Microsoft Security Operations Analyst

www.aka.ms/pathways

Microsoft CERTIFIED ASSOCIATE

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 Azure Sentinel?
- Microsoft Security YouTube Channel
- Azure Sentinel Blog

Cloud-native Security Operations with Azure Sentinel

This learning path covers basic architecture, core capabilities, and primary use cases of its products.

Microsoft Learn:

- Introduction to Azure Sentinel
- Deploy Sentinel and connect data sources
- Threat detection with Sentinel analytics
- Security incident management in Sentinel
- Threat hunting with Azure Sentinel
- Threat response with Sentinel playbooks
- Query, visualize, and monitor data in Sentinel

Microsoft Official Practice Test Coming Soon

Microsoft Security Technical Content Library

Microsoft is committed to helping build a safer world for all. Explore this library to find learning content relevant to your needs

ACCESS

Additional Study

Mitigate threats using Microsoft 365 Defender:

- Learn about common threats
- Microsoft 365 Defender Suite
- Introduction to Microsoft 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
- Azure AD Identity Protection overview
- Detect risks with Azure AD Identity Protection policies
- Building a Conditional Access policy
- Investigate and remediate risks detected by Azure AD Identity Protection
- Microsoft Secure Score
- Create an access review of Azure AD roles in Privileged Identity Management
- Azure Active Directory Identity Protection notifications
- Introduction to Microsoft Defender for Identity
- Review compromised accounts or data
- Understand the Cloud App Security Framework
- Classify and protect sensitive information
- Detect Threats
- Microsoft 365 Defender
- Manage incidents
- Use the action centre
- Hunt for threats across devices, emails, apps, and identities

Mitigate threats using Azure Defender:

- Explain Azure Defender
- Explain Azure Security Center
- Enable Azure Defender
- Data collection, retention, and storage in Application Insights
- Cloud workload protections in Azure Defender
- Explore and manage your resources with asset inventory
- Configure auto provisioning
- Configure Data Retention Policies
- Connect non-Azure resources to Azure Defender
- Understand security alerts
- Manage security incidents in Security Center
- Manage security incidents and generate threat intelligence reports
- Respond to alerts from Azure resources
- Remediate alerts and automate responses
- Automate responses to Security Center 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 Azure Sentinel workspace
- Understand Sentinel permissions and role
- Permissions in Azure Sentinel
- Configure log retention
- Archive data from Log Analytics workspace to Azure storage using Logic App
- Log Analytics workspace data export in Azure Monitor
- Azure security baseline for Azure Sentinel
- Connect data to Azure 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 Azure Active Directory connector
- Connect the Azure Active Directory identity protection connector
- Plan for Windows hosts security events connector
- Threat detection with Azure Sentinel analytics
- Threat response with Azure Sentinel playbooks
- Security incident management in Azure Sentinel
- Identify advanced threats with User and Entity Behaviour Analytics (UEBA) in Azure Sentinel
- Monitor and visualize data
- Use default Azure Sentinel Workbooks
- Create a new Azure Sentinel Workbook
- Explain threat hunting concepts in Azure Sentinel
- Explore creation and management of Azure Sentinel threat-hunting queries
- Hunt for threats with Azure Sentinel
- Hunt by using bookmarks
- Keep track of data during hunting with Sentinel
- Use hunting livestream in Azure Sentinel
- Hunt with notebooks
- Create an Azure ML workspace
- Tutorial: Detect threats out-of-the-box

Role Based Certification
Microsoft Certified: Security Operations Analyst

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 policies to appropriate stakeholders.

Exam SC-200: Microsoft Security Operations Analyst

Skills Measured:

- Mitigate threats using Microsoft 365 Defender
- Mitigate threats using Azure Defender
- Mitigate threats using Azure Sentinel

>>> Download Exam Skills Outline <<<

- Mitigate threats using Microsoft Defender for Endpoint
- Mitigate threats using Microsoft 365 Defender
- Mitigate threats using Azure Defender
- Create queries for Azure Sentinel using Kusto Query Language (KQL)
- Configure your Azure Sentinel environment
- Connect logs to Azure Sentinel
- Create detections and perform investigations using Azure Sentinel
- Perform threat hunting in Azure Sentinel

Check out the Azure Sentinel Learning Companion for more learning resources

Azure 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 Azure Sentinel?
- Microsoft Security YouTube Channel
- Azure Sentinel Blog

Cloud-native Security Operations with Azure Sentinel

This learning path covers basic architecture, core capabilities, and primary use cases of its products. You'll also learn about differences and get familiar with Azure Sentinel, a cloud-native, security information and event management (SIEM) service.

