

# Microsoft Azure Sentinel

SIEM/SOAR as a Service



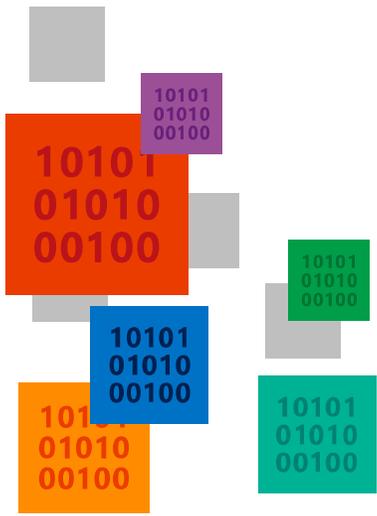
Jens Lorenz

Strategic Consultant, CISSP, CCSP

ExpertCircle GmbH

# Microsoft Security Assets

## DATA



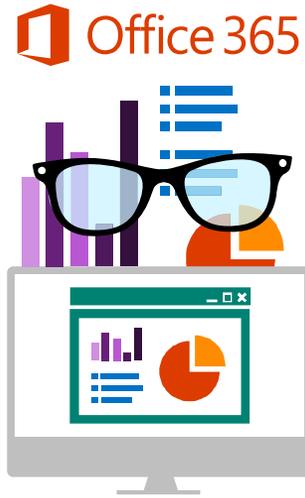
Information Protection  
Rights Management Services  
BYOK (Bring-Your-Own-Key)  
Customer Key

## CLOUD & DATACENTER



Azure Security Center  
Azure Monitor  
Log Analytics  
Azure Disk Encryption  
Azure Key Vault  
**Azure Sentinel**

## APPLICATIONS (SaaS)



Office 365 Data Loss Prevention  
Office 365 Cloud App Security  
Threat Intelligence  
Advanced Threat Protection  
Advanced eDiscovery  
Advanced Data Governance  
Compliance Manager  
Customer Lockbox  
Privileged Access Management

## ENDPOINTS (Devices)



Device Guard  
Credential Guard  
Microsoft Defender  
Microsoft Defender ATP  
Threat & Vulnerability Management  
Windows Hello (FIDO)  
Intune

## IDENTITY



Azure Active Directory  
Azure MFA  
Azure AD Identity Protection  
Privileged Identity Management  
Azure Conditional Access  
Advanced Threat Analytics/  
Advanced Threat Protection  
Access Reviews  
Microsoft Identity Manager  
Azure AD B2B / B2C

