

KOENIG SOLUTIONS • COURSE OUTLINE

SC-5004: Defend Against Cyberthreats with Microsoft Defender XDR

Learn to mitigate incidents and investigate threats using Microsoft Defender for Endpoint and Microsoft Defender XDR.

COURSE OVERVIEW

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advise on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft Defender XDR, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

WHO THIS COURSE IS FOR

Security Operations Analysts

Security Engineers

Threat Hunters

Incident Responders

PREREQUISITES

Before attending this course, students must have:

- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Microsoft Windows
- Familiarity with the Microsoft Defender portal and services
- Familiarity with Microsoft Defender for Endpoint
- Basic understanding of Kusto Query Language (KQL).

7 Modules

Course Introduction

01

Mitigate Incidents Using Microsoft Defender

02

Deploy the Microsoft Defender for Endpoint Environment

03

Configure for Alerts and Detections in Microsoft Defender for Endpoint

04

Configure and Manage Automation Using Microsoft Defender for Endpoint

05

Perform Device Investigations in Microsoft Defender for Endpoint

06

Defend Against Cyberthreats with Microsoft Defender XDR Lab Exercises

NOTES

- Labs: The labs must be completed within the lab environment provided by your lab hosting provider. Detailed step-by-step instructions are provided for each lab and presented as part of the UI experience within your lab environment.

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