Azure Sentinel

The modern SIEM system

Hannes Lagler-Gruener

Microsoft Most Valuable Professional

https://cloudblogger.at

@HannesLagler

https://bit.ly/3caxuIt

Azure Meetup BONN

Azure Meetup THÜRINGEN

@AzureBonn #AzureBonn

Agenda (advanced)

- Wie starte ich mich Azure Sentinel (advanced)
  - Daten sammeln (Advanced Connector)
  - Visuelle Darstellung (Custom Workbooks)
  - Analytics und Hunting rules (Custom Rules bauen)
  - Sentinel Automation
  - Sentinel Playbooks
- Azure Sentinel über IaC abbilden
- Aus der Praxis

Daten sammeln

Wie starte ich mit Azure Sentinel

Daten Sammeln

- Es gibt unterschiedliche Connector
  - Microsoft Produkte
  - Third Party Produkte
  - REST API Integration
  - Agent based Integration
  - Service to service integration

Wie starte ich mit Azure Sentinel

Daten Sammeln continue

- Microsoft Produkte
  - Real-time Integration
  - Kann Zusatzkosten verursachen (Lizenz)
  - Bsp:
    - Microsoft 365 Defender
    - Office 365
    - Azure Active Directory
    - Microsoft Defender for Identity
    - Microsoft Cloud App Security

Wie starte ich mit Azure Sentinel

Daten Sammeln continue

- Third Party Produkte
  - Integration über Agent, API oder Solutions
  - Bsp:
    - F5
    - Fortinet
    - CheckPoint
    - Ubiquity
    - ….

Wie starte ich mit Azure Sentinel

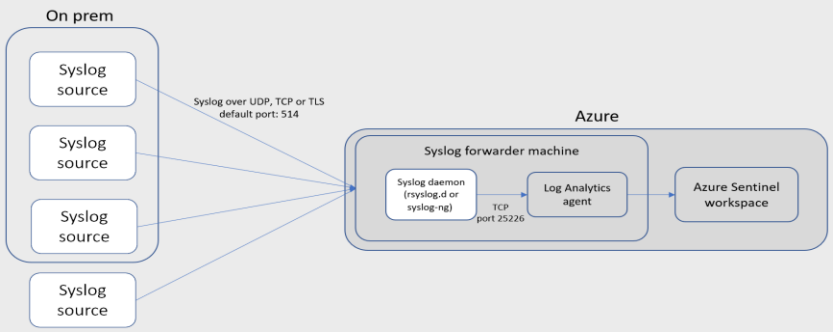
Daten Sammeln continue

- REST API Integration
  - Verwenden von externen service zur Analyse
  - Kann Zusatzkosten verursachen
  - Bsp:
    - Darktrace
    - Akamai Security Events
    - Aruba ClearPass