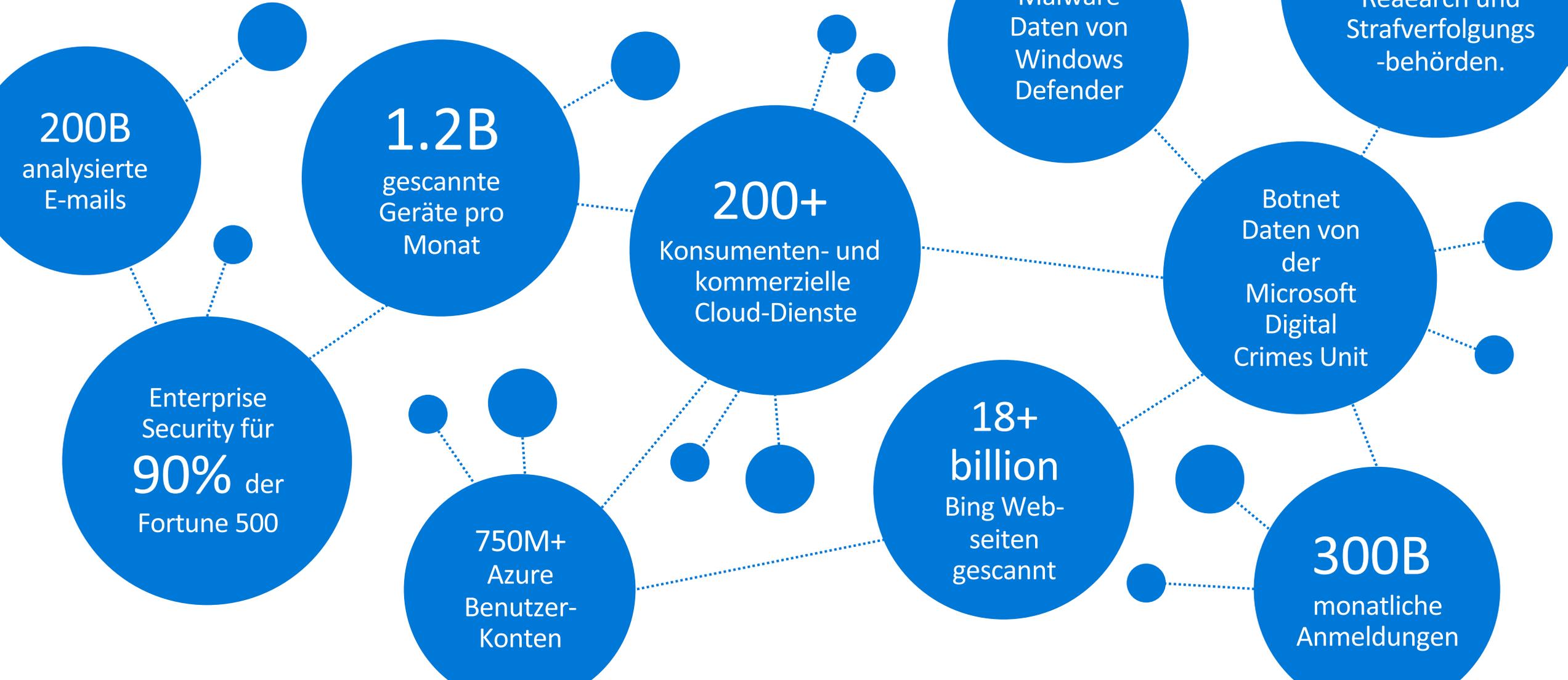
# Microsoft 365

# User-Centric IT



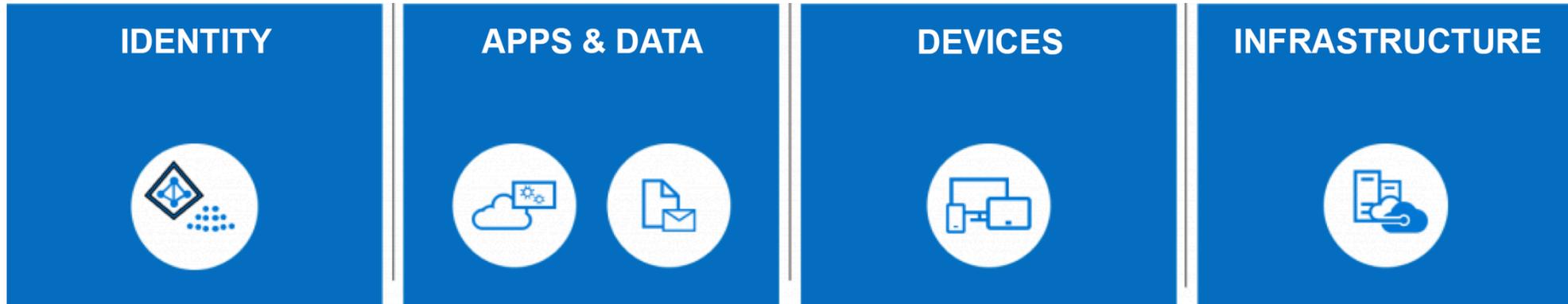
# Microsoft Intelligent Security Graph

Korrelation von Billionen von Signalen



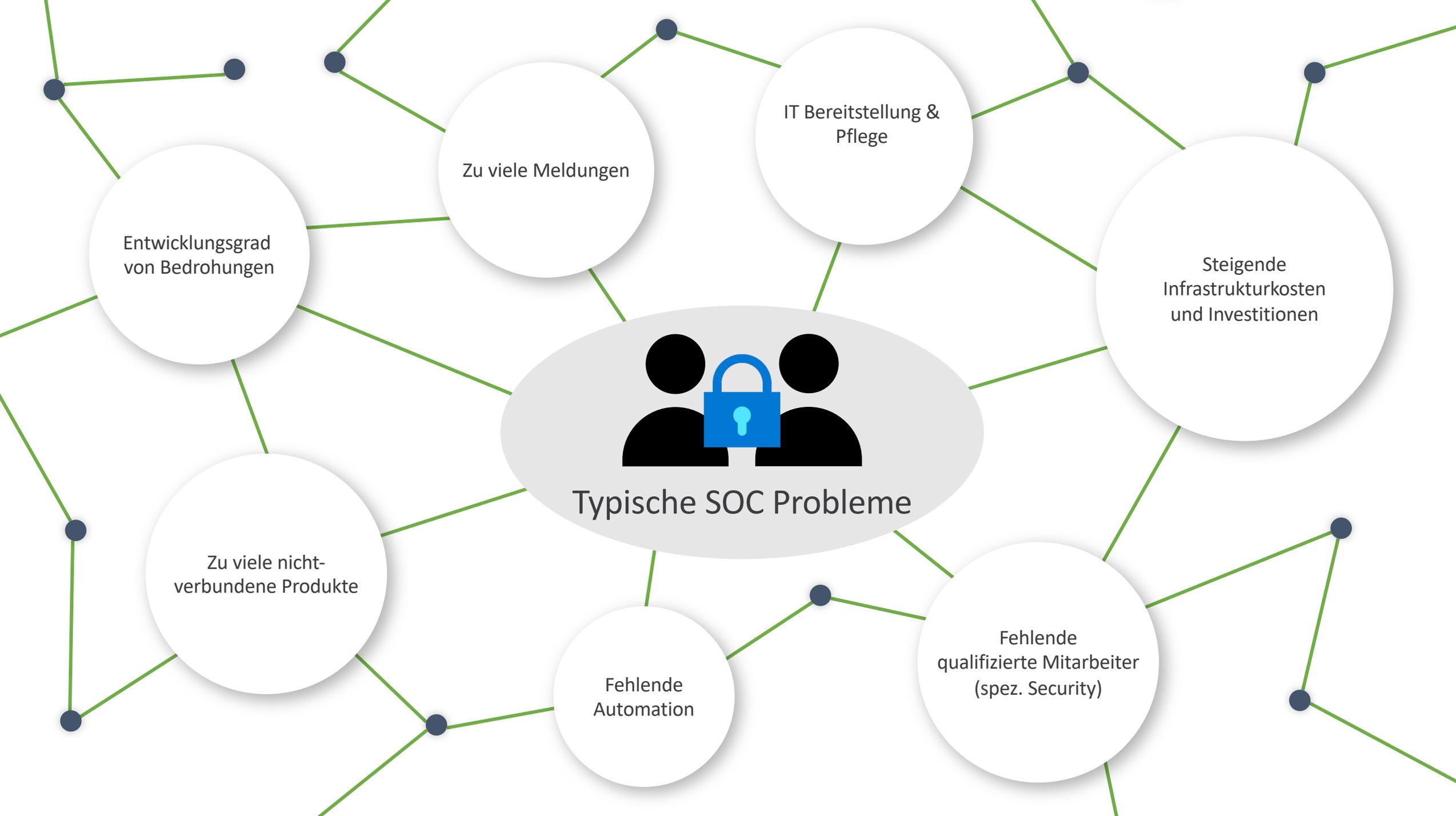
# Microsoft 365 – Threat Protection

## Plattformübergreifende Integration



# Erweiterung der digitalen Domäne





Entwicklungsgrad von Bedrohungen

Zu viele Meldungen

IT Bereitstellung & Pflege

Steigende Infrastrukturkosten und Investitionen

Zu viele nicht-verbundene Produkte

Fehlende Automation

Fehlende qualifizierte Mitarbeiter (spez. Security)



Security Operations  
Team



Cloud + Künstliche Intelligenz

# Microsoft Azure Sentinel

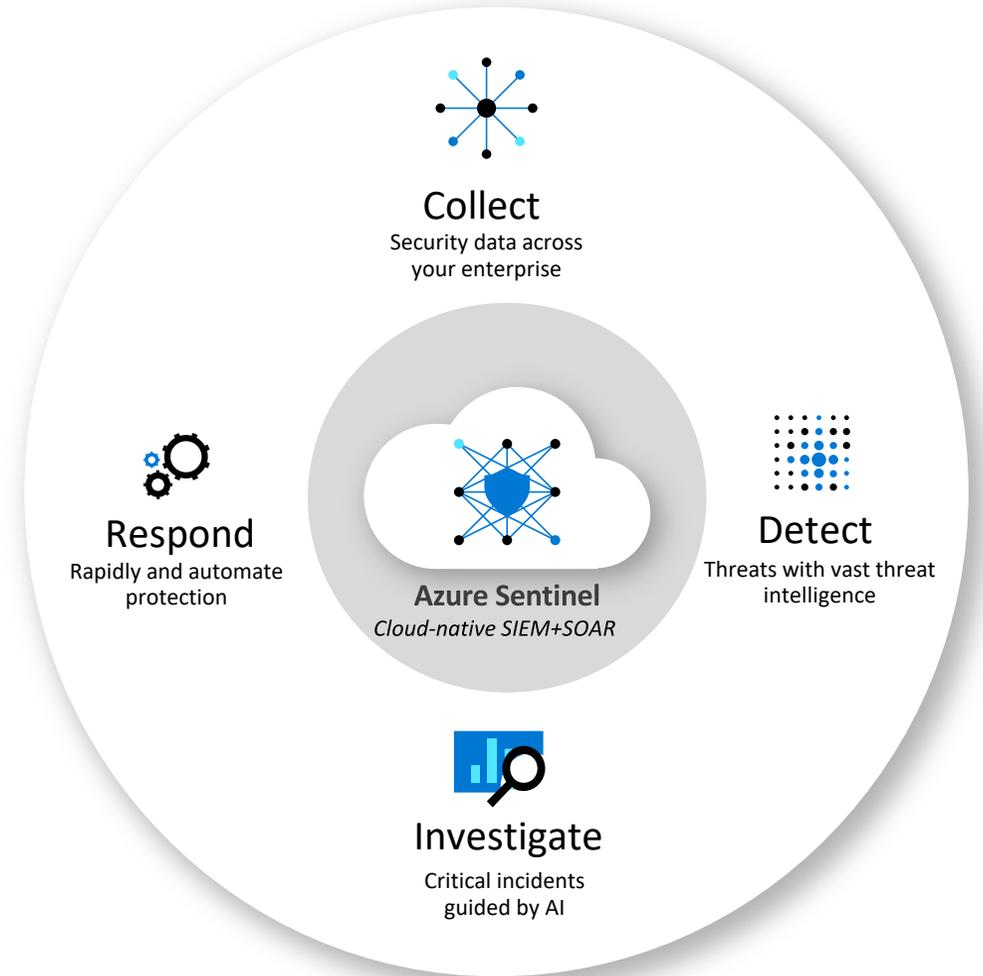
Cloud-natives SIEM für intelligente Security Analysen für die gesamte Organisation

