Click the Exhibit button.

```
<13>Apr 17 00:23:40 user_desktop AgentDevice=WindowsLog
AgentLogFile=Security Source=Microsoft-Windows-Security-
Auditing Computer=389.blackbox.computer User= Domain=
EventID=5156 EventIDCode=5156 EventType=8
EventCategory=12810 RecordNumber=148983706
TimeGenerated=1334633018 TimeWritten=1334633018
Message=The Windows Filtering Platform has permitted a
connection. Application Information: Process ID: 1772 Application
Name: \device\harddiskvolume3\windows\system32\svchost.exe
Network Information: Direction: Inbound Source Address:
224.0.0.252 Source Port: 5355 Destination Address: 11.20.13.42
Destination Port: 61903 Protocol: 17 Filter Information: Filter Run-
Time ID: 66565 Layer Name: Receive/Accept Layer Run-Time ID:
44
```

What is the appropriate regex to extract the TirneWritten field value from the payload?

A. Written=.*\s
B. TimeWritten=.*\s
C. (TimeWritten=. *?\s)
D. TimeWritten=(. *?)\s

Answer: D
Explanation:

QUESTION NO: 42

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

Answer: D
Explanation:

QUESTION NO: 43

Which tab displays correlated security alerts in IBM Security QRadar V7.0 MR4?

A. Admin
B. Reports
C. Offenses
D. Log Activity

Answer: C
Explanation:

QUESTION NO: 44

How can a user quickly reload the default filter in their current tab?

A. Use the View option
B. Use the Display option
C. Clear all the current filters
D. Double-click the Tab button

Answer: D
Explanation:

QUESTION NO: 45

How is an asset's weight used?

A. To classify the level of asset activity
B. To define the vulnerability of the asset
C. To determine how much emphasis IBM Security QRadar V7.0 MR4 gives when parsing logs
D. To determine the true severity and relevance of an event when the asset is involved in an offense

Answer: D
Explanation:

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

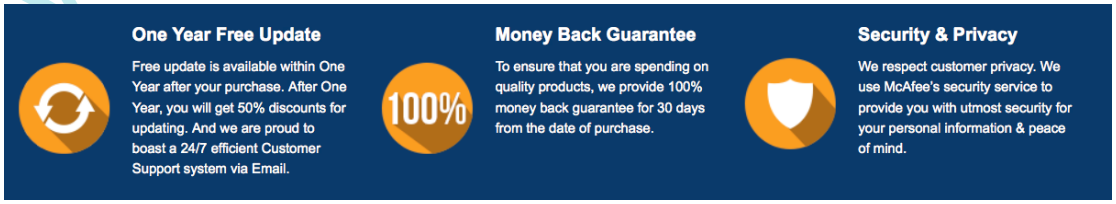
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.