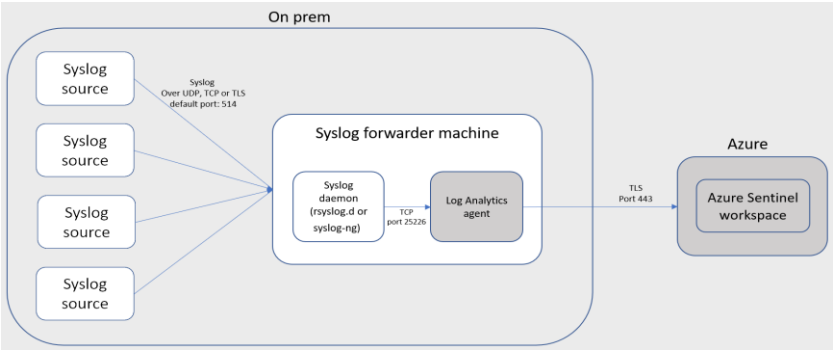
Wie starte ich mit Azure Sentinel

Daten Sammeln continue

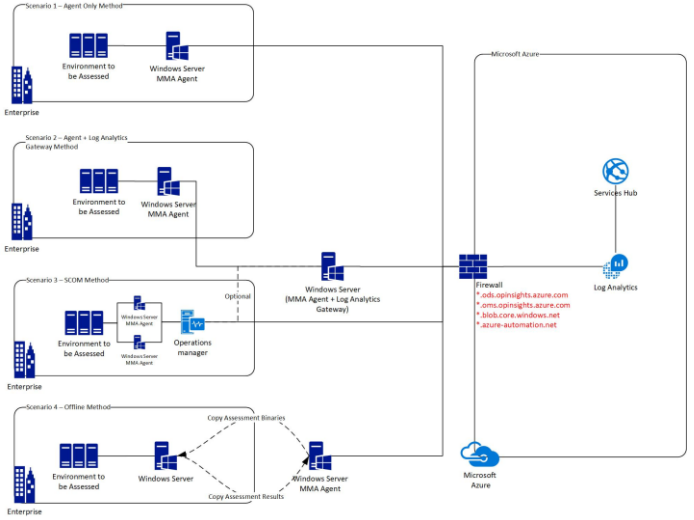
- Agent based Integration
  - Windows Events
  - Syslog Events
  - ….
- Es gibt unterschiedliche Collection Optionen
  - On-Prem
  - Azure
  - Direct
  - Gateway