Cloud-Speed und Skalierung ohne Limit

Kostenloser Office 365 Daten Import

Einfache Integration mit existierenden Tools

Schneller Schutz durch KI Unterstützung



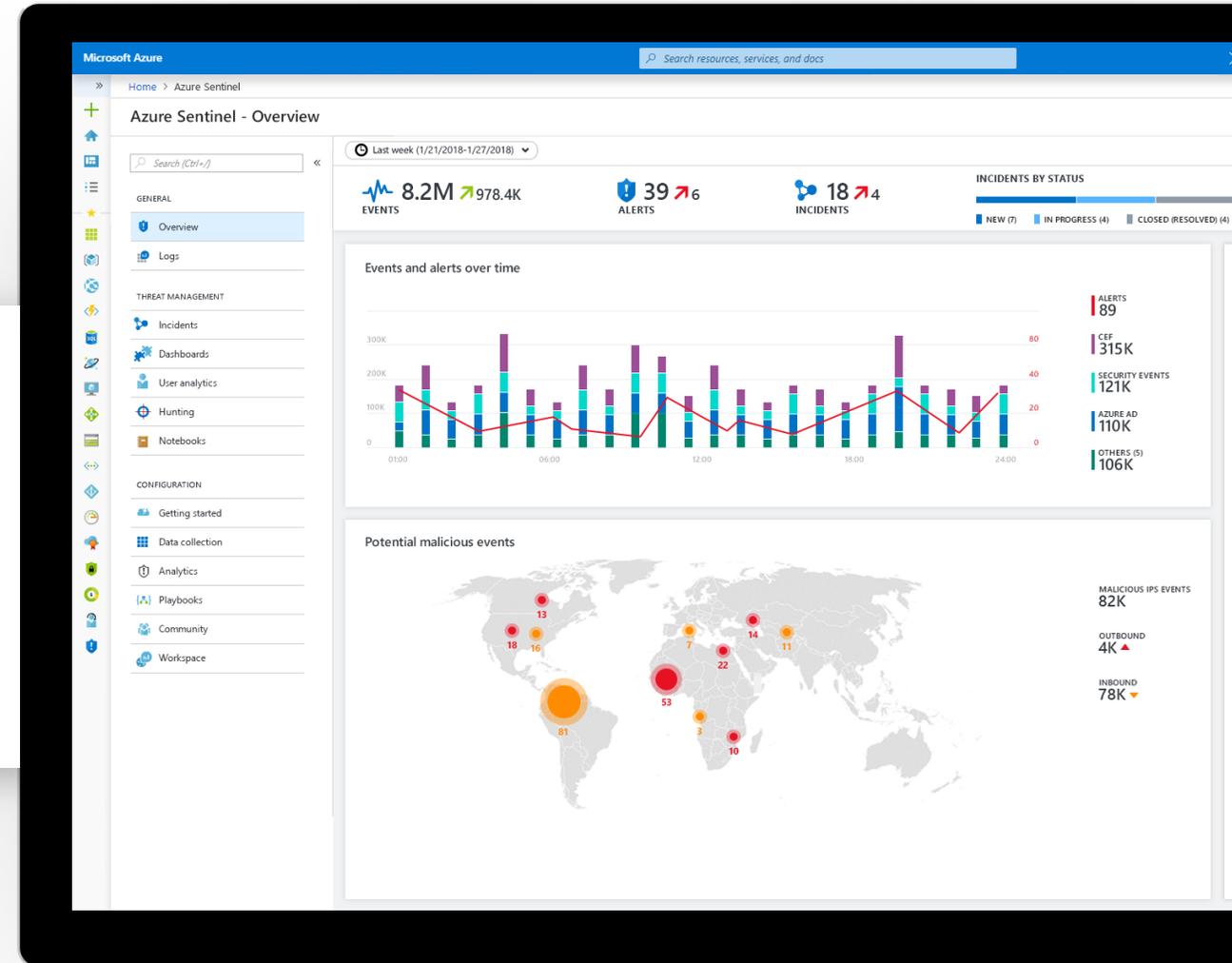
# Fokus auf **Security**, Entlstung der SecOps von IT Tasks

Kein Infrastruktur Setup oder Wartung

SIEM Service über das **Azure Portal** verfügbar

**Automatische Skalierung**, ohne Ressourcen-Limitierung

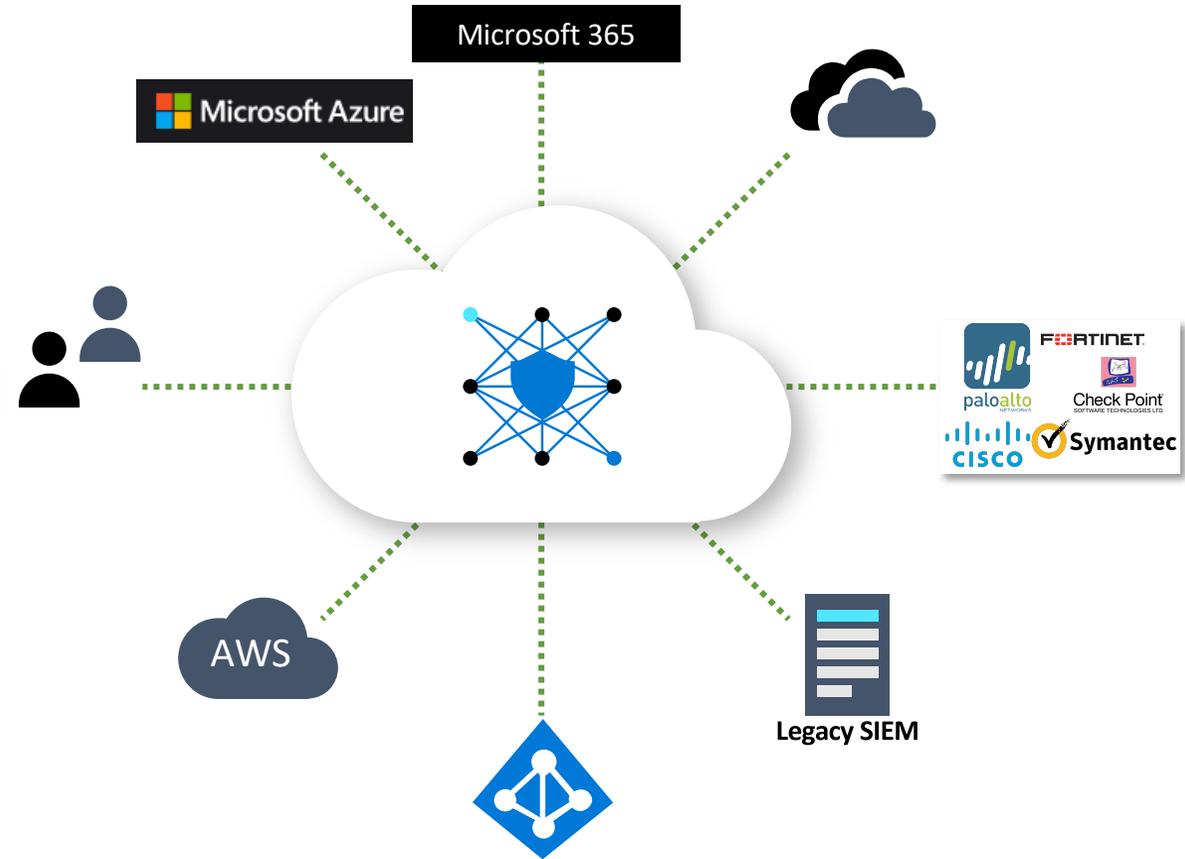
Pay-per-Use Modell



# Erfassen von Security Daten aus allen Quellen der Organisation

Vorgefertigte Konfiguration mit Microsoft Lösungen  
Connectorren für viele Dritthersteller-Lösungen  
Standard Log Formate für die Einbindung aller Quellen

