IBM

A1000-156

Assessment: IBM Security QRadar SIEM V7.5 Administration

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.**

Latest Version: 6.0

Question: 1

In QRadar, which component is primarily responsible for assigning a severity level to an offense?

A. Event Collector
B. Flow Processor
C. Offense Manager
D. Ariel Search Engine

Answer: C

Explanation:
The Offense Manager evaluates rule matches and calculates offense severity based on rule severity, magnitude, and credibility.

Question: 2

Which magnitude attribute reflects how many unique assets are involved in an offense?

A. Relevance
B. Severity
C. Credibility
D. Magnitude Score

Answer: A

Explanation:
Relevance measures the breadth ofimpact, such as the number of distinct assets, users, or IPs implicated.

Question: 3

When an offense transitions fran "Active" to "Inactive," which condition must be met?

A. All associated events are older than 24 hours
B. No new matching events have for the offense's time window
C. The offense has been manually closed by a user
D. The rule that generated it has been disabled

Answer: B

Explanation:
An offense becomes inactive when its correlation window expires without additional matching events.

Question: 4

A rule that matches on both Event and Flow data is known as a:

A. Hybrid rule
B. Composite rule
C. Dual-source rule
D. Multi-type rule

Answer: A

Explanation:
QRadar refers to rules that evaluate both event and flow criteria as hybrid rules.

Question: 5

Which of the following best describes a "Partial Match" in QRadar offense details?

A. All rule conditions are satisfied but the rule is disabled
B. Some, but not all, rule conditions are met
C. The rule matched but the offense was filtered out by a reference set
D. The rule matched only on flow data, not events

Answer: B

Explanation:
A partial match indicates that only a subset of the rule's conditions were satisfied.

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/