Source: https://docs.microsoft.com



Source: https://docs.microsoft.com



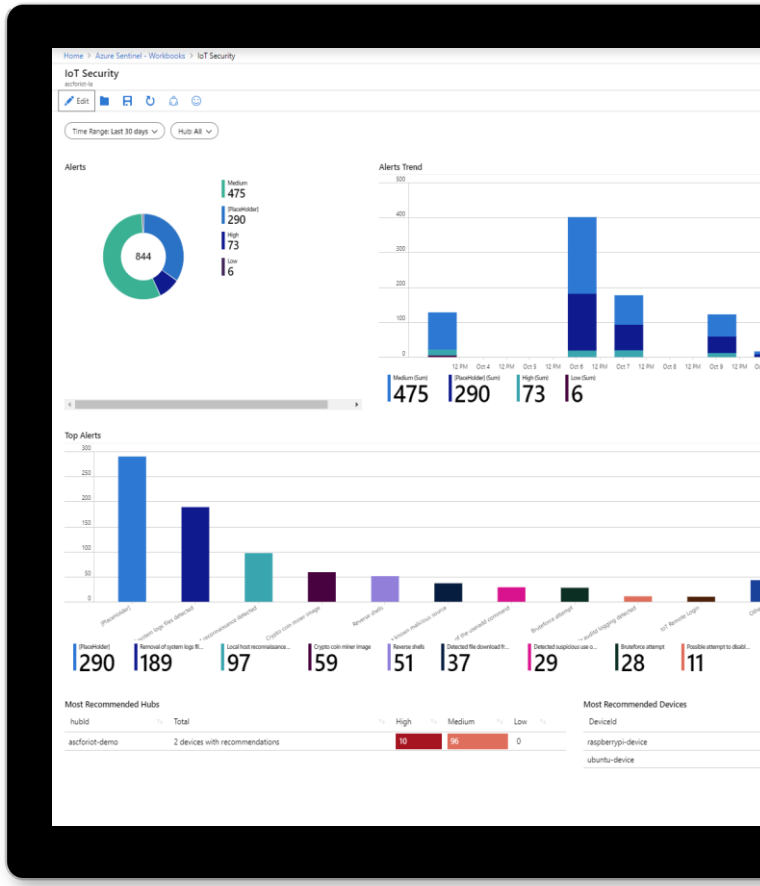
Source: https://docs.microsoft.com

Visuelle Darstellung

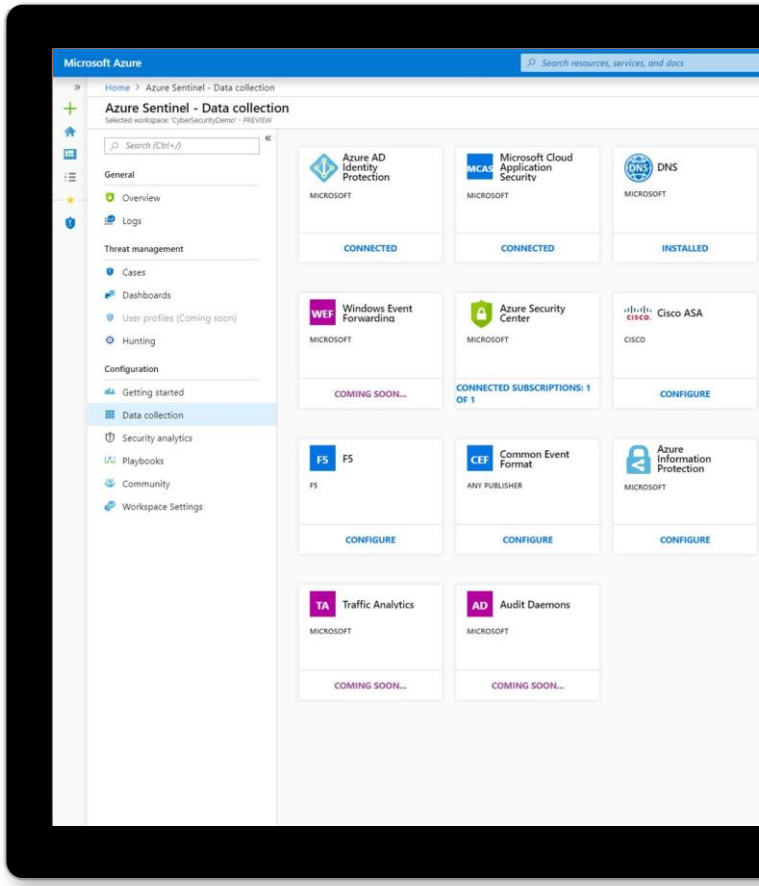
Wie starte ich mit Azure Sentinel

Visibilität schaffen

- Workbooks werden auch für andere Systeme verwendet
- Ich kann bestehende Workbooks abändern oder komplett neue bauen
- Ich kann auf andere Sourcen zugreifen und diese auswerten (bsp. Azure Security Center)
- Ich kann die Informationen von Workbooks auch auf Dashboards pinnen



DEMO



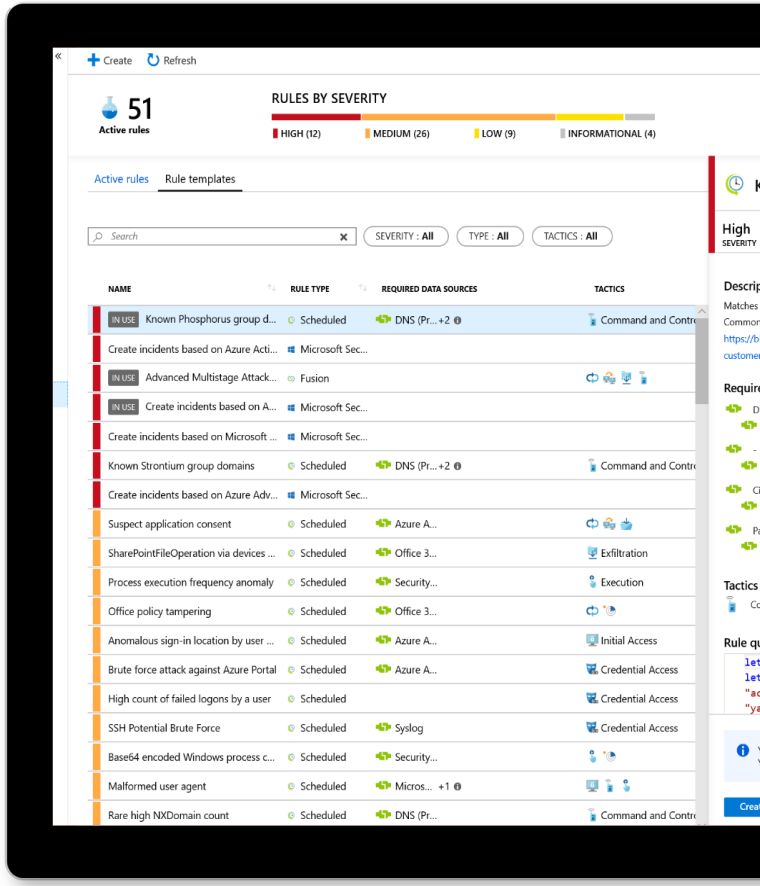
- Übersicht zu Azure Sentinel
  - Advanced Connector
  - Custom Workbooks

