INFOSOFT IT SOLUTIONS

Training | Projects | Placements

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

soft it solutions Software Training& Development 905968394,918254087

AZURE SENTINEL

Introduction to Azure Sentinel

1. Overview of Azure Sentinel
2. Key Features and Benefits
3. Comparison with SIEM Solutions

Setting Up Azure Sentinel

1. Deploying Azure Sentinel in Azure Portal
2. Connecting Data Sources to Azure Sentinel
3. Configuring Data Connectors and Integration

Data Ingestion and Querying

1. Log Analytics Workspace Integration
2. Azure Sentinel Data Types and Sources
3. Query Language (KQL) Basics for Azure Sentinel

Threat Detection and Hunting

1. Creating and Customizing Detection Rules
2. Implementing Threat Intelligence
3. Proactive Threat Hunting Techniques

Incident Management and Response

1. Incident Workflow in Azure Sentinel
2. Automated Response with Playbooks
3. Manual Investigation and Response Actions

Fusion and Machine Learning

1. Fusion Analysis in Azure Sentinel
2. Machine Learning in Sentinel for Anomaly Detection
3. Using Azure Machine Learning with Sentinel

Security Orchestration and Automation (SOAR)

1. Azure Sentinel Integration with Azure Logic Apps
2. Implementing Automated Incident Response
3. Playbook Development and Best Practices

Integration with Azure Services

1. Azure Security Center and Azure Sentinel Integration
2. Using Azure Sentinel with Microsoft Defender ATP
3. Azure AD and Office 365 Integration

Advanced Threat Detection Techniques

1. Behavioral Analytics and User Entity Behavior Analytics (UEBA)
2. Advanced Threat Detection and Analytics