IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **C1000-175**

Title : Foundations of IBM Security QRadar SIEM V7.5

Version : DEMO

1.Which of the following deployment options are available for QRadar?
A. On-premise only
B. Cloud-only
C. Hybrid (Cloud and On-premise)
D. Peer-to-peer network
Answer: BC

2.Which feature distinguishes QRadar Network Insights (QNI) from QRadar Incident Forensics (QIF)?
A. QNI analyzes and enriches flow data in real-time.
B. QIF allows for replaying and analyzing past network traffic.
C. QNI requires direct access to the network hardware.
D. QIF focuses exclusively on flow data analysis.
Answer: A

3.Which type of rule is specifically designed to detect patterns over time rather than in single events or flows?
A. Anomaly detection rule
B. Behavioral rule
C. Threshold rule
D. Correlation rule
Answer: C

4.You need to use Ariel Query Language to select the default columns from events.
Which is the correct query?
A. SELECT % FROM events
B. SELECT * FROM events
C. SELECT ALL FROM events
D. SELECT defaultcolumns from events
Answer: B

5.What happens to custom DSMs when upgrading a QRadar system?
A. Custom DSMs are renamed during the upgrade.
B. Custom DSMs remain the same during the upgrade.
C. Custom DSMs are automatically updated to the latest version.
D. Custom DSMs are replaced with default DSMs during the upgrade.
Answer: B