

Boost up Your Certification Score

IBM

A1000-162

Assessment: IBM Security QRadar SIEM V7.5 Analysis



For More Information – Visit link below:

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

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

Which QRadar component is primarily responsible for raw log events into a normalized format?

- A. Event Processor
- B. Event Collector
- C. Device Support Module (DSM)
- D. Console

Answer: C

Explanation:

DSMs contain parsing rules that translate vendor-specific log formats into QRadar's normalized schema, enabling correlation and searching.

Question: 2

In a high-availability (HA) QRadar deployment, which component must be paired with a standby instance to ensure continuous rule execution?

- A. Console
- B. Event Collector
- C. QFlow Collector
- D. Data Node

Answer: A

Explanation:

The Console runs the correlation engine; an HA pair of consoles provides failover for rule processing and UI access.

Question: 3

When sizing a QRadar deployment for 20,000 EPS with a 30-day retention, which storage type is recommended for the Data Node to achieve optimal performance?

- A. SATA HDD
- B. SAS HDD
- C. SATA SSD
- D. NVMe SSD

Answer: D

Explanation:

NVMe SSDs deliver the highest IOPS and low latency, essential for handling high EPS while maintaining fast search performance over long retention periods.

Question: 4

Which MITRE ATT&CK tactic is most directly addressed by a rule that detects "Credential Dumping" activity from Windows Security logs?

- A. Persistence
- B. Credential Access
- C. Lateral Movement
- D. Collection

Answer: B

Explanation:

Credential Dumping is a technique used to obtain account credentials, fitting the Credential Access tactic.

Question: 5

A customer wants to store events for compliance but does not need correlation on those events. Which QRadar license should be purchased?

- A. Event Processor license
- B. Data Store license
- C. Flow Processor license
- D. App Host license

Answer: B

Explanation: The Data Store license permits storage of events without requiring processing or correlation, satisfying pure archiving needs.

Thank You for Trying Our Product

For More Information – **Visit link below:**

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

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**

