

Microsoft Sentinel Learning Companion

www.aka.ms/pathways

Getting Started

Microsoft:

- [New to the Cloud or Azure? Start with Azure Fundamentals](#)
- [New to Security? Continue with Microsoft Security, Compliance, and Identity Fundamentals](#)
- [What is Microsoft Sentinel?](#)
- [Microsoft Security YouTube Channel](#)
- [Microsoft Sentinel Blog](#)

Learning Paths from Microsoft Learn

Configure your Microsoft Sentinel environment

Get started with Microsoft Sentinel by properly configuring the Microsoft Sentinel workspace. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

START

Configure SIEM security operations using Microsoft Sentinel

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events to Microsoft Sentinel.

START

Data analysis with Kusto Query Language

Learn how to analyze data in various environments using the Kusto Query Language (KQL).

START



Microsoft Applied Skill

Configure SIEM security operations using Microsoft Sentinel

START

Role based Certification

SC-200 Security Operations Analyst

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Microsoft Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting. The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

Skills measured

- Manage a security operations environment
- Configure protections and detections
- Manage incident response
- Manage security threats

Course Page

Practice Assessment

Exam Page

SecOps Learning Pathway

Microsoft Sentinel

Level 400 Ninja Training

Work through level 400 training to help you skill up on Microsoft Sentinel. The training comprises 21 modules that present relevant product documentation, blog posts, and other resources. The modules listed here are split into five parts following the life cycle of a Security Operation Center (SOC).

- [Part 1: Overview](#)
- [Part 2: Architecting and deploying](#)
- [Part 3: Creating content](#)
- [Part 4: Operating](#)
- [Part 5: Advanced](#)
- [Next Steps](#)
- [Recommended Content](#)

Doing More

- Sentinel: Keep track of [what's new](#)
- Contribute or enhance rules, queries, workbooks, connectors and more to the community on the [Sentinel GitHub](#)
- [Becoming a Sentinel Notebooks ninja](#)
- Migrating – Check out [Sentinel Migration Fundamentals](#)



KUSTO DETECTIVE AGENCY

Click Here

Microsoft Learn Security Hub

Microsoft Sentinel Documentation

YouTube Microsoft Security

Microsoft Security Copilot Documentation