# M55610A - Planning and implementing Microsoft Sentinel (SIEM & SOAR)

This course is aimed at IT professionals and Azure administrators that have some experience administering and configuring Azure, but want to gain an insight into implementing Microsoft's SIEM/SOAR solution, Microsoft Sentinel.

## Course Outline

**Duration: 3 days**

## Module 1: Overview of Microsoft Sentinel

Lessons:

- Overview of Microsoft Sentinel
- Data ingestion methods
- Microsoft Sentinel for MSSPs
- User and Entity Behaviour Analytics
- Fusion
- Notebooks
- Management & Automation Tools
- Logs & Costs

## Module 2: KQL

Lessons:

- Importance of KQL across Azure
- The User Interface (demo)
- The standard KQL Structure
- Common KQL Commands

## Module 3: Data Connectors

Lessons:

- Manage content in Microsoft Sentinel
- Connect data to Microsoft Sentinel using data connectors
- Connect Microsoft services to Microsoft Sentinel
- Connect Microsoft 365 Defender to Microsoft Sentinel
- Connect Windows hosts to Microsoft Sentinel
- Connect Common Event Format logs to Microsoft Sentinel
- Connect syslog data sources to Microsoft Sentinel
- Connect threat indicators to Microsoft Sentinel

## Module 4 – Analytics Rules

Lessons:

- Threat detection with Microsoft Sentinel analytics
- Automation in Microsoft Sentinel
- Threat response with Microsoft Sentinel playbooks

## Module 5 – Incident Management

Lessons:

- Incident management Overview
- User and Entity Behaviour Analytics
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data

## Module 6 – Hunting

Lessons:

- Threat hunting concepts
- Threat hunting with Microsoft Sentinel
- Use Search jobs in Microsoft Sentinel
- Hunt for threats using notebooks

## Module 7 – Watchlists

Lessons:

- Prioritize incidents
- Import business data
- Reduce Alert Fatigue
- Enrich Event Data

## Module 8 – Threat Intelligence

Lessons:

- Threat Intelligence Overview
- Threat Intelligence in Microsoft Sentinel