Getting Data into Azure Sentinel and Using Workbooks

Muhammad Sajid
CLOUD ARCHITECT

@sajid_nazeer www.msajid.cloud

Overview

Data Ingestion

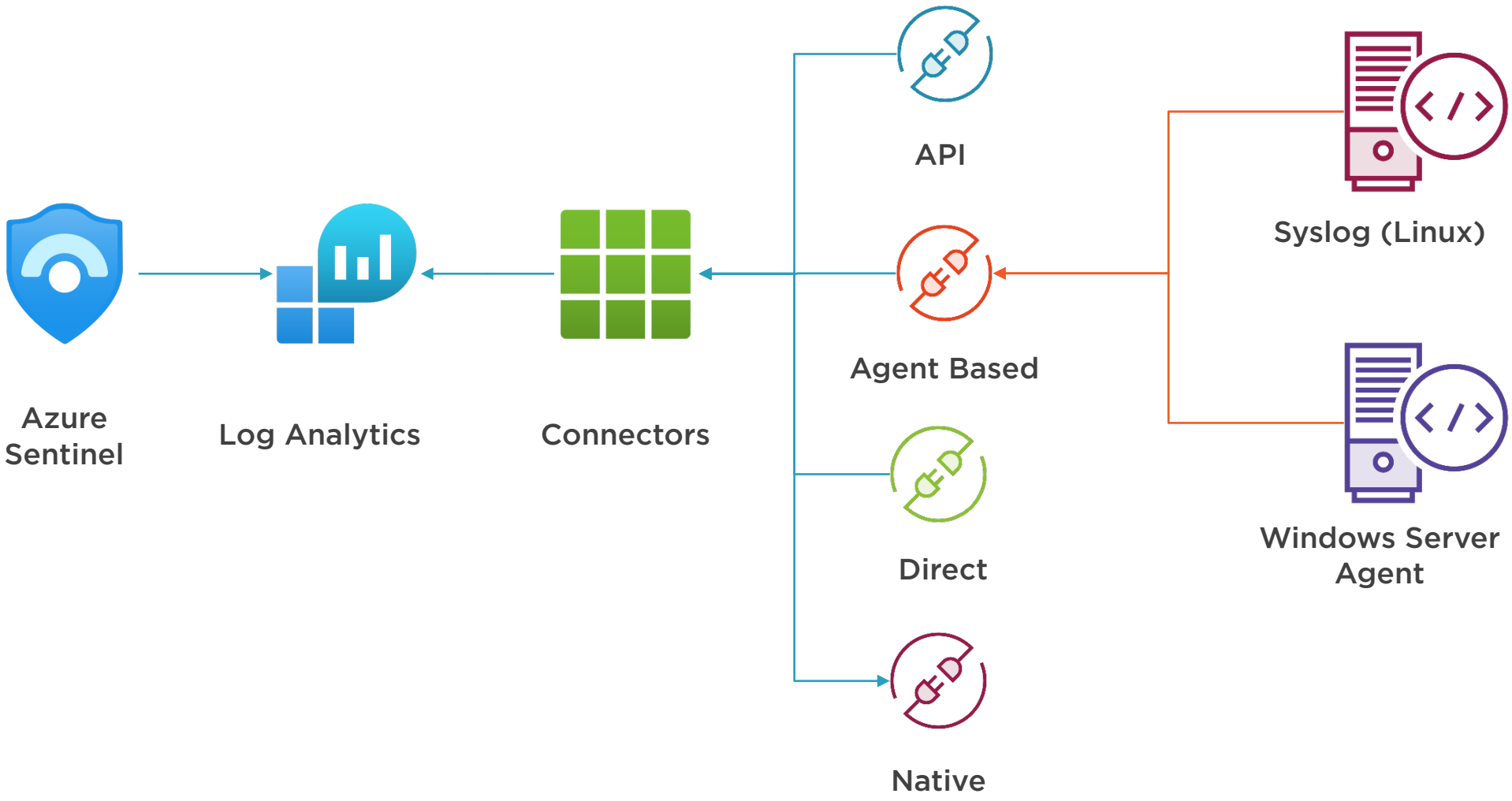
- Type of connectors
- Connecting Microsoft Services
- Connecting Partner Services

