Azure Sentinel

The modern SIEM system (overview)

Hannes Lagler-Gruener

https://cloudblogger.at

@HannesLagler

https://bit.ly/3caxuIt

Azure Meetup BONN

Azure Meetup THÜRINGEN

@AzureBonn #AzureBonn

Agenda (overview)

- Warum Azure Sentinel
- Wie starte ich mich Azure Sentinel (Basis)
  - Daten sammeln (Basis Connector)
  - Visuelle Darstellung (Default Workbooks)
  - Analytics und Hunting Rules (Vordefinierte Rules)
  - Incident Handling
- Was kostet Azure Sentinel
- Die Community hinter Azure Sentinel

Warum Azure Sentinel

Warum Azure Sentinel

Anfangsdiskussionen für ein SIEM System:

- Wo liegen meine Services und können diese Angebunden werden (Disconnected Services)?
- Wie große muss ich mein SIEM System auslegen?
- Wie hoch ist das vorab Investment
- Wie bringe ich die notwendigen Informationen von meinen Cloud Systemen in meine Umgebung
- Wie kann ich in weiterer Folge eine Automatisierung durchführen?

Warum Azure Sentinel

Wie kann Azure Sentinel die Anforderungen Lösen?

- Wo liegen meine Services und können diese Angebunden werden (Disconnected Services)?
- Wie große muss ich mein SIEM System auslegen?
- Wie hoch ist das vorab Investment

