

**Boost up Your Certification Score**

# **IBM A1000-163**

**Assessment: IBM Security QRadar SIEM V7.5 Deployment**



**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

What is the primary purpose of a Security Information and Event Management (SIEM) system?

- A. To replace firewalls
- B. To collect, store, and analyze security for detection and response
- C. To encrypt network traffic
- D. To perform vulnerability scanning

**Answer: B**

Explanation:

SIEMs aggregate logs and events, normalize them, and provide analytics to detect threats and support incident response.

## Question: 2

In QRadar, which component is responsible for parsing raw log data into normalized events?

- A. Event Processor
- B. Device Support Module (DSM)
- C. Flow Collector
- D. App Host

**Answer: B**

Explanation:

DSMs contain parsing rules that translate vendor-specific log formats into QRadar's normalized event schema.

## Question: 3

Which QRadar logical component provides the graphical user interface and central management functions?

- A. Event Processor
- B. Console
- C. Data Node
- D. Flow Processor

**Answer: B**

Explanation:

The Console hosts the GUI, admin functions, and coordinates distributed components.

### Question: 4

What does the term "event correlation" refer to in a SIEM context?

- A. Storing events in a database
- B. Linking related events to identify a pattern or incident
- C. Encrypting event data
- D. Forwarding events to external systems

**Answer: B**

Explanation:

Correlation examines multiple events to discover relationships that indicate malicious activity.

### Question: 5

Which deployment model is best suited for a small office with limited traffic?

- A. All-in-one appliance
- B. Distributed multi-node architecture
- C. Cloud-based SaaS only
- D. High-availability pair of consoles

**Answer: A**

Explanation:

An all-in-one appliance combines console, event, and flow processing on a single device, ideal for low-volume environments.

# 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**



Visit us at: <https://www.examsboost.com/test/a1000-163>