The secrets of building a SOC in Azure

Jeroen Niesen

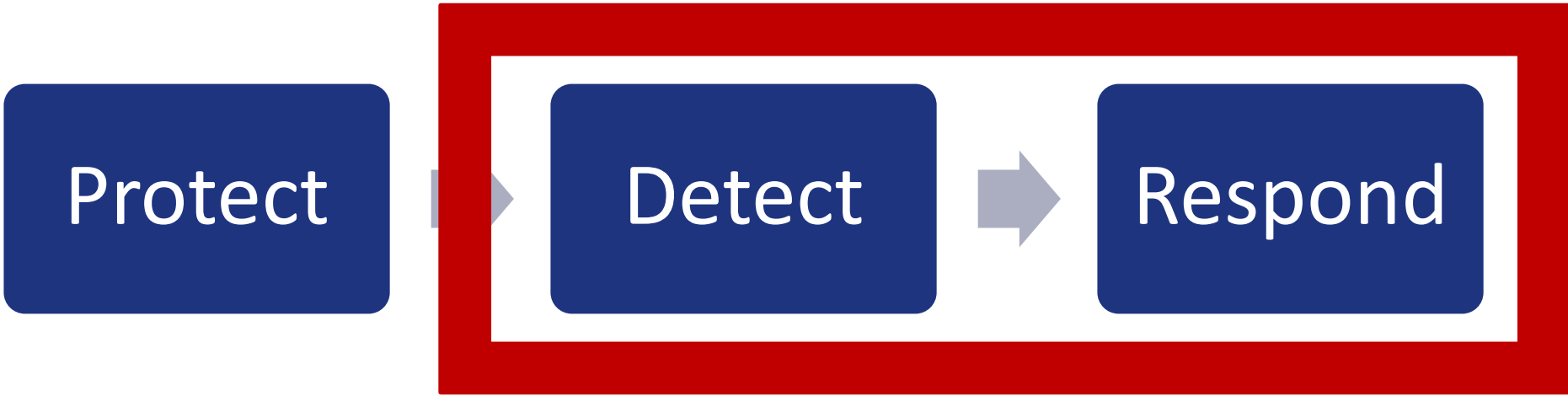
Jeroen Niesen

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.

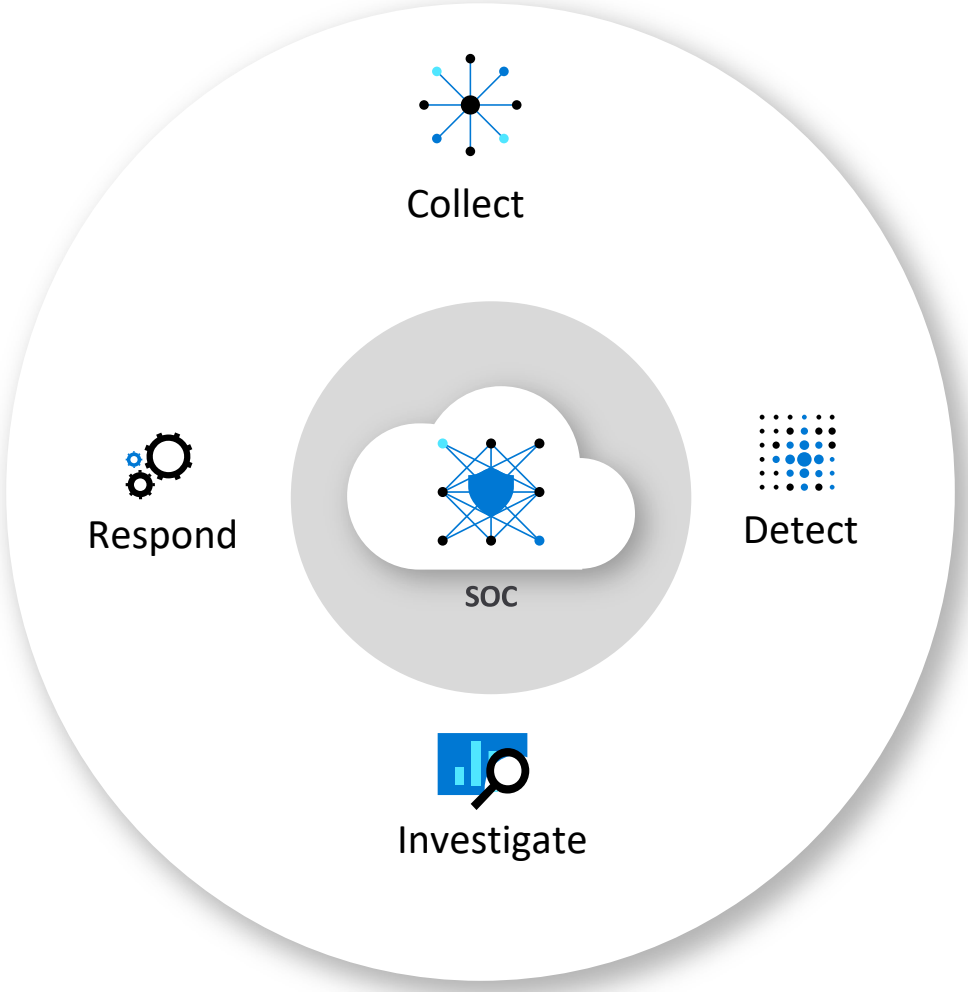
SOC Basics (cyber security)

