IT Monitoring & Incident Detection

Duration: 1 Day

Module 1: Introduction to IT Monitoring

- Importance of Monitoring in IT Operations
- Key Concepts: Observability vs Monitoring
- Overview of IT Monitoring Frameworks
    - Agent-based vs Agentless Monitoring
    - On-prem vs Cloud-native Monitoring Tools
    - Examples: Nagios, Zabbix, Prometheus, Azure Monitor

Module 2: Understanding Performance Metrics

- CPU Utilization and Bottlenecks
- Memory Usage Patterns and Leaks
- Network Latency and Bandwidth Analysis
- Disk I/O Monitoring
- Application vs System-level Metrics
- Thresholds and Baseline Concepts

Module 3: Logging & Alerting Strategies

- Types of Logs: System, Application, Security
- Centralized Log Management
- Creating Efficient Log Queries
- Designing Alert Rules and Severity Levels
- Avoiding Alert Fatigue: Best Practices

Module 4: Incident Detection & Response through Monitoring

- Correlating Logs and Metrics for Issue Detection
- Real-time Monitoring Dashboards
- Automated Response & Remediation (Runbooks/Workflows)
- Root Cause Analysis with Monitoring Tools