Managing and Responding to Security Events Using Azure Sentinel

AZURE SENTINEL GETTING STARTED

Muhammad Sajid
CLOUD ARCHITECT

@sajid_nazeer www.msajid.cloud

Overview

What is Azure Sentinel?

- Core capabilities

Why do we need Azure Sentinel?

Design considerations

- Log analytics workspace
- Permissions

Enabling Azure Sentinel

- Pre-requisites

Target Audience

Cloud Architects

Security Analysts

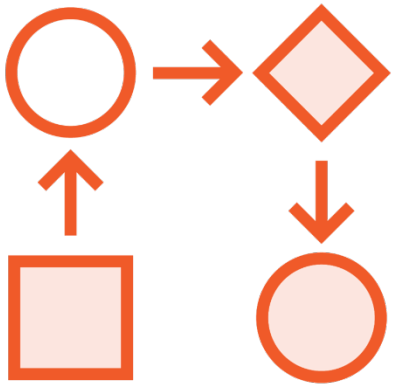
SecOps Teams

Azure Developers

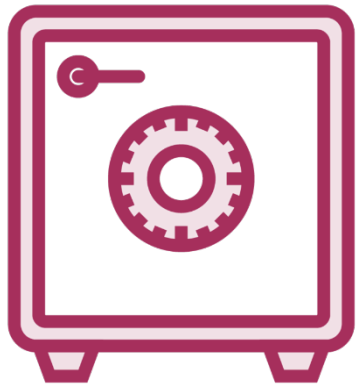
Learners Knowledge

Microsoft Azure

Kusto Query Language (KQL)



Logic Apps



Cyber security Concepts

What Is Azure Sentinel?

What is Azure Sentinel?

Azure Sentinel is a next generation Security Information and Event Management (**SIEM**) and Security Orchestration Automation Response (**SOAR**) solution provided by Microsoft.

SecOps and SOC

SecOps

A Team focused on running the day-to-day tasks of a Security Operations Center (SOC)

SOC

A Team dedicated to securing The Enterprise.

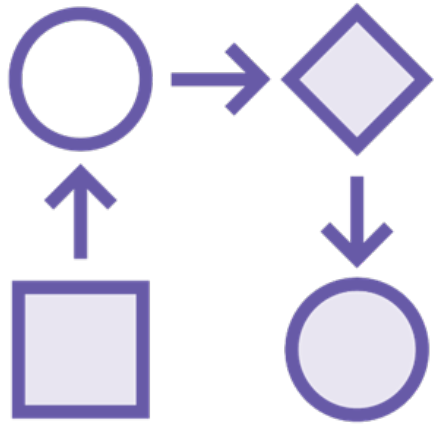
"A team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents."

Mitre (*www.mitre.org*)

Modern SIEM and SOAR

SIM and SEM

Security Information and Event Management



SOAR

Security Orchestration, Automation and Response

Core Capabilities of Azure Sentinel

Data Collection

Threat Detection

Threat Investigation

Rapid Response

Why Do Companies Need Azure Sentinel?

SecOps and SOC Challenges

Big Data Challenge

Constantly increasing security data

Alert Fatigue and Attrition

49% of Security alerts are never investigated

Staffing Challenge

4.07 M unfilled security jobs

Lack of Tools

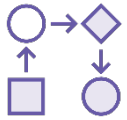
Automation, AI/ML, threat hunting and investigation