Analytics und Hunting rules

Wie starte ich mit Azure Sentinel

Analytics rules

- Erstellen von Custom Rules über KQL Query
  - Definition von Tactics
  - Einstellen der Severity
  - Entity Mapping, ein wichtiges Tool für die Analyse und für SOAR!
- Es gibt einige preview features wie
  - Alert enrichment
    - Trigger an alert for each event
  - Incident settings
    - Alert Grouping

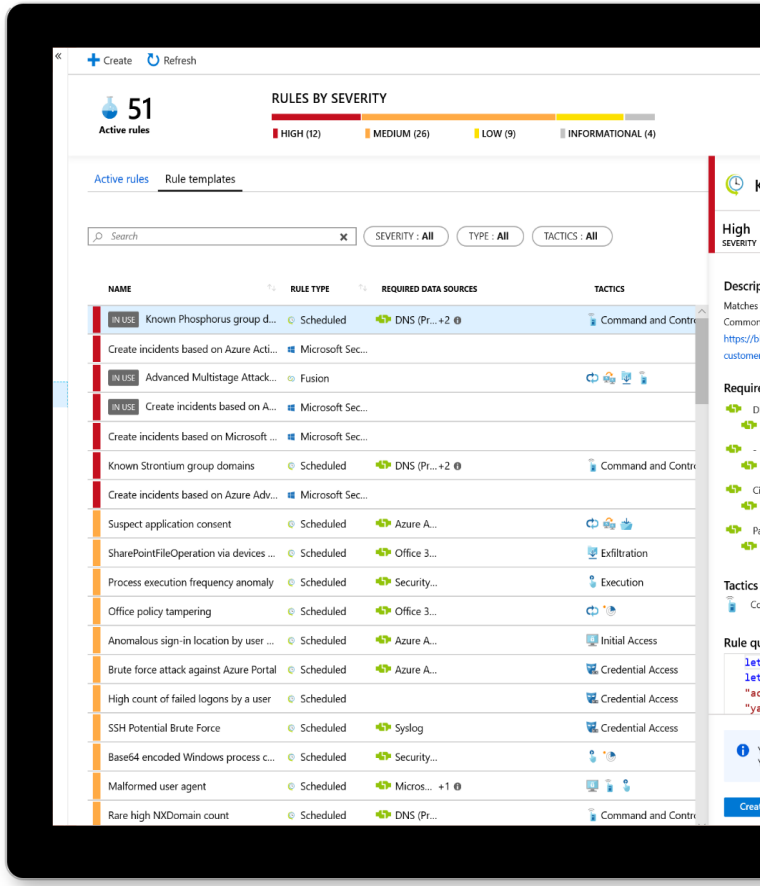


Wie starte ich mit Azure Sentinel

Analytics rules continue

- KQL schreiben
  - In Azure LogAnalytics
  - Gewisse Ähnlichkeiten zu SQL
  - Unheimlich Mächtig
  - Sehr gute Dokumentation (URL)
  - Sehr schnelle Infrastrukture
  - Export und Analyse in Data Explorer