Erprobte Log Plattform mit mehr als 10  
Petabyte am Tag



# Integration mit Daten-Konnektoren

Integration mit Daten-Konnektoren wird ständig erweitert – Microsoft und Drittanbieter

	<b>Amazon Web Services</b> Amazon
	<b>Azure Active Directory</b> Microsoft
	<b>Azure Active Directory Identity Protection</b> Microsoft
	<b>Azure Activity</b> Microsoft
	<b>Azure Advanced Threat Protection (Preview)</b> Microsoft
	<b>Azure Information Protection (Preview)</b> Microsoft
	<b>Azure Security Center</b> Microsoft
	<b>Barracuda Web Application Firewall</b> Barracuda
	<b>Check Point</b> CheckPoint
	<b>Cisco ASA</b> Cisco
	<b>Common Event Format (CEF)</b> Any
	<b>CyberArk</b> CyberArk
	<b>DNS (Preview)</b> Microsoft
	<b>F5 Networks</b> F5 Networks
	<b>Fortinet</b> Fortinet
	<b>Microsoft Cloud App Security</b> Microsoft
	<b>Microsoft Defender Advanced Threat Protection</b> Microsoft
	<b>Microsoft web application firewall (WAF)</b> Microsoft
	<b>Office 365</b> Microsoft
	<b>Palo Alto Networks</b> Palo Alto Networks
	<b>Security Events</b> Microsoft
	<b>Symantec Integrated Cyber Defense Exchange</b> Symantec
	<b>Syslog</b> Microsoft
	<b>Threat Intelligence Platforms (Preview)</b> Microsoft
	<b>Windows Firewall</b> Microsoft

### Data connectors

Search (Ctrl+F)

- GENERAL
  - Overview
  - Logs
- DETECTION
  - Cases
  - Dashboards
  - Entity analytics
  - Hunting
  - Notebooks
- CONFIGURATION
  - News & guides
  - Data connectors
  - Analytics & rules
  - Playbooks
  - Community
  - Workspace settings

Refresh

11 Connectors   8 Connected   0 issues   0 Coming soon

Multi-Cloud Anbindung

Connector	Status	Last log received	Rating
Amazon Web Services Amazon	Connected	06/25/19, 03:18 PM	★★★★★
Azure Active Directory Microsoft	Connected	06/25/19, 03:06 PM	★★★★★
Azure Active Directory Identity Protection Microsoft	Connected	10/04/2019 12:55	★★★★★
Azure Activity Microsoft	Connected		★★★★★
Azure Advanced Threat Protection Microsoft	Connected	10/04/2019 12:55	★★★★★
Azure Information Protection Microsoft	Connected		★★★★★
Azure Security Center Microsoft	Connected	10/04/2019 12:55	★★★★★
Barracuda Web Application Firewall Barracuda	Connected		★★★★★
F5 Microsoft	Connected		★★★★★
Microsoft Cloud App Security Microsoft	Connected		★★★★★
Microsoft web application firewall (WAF) Microsoft	Connected		★★★★★

Microsoft Activity Logs

Azure PaaS Anbindung

Erweiterte On-Premises und IaaS Anbindung

Meldungen von Microsoft Security Lösungen

**Azure Active Directory**  
Microsoft

Connected STATUS   Microsoft CREATED BY   2 days ago LAST LOG RECEIVED

DESCRIPTION

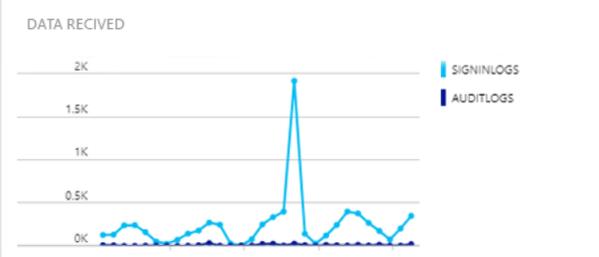
Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your SSPR usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

LAST DATA RECEIVED

Last log received: 06/25/19, 03:06 PM

RELATED CONTENT

2 Dashboards   2 Queries



DATA TYPES

SigninLogs	06/25/19 03:30 PM
AuditLogs	06/25/19 03:06 PM

View connector

# Monitoring mit Workbooks

The screenshot displays the Azure Sentinel Workbooks interface. On the left is a navigation sidebar with categories: General (Overview, Logs), Threat management (Incidents, Workbooks, Hunting, Notebooks), and Configuration (News & guides, Data connectors, Analytics, Playbooks, Community, Workspace settings). The main area shows a summary with 34 Saved workbooks, 19 Templates, and 0 Updates. Below this is a list of templates, with 'Azure Activity' selected and highlighted. The right-hand panel provides a detailed view of the 'Azure Activity' workbook, including a description: 'Gain extensive insight into your organization's Azure Activity by analyzing, and correlating all user operations and events. You can learn about all user operations, trends, and anomalous changes over time. This dashboard gives you the ability to drill down into caller activities and summarize detected failure and warning events.' It also lists 'Required data types' (AzureActivity) and 'Data sources' (AzureActivity). A preview of the workbook's dashboard is shown, featuring a line chart and a table. At the bottom of the preview are 'View Workbook' and 'Delete' buttons.

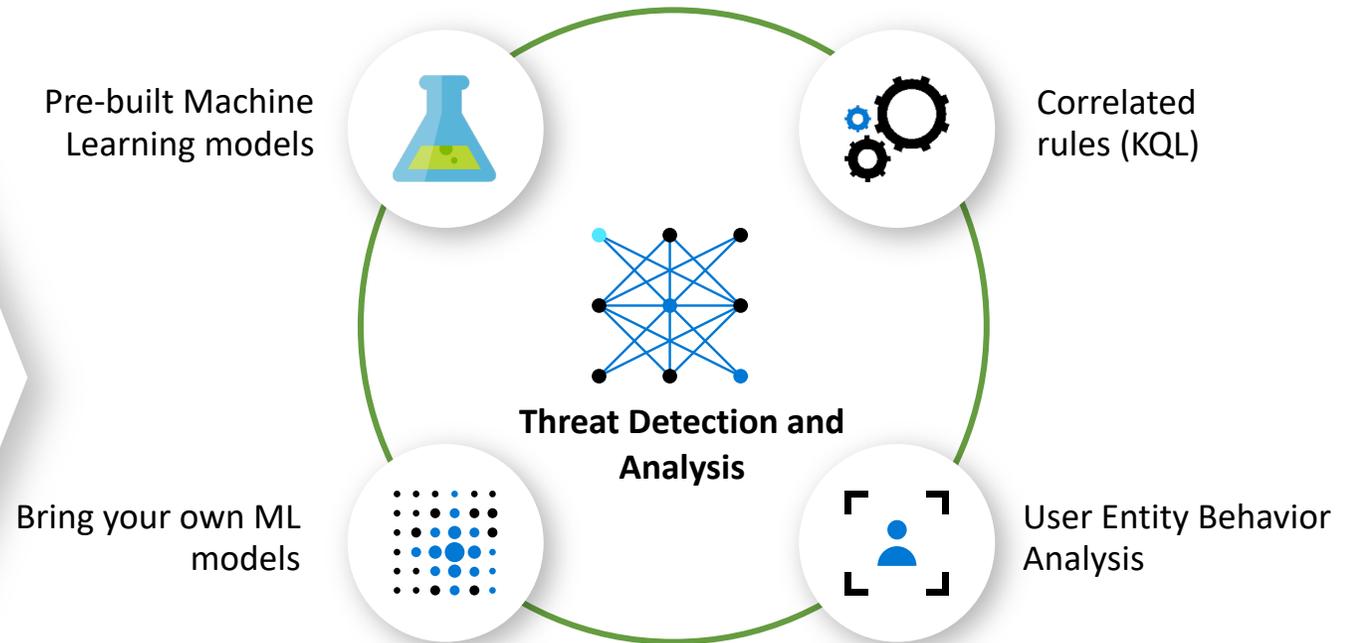
# Ermitteln von Bedrohungen und schnelle Analyse von Security Data mit der KI

