INFOSOFT IT SOLUTIONS

Training | Projects | Placements

Revathi Apartments, Ameerpet, 1st Floor, Opposite Annapurna Block,

Info soft it solutions ,Software Training& Development 905968394,918254087

IBM SECURITY QRADAR TRAINING

1. Introduction to Q Radar

- Overview of SIEM concepts
- Introduction to IBM Security Q Radar
- Understanding Q Radar architecture and components
- Key features and benefits of Q Radar

2. Installation and Configuration

- Q Radar deployment options
- System requirements and preparation
- Installation procedures
- Initial configuration and setup
- Licensing and user management

3. Q Radar User Interface

- Navigating the Q Radar user interface
- Dashboard customization
- Using the Ariel Query Language (AQL)
- Creating and managing tabs

4. Data Collection

- Log source configuration
- Protocols and log formats
- Integrating Q Radar with various data sources
- Custom log source integration
- Troubleshooting log source issues

5. Event and Flow Processing

- Event processing architecture
- Flow processing architecture
- Custom event and flow properties
- Building and managing reference sets

6. Rules and Offenses

- Rule types and rule creation
- Fine-tuning and optimizing rules
- Understanding offenses and offense management
- Correlation and event prioritization
- Custom rule development

7. Searches and Reports

- Creating and managing searches
- Using advanced search options
- Scheduled searches
- Creating and customizing reports
- Automating report generation

8. Vulnerability Management

- Integrating vulnerability assessment tools
- Managing vulnerabilities in QRadar
- Vulnerability correlation and prioritization
- Remediation workflows

9. Network Activity and Asset Management

- Monitoring network activity
- Asset discovery and management
- Asset correlation and building asset profiles
- Analyzing network behavior

10. Offense Management and Incident Response

- Incident response workflows
- Managing offenses and closing incidents
- Using the offense manager
- Integration with ticketing systems
- Forensics and deep dive analysis

11. Customization and Advanced Features

- Custom log sources and DSMs
- Custom event and flow properties
- Advanced rule creation
- Building custom dashboards
- API integration and automation
-

12. Troubleshooting and Maintenance

- Common issues and troubleshooting techniques
- System health monitoring
- Performance tuning and optimization
- Regular maintenance tasks
- Backup and recovery procedure
-

ADVANCE TOPICS ;-

1: Introduction to Q Radar

- Overview of Q Radar architecture
- Key features and functionalities
- Components and deployment options
- Licensing and capacity planning

2 : Advanced Log Management

- Custom log sources and log source extensions
- Parsing and normalization of logs
- Custom DSM (Device Support Module) creation
- Log source management and optimization

3: Advanced Network Activity Monitoring

- Flow data and flow collectors
- Network behavior analytics
- Custom flow sources and flow properties
- Tuning and optimizing network data collection

4: Advanced Rule Creation and Tuning

- Custom rule creation and testing
- Rule optimization and performance tuning
- Use of reference sets and building blocks
- Anomaly detection rules and use cases

5: Offense Management and Tuning

- Advanced offense rules and correlation
- Offense lifecycle management
- Tuning offense thresholds and rules
- Investigating and responding to offenses

6: Custom Searches and Reports

- Advanced AQL (Ariel Query Language) queries
- Custom search creation and optimization
- Scheduled searches and automated reports
- Custom report templates and dashboards

7: Integration with Other Security Tools

- Integration with IBM Resilient for SOAR (Security Orchestration, Automation, and Response)
- Integration with threat intelligence feeds
- APIs and custom integrations
- Integration with third-party security tools and platforms
-

8: Advanced Forensics and Incident Response

- Deep dive into packet capture and analysis
- Leveraging QRadar for forensic investigations
- Incident response workflows and best practices
- Case studies and real-world scenarios
-

9: User Behavior Analytics (UBA)

- Introduction to UBA and its importance
- Configuring and tuning UBA
- Investigating UBA alerts and offenses
- Integrating UBA with other Q Radar functionalities

10: Q Radar Administration and Maintenance

- Advanced system administration tasks
- Backup and recovery procedures
- Performance monitoring and troubleshooting
- Regular maintenance tasks and best practices

11: Advanced Deployment Scenarios

- Multi-tenancy and distributed deployments
- High availability and disaster recovery configurations
- Cloud deployments and hybrid environments
- Case studies on complex deployment scenarios