A2150-195^Q&As

Assess: IBM Security QRadar V7.0 MR4 Fundamentals

QUESTION 1

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

Correct Answer: C

QUESTION 2

In the Offense Summary page, which field indicates if an attack was sudden or if the attack occurred over a long period of time?

A. Duration

B. Total Time

C. Attack Length

D. Offense Period

Correct Answer: A

QUESTION 3

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.

Correct Answer: A

QUESTION 4

Which flow direction would a user specify in order to see flows that are solely related to traffic that originates from the internal networks to external networks?

A. L2L

B. R2L

C. L2R

D. R2R

Correct Answer: C

QUESTION 5

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

Correct Answer: CE

QUESTION 6

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

Correct Answer: C

QUESTION 7

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

A. FTP

B. TFTP

C. SFTP

D. FTPS

Correct Answer: A

QUESTION 8

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

Correct Answer: D

QUESTION 9

Everyone involved in 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 anoffense 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.

Correct Answer: C

QUESTION 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

Correct Answer: ABF

QUESTION 11

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

Correct Answer: BE

QUESTION 12

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

Correct Answer: D

QUESTION 13

What are two ways that asset profiles can be populated? (Choose two.)

A. Flow data

B. Heartbeat traffic

C. Router configuration

D. Windows application logs

E. Vulnerability assessment scans

Correct Answer: AE

QUESTION 14

When investigating 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

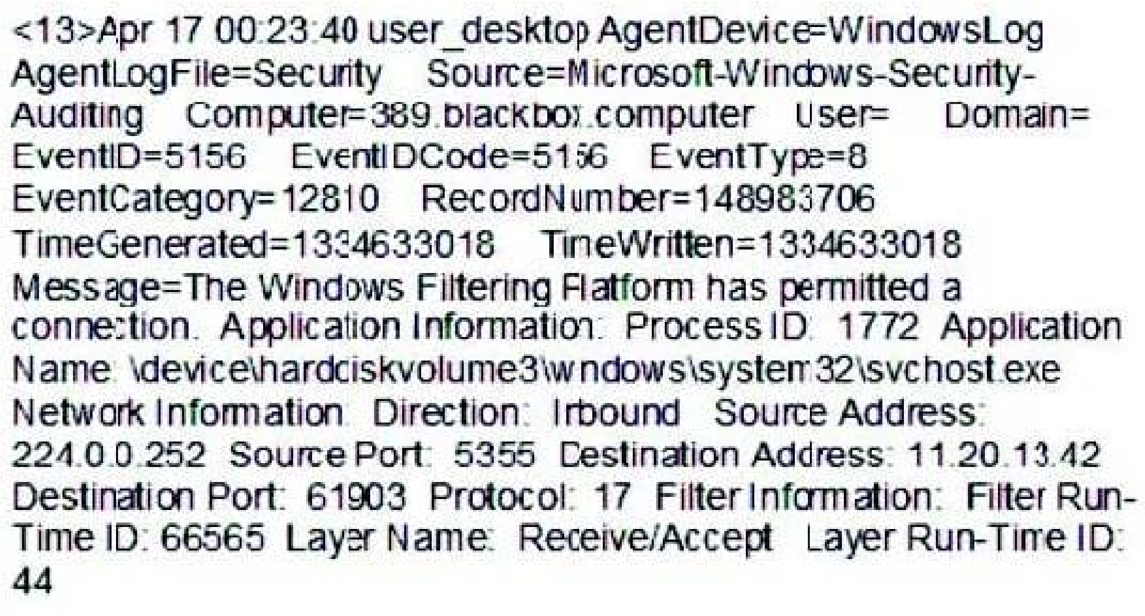
C. Analyze the destination IP addresses and look for low asset weights

D. Analyze the destination IP addresses and look for critical services to determine if they are local or remote

Correct Answer: D

QUESTION 15

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

Correct Answer: D

[A2150-195 Practice Test](#) [A2150-195 Study Guide](#) [A2150-195 Braindumps](#)