ML Modelle basierend auf **jahrelanger Microsoft Erfahrung**

Millionen von Signalen in **korrelierte und priorisierte Security Incidents** zusammengeführt

Unerreichte Threat Intelligence, **Analyse diverser Sets von mehr als 6.5 Billionen Signalen am Tag**

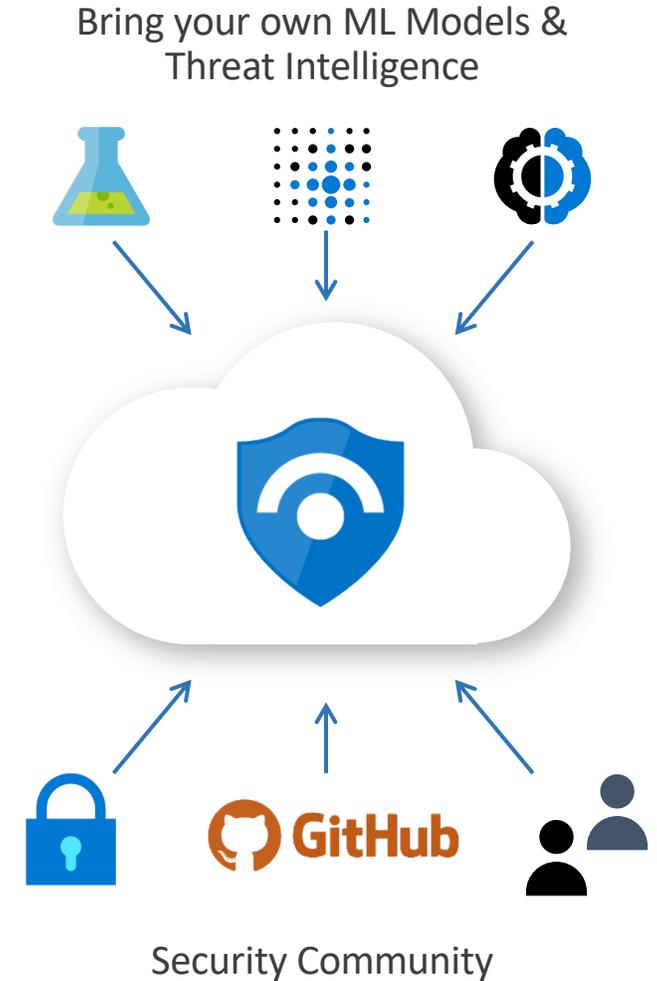
Reduziert "Alert Fatigue" bis zu 90%



# Auf individuelle Anforderungen optimiert

Bring your own Insights, Modelle für Maschinelles Lernen und Threat Intelligence

Nutzen der Security Community um Erkennungen, Threat Intelligence, und automatisierte Reaktionen zu verwenden.

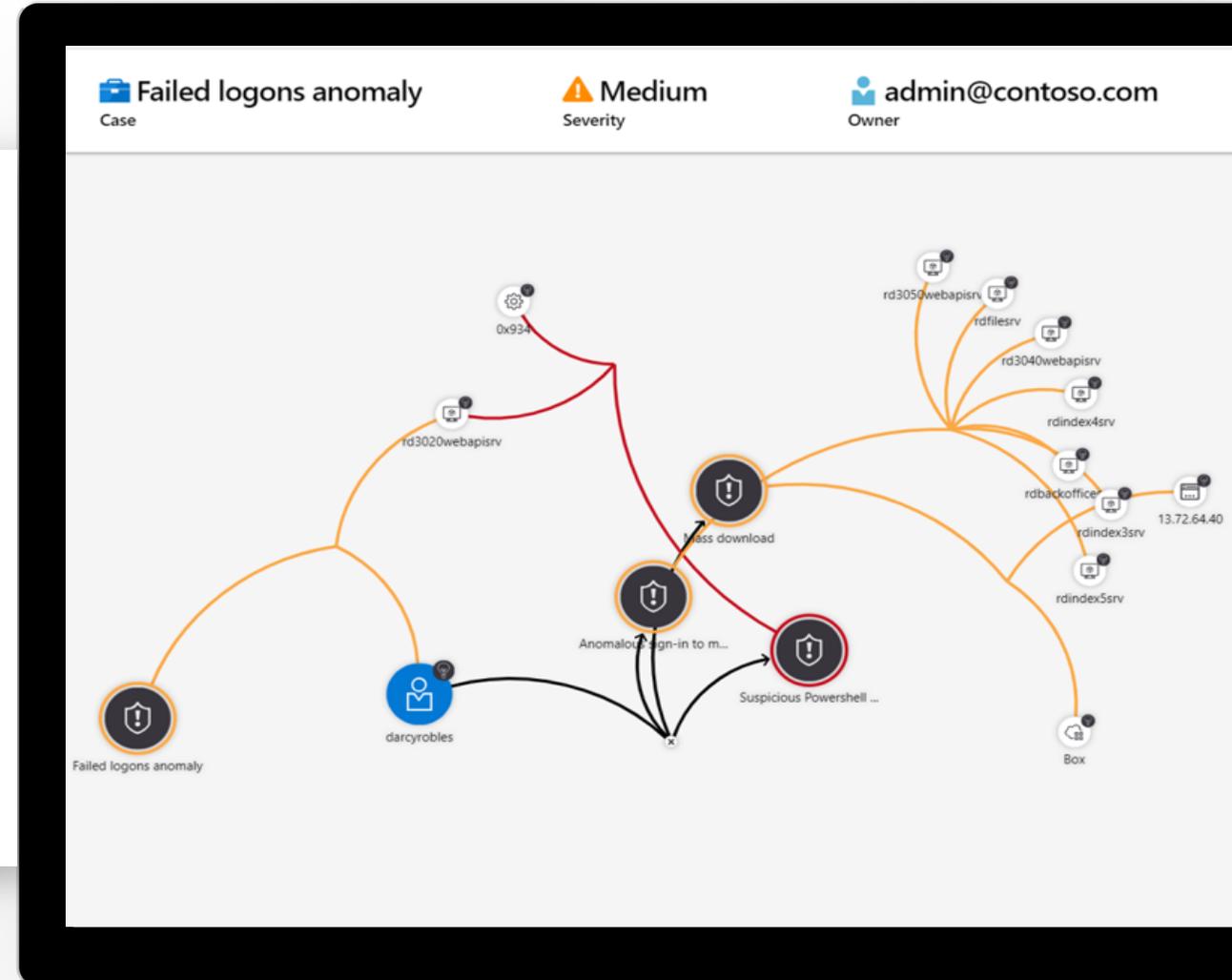


# Untersuchen von Bedrohungen mit KI und nachverfolgen von auffälligen Aktivitäten, Verwendung der Microsoft Cybersecurity Arbeit von Jahren

