SIEM Tools

Duration: 1 day

1. **Introduction to SIEM**
    - Role of SIEM in security operations
    - Key functions and capabilities
2. **SIEM Architecture and Components**
    - Data sources and log collectors
    - Correlation engine and storage
    - Dashboards and reporting modules
3. **Log Aggregation & Normalization**
    - Log collection methods
    - Normalization and standardization processes
    - Challenges in aggregation
4. **Event Correlation & Alerting**
    - Rule-based and behavioral correlation
    - Alert generation and tuning
    - Avoiding alert fatigue
5. **Threat Detection with SIEM**
    - Identifying anomalies and suspicious patterns
    - Mapping events to known attack stages
    - Improving detection coverage
6. **SOAR Integration**
    - Identifying anomalies and suspicious patterns
    - Introduction to SOAR (Security Orchestration, Automation, and Response)
    - SOAR Playbooks: Automating and streamlining response actions
    - Case Management: Managing incidents and investigations
    - Connectors and Actions: Integrating external tools and systems for automated workflows