Warum Azure Sentinel

Disconnected Services

Security
Operations Team

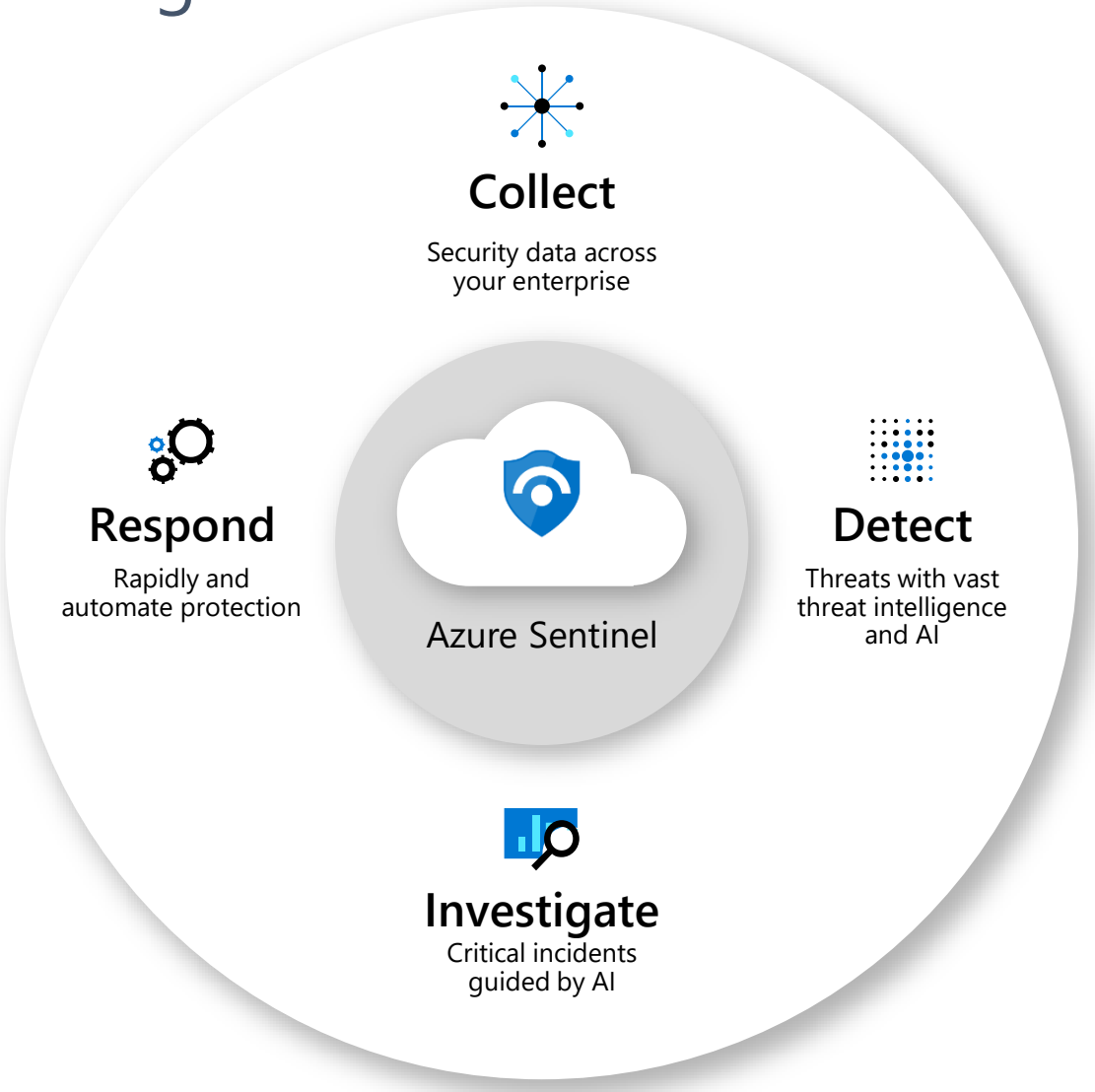
+

Cloud + Artificial Intelligence

Warum Azure Sentinel

Right-sizing

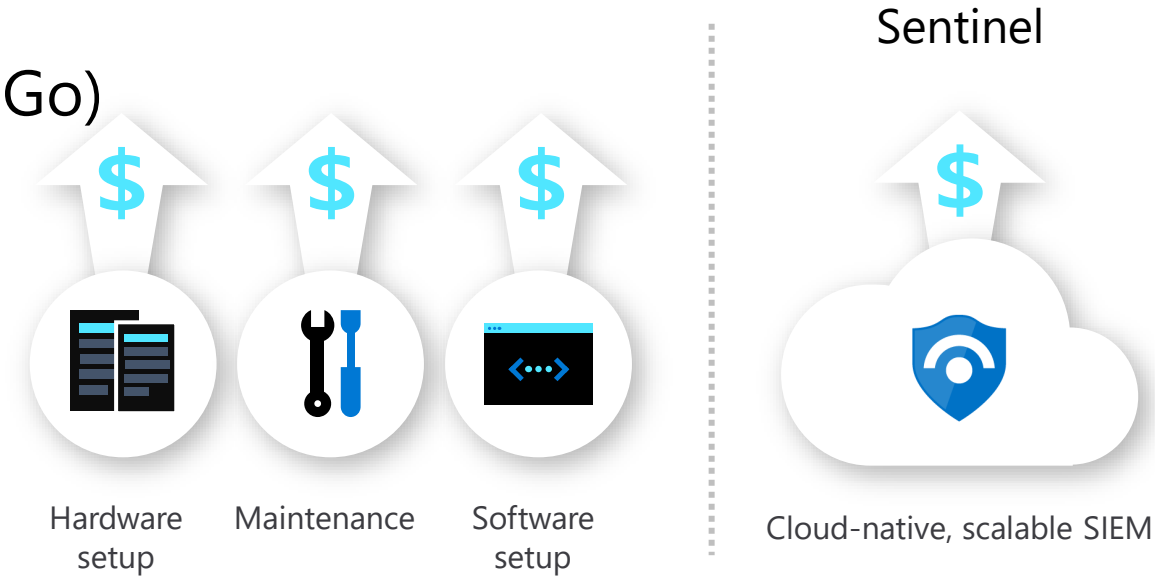
- „Grenzenlose“ Cloudgeschwindigkeit
- Skaliert automatisch



Warum Azure Sentinel

Upfront-Investment

- Keine Infrastruktur kosten (Pay-as-you-Go)
- Kapazitäts-Reservierung
- Flexibles Model



48% reduction in costs compared to legacy SIEMs[1]