Microsoft Learn:

- Introduction to Azure Sentinel
- Deploy Sentinel and connect data sources
- Threat detection with Sentinel analytics
- Security incident management in Sentinel
- Threat hunting with Azure Sentinel
- Threat response with Sentinel playbooks
- Query, visualize, and monitor data in Sentinel

Quickstarts/Tutorials

- Quickstart: On-board Azure Sentinel
- Quickstart: Get visibility into alerts
- Detect threats out-of-the-box
- Create custom analytics rules to detect threats
- Visualize and monitor your data
- Investigate incidents
- Use playbooks with automation rules
- Create queries for Azure Sentinel using Kusto Query Language (KQL)

Microsoft Docs & Reference

Learn More:

- Azure Sentinel documentation
- Azure Sentinel and Microsoft Teams
- Manage Sentinel workspaces at scale
- Cyber threat intelligence with Sentinel
- Useful resources for working with Sentinel
- Become an Azure Sentinel Ninja (from Sentinel Blog)
- Azure Sentinel integration with Microsoft Cloud App Security
- Build a scalable security practice with Azure Lighthouse and Azure Sentinel
- Safeguard multi-cloud apps and resources with cloud security solutions from Microsoft
- Defend against threats with Microsoft Threat Protection
- Commonly used Azure Sentinel workbooks

Concepts:

- Classify and analyse data
- Permissions in Azure Sentinel
- Manage access to Sentinel data by resource
- Protecting MSSP intellectual property
- Advanced multistage attack detection
- Security Orchestration, Automation, and Response (SOAR) in Sentinel
- Automation Rules for incident handling
- Advanced automation with playbooks
- Identify advanced threats with User and Entity Behaviour Analytics (UEBA)
- Use SOC-ML anomalies to detect threats
- Import threat intelligence
- Threat intelligence integration
- Bring your own Machine Learning (ML) into Azure Sentinel
- Microsoft 365 Defender integration with Sentinel
- Use external data with watchlists
- Extend Azure Sentinel across workspaces and tenants

Azure Sentinel Level 400 Ninja Training

The Azure Sentinel Level 400 Ninja Training Blog Post **has been designed to help you become an Azure Sentinel master. We've categorised the modules within the posting by job role to ensure the most appropriate learning path for you.** Check out the Ninja FAQ before starting

Sentinel Ninja

Everything you need to know and perhaps a little more….

- Module 1: Getting Started with Sentinel
- Module 2: How is Azure Sentinel used?
- Module 3: Workspace and tenant architecture
- Module 4: Data collection
- Module 5: Log Management
- Module 6: Enrichment: TI, Watchlists and more
- Module 7: Kusto Query Language (KQL)
- Module 8: Analytics
- Module 9: Implementing SOAR
- Module 10: Workbooks, reporting & visualization
- Module 11: Use cases and solutions
- Module 12: Handling incidents
- Module 13: Hunting
- Module 14: User and Entity Behaviour Analytics
- Module 15: Monitoring Azure Sentinel's health
- Module 16: Extending and Integrating using Azure Sentinel APIs
- Module 17: Bring your own ML

SOC Analyst

Advanced use of Azure Sentinel including creating and managing automation and threat intelligence

- Module 1: Getting Started with Sentinel
- Module 10: Workbooks, reporting, and visualization
- Module 11: Use cases and solutions
- Module 12: Handling incidents
- Module 13: Hunting
- Module 14: User and Entity Behaviour Analytics (UEBA)

SOC Engineer

Basic use of Azure Sentinel including dealing with incidents and using dashboards

- Module 1: Getting Started with Sentinel
- Module 2: How is Azure Sentinel used?
- Module 3: Workspace and tenant architecture
- Module 4: Data collection
- Module 5: Log Management
- Module 6: Enrichment: TI, Watchlists, and more
- Module 7: Kusto Query Language (KQL)
- Module 8: Analytics
- Module 9: Implementing SOAR
- Module 10: Workbooks, reporting, and visualization
- Module 15: Monitoring Azure Sentinel's health
- Module 16: Extending and Integrating using Azure Sentinel APIs

Doing More

- Sentinel : Keep track of what's new
- Ask, or answer others on the Azure Sentinel Tech Community
- Contribute or enhance rules, queries, workbooks, connectors and more to the community on the Azure Sentinel GitHub

Microsoft Security
Technical Content Library
Microsoft is committed to helping build a safer world for all. Explore this library to find learning content relevant to your needs

ACCESS