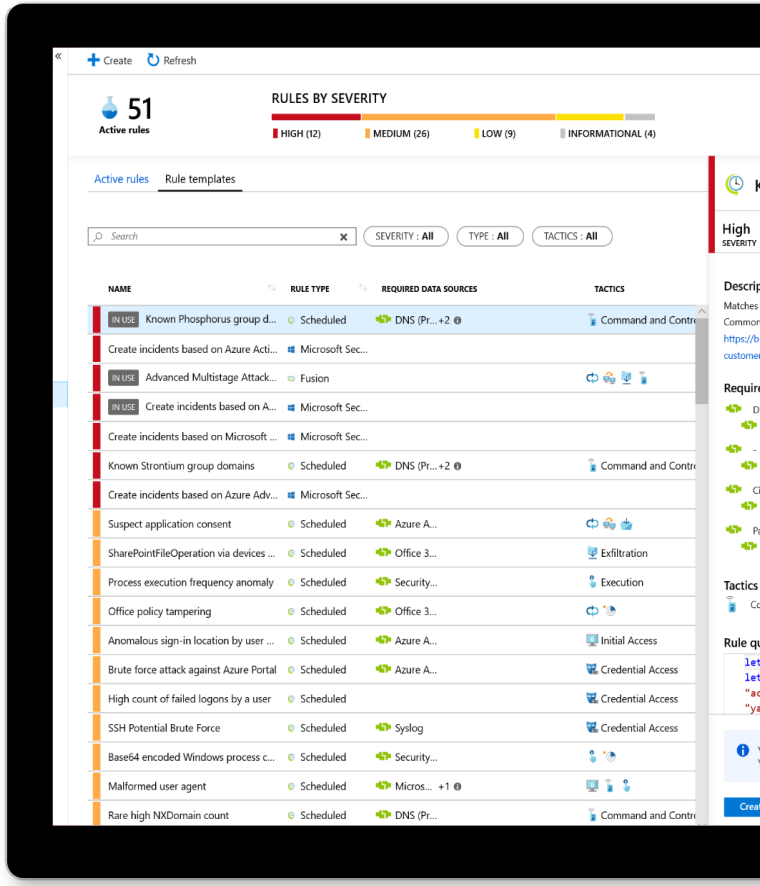
```
let emaccounts= GetWatchlist('EmergencyAccounts') | project ID;
SigninLogs
| project UserId, IPAddress, Location, SourceSystem, TimeGenerated, UserPrincipalName
| where UserId in (emaccounts)
| extend IPCustomEntity = IPAddress
| extend HostCustomEntity = SourceSystem
| extend URLCustomEntity = Location
| extend AccountCustomEntity = UserPrincipalName
```



Wie starte ich mit Azure Sentinel

Hunting rules

- Ich sollte nicht nur auf den Thread warten sondern Pro aktive tätig werden
  - Es gibt mehr als 100 build-in rules
  - Erstelle deine eigenen rules ebenso über KQL queries
- Während eines Incidents die weiteren Auswirkungen im Blick haben
  - Schreibe deine Livestream über KQL
  - Füge Build-in Hunting rules zum Livestream hinzu

