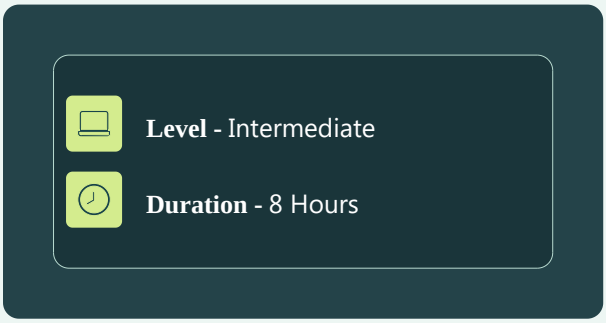
Technofocus

# Implement with impact Threat Protection and Incident response with Microsoft Sentinel within Unified Platform

## Course Overview

Learn how to implement end-to-end threat protection and incident response using the new unified Microsoft Defender portal. This course equips technical teams to deploy, investigate, automate, and integrate Microsoft Sentinel with Microsoft's security suite—using a single, streamlined SecOps experience enhanced by AI, UEBA, SOAR, and Security Copilot.




## Course Modules

### Day 1

### Module 1: Threat Intelligence in Microsoft Sentinel

The threat landscape and SOC challenge

Modernize the SOC to defend against the evolving threat landscape

Microsoft Sentinel SIEM Overview

Unified Security Operations with Defender Portal

Planning and Deployment of Microsoft Sentinel SIEM

Sentinel Platform Deployment

Get started with Microsoft Sentinel MCP server and tools

Microsoft Sentinel Graph (Preview) Overview

Onboarding Sentinel to Data Lake and Graph

Sentinel experience in Microsoft Defender portal

Threat intelligence with Microsoft Sentinel in Defender portal

### Module 2: Investigation in Microsoft Sentinel

Watchlists overview

User and Entity Behavior Analytics (UEBA)

Enable User and Entity Behavior Analytics (UEBA)

Investigating with UEBA

### Interactive Simulated Labs

Microsoft Sentinel Deployment

Enabling Data Connectors in Microsoft Sentinel in Microsoft Defender Portal

Getting a Connector via the Microsoft Security Store

Threat Intelligence connector and Content hub

UEBA with Microsoft Sentinel

## Day 2

### Module 3: Automation and response with Microsoft Sentinel

Introduction to SOAR in Microsoft Sentinel

Automation with Playbooks and Azure Logic Apps

Customizing Microsoft Sentinel playbooks from templates

Enhance detection with unified engine

Data Analysis and Threat Detection

Threat hunting

Threat Analysis in Microsoft Defender

### Module 4: Integration with other Security Solutions

Integration with Microsoft Defender for Cloud

Integration with Microsoft Defender XDR

Enhance detection with unified engine

Access Control and migration

### Module 5: Security Copilot and Unified SOC

Microsoft Security Copilot for SOC

Security Copilot agents and Security Store

Investigate incidents in Security Copilot

Manage your unified SOC in Defender portal

### Interactive Simulated Labs

Responding to threats using Automation

Hunt threats using KQL across the data lake

Analytics Rules and Incident Management

Hunting queries and Watchlists

Threat hunting with Jupyter notebooks

Exploring Microsoft Sentinel Advanced Features

Repositories in Microsoft Sentinel