



# *IBM*

*C1000-175*

*Foundations of IBM Security QRadar SIEM V7.5*

## Questions & Answers PDF

**For More Information:**

**<https://www.certswarrior.com/>**

## **Features:**

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24/7 Online Chat Support
- Its Latest Version

---

# Latest Version: 6.0

## Question: 1

From which IBM site can Content Packs including Custom Properties be downloaded?

Response:

- A. IBM Support
- B. IBM API Hub
- C. IBM Fix Central
- D. IBM App Exchange

**Answer: D**

## Question: 2

Why is it important to define a parsing order for log sources that share a common Log Source Identifier in QRadar?

Response:

- A. Prioritize low-level event sources for faster processing
- B. Accommodate frequent changes to log source configuration
- C. Allow random parsing of log sources for performance optimization
- D. Ensure a specific order of parsing, prevent unnecessary parsing, and maintain system performance

**Answer: D**

## Question: 3

QRadar SIEM ingests event data from a wide range of sources, including on-premises and cloud environments. Which SIEM functionality is described?

Response:

- A. Log Management
- B. Event Correlation and Analytics
- C. Incident Monitoring and Security Alerts
- D. Compliance Management and Reporting

**Answer: A**

---

### Question: 4

What happens to a rule when it is deleted from a group?

Response:

- A. The rule remains in disabled state.
- B. The rule is flushed from the system.
- C. The rule remains available on the Rules page.
- D. The rule is no longer available on the Rules page.

**Answer: C**

### Question: 5

Who can edit the account of an administrative role user?

Response:

- A. The user can edit their own administrative account
- B. Only a user with Delegated Administration functions
- C. Any user can edit the account of an administrative user
- D. Another administrative user must make any account changes

**Answer: D**

### Question: 6

You need to use Ariel Query Language to select the default columns from events. Which is the correct query?

Response:

- A. SELECT % FROM events
- B. SELECT \* FROM events
- C. SELECT ALL FROM events
- D. SELECT defaultcolumns from events

**Answer: B**

### Question: 7

Which two properties are the magnitude rating of an offense based on?

---

Response:

- A. Severity
- B. Priority
- C. Credibility
- D. Accuracy
- E. Offense correlation

**Answer: A,C**

### Question: 8

Which QRadar application supports building dashboards from custom AQL (Ariel Query Language) queries and QRadar offenses?

Response:

- A. Pulse
- B. Use Case Manager
- C. Threat Intelligence
- D. User Behavioral Analytics

**Answer: A**

### Question: 9

Which QRadar application can delete, stop, or start other installed QRadar applications?

Response:

- A. Pulse
- B. QRadar Assistant
- C. Use Case Manager
- D. Threat Intelligence

**Answer: B**

### Question: 10

A customer wants to implement QRadar Network Insights to detect suspicious traffic content using YARA rules. What is the minimum inspection level?

Response:

- A. Basic

- 
- B. Advanced
  - C. Enriched
  - D. Advanced, but without SSL/TLS certificate inspection enabled

|                  |
|------------------|
| <b>Answer: C</b> |
|------------------|



# CERTSWARRIOR

## FULL PRODUCT INCLUDES:

Money Back Guarantee



Instant Download after Purchase



90 Days Free Updates



PDF Format Digital Download



24/7 Live Chat Support



Latest Syllabus Updates



For More Information – Visit link below:

**<https://www.certswarrior.com>**

**16 USD Discount Coupon Code: U89DY2AQ**