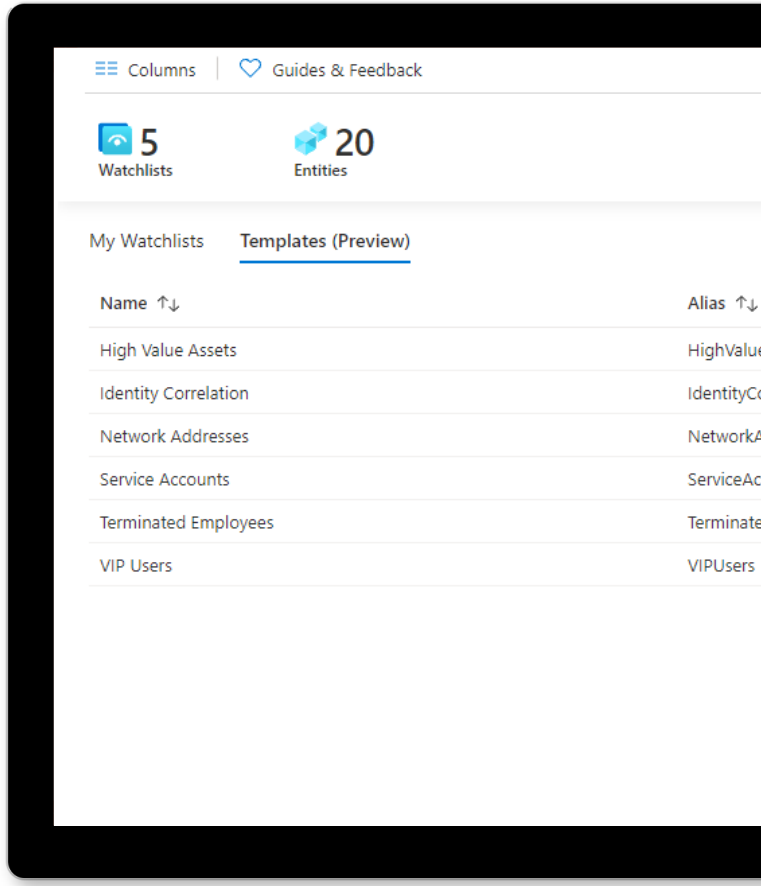


Wie starte ich mit Azure Sentinel

Analytics/Hunting rules continue

Neues und sehr wichtiges feature!

- Azure Sentinel **Watchlist**
  - Lagere deine Informationen von der KQL Querie aus in eine Watchlist
  - Einfaches Handling von Listen
- Import über CSV Files
- Import von Templates (preview)



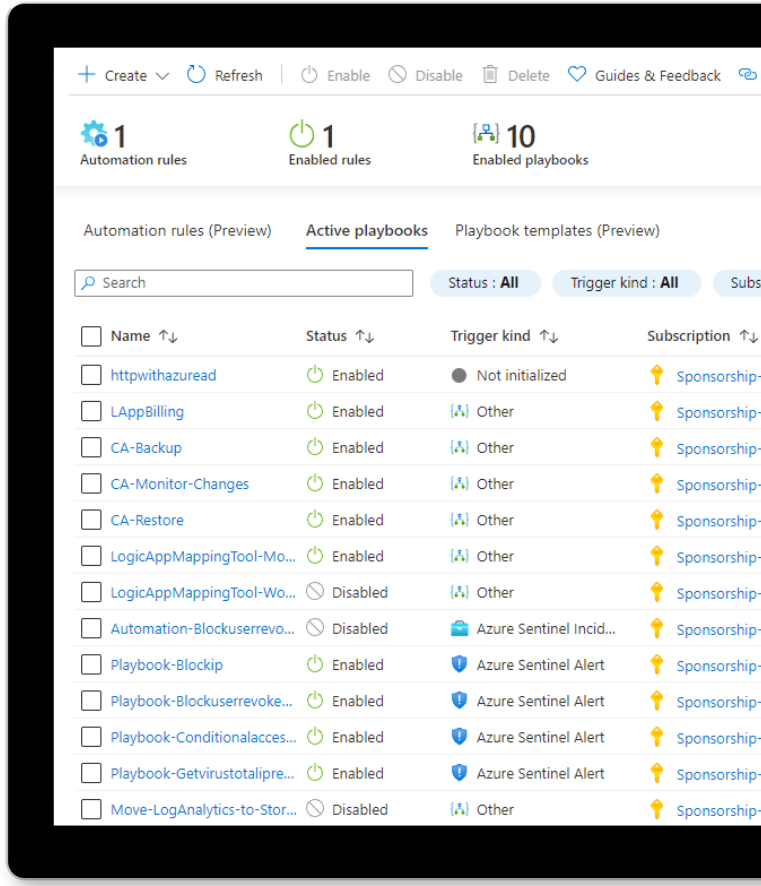
Sentinel Automation und Sentinel Playbooks