Warum Azure Sentinel

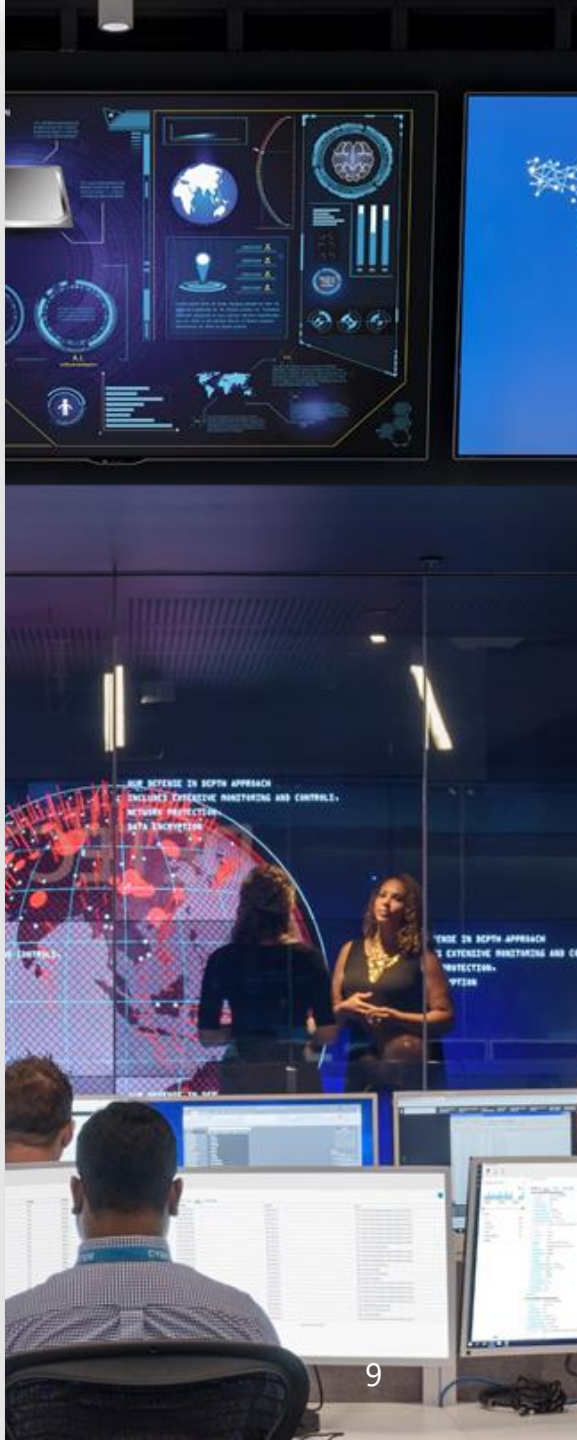
Weitere Aspekte für Sentinel

- Einfache Integration von bestehenden Tools
- Schnellere thread protection with AI
- Keine Infrastruktur Setup oder Maintenance

Der Microsoft Sicherheitsvorteil

- $1B Investment in cybersecurity
- Mehr als 3500 Security experten weltweit
- Billionen unterschiedlicher Signale sorgt für eine unglaubliche AI

67% faster time to deployment
compared to legacy SIEMs[1]



Wie starte ich mit Azure Sentinel

Schritte für die Implementierung von Sentinel:

