INFOSECTRAIN

QRadar SIEM Security

Course Agenda

sales@infosectrain.com | www.infosectrain.com

Course Outline

1. Introduction to SOC

- Building a successful SOC
- Functions of SOC
- Heart of SOC- SIEM
- Gartner's magic quadrant

2. Introduction to Qradar

- IBM QRadar SIEM component architecture and data flows
- Using the QRadar SIEM User Interface

3. Working with logs

- Working with offense triggered by events
- Working with offense triggered by flows
- Working with events of an offense

4. Monitoring

- Monitor QRadar Notifications and error messages.
- Monitor QRadar performance
- Review and interpret system monitoring dashboards.
- Investigate suspected attacks and policy breaches
- Search, filter, group, and analyze security data

5. Intercep

Investigate the vulnerabilities and services of assets

Investigate events and flows

Use index management

Index and Aggregated Data Management

Use AQL for advanced searches

Creating Alerts for intrusions

Explain error messages and notifications.

Analyze a Real-World Scenario.

Creating Reports

Case Studies

6. Advanced Topics

Creating log source types

Leveraging reference data collections

Developing custom rules

Creating Custom Action Scripts

Developing Anomaly Detection Rules

INFOSECTRAIN

New York, United States

99 Wall Street #599 New York, NY 10005, United States
Phone No: +1 657-207-1466

UAE

Gasco Tower, Near Corniche, P.O. Box 665, Abu Dhabi, UAE
Phone No: +971-569908131

Canada

170 The Donway West, Suite # 6A, Toronto, Ontario M3C2E8, Canada
Phone No: +1-657-207-1466

Delhi

4B, 4th Floor, Plot No. A-8, Bigjos Tower, Netaji Subhash Place,
Pitampura, Delhi - 110034, India
Phone No: +91-97736-67874

Bangalore

Manyata Embassy Business Park, Ground Floor, E1 Block, Beech Building,
Outer Ring Road, Bangalore - 560045

Kerala

Trivandrum, 1st Floor, RRD Building, Sasthamangalam Junction,
Sasthamangalam, Thiruvananthapuram, Kerala 695010

sales@infosectrain.com | www.infosectrain.com