January 2024

Microsoft Security Operations Analyst (1/2)

Download the latest copy of this pathway: www.aka.ms/SecOpsLearningPathway

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

Learning Paths from Microsoft Learn

Cloud-native security operations with Microsoft Sentinel
This learning path describes basic architecture, core capabilities, and primary use cases of its products. You'll also learn about differences and get familiar with Microsoft Sentinel. START

Detect threats and protect information in cloud apps using Microsoft Defender for Cloud Apps
This learning path investigates Microsoft Defender for Cloud Apps, discovery, information protection and threat detection at an intermediate level. 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

Microsoft Applied Skill
Configure SIEM security operations using 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 analyze data in various environments using the Kusto Query Language (KQL). START

Secure cloud apps using Microsoft Defender for Cloud Apps
Learn how Microsoft Defender for Cloud Apps can help you proactively identify and defeat app-based security threats across your organization. START

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

- Mitigate threats using Microsoft Defender XDR
- 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 Microsoft Sentinel
- Perform threat hunting in Microsoft Sentinel

Skills measured

- Mitigate threats using 365 Defender
- Mitigate threats using Defender for Cloud
- Mitigate threats using Microsoft Sentinel

Exam Study Guide | Course Page | Practice Assessment

Exam Page | Security Documentation | Sentinel Learning Companion

Microsoft Security Operations Analyst (2/2)

www.aka.ms/pathways

Microsoft Learn/Documentation

Mitigate threats using Microsoft 365 Defender

- Learn about common threats
- Microsoft 365 Defender Suite
- Introduction to Defender for Office 365
- Automate, investigate, and remediate
- Configure, protect, and detect
- Describe data loss prevention alerts
- Investigate data loss prevention alerts in Microsoft 365 compliance
- Investigate data loss prevention alerts in Microsoft Cloud App Security
- Insider risk management overview
- Introduction to managing insider risk policies
- Explain security operations in Microsoft Defender for Endpoint
- Understand attack surface reduction
- Enable attack surface reduction rules
- Configure advanced features
- Configure alert notifications
- Manage custom detections
  Manage and investigate incidents
- Manage and investigate alerts
- Configure automated investigation and remediation capabilities
- Explore vulnerabilities on your devices
- Understand threat intelligence concepts
- Track emerging threats with threat analytics
- Entra Identity Protection overview
- Detect risks with Microsoft Entra Protection policies
- Building a Conditional Access policy
- Investigate and remediate risks detected by Microsoft Entra Identity Protection
- 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 Cloud App Security Framework
- Microsoft 365 Defender
- 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
- Data collection, retention, and storage in Application Insights
- Explore and manage your resources with asset inventory
- Configure auto provisioning
- Configure Data Retention Policies
- Protect non-Azure resources
- Understand security alerts
- Manage security incidents and generate threat intelligence reports
- Respond to alerts from Azure resources
- Remediate alerts and automate responses
- Automate responses to Microsoft Defender for Cloud triggers
- Explore Azure Resource Manager
- Structure and syntax of ARM templates
- Quickstart: Create an automatic response to a specific security alert using an ARM template

Mitigate threats using Azure Sentinel

- Define the concepts of SIEM, SOAR, XDR
- Describe how Sentinel provides integrated threat protection
- Plan for the Microsoft Sentinel workspace
- Permissions in Microsoft Sentinel
- Archive data from Log Analytics workspace to Azure storage using Logic App
- Log Analytics workspace data export in Azure Monitor
- Azure 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 log analytics agent
- Common Event Format connector
- Connect your external solution using the Common Event Format connector
- Connect the Microsoft Office 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 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
- Hunt by using bookmarks