Priorisierte Meldungen und **automatisierte Experten-Unterstützung**

**Visualisierung** des kompletten Angriffs und der Auswirkungen

Nachverfolgen von auffälligen Aktivitäten mit **vorgefertigten Abfragen und Azure Notebooks**



# Investigation

PREVIEW

Undo Redo

**Anomalous login**

Case

**Medium**

Severity

**New**

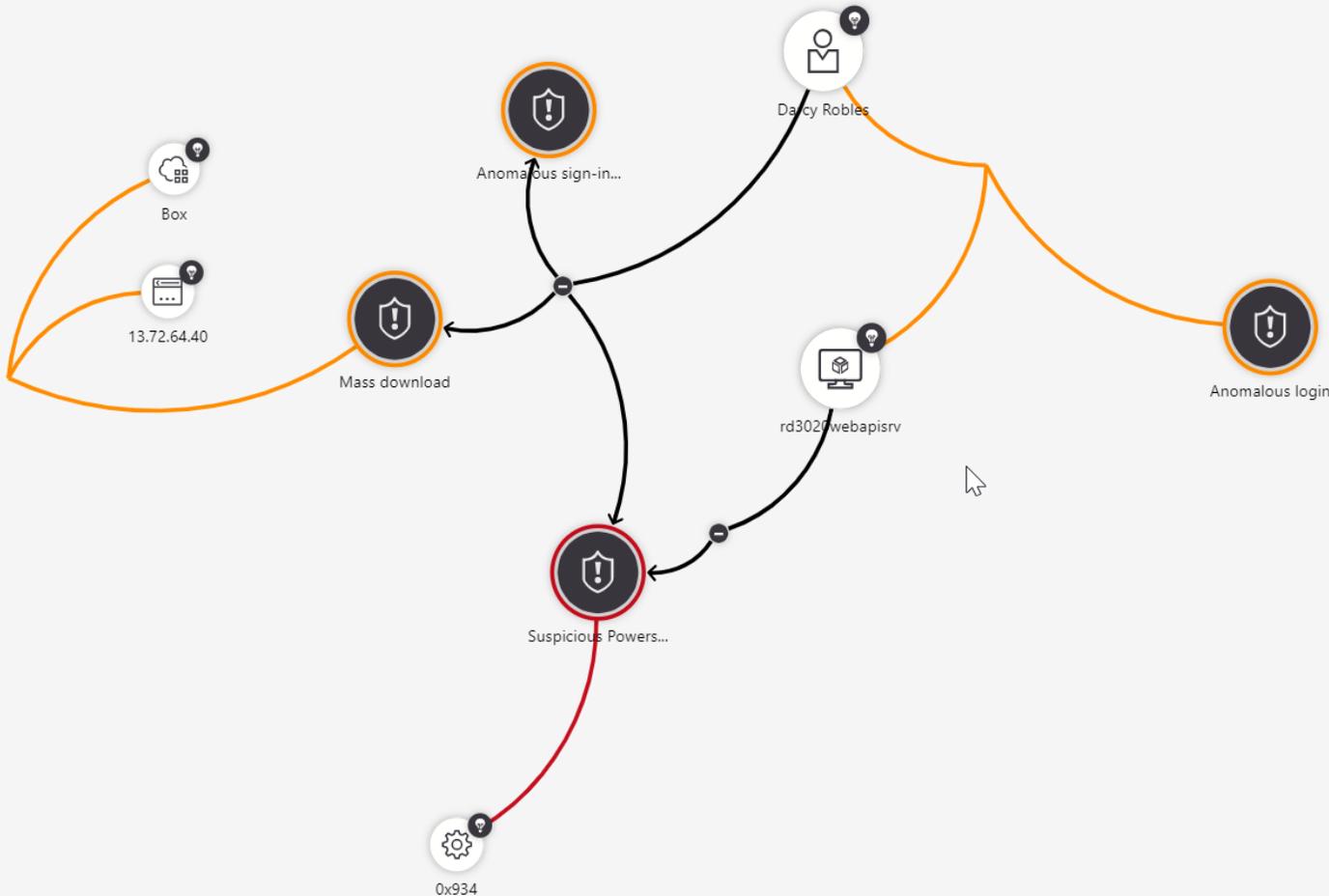
Status

**admin@contoso.com**

Owner

**3/14/2019, 11:32:00 AM**

Last modification time



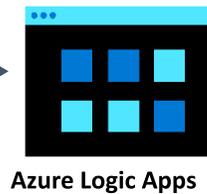
## Timeline

- Anomalous login**  
3/13/2019, 10:21:00 AM  
Finds cases in which we had more than 400 failed logins i...
- Suspicious Powershell Activity Detec...**  
3/13/2019, 11:25:00 AM  
Analysis of host data detected a powershell script running ...
- Anomalous sign-in to multiple comp...**  
3/13/2019, 1:51:00 PM  
Account sign-in activity indicates numerous sign-ins to mu...
- Mass download**  
3/13/2019, 2:48:00 PM  
The user 'Darcy Robles (darcyrobles@contoso.com)' down...

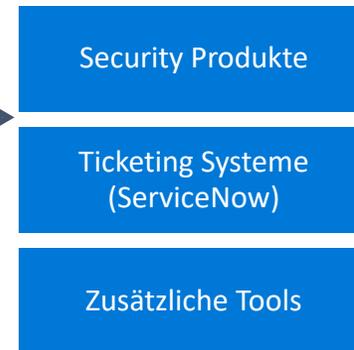


# Schnelle Reaktion mit eingebauter Orchestrierung und Automatisierung

Zusammenstellen von automatisierten und skalierbaren Playbooks, die sich in verschiedene Tools integrieren



Azure Logic Apps



# Orchestrierung von Bedrohungserkennung, Überprüfung und Reaktion

The screenshot displays the Microsoft Azure Logic Apps Designer interface. The breadcrumb navigation at the top indicates the path: Home > Azure Sentinel - Cases > Case > Alert playbooks > Logic Apps Designer. The workflow is titled "Logic Apps Designer" and includes the following steps:

- When a response to an Azure Security Center alert is triggered
- Create incident in Service Now(Preview)
- Post message to SOC channel(Preview)
- Send approval email
- Condition: Selected... x is equal to Block user and IP
- If true:
  - Block user in Azure AD
  - BlockIPPalto
- If false:
  - Close incident in Service Now(Preview)

The interface also shows standard actions like Save, Discard, Run, Designer, Code view, Templates, Connectors, and Help. A "+ New step" button is visible at the bottom right of the workflow canvas.