Wie starte ich mit Azure Sentinel

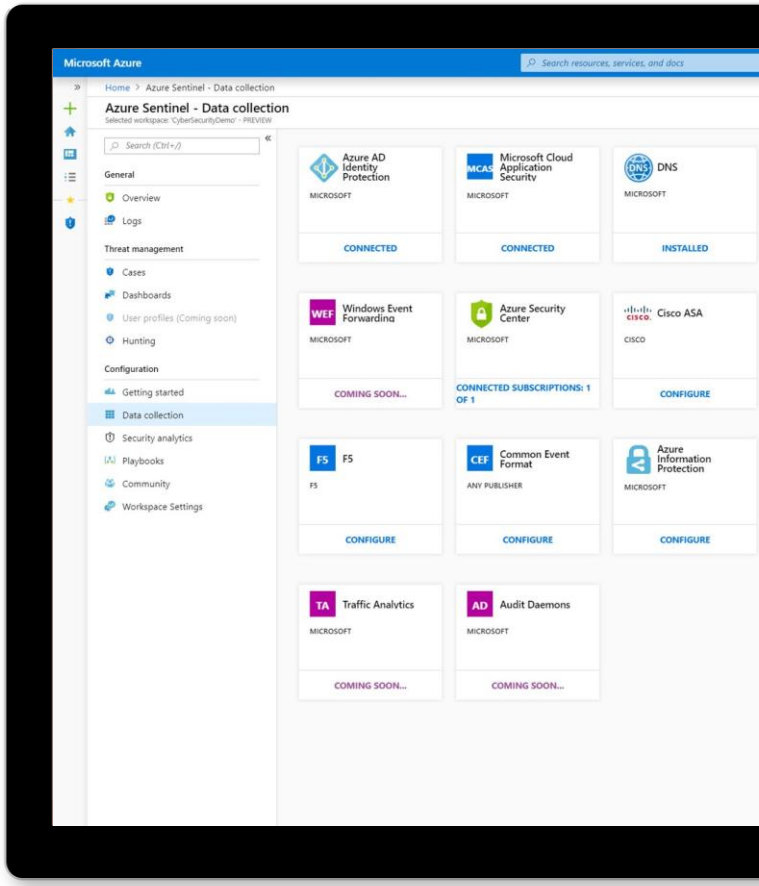
Automation und Playbooks

Basieren auf Azure LogicApps

- Sehr Mächtiges Tool mit unzähligen Connectoren (Microsoft und Thrid Party)
- Trigger based automation
  - Alert Trigger
  - Incident Trigger (preview)
- Basierend auf
  - Playbooks
  - Automation rules (Preview)
- Es gibt mittlerweile auch Playbook templates



DEMO



- Übersicht zu Azure Sentinel
  - Hunting und Analytics Rules
  - Automation und Playbooks inkl. Samples

