

The secrets of building a SOC in Azure

Jeroen Niesen



Jeroen Niesen

Security Expert by day,
Developer by night

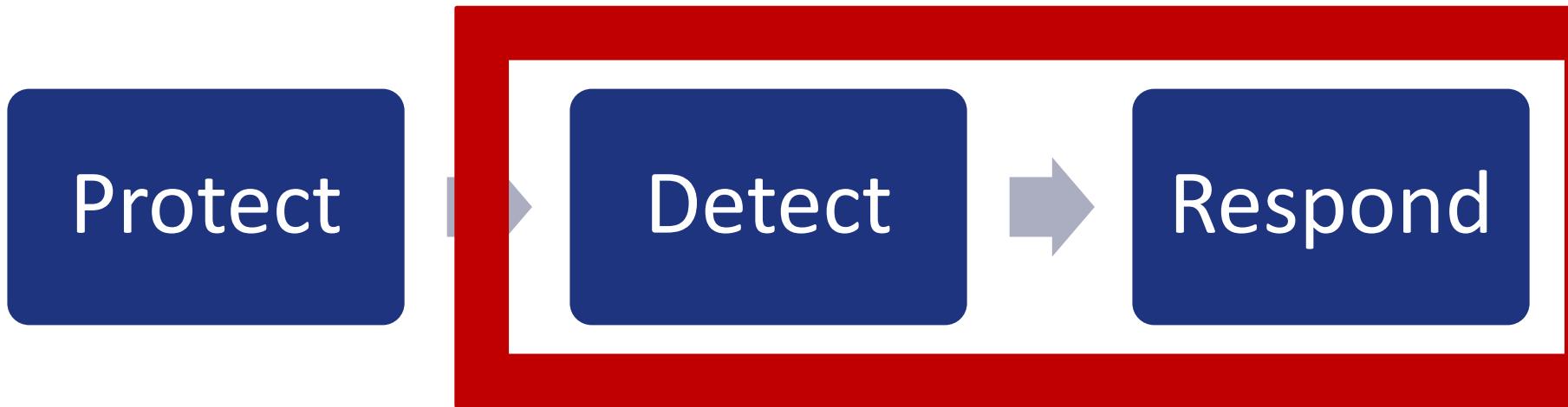


AzureVlog



@jeroenniesen

Security Posture



SOC basics (non-cyber security)

Common sense of security rules applies

- Have locks on exits and entrances
- Have locks on vaults and cash registers
- Have CCTV cameras pointed at valuable objects and throughout the whole facility

Have analysts that monitor the CCTV cameras.

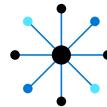
SOC Basics (cyber security)

Common sense of cyber security rules applies:

- Control access with passwords, ACLs, firewall rules etc.
- Monitor critical infrastructure on anomalous activity

Have analysts that monitors for security incidents

Cyber threads are hidden away



Collect



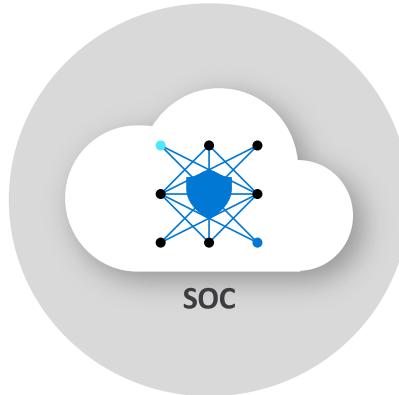
Respond



Detect



Investigate



Security Operations Center

People (the SOC team)

Processes

- Classification, Triage, Prioritization
- Analysis, Remediation
- Audit

Tools

- Asset discovery, Vulnerability Assessment
- Intrusion detection, Behavioral monitoring
- SIEM

