Microsoft Security Operations Analyst

www.aka.ms/pathways

Getting started

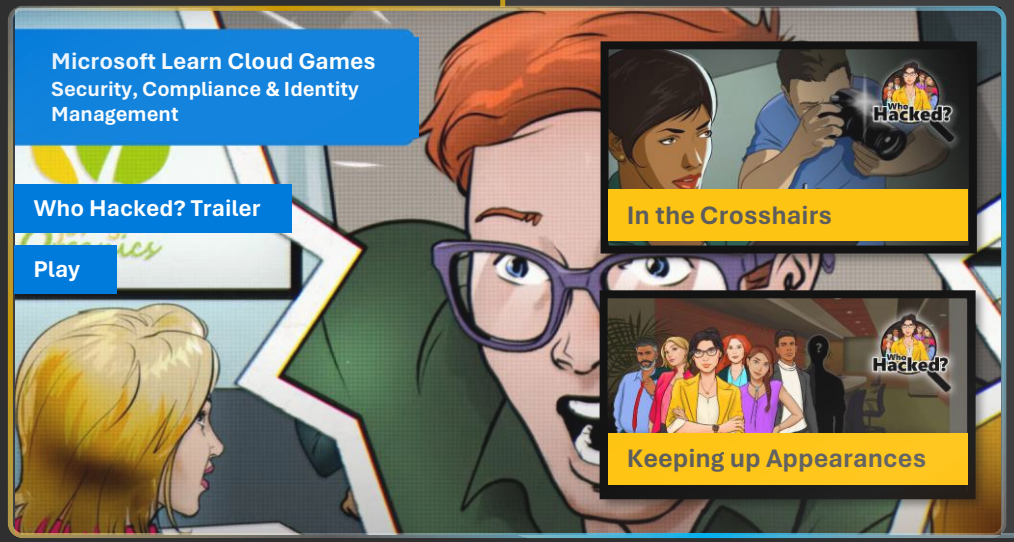
Microsoft:

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

Cloud-native Security Operations with Microsoft Sentinel

Explore basic architecture, core capabilities, and primary use cases of its products.

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



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 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 Azure Active Directory connector
- Connect the Azure Active Directory identity 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

Role Based Certification

Security Operations Analyst

Exam SC-200: Microsoft Security Operations Analyst

Skills Measured:

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

Microsoft Learn

- Mitigate threats using 365 Defender
- 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

Exam Study Guide | Course Page

Exam Page | Practice Assessment

Security Documentation | Sentinel Learning