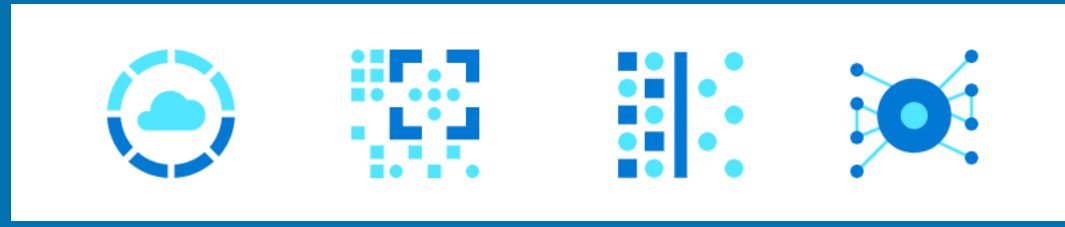
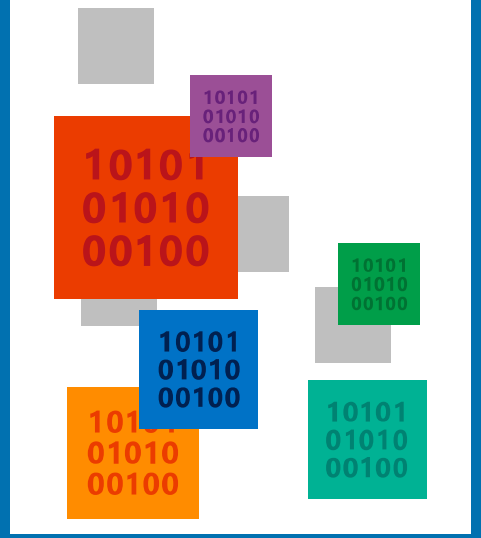
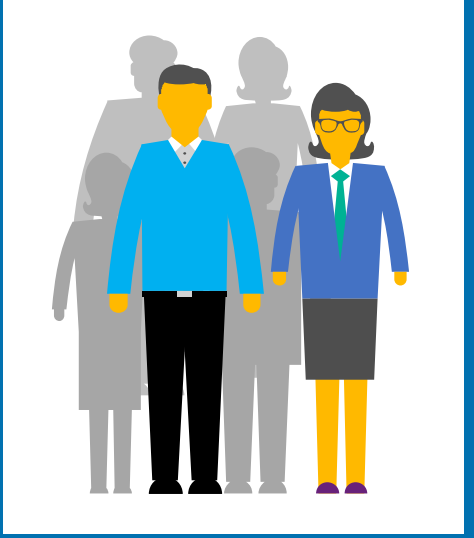
Microsoft Azure Sentinel

SIEM/SOAR as a Service



Jens Lorenz
Strategic Consultant, CISSP, CCSP
ExpertCircle GmbH

Microsoft Security Assets

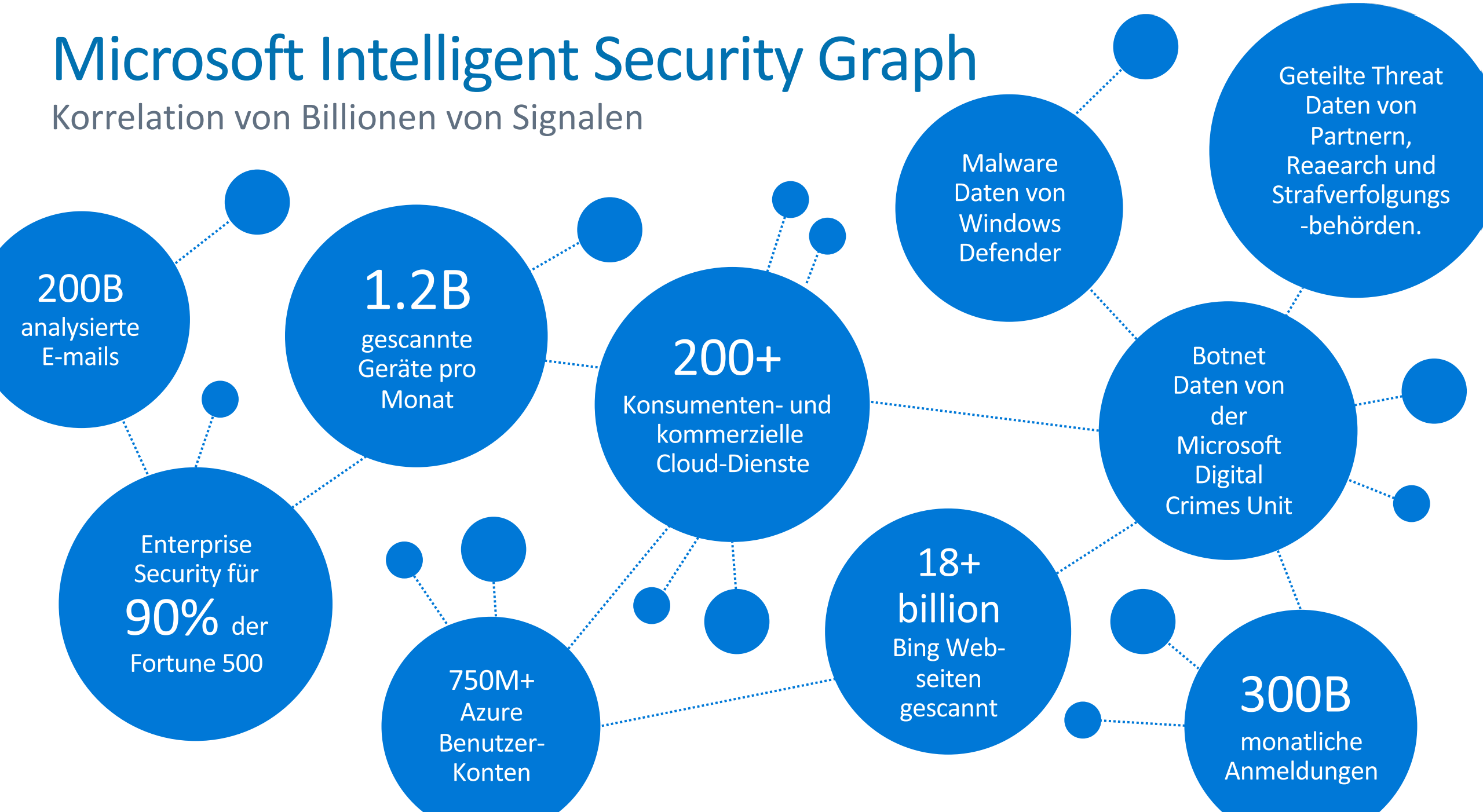
DATA	CLOUD & DATACENTER	APPLICATIONS (SaaS)	ENDPOINTS (Devices)	IDENTITY
				