Workbooks in Azure Sentinel

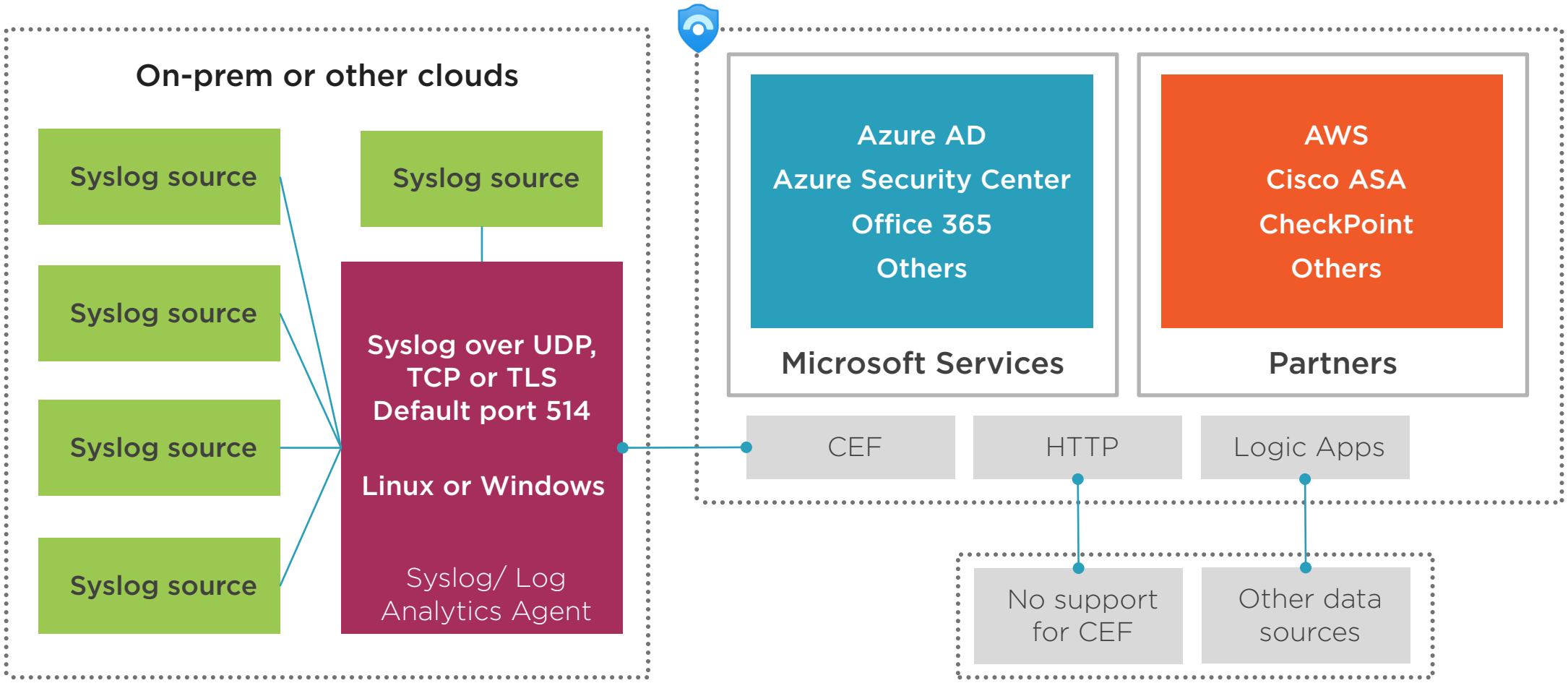
- Built-in Workbooks
- Custom Workbooks

Azure Sentinel Connector Types

Azure Sentinel Connector Types



Azure Sentinel Connector Types



Free Ingestion Options

Azure

Azure Activity, Azure Active Directory Identity Protection, Azure Information Protection, Azure Security Center