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
SOC
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

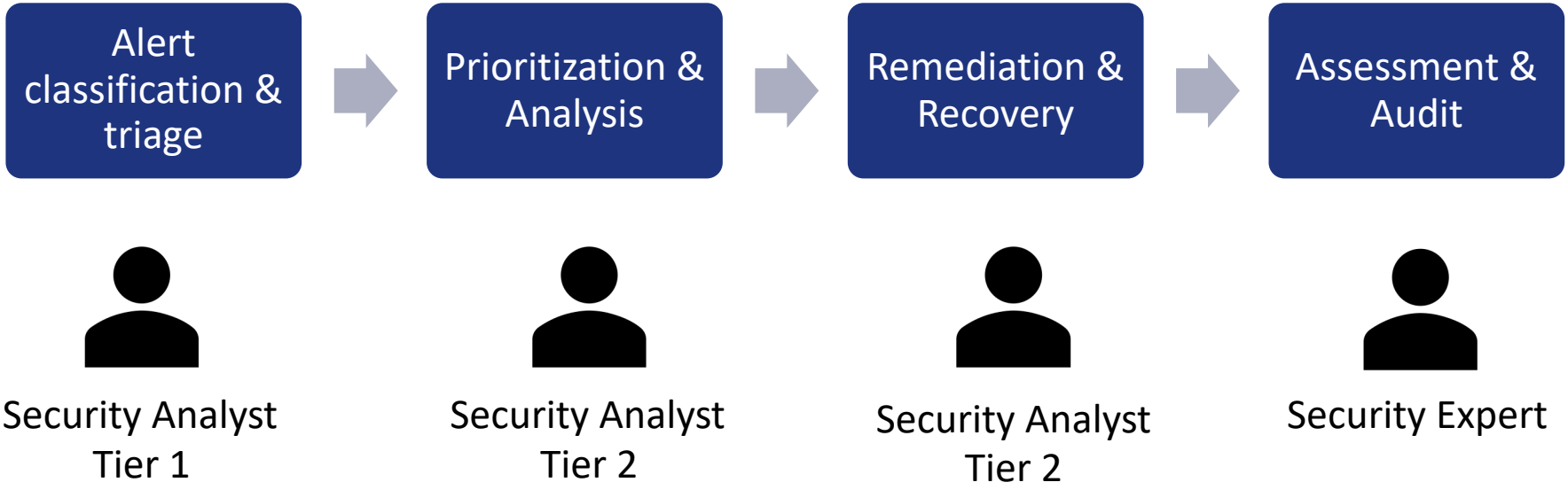
People

Role	Description	Responsibilities
Security Analyst/Engineer	Triage specialist Incident responder	• 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	• Reviews asset data from security incidents • Explores ways to identify hidden threats using latest threat intelligence
SOC Manager	Manager	• Executes crisis communication • Making sure the SOC follows the right processes (compliance)