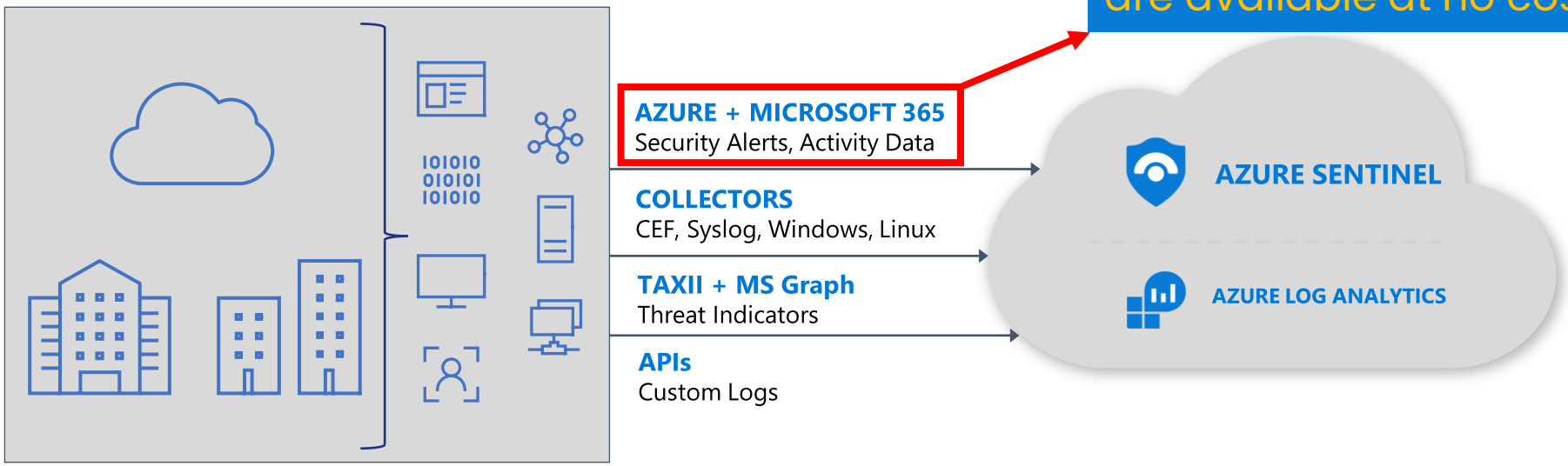
- UseCases entwerfen
  - Daten Sammeln
  - Visibilität schaffen
  - Analytics/Hunting Rules
  - Incident Handling

Daten sammeln

Wie starte ich mit Azure Sentinel

Daten Sammeln

Azure Activity Logs, Office 365 Activity Logs, Alerts from Microsoft Threat Protection are available at no cost.

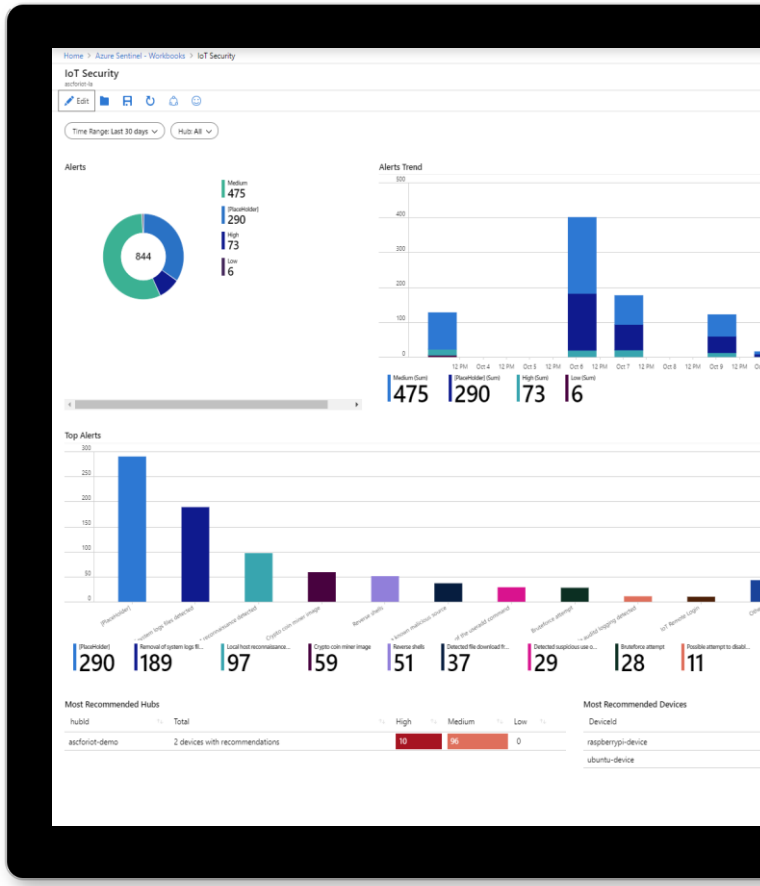


Visuelle Darstellung

Wie starte ich mit Azure Sentinel

Visibilität schaffen

- Pre-defined Workbooks
- Custom Workbooks
- Unterschiedliche Visualisierung:
  - Text
  - Charts
  - Grids
  - …
- Unterschiedliche Data sources
  - Logs
  - Metric
  - ….

