

KOENIG SOLUTIONS • COURSE OUTLINE

SC-5001: Configure SIEM Security Operations Using Microsoft Sentinel

Learn to configure Microsoft Sentinel workspaces, connect data sources, and build analytics and automation rules to detect and respond to threats.

1 Day

8 HOURS

5

MODULES

22

TOPICS

5

HANDS-ON EXERCISES

COURSE OVERVIEW

The SC-5001 certification pertains to configuring SIEM (Security Information and Event Management) operations using Microsoft Sentinel. This certification represents expertise in using Microsoft's cloud-native SIEM solution to collect, detect, investigate, and respond to security threats across an organization's IT environment. It is valuable for security operations professionals who need to implement and manage Sentinel to safeguard enterprise systems. By obtaining this certification, individuals demonstrate their skills in leveraging Sentinel for Real-time analysis, maintaining security data, Creating alerts, and orchestrating threat responses. Industries use it to ensure their security teams are proficient in using advanced tools to protect their infrastructure from cyber threats.

WHO THIS COURSE IS FOR

IT professionals managing security operations - Security analysts and engineers

Security architects

System administrators focused on security

Technical personnel implementing Microsoft Sentinel

Professionals seeking to understand SIEM with Microsoft Sentinel

LEARNING OBJECTIVES

- Plan and create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Configure Microsoft Sentinel permissions, roles and settings
- Connect Microsoft services such as Office 365 and Entra ID
- Connect Windows hosts using AMA or legacy agent connectors
- Create analytics rules from templates and wizard
- Manage analytics rules within Microsoft Sentinel
- Create automation rules to orchestrate threat responses

5 Modules, 22 Topics

01

Create and Manage Microsoft Sentinel Workspaces

TOPICS

- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs

02

Connect Microsoft Services to Microsoft Sentinel

TOPICS

- Plan for Microsoft services connectors
- Connect the Microsoft Office 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector

03

Connect Windows Hosts to Microsoft Sentinel

TOPICS

- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector
- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs

04

Threat Detection with Microsoft Sentinel Analytics

Exercise

TOPICS

What is Microsoft Sentinel Analytics · Types of analytics rules · Create an analytics rule from templates · Create an analytics rule from wizard · Manage analytics rules

05

Automation in Microsoft Sentinel

TOPICS

Understand automation options · Create automation rules

HANDS-ON EXERCISES

Practise What You Learn

#	MODULE	ACTIVITY
04	Threat Detection with Microsoft Sentinel Analytics	Detect threats with Microsoft Sentinel analytics
	Configure SIEM Security Operations Using Microsoft Sentinel	■ Configure SIEM operations using Microsoft Sentinel ■ Install Microsoft Sentinel Content Hub solutions and data connectors ■ Configure a data connector Data Collection Rule ■ Perform a simulated attack to validate the Analytic and Automation rules

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

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.

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