Benefits of Azure Sentinel

Scales automatically to meet the data storage needs

Direct integration with Microsoft Intelligent Security Graph

Advanced anomaly detections using Microsoft's machine learning

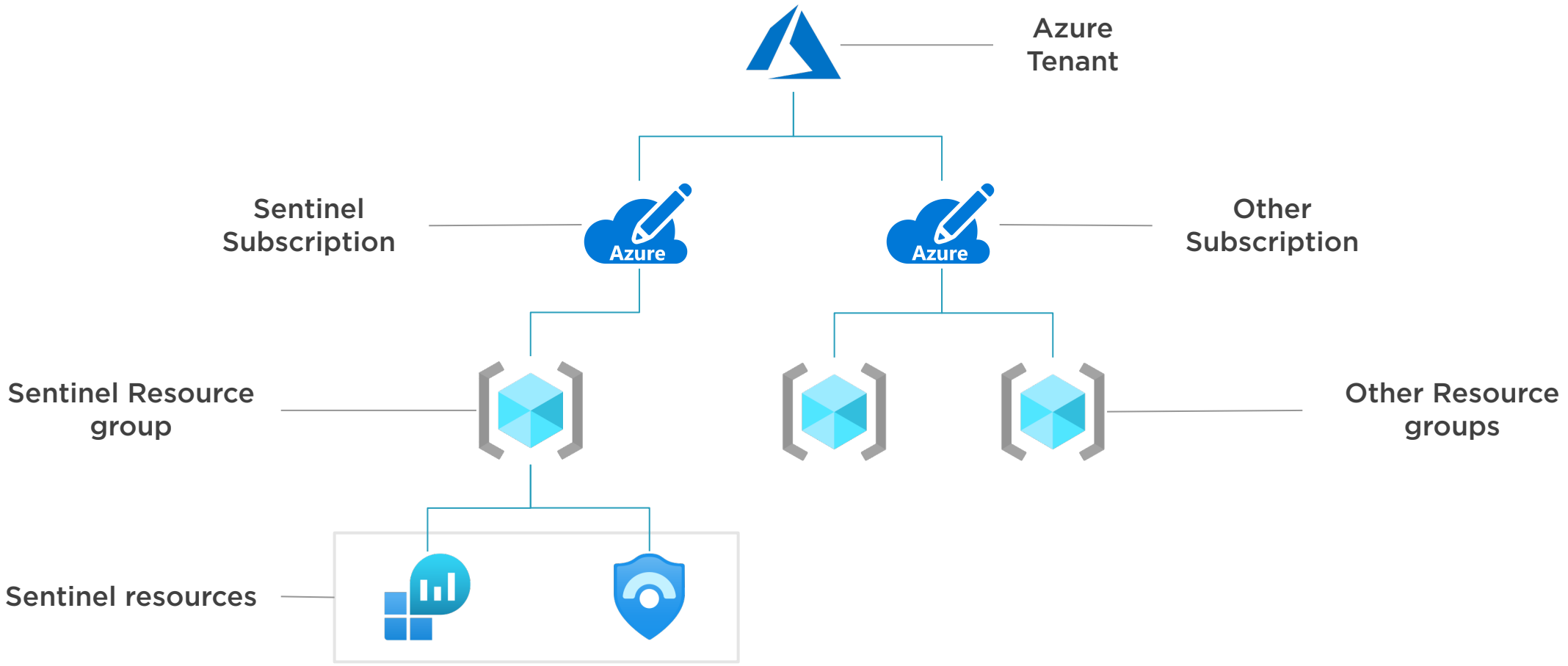


Automation capability for investigating and responding to alerts

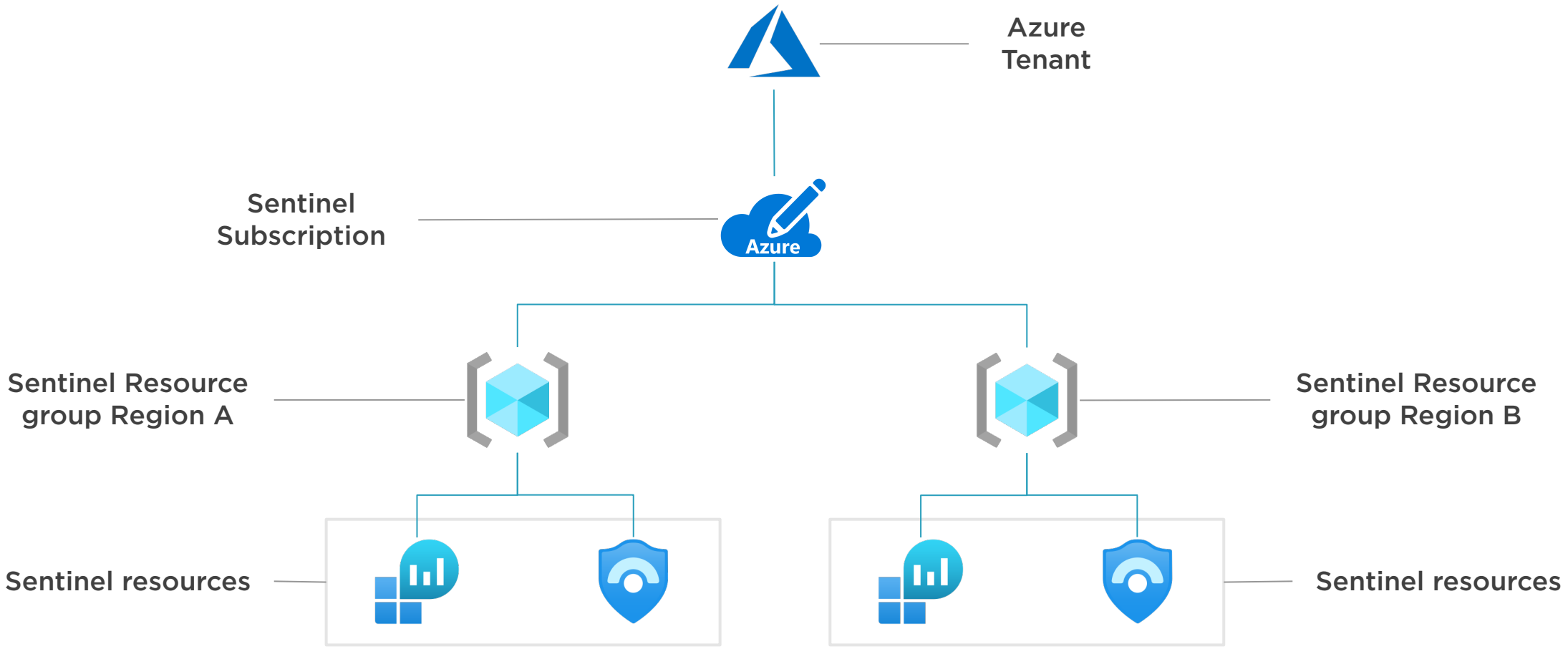
Intuitive dashboards and querying capability

