A2150-195 Q&As

Assess: IBM Security QRadar V7.0 MR4 Fundamentals

QUESTION 1

A flow is always based on what?

A. unicast and any cast traffic

B. unicast and broadcast traffic

C. unicast. multicast, and anycast traffic

D. unicast, broadcast, and multicast traffic

Correct Answer: C

QUESTION 2

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 3

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

A. Start Date

B. Magnitude

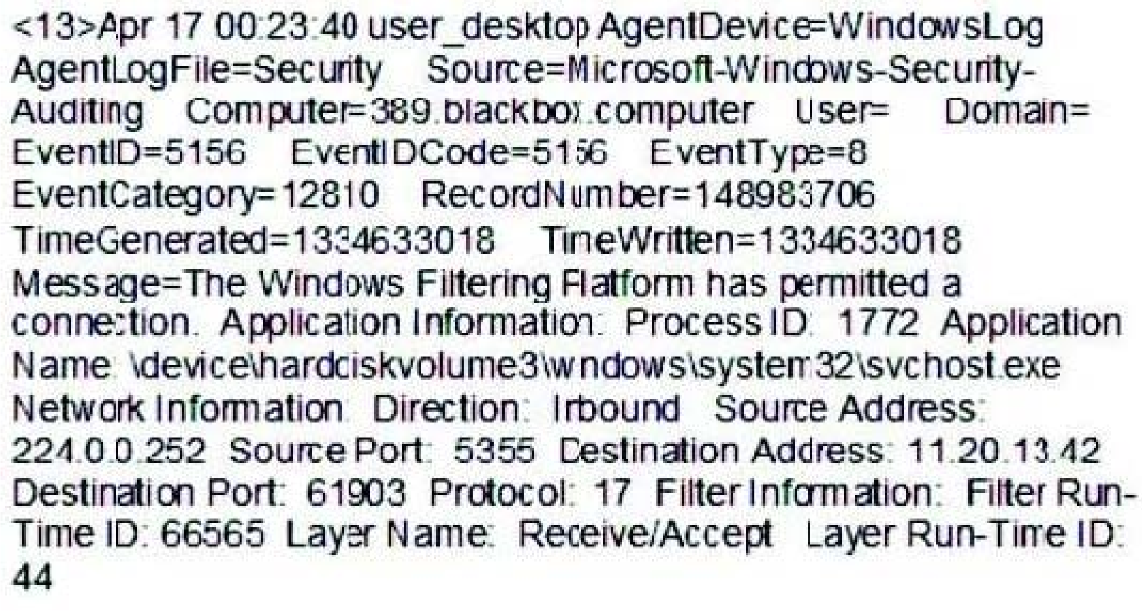
C. Description

D. Offense Type

Correct Answer: B

QUESTION 4

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

QUESTION 5

By default how often is the information on the Dashboard refreshed?

A. Every 30 seconds

B. Every 60 seconds

C. Every 90 seconds

D. Every 120 seconds

Correct Answer: B