# Azure Sentinel - Cases

Selected workspace: 'CyberSecurityDemo' - PREVIEW

Refresh Last 24 hours

**8**  
OPEN CASES

**8**  
NEW CASES

**0**  
IN PROGRESS

## Open Cases By Severity



Search

SEVERITY : Informational, Low, Medium, High, Critical

STATUS : New, In Progress

TITLE	ALERTS	CREATED TIME	OWNER	STATUS
Anomalous login	1	03/14/19, 11:32 AM	admin@contoso.com	New
User Account Created and Deleted within 24 hours	1	05/20/19, 6:50 PM	Unassigned	New
DNS tor proxies	1	05/20/19, 6:48 PM	Unassigned	New
Signins from IP's that attempted to sign in to disabled accounts	1	05/20/19, 6:47 PM	Unassigned	New
Base64 encoded Windows executables in process commandlines	1	05/20/19, 6:45 PM	Unassigned	New
AWS - Login to AWS Management Console without MFA	1	05/20/19, 6:44 PM	Unassigned	New
Malware in the recycle bin	1	05/20/19, 6:41 PM	Unassigned	New
Kerberos service ticket was requested	1	05/20/19, 10:05 AM	Unassigned	New
AWS - Monitor Credential abuse or hijack	1	05/20/19, 10:03 AM	Unassigned	New

## Anomalous login

Medium SEVERITY

New STATUS

admin@con. OWNER

DESCRIPTION

LAST UPDATE TIME

03/14/19, 11:32 AM

CREATION TIME

03/14/19, 11:32 AM

EVIDENCE

**1**  
Alerts

ENTITIES

**1** Account **1** Host **0** IP

Investigate

View full details

Cases und Meldungen

# Azure Sentinel - Analytics

Selected workspace: 'CyberSecurityDemo' - PREVIEW

Search (Ctrl+)

+ Add Refresh Last 24 hours

- General
  - Overview
  - Logs
- Threat management
  - Cases
  - Dashboards
  - Hunting
  - Notebooks
- Configuration
  - Getting started
  - Data connectors
  - Analytics
  - Playbooks
  - Community
  - Workspace settings



Search alert rules...

NAME	DESCRIPTION
AWS - Monitor Credential abuse or hijack	This Alert monitors for GetCallerIdentity Events where the UserID Typ...
PowerShell Empire	Finds instances of PowerShell Empire cmdlets in powershell process e...
Malware in the recycle bin	finding attackers hiding malware in the recycle bin. Read more here:...
Traffic to known IP	Microsoft tracks a significant number of threat actors/malware/botn...
Anomalous File Share Access	Users accessing file shares that they normally do not access. This det...
Base64 encoded Windows executables in process comman...	Instances of base64 encoded PE files header seen in process comman...
Granting permissions to account	looks for IPs from which users grant access to others on azure resour...
Signins from IP's that attempted to sign in to disabled acc...	an IP address that had a (failed) attempts to sign in to one or more d...
User Account Created and Deleted within 24 hours	User account created and then deleted within 10 minutes
Creation of an anomalous number of resources	looks for anomalous number of resources creation or deployment ac...
User Account added to Built in Domain Local or Global Gr...	User account was added to a privileged built in domain local group d...
DNS high reverse DNS count	clients with a high reverse DNS count could be carrying out scanning...
Kerberos service ticket was requested	Privilege escalation technique which proves to be very effective in ex...
Process executed from binary hidden in Base64 encoded f...	Encoding malicious software is a technique to obfuscate files from d...
DNS high NXDomain count	clients with a high NXDomain count could be indicative of a DGA (cy...
Attempts to sign in to disabled accounts	Attempts to sign in to disabled accounts summarized by account nar...

Malware in the recycle bin

## Edit alert rule

PREVIEW

Status ⓘ

Enabled Disabled

### Details

\* Name

Granting pe...

Id

96e1742a-d...

Description

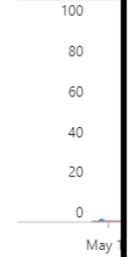
looks for IPs from which users grant access to others on azure resour...

Severity

High

### Logic

Alert simulat...



\* Set alert qu...

Set time and...

let createRo... | where Ope... | where Acti... | project Tim... Subscription... // The numb...

### Entity mapping - more entities coming soon!

Use Entity type fields to map the fields in your query to entities recognized by Azure Sentinel. Entity type must be a string or Datetime.

ENTITY TYPE	PROPERTY
Account	Choose column Add
Host	Choose column Add
IP address	Defined in query

### Alert trigger

Operator: Number of results greater than

Threshold: 0

### Alert scheduling

\* Frequency: 24 Hours

\* Period: 24 Hours

### Realtime automation

Triggered playbooks: Select playbooks

### Alert suppression

Suppression status ⓘ: On Off

# Erzeugen eigener Korrelationsregeln

# Automatische Erzeugung von Incidents durch die Integration von Microsoft Security Meldungen

**Azure Sentinel - Analytics**  
Selected workspace: contoso

Search (Cmd+/) **+ Create** Refresh

**182** Active rules

**RULES BY SEVERITY**  
HIGH (25) MEDIUM (107) LOW (47) INFORMATIONAL (3)

Active rules Rule templates

Search SEVERITY: All TYPE: All STATUS: All TACTICS: All

NAME	RULE TYPE	STATUS	TACTICS	LAST MODIFIED
Advanced Multistage Attack Detection	Fusion	Enabled		09/08/19, 04:17 PM
Create incidents based on Azure Advanced Threat ...	Microsoft Secur...	Disabled		09/05/19, 03:08 PM
Create incidents based on Microsoft Cloud App Se...	Microsoft Secur...	Disabled		09/05/19, 03:08 PM
Create incidents based on Azure Security Center al...	Microsoft Secur...	Enabled		09/08/19, 04:09 PM
Create incidents based on Azure Active Directory I...	Microsoft Secur...	Enabled		09/08/19, 04:34 PM
Create incidents based on Azure Active Directory I...	Microsoft Secur...	Enabled		09/10/19, 10:51 AM
Create incidents based on Azure Security Center al...	Microsoft Secur...	Enabled		09/11/19, 02:41 PM
Create incidents based on ASC alerts	Microsoft Secur...	Enabled		09/05/19, 03:35 PM
Create incidents based on Azure Active Directory I...	Microsoft Secur...	Disabled		09/05/19, 03:08 PM
Create incidents based on Microsoft Cloud App Se...	Microsoft Secur...	Enabled		09/08/19, 12:37 PM
Grumpy Cat	Scheduled	Enabled		09/05/19, 11:26 AM
Juniper Admin logged on via SSH	Scheduled	Disabled		09/05/19, 11:26 AM
Alert signature	Scheduled	Enabled	Credential Access	09/11/19, 02:40 PM
Global domain trust creation - Demo	Scheduled	Disabled		08/19/19, 05:39 PM