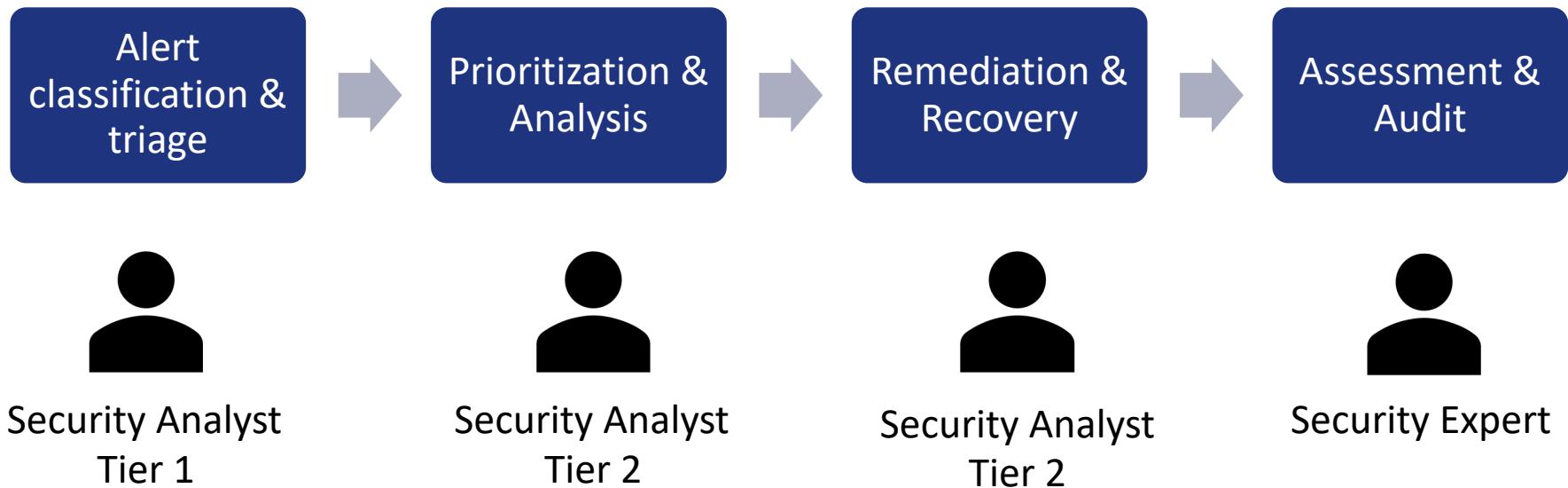
People

Role	Description	Responsibilities
Security Analyst/Engineer	Triage specialist Incident responder	<ul style="list-style-type: none">• Reviews alerts• determine relevancy• converts alerts into security incidents• Identify scope of the attack• Remediate/recover environment• Collect asset data for further investigation
Security Expert	Thread Hunter	<ul style="list-style-type: none">• Reviews asset data from security incidents• Explores ways to identify hidden threats using latest threat intelligence
SOC Manager	Manager	<ul style="list-style-type: none">• Executes crisis communication• Making sure the SOC follows the right processes (compliance)