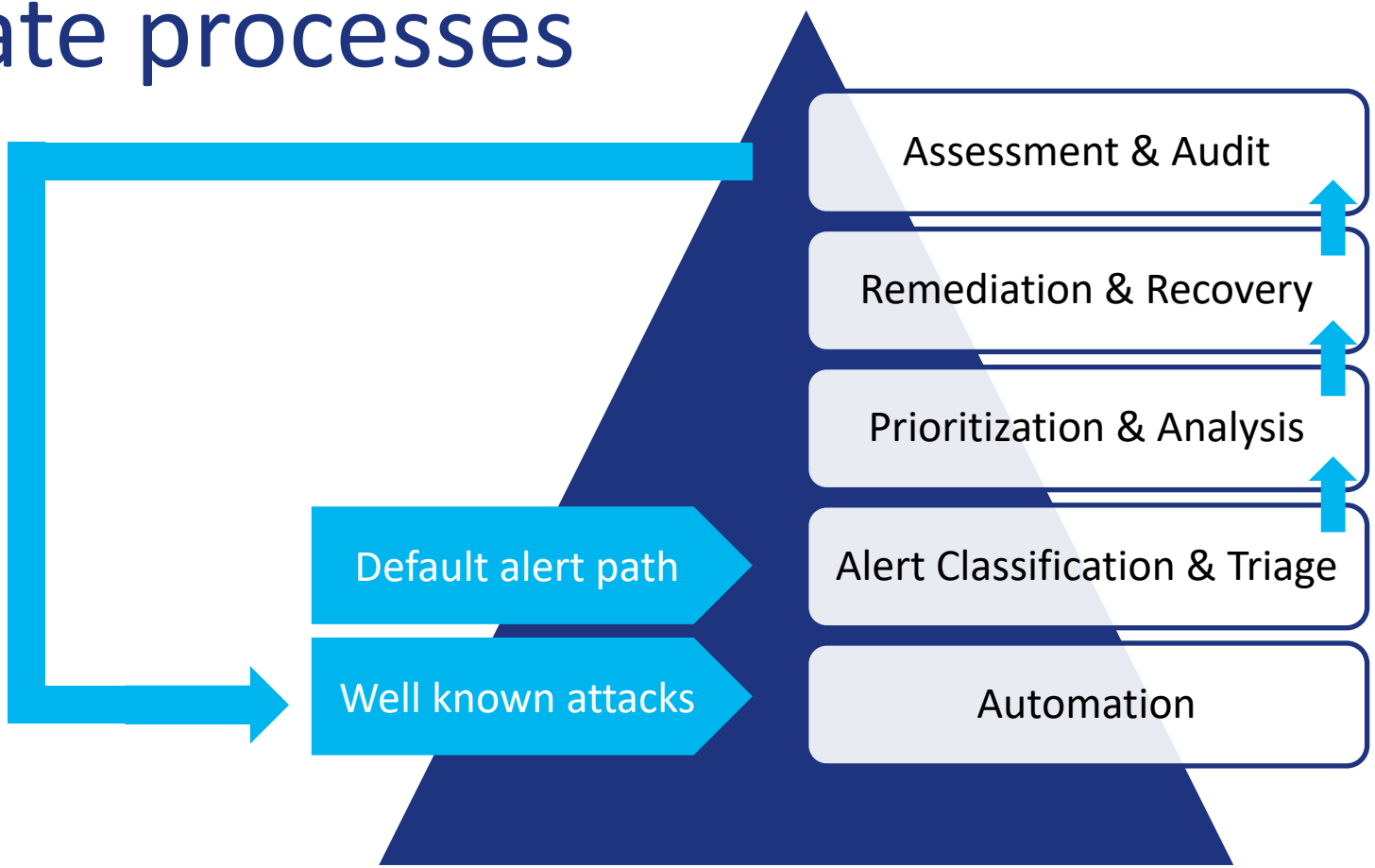
People (larger SOC)

Role	Description	Responsibilities
Security Analyst Tier 1	Triage specialist	• Reviews alerts • determine relevancy • converts alerts into security incidents
Security Analyst Tier 2	Incident responder	• Identify scope of the attack • Remediate/recover environment • Collect asset data for further investigation
Security Expert	Thread Hunter	• Reviews asset data from security incidents • Explores ways to identify hidden threats using latest threat intelligence
SOC Manager	Manager	• Executes crisis communication • Making sure the SOC follows the right processes (compliance)