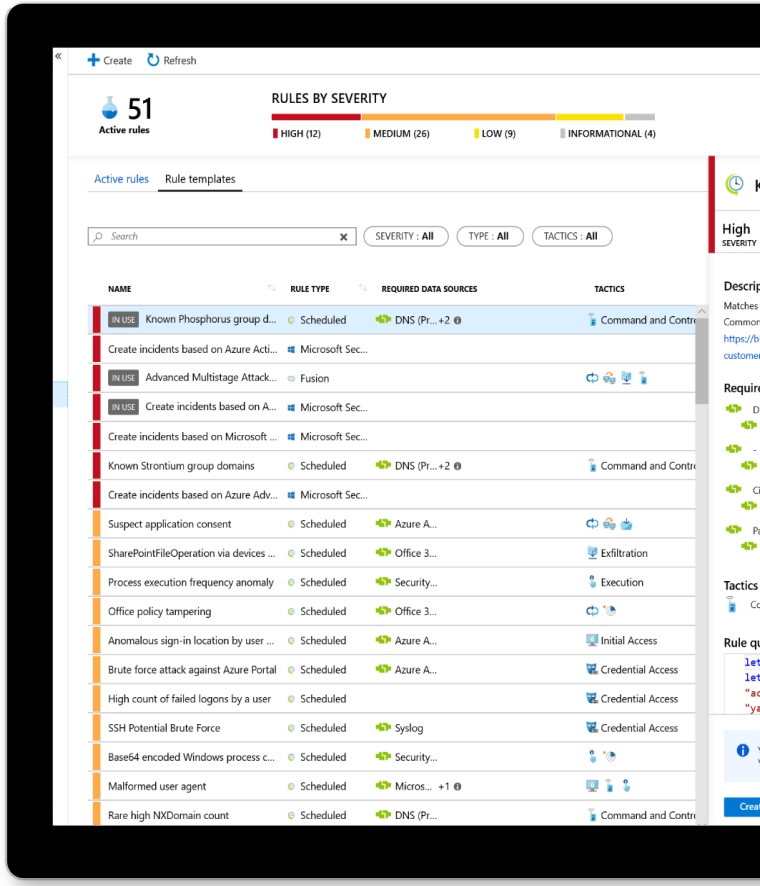


Analytics und Hunting Rules

Wie starte ich mit Azure Sentinel

Analytics rules

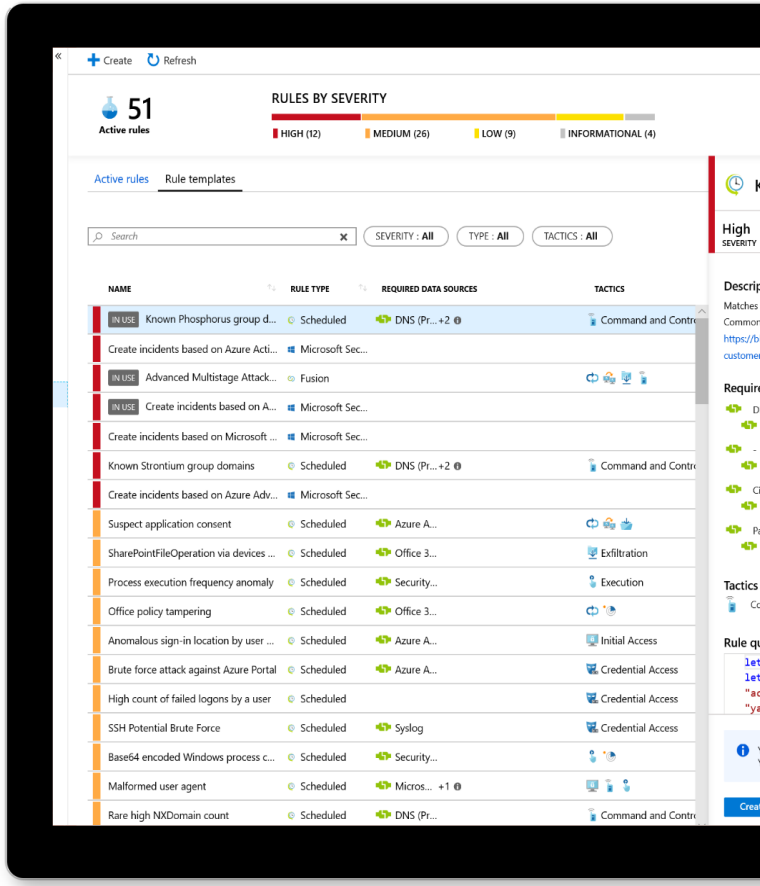
- Mehr als 100 built-in Rules
- Erstelle deine eigenen Rules auf KQL basis
- Export und Import Funktionalität
- Unterschiedliche Typen:
  - Microsoft Security (MCAS, MDI,…)
  - Fusion
  - Machinelearing
  - Scheduled



