

KOENIG SOLUTIONS • COURSE OUTLINE

DW-350 - Modernize and Optimize Your SOC Deployment with Microsoft Sentinel

Learn to plan, deploy, configure and optimize a modernized security operations center with Microsoft Sentinel.

2 Days

3 HOURS A DAY

4

MODULES

26

TOPICS

3

HANDS-ON ACTIVITIES

COURSE OVERVIEW

This course covers modernizing a security operations center with Microsoft Sentinel, beginning with the threat landscape, SIEM overview and platform architecture. It then addresses planning a Sentinel deployment, including workspace architecture, data connectors, data retention and tiering, and cost and billing considerations. It continues with deploying and configuring Microsoft Sentinel, covering roles and permissions, content hub solutions, data source connections, log forwarders, the AWS S3 connector, and onboarding to Data Lake and Graph. It closes with areas of optimization, SIEM best practices and Microsoft Sentinel use cases.

WHO THIS COURSE IS FOR

Technical security teams

LEARNING OBJECTIVES

- Describe the threat landscape and drivers for SOC modernization
- Explain Microsoft Sentinel SIEM platform architecture and capabilities
- Plan workspace architecture and sample workspace designs
- Prioritize data connectors for a Sentinel deployment
- Plan data retention and tiering models across Analytics and Data Lake
- Configure roles, permissions and initial content in Microsoft Sentinel
- Connect data sources such as log forwarders and the AWS S3 connector
- Apply SOC optimization areas and Microsoft Sentinel best practices

TRAINING APPROACH

Instructor-led + Interactive Simulated Labs

4 Modules, 26 Topics

DAY 1

01

Modernizing Your SOC with Microsoft Sentinel

TOPICS

- 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

02

Activity

Planning for Sentinel Deployment

TOPICS

- 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

03

Deploy and Configure Microsoft Sentinel

TOPICS

- 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

04

2 Activities

SOC Optimizing and Best Practices

TOPICS

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

NOTES

- Level: Intermediate

HANDS-ON ACTIVITIES

Practise What You Learn

#	MODULE	ACTIVITY
02	Planning for Sentinel Deployment	Interactive Simulated Labs — Day 1: Microsoft Sentinel Overview Lab
04	SOC Optimizing and Best Practices	INTERACTIVE SIMULATED LABS — DAY 2 ■ Enabling Data Connectors in Microsoft Sentinel in Microsoft Defender Portal ■ Getting a Connector via the Microsoft Security Store

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com