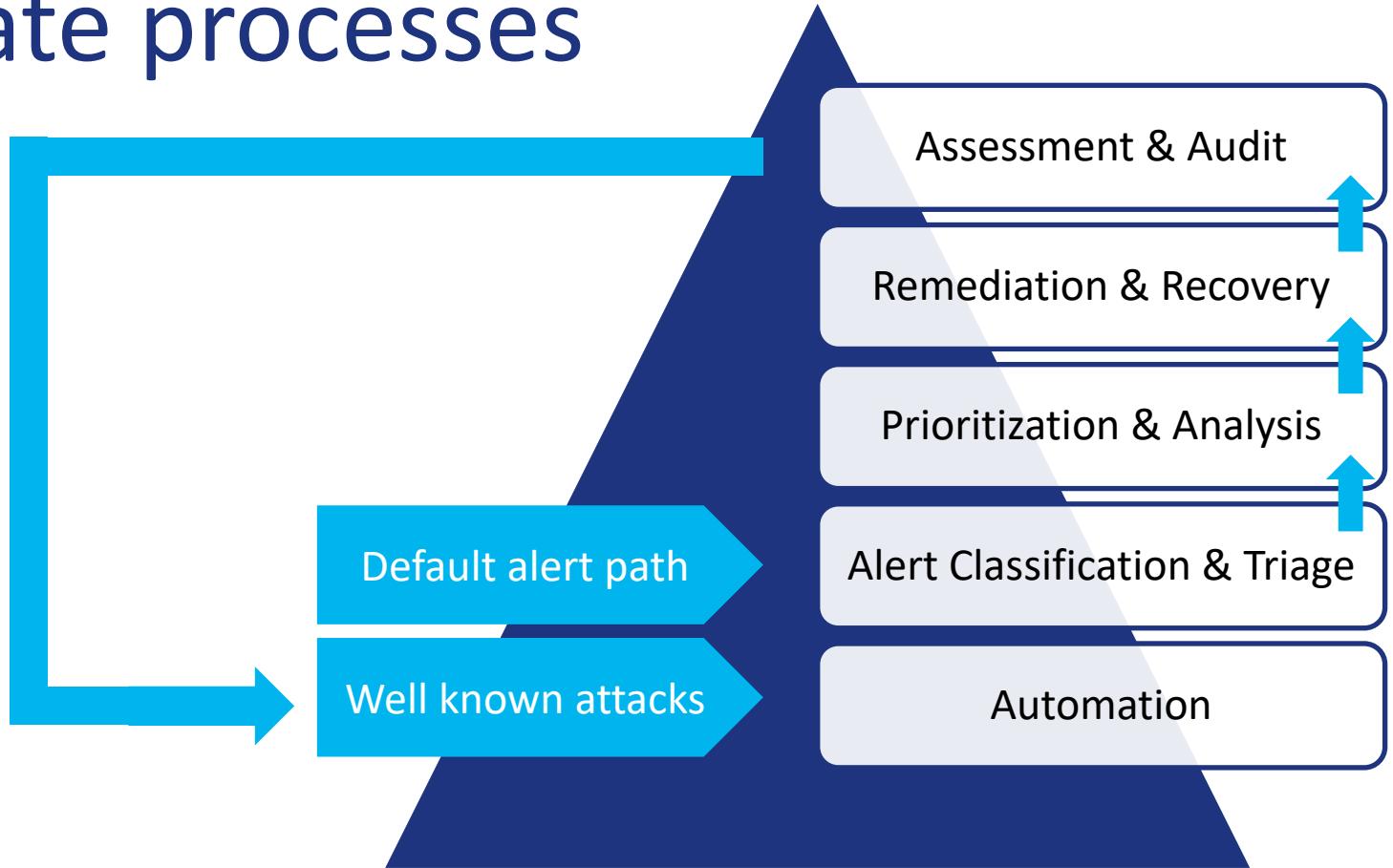
People (larger SOC)

Role	Description	Responsibilities
Security Analyst Tier 1	Triage specialist	<ul style="list-style-type: none">• Reviews alerts• determine relevancy• converts alerts into security incidents
Security Analyst Tier 2	Incident responder	<ul style="list-style-type: none">• Identify scope of the attack• Remediate/recover environment• Collect asset data for further investigation
Security Expert	Thread Hunter	<ul style="list-style-type: none">• Reviews asset data from security incidents• Explores ways to identify hidden threats using latest threat intelligence
SOC Manager	Manager	<ul style="list-style-type: none">• Executes crisis communication• Making sure the SOC follows the right processes (compliance)