Wie starte ich mit Azure Sentinel

Hunting rules

- Mehr als 100 built-in Rules
- Erstelle deine eigenen Rules auf KQL basis
- Wann soll ich Hunting Rules verwenden?
  - Before an incident occurs
  - During a compromise (livestream)
  - After a compromise

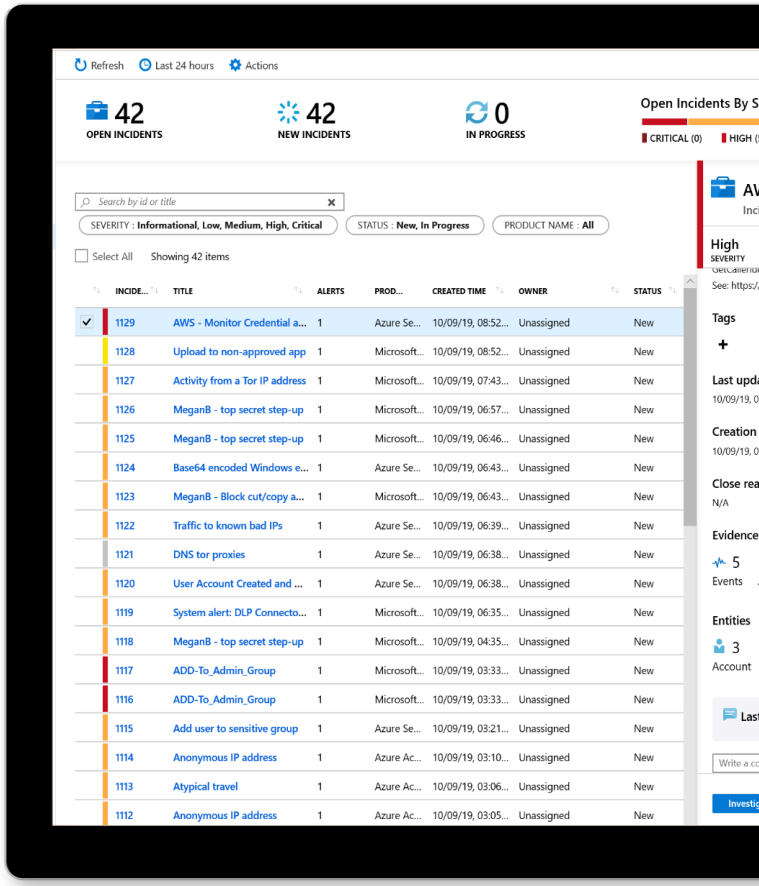


Incident Handling

Wie starte ich mit Azure Sentinel

Incident Handling

- Verwende inzident um Alerts, Events und Bookmarks zusammen zu fassen
- Inzident können Azure-AD User zugewiesen werden
- Ich kann jederzeit den Status und die Priorität ändern
- Zur nach Vollziehbarkeit sind Tags und Kommentare möglich
- Inzident werden als ersten Schritt für SOAR

