March 2025

# Microsoft Security Operations Analyst (1/2)

www.aka.ms/pathways

## Getting Started

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, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

**Microsoft:**

- New to the Cloud or Azure? Start with Azure Fundamentals
- New to Security? Continue with Microsoft Security, Compliance, and Identity Fundamentals
- Microsoft Security Copilot

## Applied Skills

Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls

START

Configure SIEM security operations using Microsoft Sentinel

START

Defend against cyberthreats with Microsoft Defender XDR

START

## Learning Paths from Microsoft Learn

**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

**Defend against threats with Microsoft 365**
This learning path introduces Microsoft 365 Defender, Defender for Endpoint, Defender for Identity, and Defender for Office 365.

START

**Data analysis with Kusto Query Language**
Learn how to analyse data in various environments using the Kusto Query Language (KQL).

START

## Security Copilot on Microsoft Learn

**Enhance security operations by using Microsoft Security Copilot** (full track)

- Fundamentals of Generative AI
- Describe Microsoft Security Copilot
- Describe the core features of Microsoft Security Copilot
- Describe the embedded experiences of Microsoft Security Copilot
- Explore use cases of Microsoft Security Copilot

**Enhance endpoint security with Microsoft Intune and Microsoft Copilot for Security** (full track)

- Discover Microsoft Intune essentials
- Unlock Insights with Microsoft Copilot for Security
- Optimize Microsoft Intune for Microsoft Copilot for Security Integration

## Certification - 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.

**Skills measured**

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

- Mitigate threats using Microsoft Defender XDR
- Mitigate threats using Microsoft Security Copilot
- Mitigate threats using Microsoft Purview
- Mitigate threats using Defender for Endpoint
- Mitigate threats using Defender for Cloud
- Create queries for Sentinel using Kusto Query Language (KQL)
- Configure your Sentinel environment
- Connect logs to Microsoft Sentinel
- Create detections and perform investigations using Sentinel
- Perform threat hunting in Microsoft Sentinel

Exam Study Guide

Microsoft Learn Security Hub

Exam Page

Practice Assessment

Course Page

# Microsoft Security Operations Analyst (2/2)

www.aka.ms/pathways

## Microsoft Learn/Documentation

### Mitigate threats using Microsoft 365 Defender

- Describe basic cybersecurity threats, attacks, and mitigations
- Automate, investigate, and remediate
- Configure, protect, and detect
- Describe data loss prevention alerts
- Investigate data loss prevention alerts in Microsoft Purview
- Investigate data loss prevention alerts in Microsoft Defender for Cloud Apps
- Insider risk management overview
- Introduction to managing insider risk policies
- Mitigate incidents using Microsoft Defender
- Understand attack surface reduction
- Enable attack surface reduction rules
- Configure advanced features
- Configure alert notifications
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Configure automated investigation and remediation capabilities
- Explore vulnerabilities on your devices
- Understand threat intelligence concepts
- Utilize Vulnerability Management in Microsoft Defender for Endpoint
- What is Microsoft Entra ID Protection?
- Building a Conditional Access policy
- Microsoft Secure Score
- Create an access review of Azure resource and Microsoft Entra roles in PIM
- Microsoft Entra Identity Protection notifications
- Introduction to Microsoft Defender for Identity
- Review compromised accounts or data
- Understand the Defender for Cloud Apps Framework
- Manage incidents
- Use the action centre
- Classify and protect sensitive information
- Detect Threats
- Hunt for threats across devices, emails, apps, and identities

### Mitigate threats using Azure Defender

- Explain Microsoft Defender for Cloud
- Enable Microsoft Defence for Cloud
- Review the asset inventory
- Configure auto provisioning
- Protect non-Azure resources
- Understand security alerts
- Generate threat intelligence reports
- Respond to alerts from Azure resources
- Remediate alerts and automate responses
- Automate remediation responses
- Explore Azure Resource Manager template structure
- Structure and syntax of ARM templates
- Quickstart: Create an automatic response to a specific security alert using an ARM template or Bicep

### Mitigate threats using Azure Sentinel

- Define the concepts of SIEM and SOAR
- Describe threat detection and mitigation capabilities in Microsoft Sentinel
- Plan for the Microsoft Sentinel workspace
- Roles and permissions in Microsoft Sentinel
- Export data from a Log Analytics workspace to a storage account by using Logic Apps
- Log Analytics workspace data export in Azure Monitor
- Microsoft security baseline for Microsoft Sentinel
- Connect data to Microsoft Sentinel using data connectors
- Collect Syslog data sources with Log Analytics agent
- Collect data from Linux-based sources using syslog
- Configure the Data Collection Rule for Syslog Data Sources
- Common Event Format connector
- Connect your external solution using the Common Event Format connector
- Connect the Microsoft 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID protection connector
- Plan for Windows hosts security events connector
- Threat detection with Sentinel analytics
- Threat response with Sentinel playbooks
- Security incident management in Microsoft Sentinel
- Monitor and visualize data
- Use default Sentinel Workbooks
- Create a new Sentinel Workbook
- Explain threat hunting concepts in Sentinel
- Explore creation and management of Sentinel threat-hunting queries
- Hunt for threats with Sentinel