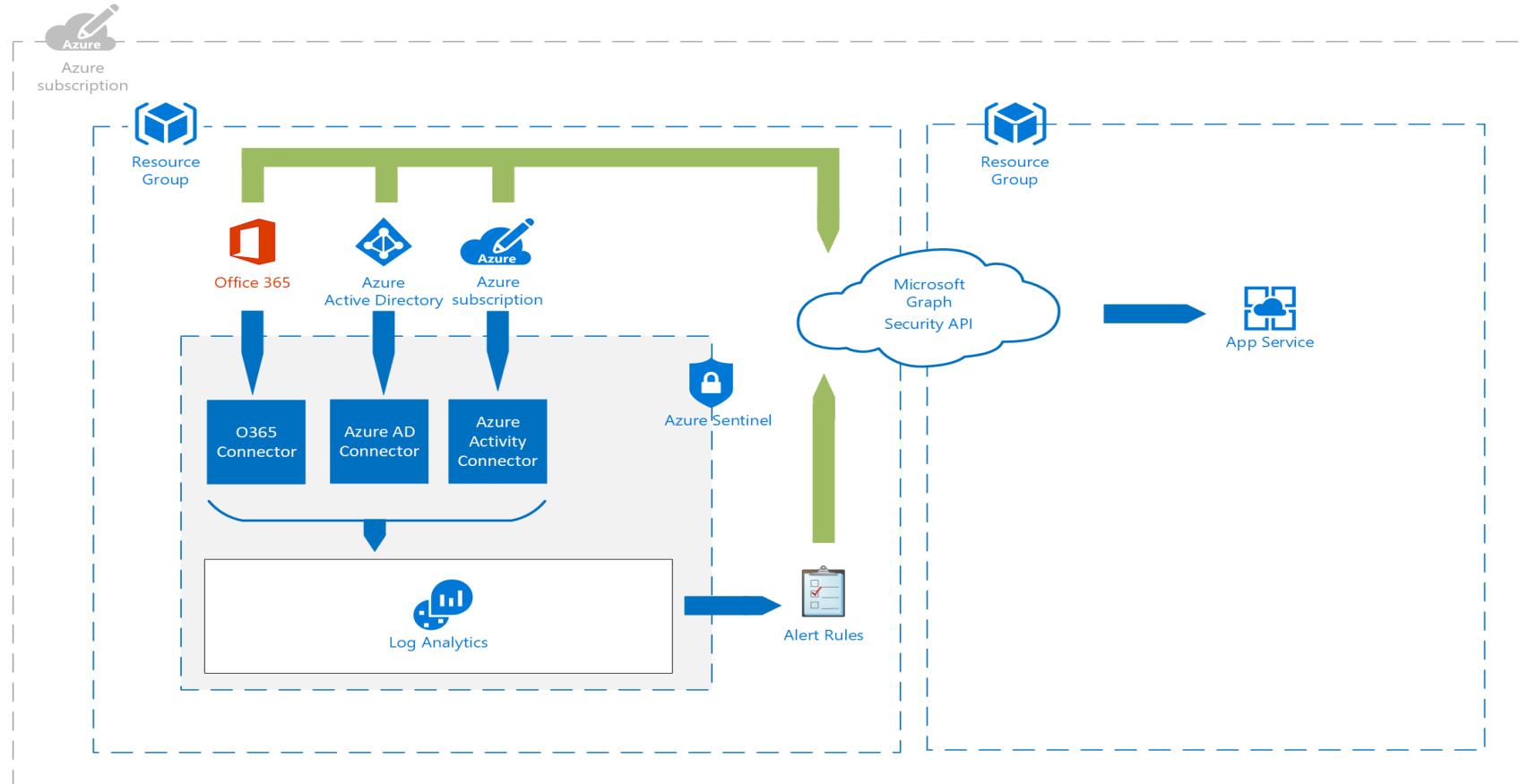
Processes



Automate processes



Architecture



Azure Sentinel

Microsoft Azure Search resources, services, and docs admin@contoso.com CONTOSO

Home > Azure Sentinel

Azure Sentinel - Overview

Last week (1/21/2018-1/27/2018)