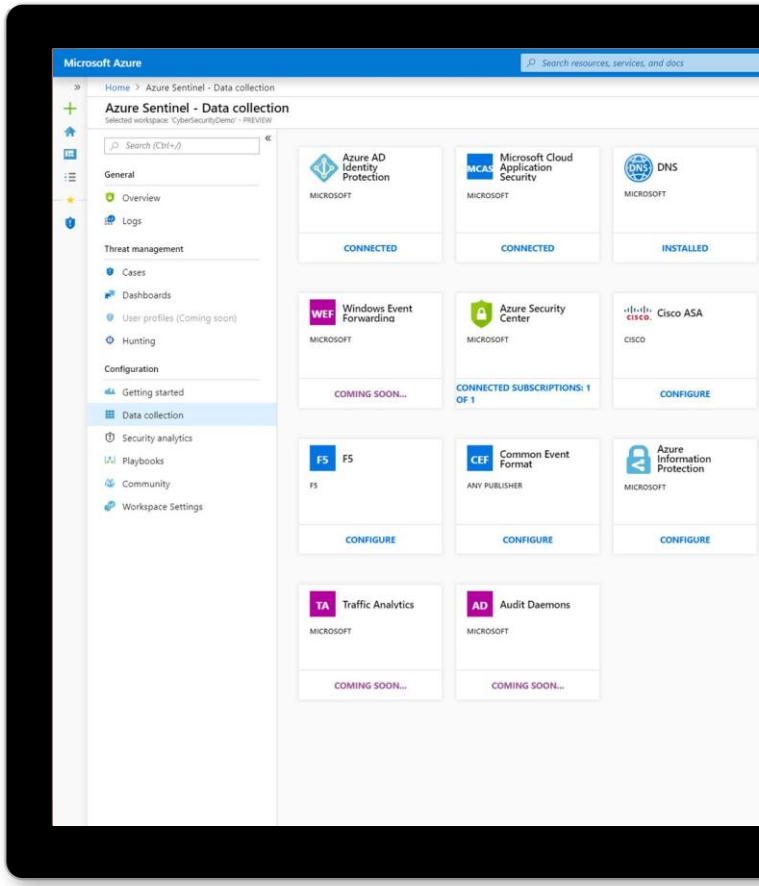


Wie starte ich mit Azure Sentinel

Incident Handling continue

- Definiere Incident classification weil:
  - „Improve the out of the box (OOTB) classification“
  - Typen:
    - **True Positive – suspicious activity** > Ja stimmt, war ein incident
    - **Benign Positive – suspicious but expected** > War geplant, möchte aber in Zukunft informiert werden!
    - **False Positive – incorrect alert logic** > Nicht richtig, falsche Logic
    - **False Positive – inaccurate data** >Nicht richtig, falsche Daten
    - **Undetermined** > Absoluter schwachsinn diese Rule ☺

DEMO



- Übersicht zu Azure Sentinel
  - Connector
  - Workbooks
  - Rules

Was kostet Azure Sentinel

Was kostet Azure Sentinel

- KEINE Infrastruktur Kosten, **Pay-as-you-Go**
- Office 365 Daten sind gratis
- Azure AD Daten sind gratis

