IBM

A2150-195

Assess- IBM Security QRadar V7.0 MR4 Fundamentals

QUESTION: 89
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 ofan event
D. To show the user information relative to an event

Answer: D

QUESTION: 90
Which column in the log activity displays the coalesced value?

A. Count
B. Raw Count
C. Event Count
D. Roll-up Count

Answer: C

QUESTION: 91
Wheninvestigating an offense, what is the best option to gather information about the destination IP addresses within IBM Security QRadar V7.0 MR4?

A. Analyze the destination IP addresses and look for recent activity
B. Analyze the destination IP addresses and look for DHCP addresses
C. Analyze the destination IP addresses and look for low asset weights
D. Analyze the destination IP addresses and look for critical services to determine if they are local or remote

Answer: D

QUESTION: 92
Everyone involvedin a forensic analysis is now convinced that account management events involving promotion of accounts to AD administrator groups must be reported on daily.
What is the most efficient method to accomplish this in IBM Security QRadar V7.0 MR4 (QRadar)?

A. Such a report requires additional parsing of events using extra custom properties and then including these properties in a manual report.
B. A new rule must be created which triggers an offense every time an account is assigned to an AD administrator group. By examining the event in detail it can be determined if this was really an offense or not.
C. The detailed search that the user has used to identify the relevant events must be saved first. Once it is saved, then it can be reused on demand, and it can also be used to build a custom report which can then be scheduled.
D. Automation or scripting is out of the question. The user has to repeat the analysis manually every time a similar incident occurs. The best the user can do is document the steps so that it is repeatable by anyone with access to the QRadar interface.

Answer: C

QUESTION: 93
An IBM Security GRadar V7.0 MR4 (QRadar) user has access to QRadar offenses. How do offenses appear in their My Offenses page?

A. Rules that have been created bythe admin and that trigger an offense will also automatically put the triggered offense under their My Offenses page.
B. When the admin accesses the All Offenses option, they select Offenses and drag and drop them to their My Offenses page. Other QRadar users will no longer see the offenses that are put under their My Offenses page.
C. Anyone with access to the Offenses page will see all offenses. Under the My Offenses option, the person will see all offenses that have been assigned to them for further analysis and processing. These offenses are assigned from the All Offenses page by choosing the Assign option from the Action menu.
D. Rules that trigger an offense can also be configured in such way that the resulting offense is automatically assigned to theQRadar user who is notified of the offense by e- mail. The rule is configured to send an e-mail and if the e-mail address matches an e-mail addresse of any of the QRadar users then this offense is automatically added to the My Offenses page of this user.

Answer: C

QUESTION: 94
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