EVENTS 8.2M ↑978.4K **ALERTS** 39 ↑6 **INCIDENTS** 18 ↑4

INCIDENTS BY STATUS

Status	Count
NEW (7)	7
IN PROGRESS (4)	4
CLOSED (7)	7

Events and alerts over time

Event Types

Type	Count
ALERTS	89
CEF	315K
SECURITY EVENT	121K
AZURE AD	110K
OTHERS (5)	106K

Potential malicious events

Most anomalous data sources

Source	Value
Azure AD	82K
Office	4K
SecurityEvents	78K

Democratize ML for your SecOps

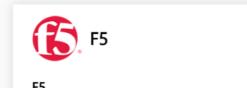
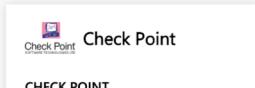
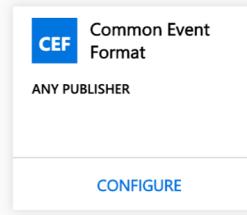
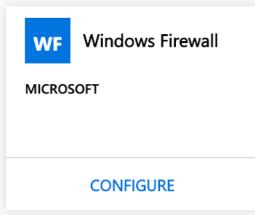
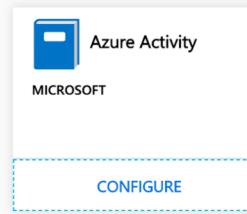
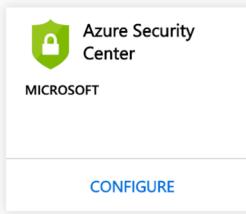
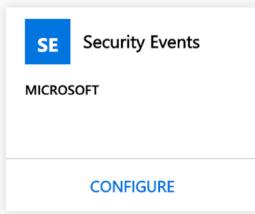
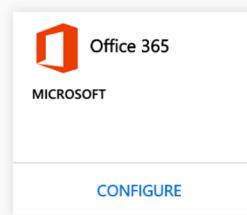
Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

Learn more >

Azure Sentinel

- Collects raw logs via connectors
 - Office 365
 - Azure Active Directory
 - Azure
- Dashboards
- Alert generation
- Thread Hunting

Sentinel Connectors



Azure Sentinel – Alert Generation

- Analysis raw logs with queries that run with an interval
- Correlate alerts by using fusion (AI)

Azure Sentinel - Alerts

- Published in the Microsoft Graph Security API
- Published in Azure Monitor
- Realtime automation

