Microsoft Azure Security Engineer: Monitor Security Using Azure Sentinel

EXPLORE DATASOURCES

Sahil Malik
WWW.WINSMARTS.COM
@sahilmalik

Overview

Azure Sentinel

Layout of This Course

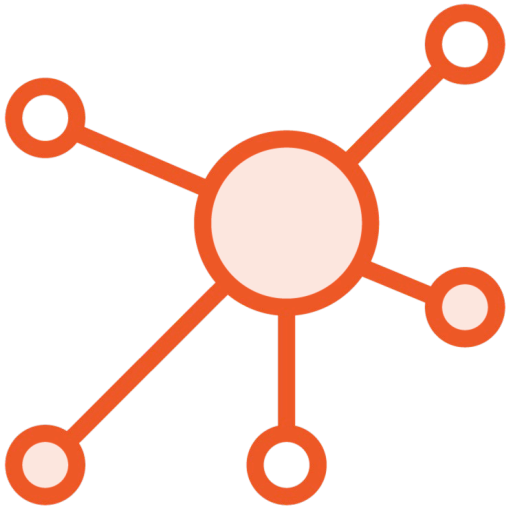
Data Sources

Demos

- Onboard Azure Sentinel
- Connect Azure Sentinel to Azure Active Directory

Azure Sentinel

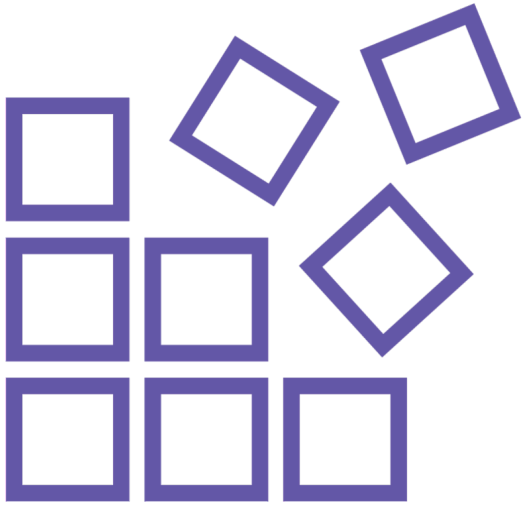
Azure Sentinel



Security Information Event Management

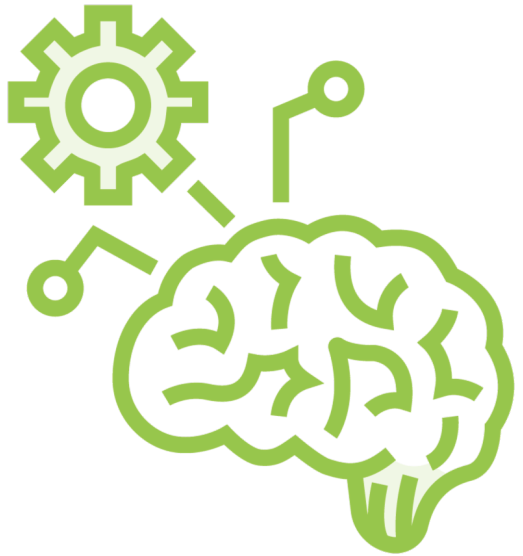
Security Orchestration Automated Response

