INFOSOFT IT SOLUTIONS

Training | Projects | Placements

Revathi Apartments, Ameerpet, 1st Floor, Opposite Annapurna Block, Infosoft It solutions, Software Training & Development Institute, +91 - 9059683947 | +91 – 9182540872

IBM Security QRadar SIEM

Introduction to QRadar

1.1 Overview of QRadar SIEM 1.2 Key features and capabilities 1.3 Use cases and benefits 1.4 Architecture overview

QRadar Installation and Configuration

2.1 Planning and prerequisites 2.2 Installing QRadar components 2.3 Configuring deployment settings 2.4 License management 2.5 High availability and disaster recovery setup

Log Source Management

3.1 Understanding log sources and event collection 3.2 Configuring log sources 3.3 Device Support Modules (DSMs) and parsing rules 3.4 Log source protocols and configurations

Flow and Network Activity Monitoring

4.1 Flow data collection methods 4.2 Configuring flow sources 4.3 Flow processing and analysis 4.4 Detecting network anomalies and threats

Offense Management and Correlation

5.1 Understanding offenses 5.2 Correlation rules and building blocks 5.3 Customizing offense rules and thresholds 5.4 Offense investigation and prioritization

Incident Detection and Response

6.1 Real-time event monitoring 6.2 Incident investigation workflows 6.3 Advanced search and filtering techniques 6.4 Response actions and mitigation strategies

Customization and Tuning

7.1 Custom properties and reference data 7.2 Building custom rules and reports 7.3 Tuning QRadar for performance 7.4 Managing storage and retention policies

QRadar Administration

8.1 User management and access control 8.2 System settings and configuration management 8.3 Backups and disaster recovery procedures 8.4 Monitoring system health and status

Integration with Other Tools and Technologies

9.1 Integrating QRadar with third-party tools 9.2 Utilizing RESTful APIs for automation 9.3 SIEM ecosystem and interoperability 9.4 Common integration use cases

Compliance and Reporting

10.1 Compliance requirements and standards 10.2 Generating compliance reports 10.3 Auditing and log management best practices 10.4 Demonstrating compliance with QRadar

Advanced Topics and Best Practices

11.1 AI and machine learning in QRadar 11.2 Threat hunting methodologies 11.3 Incident response planning and execution 11.4 Best practices for optimizing QRadar deployment