Design Considerations

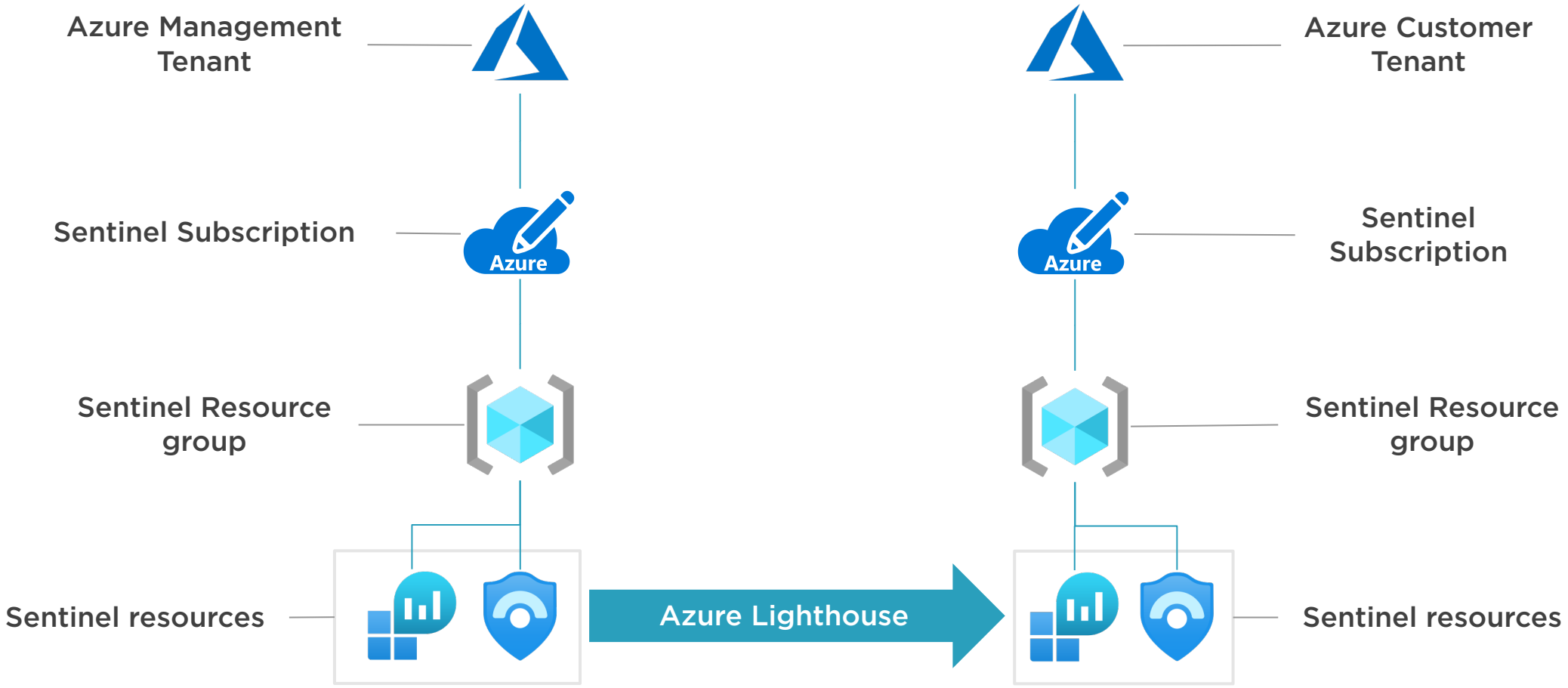
Workspace Design (Single Tenant)



Workspace Design (Single Tenant)

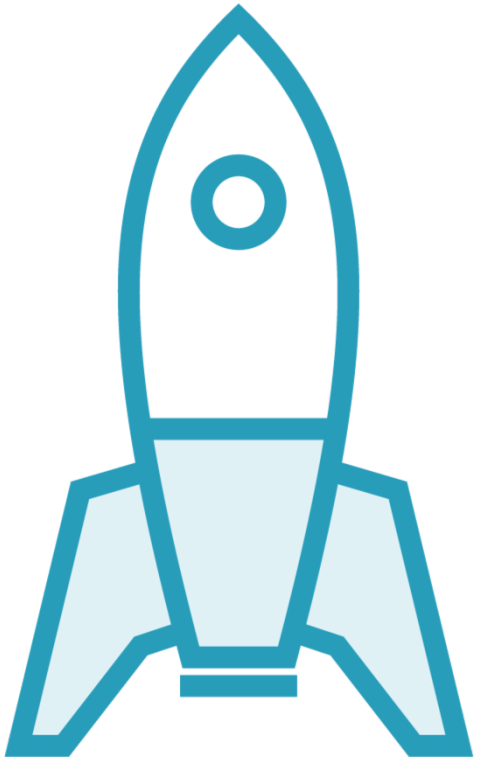


Workspace Design (Multi Tenant)



Getting Our Feet Wet

Pre-requisites to Enable Azure Sentinel



Azure Subscription

Log Analytics workspace

Permissions

- Azure Subscription
  - Contributor
- Resource group or Resource
  - Contributor
  - Reader

Demo

Enabling Azure Sentinel

- Using Azure Portal
- Using Resource Manager templates

Summary

Summary

What and Why of Azure Sentinel

Design considerations

Enabling Azure Sentinel

Up Next:
Getting Data into Azure Sentinel and Using Workbooks