



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 Sentinel?](#)
- [Microsoft Security YouTube Channel](#)
- [Azure Sentinel Blog](#)

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](#)

Microsoft Learn Cloud Games Security, Compliance & Identity Management



Who Hacked? Trailer

Play



Microsoft Docs, Microsoft Learn and Reference

Learn More:

- [Microsoft Sentinel and Microsoft Teams](#)
- [Manage Sentinel workspaces at scale](#)
- [Cyber threat intelligence with Sentinel](#)
- [Useful resources for working with Sentinel](#)
- [Microsoft Sentinel integration with Microsoft Cloud App Security](#)
- [Build a scalable security practice with Azure Lighthouse and Microsoft Sentinel](#)
- [Safeguard multi-cloud apps and resources with cloud security solutions from Microsoft](#)
- [Defend against threats with Microsoft Threat Protection](#)
- [Commonly used Sentinel workbooks](#)
- [Workspace architecture best practices](#)
- [Design your Sentinel workspace architecture](#)
- [Sentinel sample workspace designs](#)

Concepts:

- [Classify and analyse data](#)
- [Permissions in Microsoft 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 Microsoft Sentinel across workspaces and tenants](#)

- [Threat response with Sentinel playbooks](#)
- [Threat detection with Sentinel analytics](#)
- [Security incident management in Sentinel](#)
- [Query, visualize, and monitor data in Sentinel](#)
- [Identify threats with User and Entity Behavior Analytics in Microsoft Sentinel](#)
- [Describe security capabilities of Sentinel](#)
- [Introduction to Microsoft Sentinel](#)
- [Design a holistic monitoring strategy on Azure](#)
- [Configure and monitor Microsoft Sentinel](#)
- [Query logs in Microsoft Sentinel](#)
- [Threat hunting with Microsoft Sentinel](#)
- [Create and manage Sentinel workspaces](#)
- [Use watchlists in Microsoft Sentinel](#)
- [Hunt for threats using notebooks in Sentinel](#)
- [Explain threat hunting concepts in Sentinel](#)
- [Connect Microsoft services to Sentinel](#)
- [Construct KQL statements for Sentinel](#)
- [Build multi-table statements using KQL](#)
- [Work with data in Microsoft Sentinel using Kusto Query Language](#)
- [Deploy Sentinel and connect data sources](#)
- [Connect Common Event Format logs](#)
- [Connect data using data connectors](#)
- [Connect threat indicators to Sentinel](#)
- [Connect Microsoft 365 Defender to Sentinel](#)
- [Connect syslog data sources to Sentinel](#)
- [Connect Windows hosts to Sentinel](#)
- [Improve your cloud security posture with Microsoft Defender for Cloud](#)

KQL:

- [Write your first query with KQL](#)
- [Work with data in Sentinel using KQL](#)
- [Write multi-table queries by using KQL](#)
- [Gain insights from your data by using KQL](#)
- [Analyze query results using KQL](#)
- [Data analysis in Azure Data Explorer with KQL](#)
- [Guided project - Analyze logs in Azure Monitor with KQL](#)

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](#)

Microsoft Sentinel Documentation

[YouTube](#) Microsoft Security

QuickStart / How-to

- [Quickstart: On-board Microsoft Sentinel](#)
- [Migrate to Sentinel](#)
- [Plan your migration to Sentinel](#)
- [Track your migration with a workbook](#)
- [Migrate ArcSight detection rules](#)
- [Migrate ArcSight SOAR automation](#)
- [Export historical data from ArcSight](#)
- [Migrate Splunk detection rules](#)
- [Migrate Splunk SOAR automation](#)
- [Export historical data from Splunk](#)
- [Migrate QRadar detection rules](#)
- [Migrate QRadar SOAR automation](#)
- [Export historical data from QRadar](#)
- [Deploy Microsoft Sentinel side-by-side to an existing SIEM](#)

Collect Data

- [Find your Sentinel data connector](#)
- [Connect Sentinel to Amazon Web Services](#)
- [Connect Azure Active Directory data](#)
- [Connect Microsoft Defender for Cloud alerts](#)
- [Connect Microsoft 365 Defender data](#)
- [Windows Security Events via AMA connector](#)

Hunt for Threats

- [Conduct end-to-end threat hunting](#)
- [Get started with Jupyter notebooks and MSTICPy](#)
- [Hunt for security threats with Jupyter notebooks](#)
- [Hunt on large firewall logs by using a notebook](#)
- [Use hunting bookmarks for data investigations](#)
- [Use hunting Livestream in Microsoft Sentinel](#)

Doing More

- [Sentinel : Keep track of what's new](#)
- [Ask, or answer others on the Sentinel Tech Community](#)
- [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](#)

Role Based Certification Security Operations Analyst



Interested in certification. Check out exam SC-200: Microsoft Security Operations Analyst and the associated learning pathway