

IBM

A1000-175

**Assessment: Foundations of IBM Security QRadar SIEM
V7.5**

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

- 1. Up to Date products, reliable and verified.**
- 2. Questions and Answers in PDF Format.**



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/a1000-175>

Latest Version: 6.0

Question: 1

Which component of QRadar is primarily responsible for normalizing incoming log data into a common format?

- A. Event Processor
- B. Event Collector
- C. Ariel Database
- D. Flow Processor

Answer: B

Explanation:

The Event Collector receives raw log data from sources and normalizes it into QRadar's Common Event Format (CEF) before forwarding it to the Event Processor.

Question: 2

In QRadar, what is the purpose of an "Offense"?

- A. To store raw log data permanently
- B. To aggregate related security events that indicate a potential threat
- C. To route network flows to the appropriate destination
- D. To manage user authentication for the console

Answer: B

Explanation:

An Offense groups events that share common attributes (e.g., source IP, rule trigger) and represent a possible security incident.

Question: 3

Which of the following best describes the function of the Ariel Query Language (AQL)?

- A. It defines network flow collection parameters
- B. It provides a way to query the Ariel database for events, flows, and offenses
- C. It configures user roles and permissions
- D. It encrypts log data before storage

Answer: B

Explanation:

AQL is QRadar's SQL-like language used to retrieve data from the Ariel database, allowing custom searches of events, flows, and offenses.

Question: 4

When configuring a new log source, which property determines how QRadar parses the incoming data?

- A. Log Source Identifier
- B. Protocol Type
- C. Log Source Type
- D. Credential Set

Answer: C

Explanation:

The Log Source Type tells QRadar which parser to apply (e.g., Syslog, Windows Event Log, Database) to correctly interpret the data.

Question: 5

What does the "QID" (QRadar Identifier) represent?

- A. A unique identifier for a network flow
- B. A unique identifier for a normalized event type
- C. The ID of a user role in QRadar
- D. The version number of a deployed rule

Answer: B

Explanation:

QID is QRadar's internal classification for a specific type of normalized event, enabling consistent rule processing.

Thank You for Trying Our Product
Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>