**Create incidents based on Azure Active Dire...**

High SEVERITY Enabled STATUS

**Description**  
Create incidents based on all alerts generated in Azure Active Directory Identity Protection

**Filter by Microsoft security service**  
Azure Active Directory Identity Protection

**Filter by severity**  
High

**Filter by alert name**  
Any

Edit

# Threat Hunting

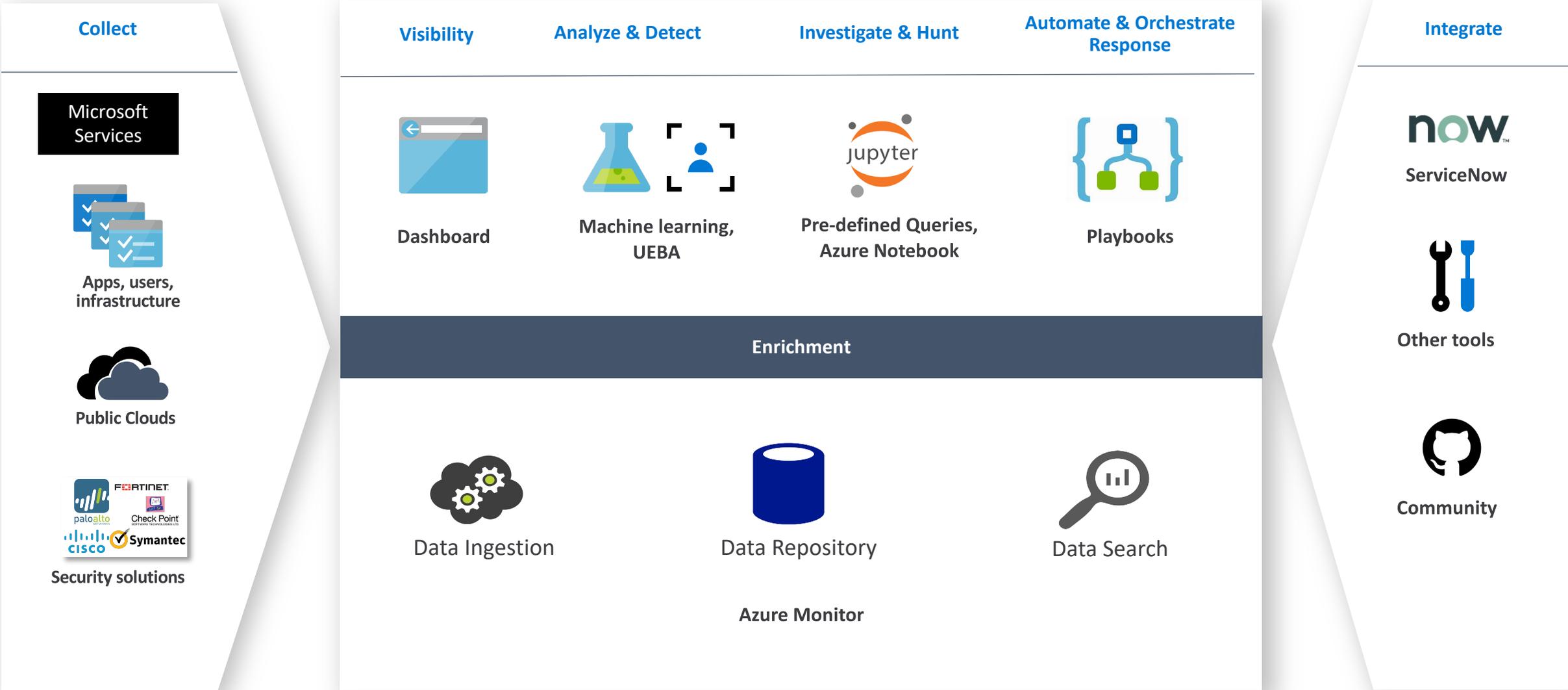
The screenshot displays the Azure Sentinel Hunting interface. At the top, it shows the workspace name 'Azure Sentinel - Hunting' and a search bar. Below the search bar, there are four summary cards: '20 Total Queries', '94 Total Results', '4 Total Bookmarks', and '0 My Bookmarks'. The main area is divided into a table of queries and a detailed view of the selected query.

QUERY	DESCRIPTION	PROVIDER	DATA SOURCE	RES...	TACTICS
★ Uncommon processes/files - bottom 5%	Shows the rarest processes seen running for the first...	Microsoft	SecurityEvent	12	[Icons]
★ Script usage summary (cscript.exe)	Daily summary of vbs scripts run across the environ...	Microsoft	SecurityEvent	2	[Icons]
★ Summary of users created using uncommon ...	Summarizes users of uncommon & undocumented ...	Microsoft	SecurityEvent	0	[Icons]
★ Office365 authentications	Shows authentication volume by user agent and IP ...	Microsoft	OfficeActivity	0	[Icons]
★ New processes observed in last 24 hours	Shows new processes observed in the last 24 hours ...	Microsoft	SecurityEvent	80	[Icons]
★ Summary of failed user logons by reason of f...	A summary of failed logons can be used to infer lat...	Microsoft	SecurityEvent	0	[Icons]
★ Anomalous Azure AD apps based on authent...	This query over Azure AD sign-in activity highlights...	Microsoft	SignInLogs	--	[Icons]
★ Processes executed from base-encoded PE fil...	Finding base64 encoded PE files header seen in the ...	Microsoft	SecurityEvent	--	[Icons]
★ Processes executed from binaries hidden in ...	Process executed from binary hidden in Base64 enc...	Microsoft	SecurityEvent	--	[Icons]
★ Summary of users creating new user accounts	New user accounts may be an attacker providing th...	Microsoft	OfficeActivity	--	[Icons]
★ User and Group enumeration	The query finds attempts to list users or groups usi...	Microsoft	SecurityEvent	--	[Icons]
★ Hosts with new logons	Shows new accounts that have logged onto a host f...	Microsoft	SecurityEvent	--	[Icons]
★ Malware in the recycle bin	Finding attackers hiding malware in the recycle bin. ...	Microsoft	SecurityEvent	--	[Icons]
★ Masquerading files	Malware writers often use windows system process ...	Microsoft	SecurityEvent	--	[Icons]
★ Accounts and User Agents associated with m...	Summary of users/user agents associated with auth...	Microsoft	OfficeActivity	--	[Icons]
★ Azure AD signins from new locations	New AzureAD signin locations today versus historic...	Microsoft	SignInLogs	--	[Icons]
★ Powershell downloads	Finds PowerShell execution events that could invol...	Microsoft	SecurityEvent	--	[Icons]
★ Sharepoint downloads	Shows volume of documents uploaded to or downl...	Microsoft	OfficeActivity	--	[Icons]
★ Summary of user logons by logon type	Comparing successful and unsuccessful logon atte...	Microsoft	SecurityEvent	--	[Icons]
★ SSH Brute Force Attacks	Identifies anomalous SSH Logon attempts on Linux ...	Custom Queries	SecurityAlert	--	[Icons]

The detailed view on the right shows the query 'Uncommon processes/files - bottom 5%' with 12 results from the SecurityEvent data source. It includes a description of the query, the KQL query text, and a list of tactics such as Execution, Initial Access, Persistence, and Privilege Escalation.

```
let start=datettime("2019-02-19T18:26:31.916Z");
let end=datettime("2019-02-20T18:26:31.916Z");
let ProcessCreationEvents=() {
  let processEvents=SecurityEvent
  | where TimeGenerated > start and TimeGene
  | where EventID==4688
```

# Übersicht



# Sentinel Preise

## Verwendungsbezogene Preise

- Datenvolumen, Funktionen und Region
- Pay-as-you-go  
(z.B. EU Nord = €2.03/GB)
- Capacity Reservation => ab 100GB/Tag, 50%-60% Rabatt  
(z.B. EU Nord 100GB/Tag = €101,20 )
- LogAnalytics Ingest und Data Retention
- Automation (Azure Logic Apps)
- Bring Your Own Machine Learning Models

**Jens Lorenz**

Strategic Consultant, CISSP, CCSP

fon: +49-170-4516565

mail: jens.lorenz@expertcircle.de

LinkedIn: <https://de.linkedin.com/in/jenslorenz>