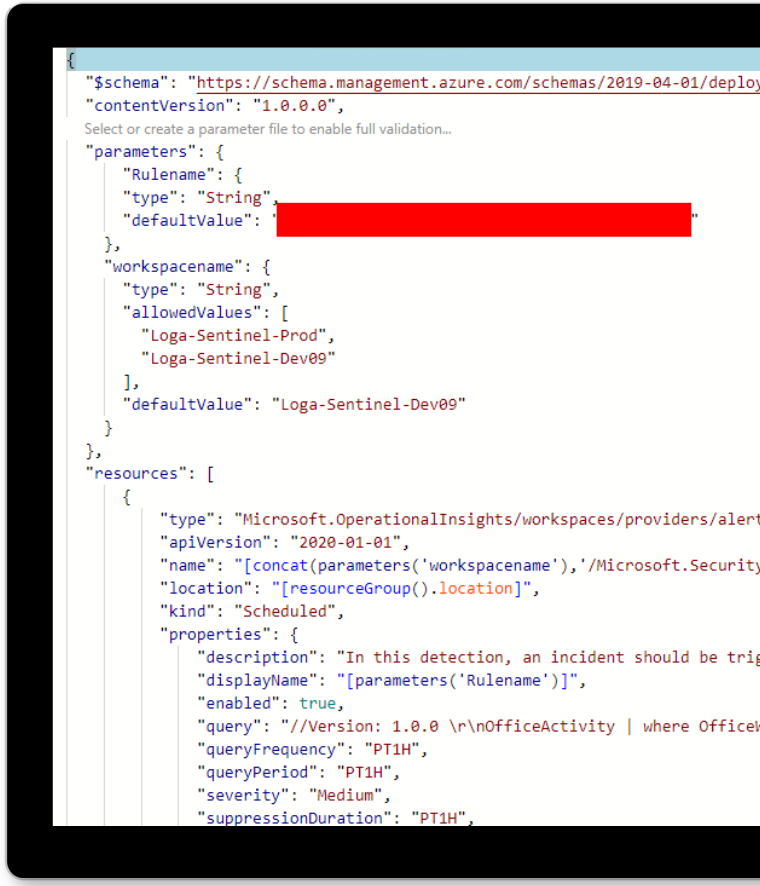
Azure Sentinel über IaC abbilden

Azure Sentinel über IaC abbilden

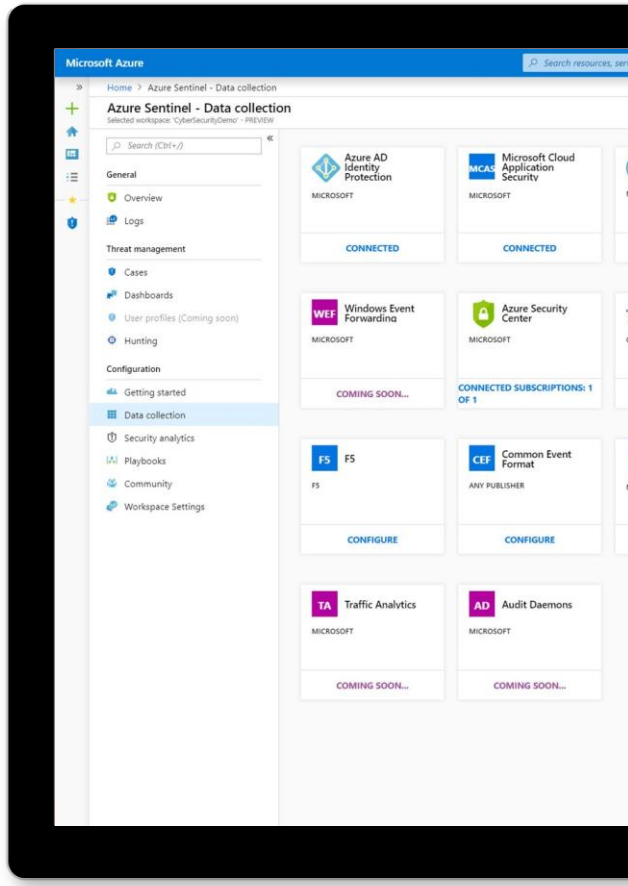
Stand heute sind folgende Abbildungen möglich

- Analytics Rules: API, PowerShell, ARM
- Hunting Rules: API, PowerShell, ARM
- Playbooks: ARM
- Workbooks: ARM
- Connectors: API

- Es gibt ein eigenes Azure Sentinel Module (AzSentinel)



Aus der Praxis (DEMO)



- Aufbau einer Sentinel Umgebung (Strukturierung in RGs)
- Aufbau einer RBAC Matrix (Simple)
  - Simple über IAM Permissions
  - Advanced Berechtigungen auf LogA Table Ebene
- Longterm Data Retention

Azure Sentinel

The modern SIEM system (overview)

Hannes Lagler-Gruener

https://cloudblogger.at

@HannesLagler

https://bit.ly/3caxult

Vielen Dank

Q&A

@AzureBonn #AzureBonn