Azure Sentinel

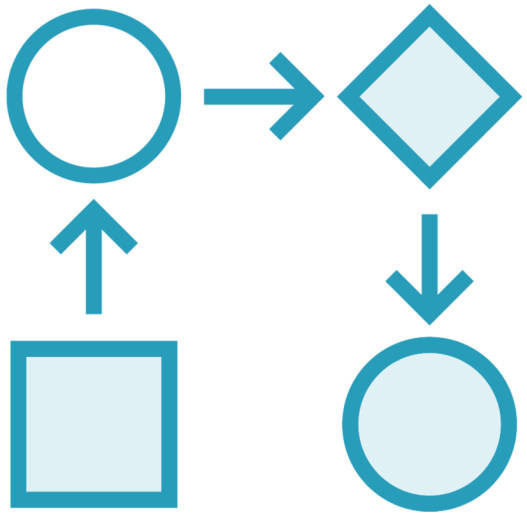


Collect

Detect



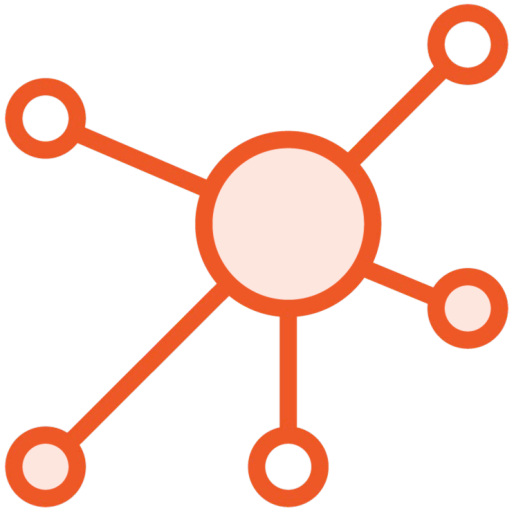
Investigate



Respond

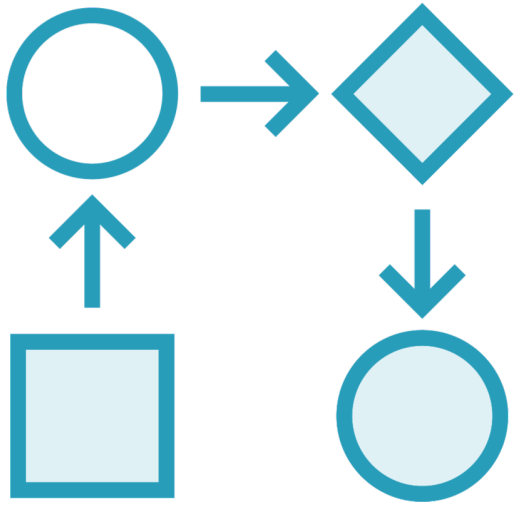
Layout of This Course

Layout of This Course



Data Sources

Evaluate Results



Automated Response

Data Sources

Data Sources

Data sources, also known as connectors is how Azure Sentinel collects signals from various sources.

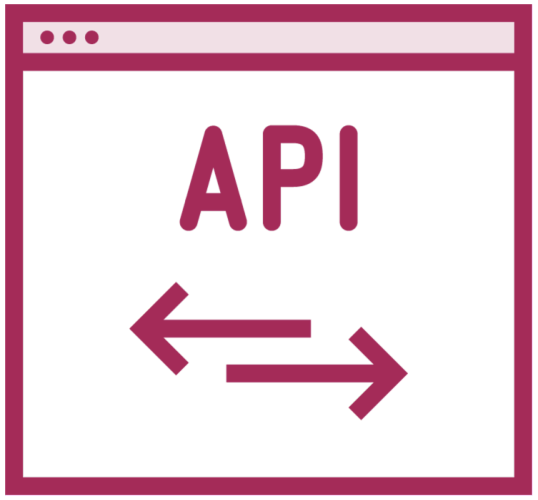
Azure Services

Other Clouds

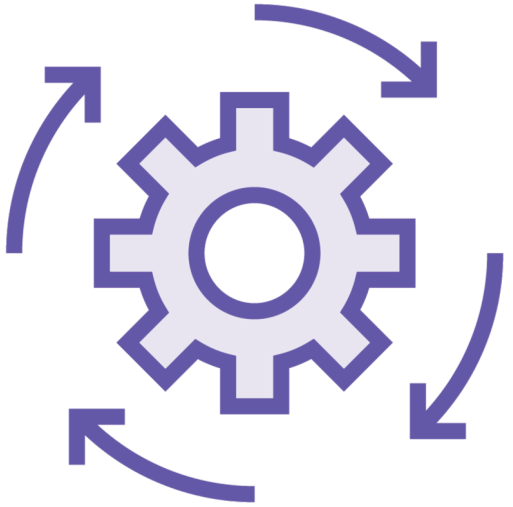
On-Prem

Data Collection Methods

Service to Service

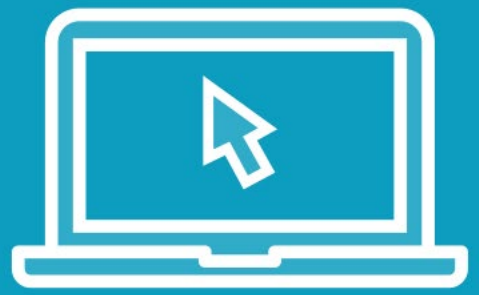


Via an API



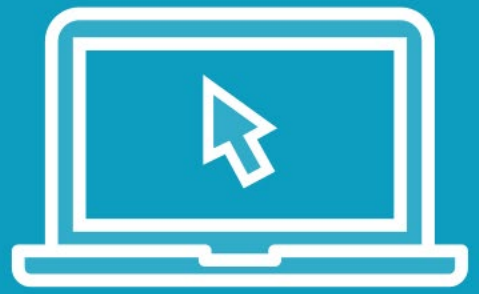
Via an Agent

Demo



Onboard Azure Sentinel

Demo



Connect Azure Sentinel to Azure Active Directory

Summary

Azure Sentinel

Layout of This Course

Data Sources

Demos

- Onboard Azure Sentinel
- Connect Azure Sentinel to Azure Active Directory