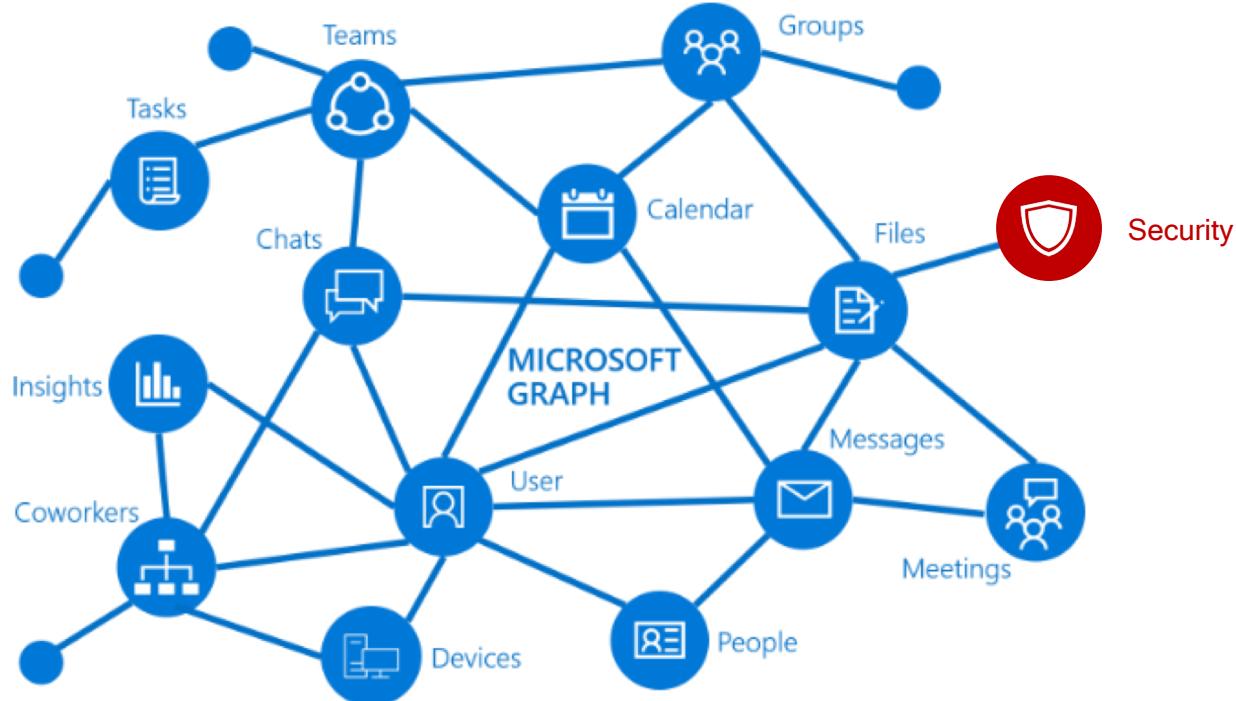
DEMO

Exploring Azure Sentinel

- Connecting Sources
- Configuring Alerts
- Exploring Azure Sentinel Cases



Microsoft Graph Security API



Graph Security vs. Sentinel

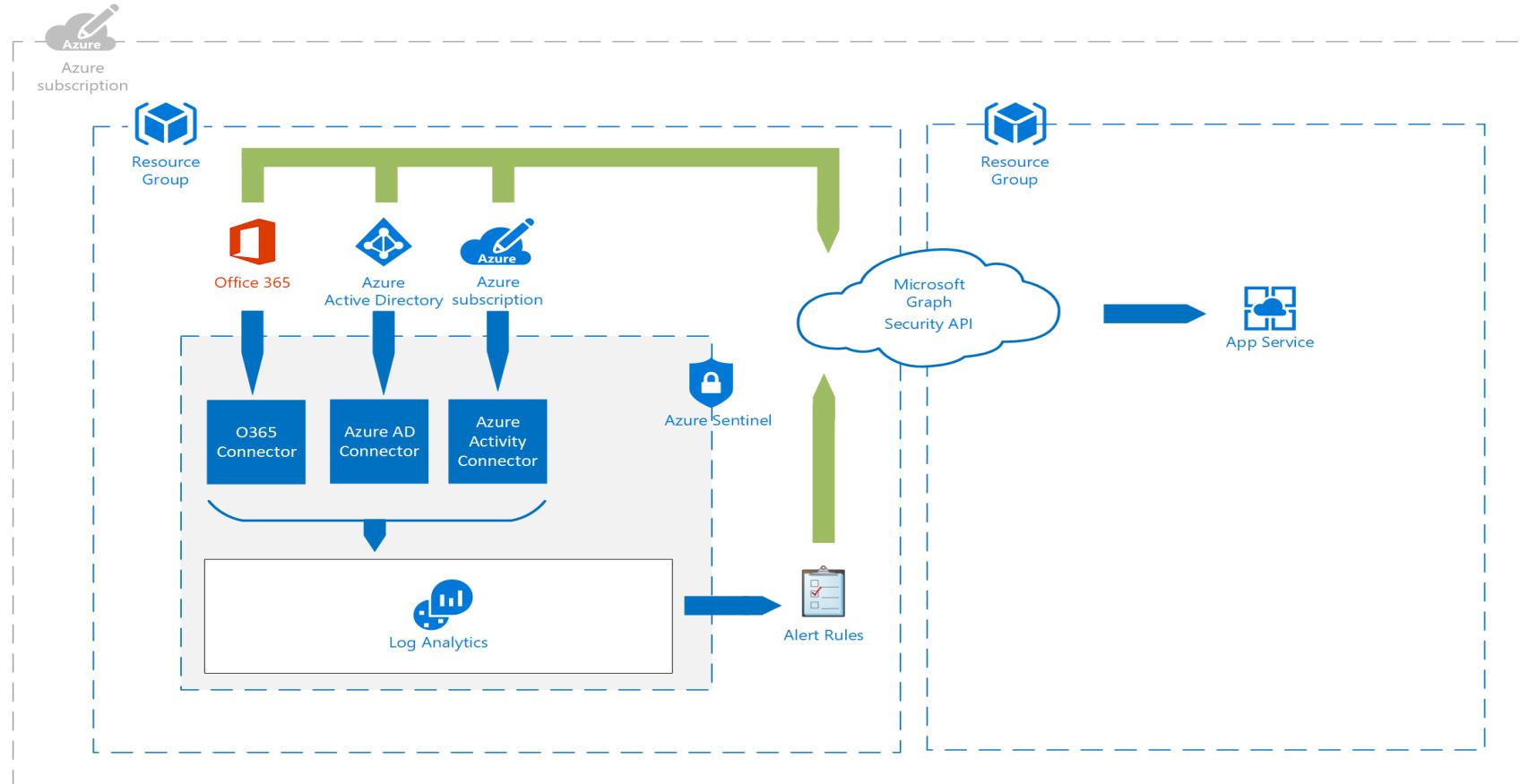
Azure Sentinel is a SIEM solution

- It collects logs, and based on those logs alerts will be generated
- It contains log data
- It has a user interface in the Microsoft Azure Portal

Microsoft Graph Security API

- It is an API where security alerts from Graph Security Providers will be published to
- It has no interface, alerts can only be collected via an API

Architecture



Graph Security API

Uses service principal (app registration) to receive data

Data in Graph

- Alerts
 - Alert details
 - Alert remediation
- Secure Score
 - Value of the score
 - Recommendations

Alert Sources

- Azure Security Center
- Azure Active Directory Identity Protection
- Microsoft Cloud App Security
- Windows Defender ATP
- Azure ATP
- Office 365
- Azure Information Protection
- Azure Sentinel
- Palo Alto Networks

Secure Scores

- Azure Security Center
- Office 365
- Azure Active Directory

DEMO

Exploring Graph API

- With Graph Explorer
- With PowerShell
- With an demo app



Translating Alerts into Tickets

- Use of a logic app to connect the Graph Security API with Fresh Desk (Ticketing Service)

The screenshot shows a list of three tickets in Fresh Desk:

- [Preview] Traffic from unrecommended IP addresses was detected #35**
Overdue by 5 days
Created 6 days ago
Assigned to Jeroen Niesen
- Multiple login attempts from the same IP #34**
Overdue by 5 days
Created 6 days ago
Assigned to Jeroen Niesen
- Multiple login attempts from the same IP #33**
Overdue by 5 days
Created 6 days ago
Assigned to Jeroen Niesen