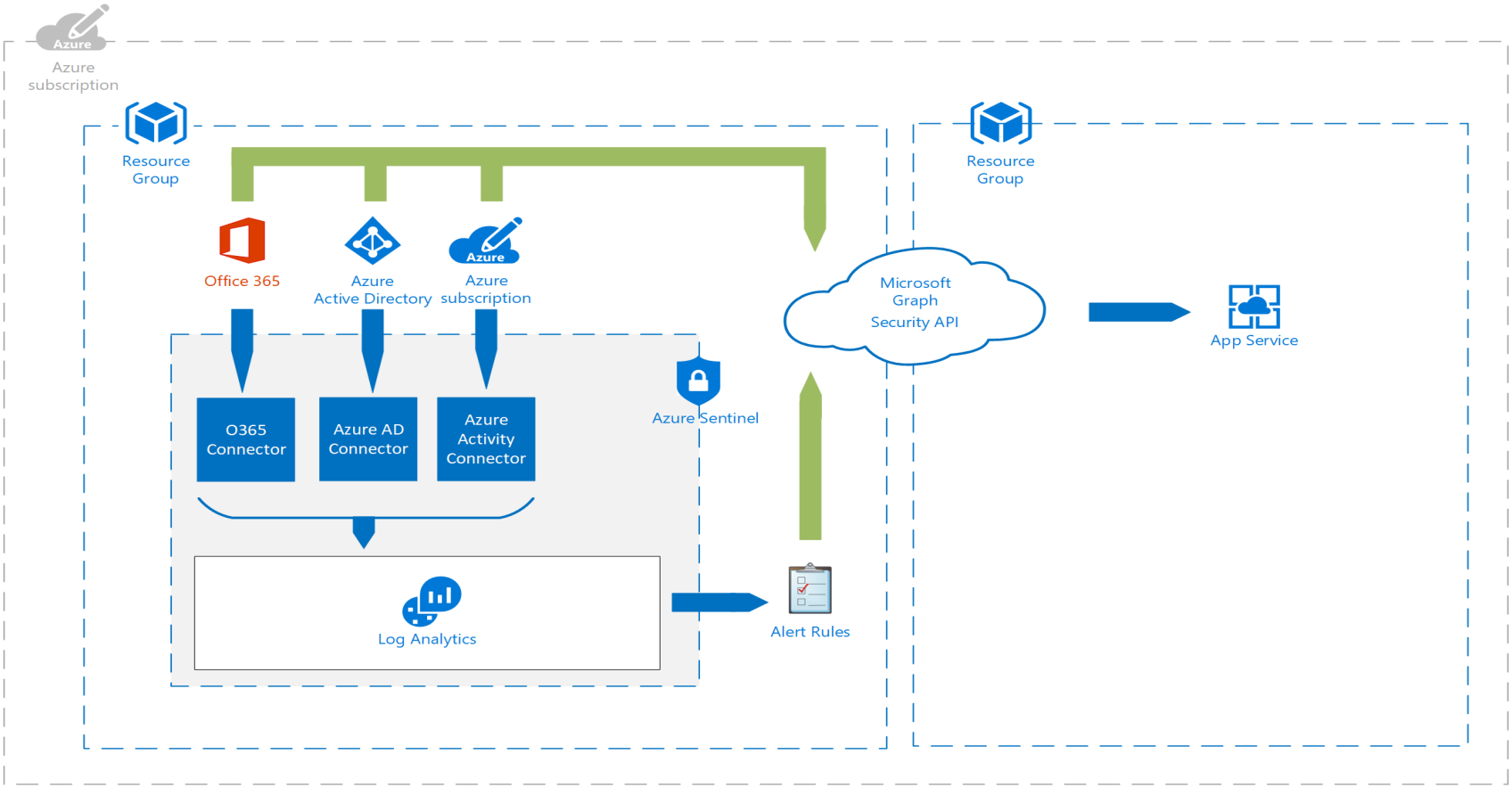
Processes


Alert classification & triage
Prioritization & Analysis
Remediation & Recovery
Assessment & Audit
Security Analyst Tier 1
Security Analyst Tier 2
Security Analyst Tier 2
Security Expert