Was kostet Azure Sentinel

Detail

Azure Monitor – Log Analytics Ingestion

1	×	30	×	€2.52
Daily logs ingested (GB)		Days		Per GB/day

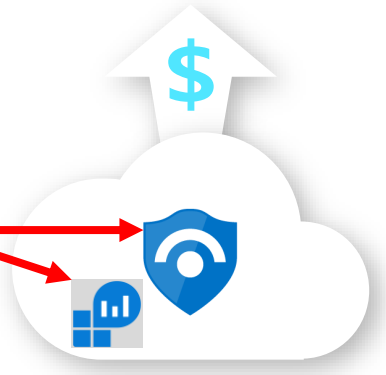
Azure Sentinel

1	×	30	×	€2.19
Daily logs ingested (GB)		Days		Per GB/day

Azure Monitor – Log Analytics Retention

30	×	3	×	€0.11
Total monthly ingestion in GB		Total retention (months)		Per GB

Sentinel



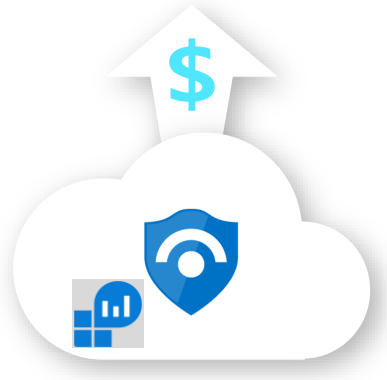
Cloud-native, scalable SIEM

Was kostet Azure Sentinel

Detail

Tier	Price	Effective Per GB Price[1]	Savings Over Pay-As-You-Go
100 GB per day	€110 per day	€1.10 per GB	50%
200 GB per day	€198 per day	€0.99 per GB	55%
300 GB per day	€286 per day	€0.96 per GB	57%
400 GB per day	€366 per day	€0.92 per GB	58%
500 GB per day	€439 per day	€0.88 per GB	60%
1,000 GB per day	€856 per day	€0.86 per GB	61%
2,000 GB per day	€1,623 per day	€0.82 per GB	63%
5,000 GB per day	€3,838 per day	€0.77 per GB	65%

Sentinel



Cloud-native, scalable SIEM

Was kostet Azure Sentinel (SOAR)

Detail continue

Logic App (PlayBooks)

Workflows

PLAN:

Consumption

The first 4,000 actions are free

0	×	1	×	€0.001	
Action Executions per day		Day		Per execution	

Data Retention

0 GB	×	€0.10		
		Per GB/month		

Connectors

0	×	1	×	€0.001	
Standard Connector Executions per day		Day		Per execution	
0	×	1	×	€0.001	
Enterprise Connector Executions per day		Day		Per execution	

Sentinel

Cloud-native, scalable SIEM

Was kostet Azure Sentinel (optional)

Detail continue

Databricks

Azure Databricks

REGION: West Europe

WORKLOAD: All-Purpose Compute

TIER: Premium

CATEGORY: All

INSTANCE SERIES: All

INSTANCE: D3 v2: 4 vCPUs, 14 GB RAM, 200 GB Temporary storage, 0.75 Databricks Unit(s), €

Savings Options

Save up to 72% on pay-as-you-go prices with 1-year or 3-year Reserved Virtual Machine Instances. Reserved Instances are great for applications with steady-state usage and applications that require reserved capacity. Learn more about Reserved VM Instances pricing.

- (•) Pay as you go
- ( ) 1 year reserved (~40% savings)
- ( ) 3 year reserved (~59% savings)

€167.45
Average per month
(€0.00 charged upfront)

= €167.45
Average per month
(€0.00 charged upfront)

1 Virtual machines × 730 Hours

DBU (Databricks Unit)

0.75 DBU × €0.464 Per DBU per hour × 730 Hours = €253.94

Sentinel

Cloud-native, scalable SIEM

Was kostet Azure Sentinel (optional)

Detail continue

Machine Learning Studio

Machine Learning Studio (classic)

REGION: West Europe

FEATURE: Workspace

TIER: Standard

ML studio workspace

0 Workspaces × €8.42 Per month

Studio usage

0 Experiment hours per seat × 0 Seats × €0.84 Per month

Sentinel

Cloud-native, scalable SIEM

Die Community hinter Azure Sentinel

@AzureBonn #AzureBonn

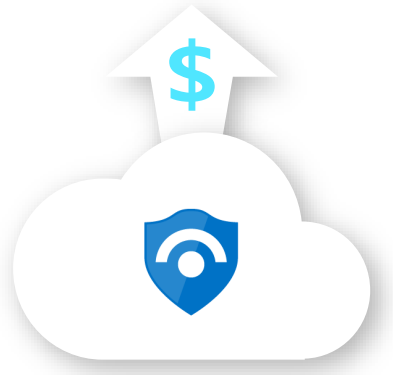
Die Community hinter Azure Sentinel

- Starke Azure Sentinel Community (Techcommunity)
- Viele Samples in GitHub
- Azure Sentinel Ninja Training

Zusammenfassung

- Cloud native SIEM System
- Kein Upfront Investment notwendig
- SIEM und AI hilft für eine bessere Thread Erkennung
- Sehr einfache Anbindung an Cloud Services
- Anbindung von Third Party Systemen einfach möglich

Sentinel



Cloud-native, scalable SIEM

Azure Sentinel

The modern SIEM system (overview)

Hannes Lagler-Gruener

https://cloudblogger.at

@HannesLagler

https://bit.ly/3caxult

Vielen Dank

Q&A

@AzureBonn #AzureBonn