# Azure Sentinel course outline

**Day 1:**

Introduction to Azure Analytics
Introduction to Azure Sentinel
Traditional SIEM vs Cloud native SIEM
Phases of Azure Sentinel
Introduction to Workbook
**Phase 1 : Collect**
Data Collection
Visualization
Querying the logs
Introduction to Kusto Query Language (KQL)
useful Queries in KQL
Advanced Queries in KQL
Lab

**Day 2:**
**Phase 2: Detect**
Detecting Threats using correlation Rules.
Out of the box Detection
Custom threat detection rules
Advanced multistage attack detection
Intro to Use cases
Real time use cases for Cloud
User Behavior related use cases
Introduction to Threat hunting
Life cycle of Threat hunting
Use Note books to hunt
Lab

Day 3:
**Phase 3: Investigate**
Introduction to Threat investigation
Investigating Incidents
Use the investigation graph to deep dive
**Phase 4: Respond**
Introduction to SOAR
Introduction to Play Books
Creating Security Play Books
Creating Logic through Logic App Designer
Threat Response Automation
Lab