Automate processes



Architecture

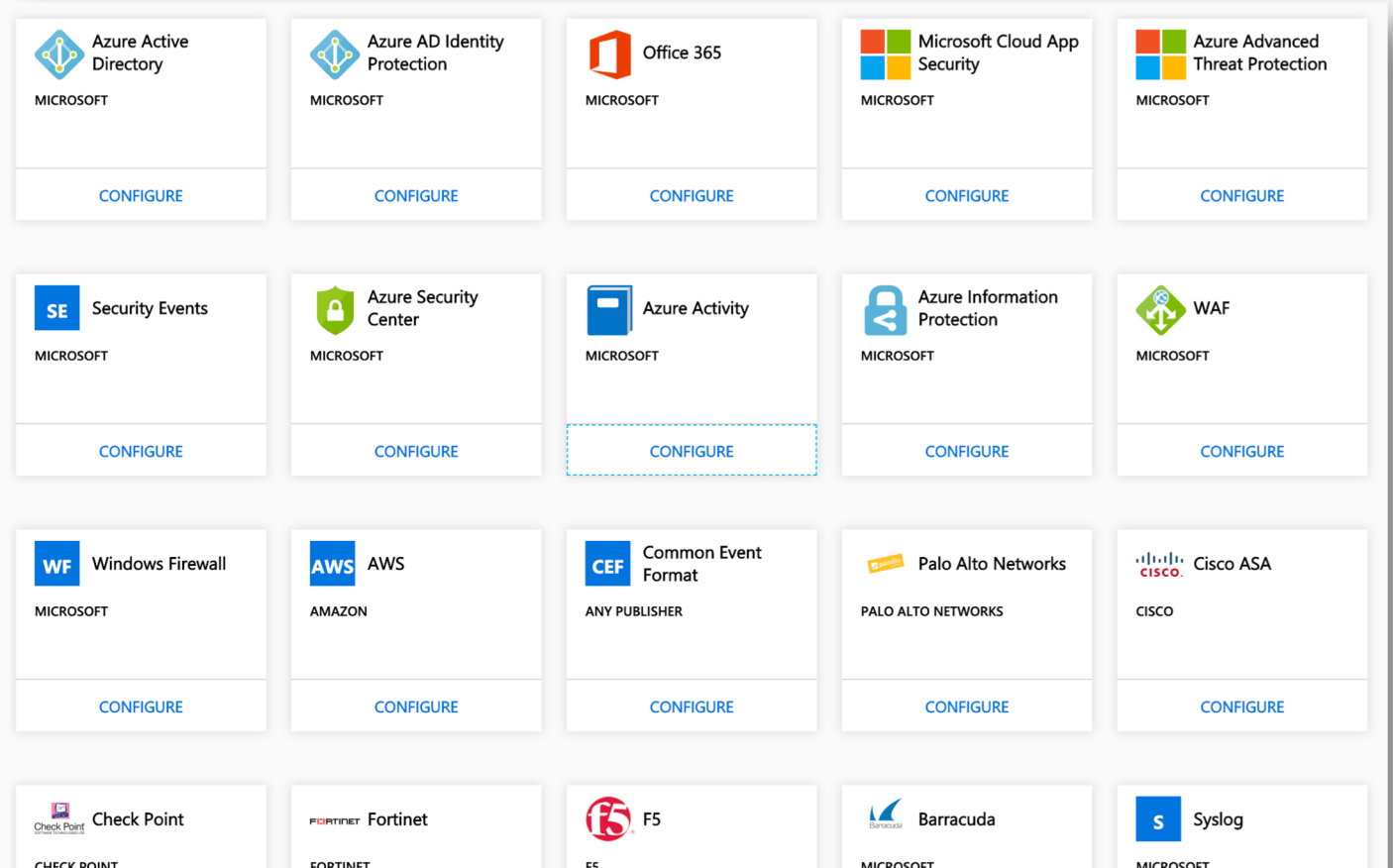


Azure Sentinel

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