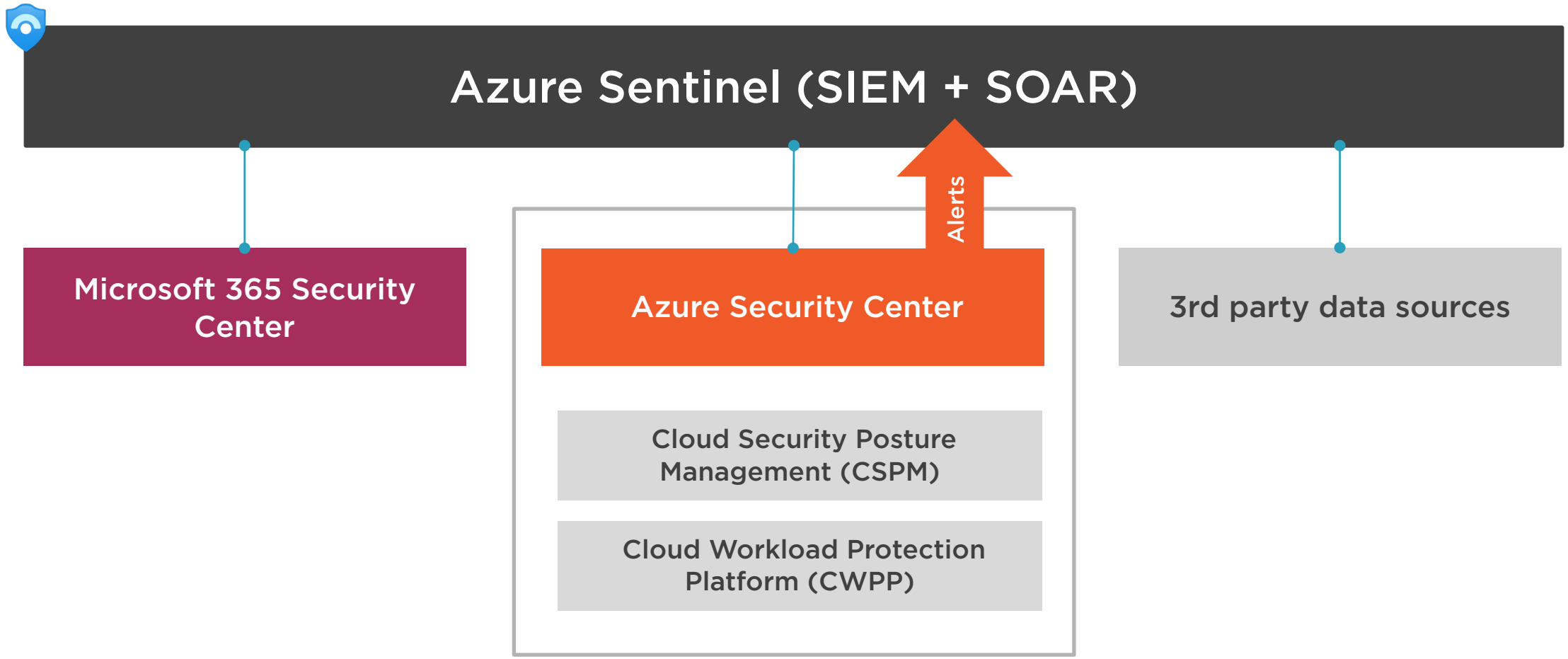
Office 365

Exchange and Sharepoint Logs

Azure AD/Office365 audit logs are NOT free

Connecting Azure Security Center

Azure Sentinel and Security Center Better Together



Azure Sentinel and Azure Security Center

Azure Sentinel

A Cloud-based SIEM and SOAR Solution that depends on various security solutions to provide threat detection, investigation, hunting, and automated response capabilities.

Azure Security Center

A Cloud Security Posture Management and Cloud Workload Platform Protection solution.

Complements Azure Sentinel

Pre-requisites for Connecting ASC

Read and Write Permissions on the Workspace

Security Reader role in the source subscription

Azure Security Center Standard Tier

Demo

Configuring Azure Sentinel Connectors

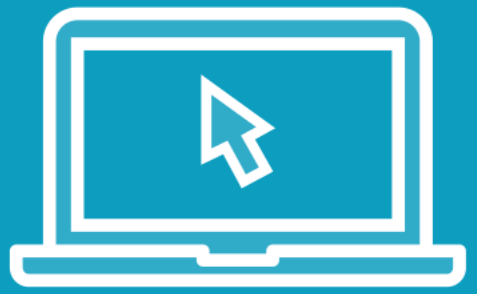
- Azure Security Center

Connecting Azure AD

Pre-requisites for Connecting Azure AD

- Azure AD P1 or P2 license
- Global Admin or Security Admin permissions on the Tenant of source Subscription
- Permission to access Azure AD diagnostic logs

Demo

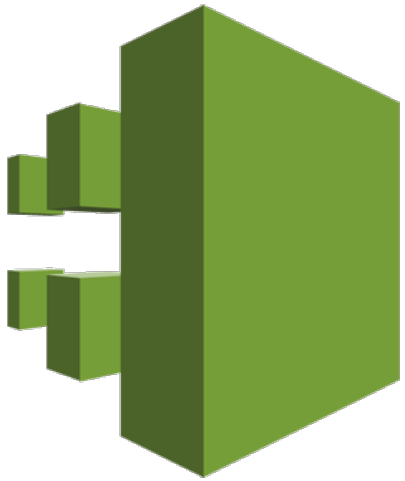


Configuring Azure Sentinel Connectors

- Azure Active Directory

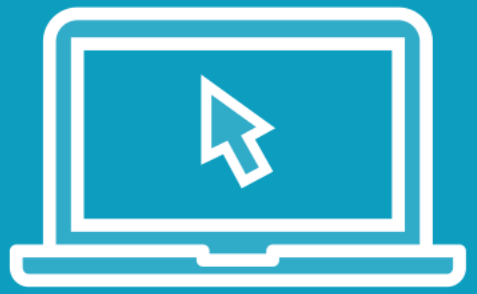
Connecting AWS CloudTrail

Pre-requisites for Connecting AWS CloudTrail



Write permission on the Azure Sentinel workspace

Demo

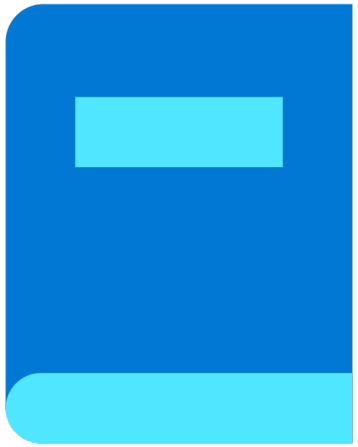


Configuring Azure Sentinel Connectors

- AWS CloudTrail

Using Azure Sentinel Workbooks

Pre-requisites



- Azure Sentinel Contributor permissions
- Azure Workbooks Contributor permissions
- Available Data in Azure Sentinel workspace

Demo

Workbooks In Azure Sentinel

- Using Built-in Workbooks
- Creating Custom Workbooks

Summary

Summary

Azure Sentinel Connectors

- Types
- Connectors

Workbooks

- Built-in
- Custom

Up Next:
Threat Detection Using Analytics