Modernize and Optimize Your SOC Deployment with Microsoft Sentinel

Duration: 2 Days (3 hrs/day)

Level: Intermediate
Format: Instructor-led + Interactive Simulated Labs
Target Audience: Technical security teams

Day 1

Module 1: Modernizing your SOC with Microsoft Sentinel

- The threat landscape and SOC modernization
- Modernize the SOC to defend the evolving threat landscape
- Microsoft Sentinel SIEM Overview
  - Platform Architecture
  - SIEM Key capabilities
  - Detect, Investigate and Respond
  - Unified Security Operations with Microsoft Defender Portal

---

Module 2: Planning for Sentinel Deployment

- Planning for a Sentinel SIEM deployment
- Workspace Architecture Planning
- Sample workspace designs
- Prioritize Data Connectors
- Plan data retention and data tiering models with Analytics and Data Lake
- Plan costs and understand billing

Interactive Simulated Labs — Day 1

- Microsoft Sentinel Overview Lab

Day 2

Module 3: Deploy and Configure Microsoft Sentinel

- Manage roles and permissions
- Deploy Microsoft Sentinel SIEM
  - Enable initial content
  - Connect Microsoft Sentinel to the Microsoft Defender portal
- Introduction to Microsoft content hub solutions
- Connect data sources to Microsoft Sentinel
- Deploying a log forwarder
- AWS S3 connector—architecture overview
- Microsoft Security Store
- Get started with Microsoft Sentinel MCP server and tools

Deploy Microsoft Sentinel Platform

- Microsoft Sentinel Graph (Preview) Overview
- Onboarding Sentinel to Data Lake and Graph

Module 4: SOC Optimizing and Best Practices

- Areas of optimization in Microsoft Sentinel
- SIEM best practices in Microsoft Sentinel
- Microsoft Sentinel Use Cases

Interactive Simulated Labs — Day 2

- Enabling Data Connectors in Microsoft Sentinel in Microsoft Defender Portal
- Getting a Connector via the Microsoft Security Store