A sidebar on the left contains icons for user management, ticket creation, and other Fresh Desk features. A green header bar at the top indicates the view is for "All unresolved tickets". On the right, there are dropdown menus for priority (Medium), escalation, and status (Open). At the bottom right, there is a button labeled "Assign a group or agent" followed by the escalation and status dropdowns.



DEMO

Integrating with the Microsoft
Graph Security API

Interesting documentation

- <https://github.com/microsoftgraph>
- <https://github.com/Azure/Azure-Sentinel>

The screenshot shows two GitHub repository pages side-by-side.

microsoftgraph/microsoft-graph-docs (Top Repository):

- Code: 421 Issues, 74 Pull requests, 0 Projects, 0 Wiki, Insights
- Branch: master → [microsoft-graph-docs / api-reference / beta / resources / security-api-overview.md](#)
- Commit history:
 - edwardkoval update provider name (90f9fe 25 days ago)
 - 8 contributors (list of icons)
- 126 lines (91 sloc) | 17.6 KB
- Raw, Blame, History, Copy path

title	description	localization_priority	author	ms.prod
Use the Microsoft Graph Security API	> **Important:** APIs under the /beta version in Microsoft Graph are in preview and are subject to change. Use of these APIs in production applications is not supported.	Priority	preetikr	security

Use the Microsoft Graph Security API

[INCLUDE beta-disclaimer]

The Microsoft Graph Security API provides a unified interface and schema to integrate with security solutions from Microsoft and ecosystem partners. This empowers customers to streamline security operations and better defend against increasing cyber threats. The Microsoft Graph Security API federates queries to all onboarded security providers and

Azure/Azure-Sentinel (Bottom Repository):

- Code: 53 Issues, 109 Stars, 25 Forks
- Search, Sign in, Sign up

Commit history (partial):

- Clone or download
- commit 4ad98a2 a day ago (6 days ago)
- a day ago
- 5 days ago
- 7 days ago
- 2 months ago
- a day ago
- 13 days ago
- 7 months ago
- a month ago
- 3 months ago
- a month ago

Thanks!