



# A2150-195<sup>Q&As</sup>

Assess: IBM Security QRadar V7.0 MR4 Fundamentals

**Pass IBM A2150-195 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/a2150-195.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by IBM Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### 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 TimeWritten 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



VCE & PDF

GeekCert.com

<https://www.geekcert.com/a2150-195.html>

2024 Latest geekcert A2150-195 PDF and VCE dumps Download

---

[Latest A2150-195 Dumps](#)

[A2150-195 Practice Test](#)

[A2150-195 Exam Questions](#)