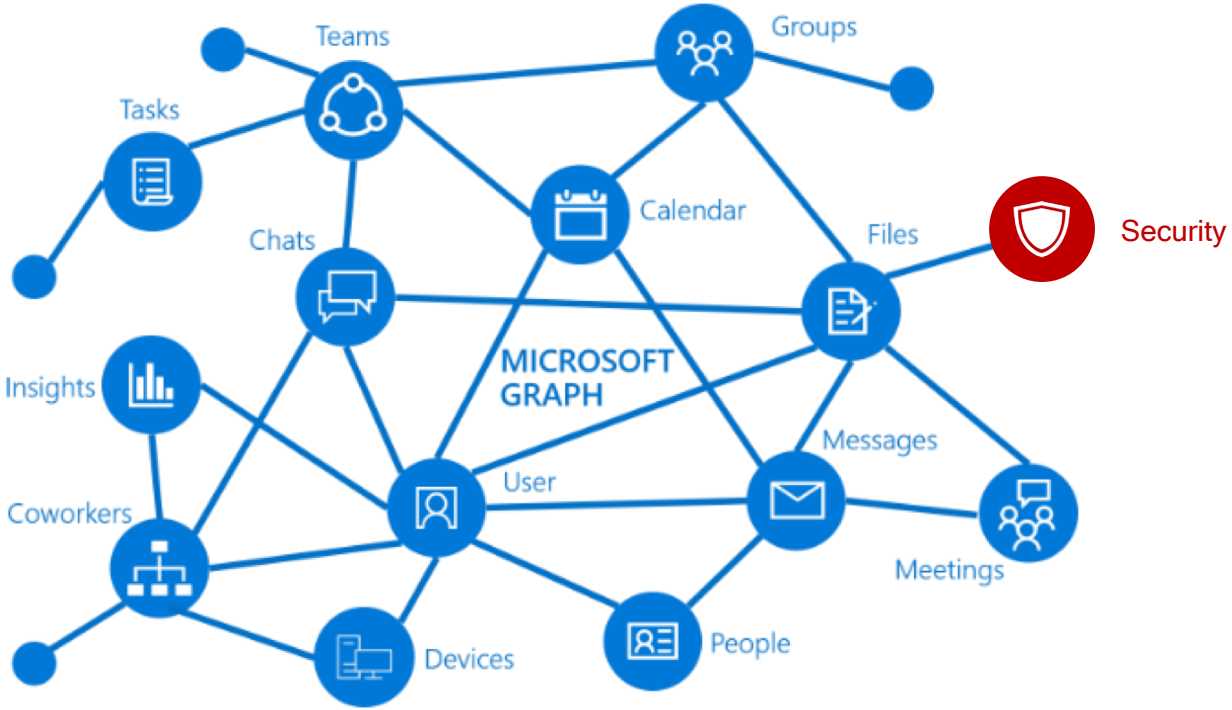
- Published in the Microsoft Graph Security API
- Published in Azure Monitor
- Realtime automation

