IBM

C2150-195

IBM Security QRadar V7.0 MR4

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

Answer: C

QUESTION: 95
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 detailsof 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 topapplications 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

Answer: A

QUESTION: 96
Given the IBM Security Framework, IBM SecurityQRadar V7.0 MR4 fits into which two security domains? (Choose two.)

A. Data
B. People and Physical Security
C. Infrastructure, Network, or Endpoint
D. Applications and Application Security
E. IT Security/Compliance Analytics and Reporting

Answer: C, E

QUESTION: 97
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

Answer: A, C, F

QUESTION: 98
How can a user pause live streamingevents?

A. Action menu > Pause
B. Select the Pause icon
C. Display drop-down > Pause
D. Right-click on Events > Pause

Answer: B

QUESTION: 99
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

Answer: C, E

QUESTION: 100
If a user wants to search for Windows user login failures, which high/low level category should beused?

A. Windows/Failures
B. Authentication/Failures

C. Windows/User Login Failures
D. Authentication/User Login Failure

Answer: D

QUESTION: 101
On the Offense Summary page, which filter is executed when the Flows icon or the link with the number offlows 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

Answer: D

QUESTION: 102
On the Offenses tab, which option displays offenses by access, exploit, or malware?

A. By Rules
B. By Category
C. By Definition
D. By Source IP

Answer: B

QUESTION: 103
The remote directory field can be left blank for which protocol?

A. FTP
B. TFTP
C. SFTP
D. FTPS

Answer: A

QUESTION: 104
What are two instances when IBM Security QRadar V7.0 MR4 performs a magnitude re-evaluation for an offense? (Choose two.)

A. At scheduled intervals
B. When the offense is closed
C. When the offense is created
D. When each event or flow is added
E.When the offense is assigned to a user

Answer: A, D

Pass your exam at First Attempt....Guaranteed!