DEMO

Exploring Azure Sentinel

- Connecting Sources
- Configuring Alerts
- Exploring Azure Sentinel Cases

Microsoft Graph Security API



Graph Security vs. Sentinel

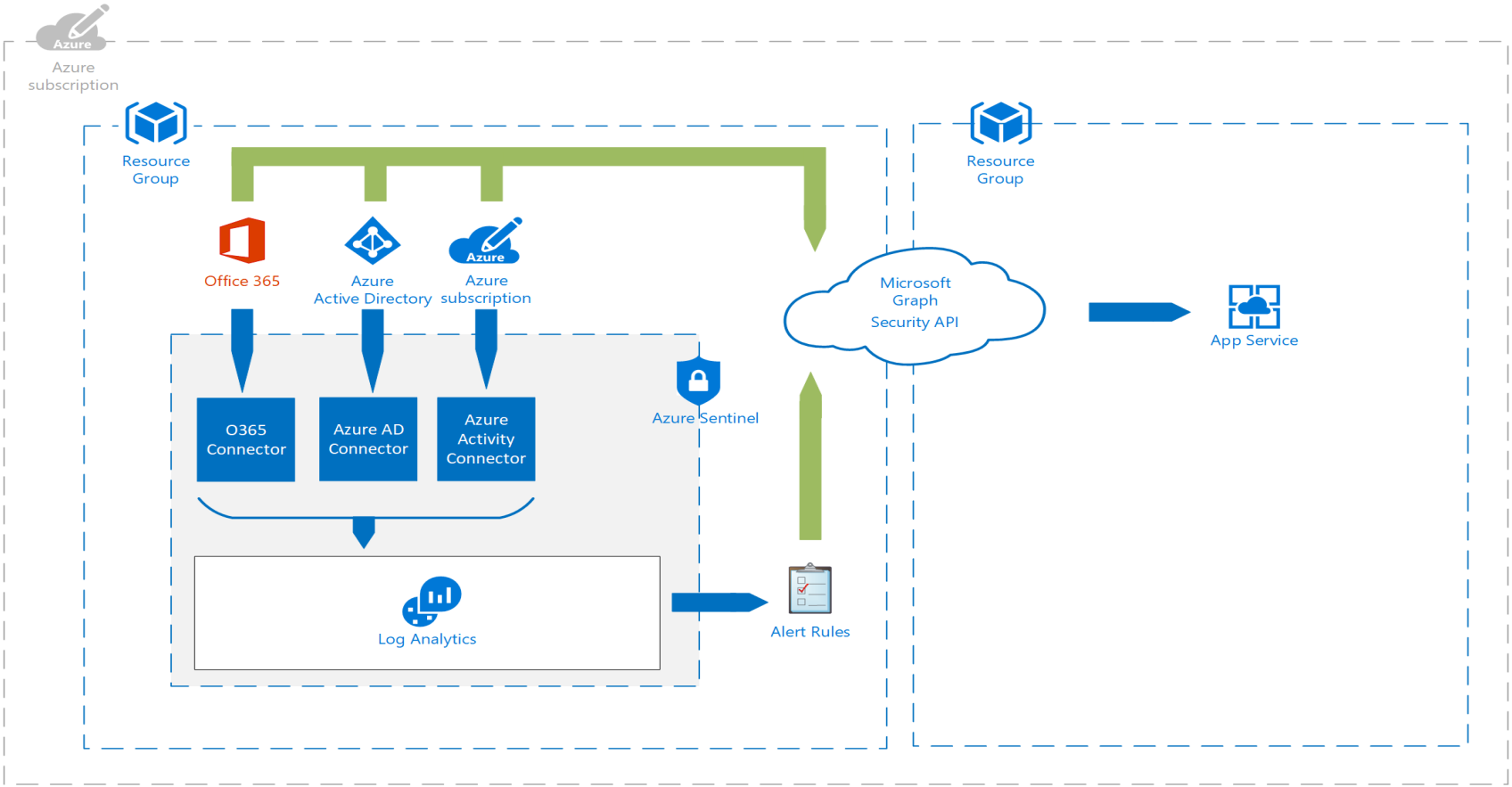
Azure Sentinel is a SIEM solution

- 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

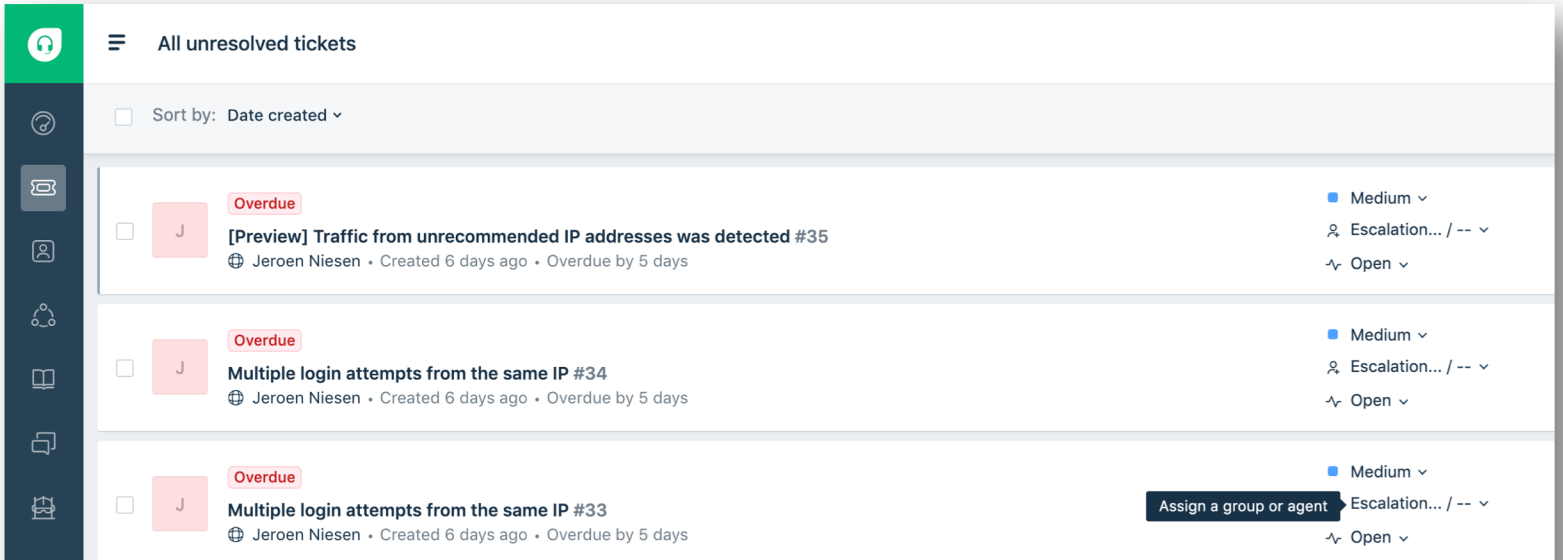
DEMO

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)

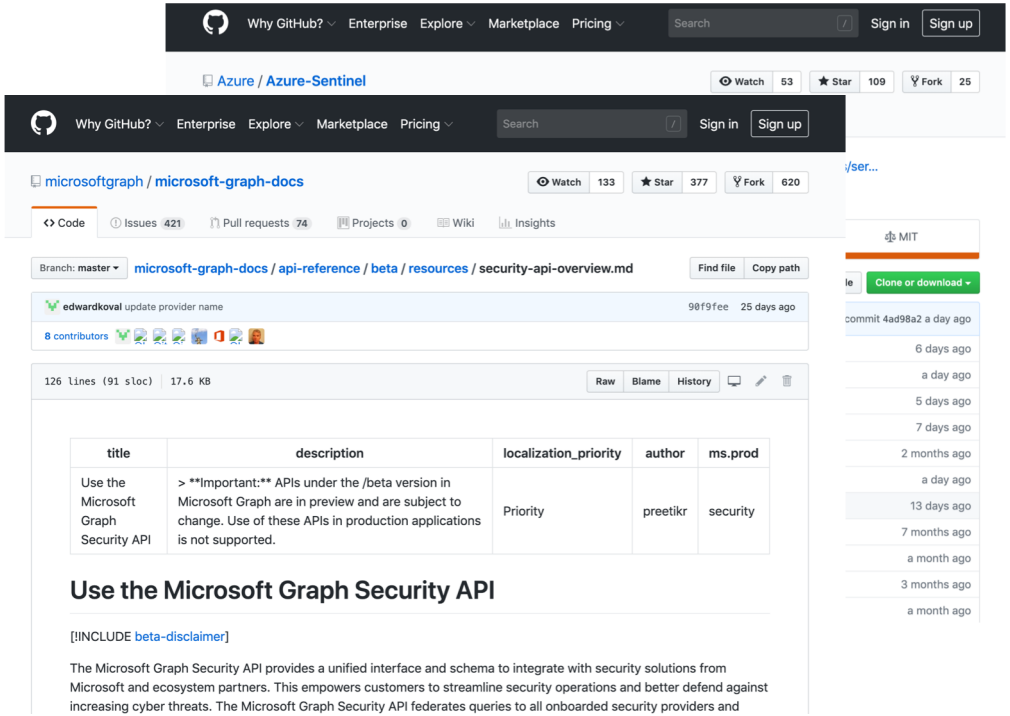


DEMO

Integrating with the Microsoft Graph Security API

Interesting documentation

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



Thanks!