Information Protection	Azure Security Center	Office 365 Data Loss Prevention	Device Guard	Azure Active Directory
Rights Management Services	Azure Monitor	Office 365 Cloud App Security	Credential Guard	Azure MFA
BYOK (Bring-Your-Own-Key)	Log Analytics	Threat Intelligence	Microsoft Defender	Azure AD Identity Protection
Customer Key	Azure Disk Encryption	Advanced Threat Protection	Microsoft Defender ATP	Privileged Identity Management
	Azure Key Vault	Advanced eDiscovery	Threat & Vulnerability Management	Azure Conditional Access
	Azure Sentinel	Advanced Data Governance	Windows Hello (FIDO)	Advanced Threat Analytics/ Advanced Threat Protection
		Compliance Manager	Intune	Access Reviews
		Customer Lockbox		Microsoft Identity Manager
		Privileged Access Management		Azure AD B2B / B2C

Microsoft 365

User-Centric IT

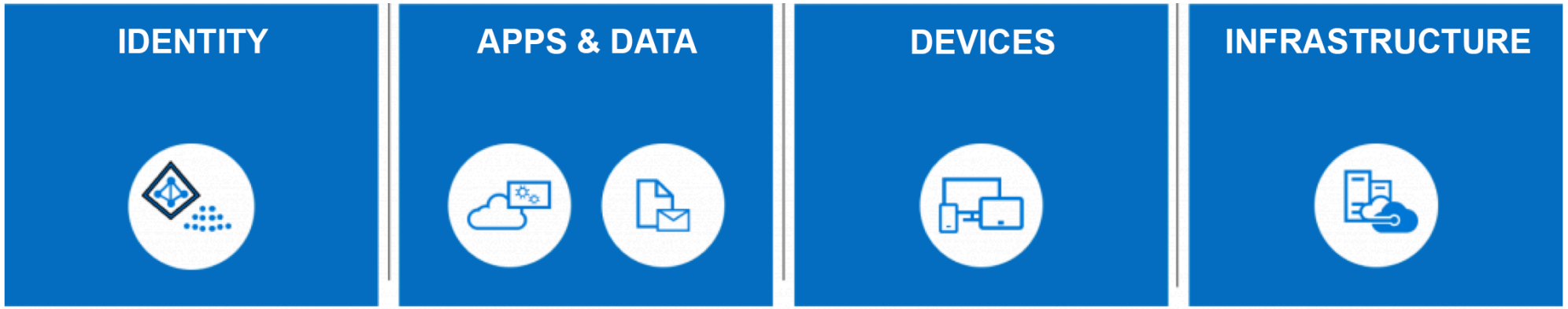
Microsoft Intelligent Security Graph

Korrelation von Billionen von Signalen



Microsoft 365 – Threat Protection

Plattformübergreifende Integration



https://cloudblogs.microsoft.com/microsoftsecure/2018/04/24/securing-the-modern-workplace-with-microsoft-365-threat-protection-part-1/

Erweiterung der digitalen Domäne

Zu viele Meldungen

IT Bereitstellung & Pflege

Entwicklungsgrad von Bedrohungen

Steigende Infrastrukturkosten und Investitionen

Typische SOC Probleme

Zu viele nicht-verbundene Produkte

Fehlende Automation

Fehlende qualifizierte Mitarbeiter (spez. Security)

Security Operations Team

+

Cloud + Künstliche Intelligenz

Microsoft Azure Sentinel

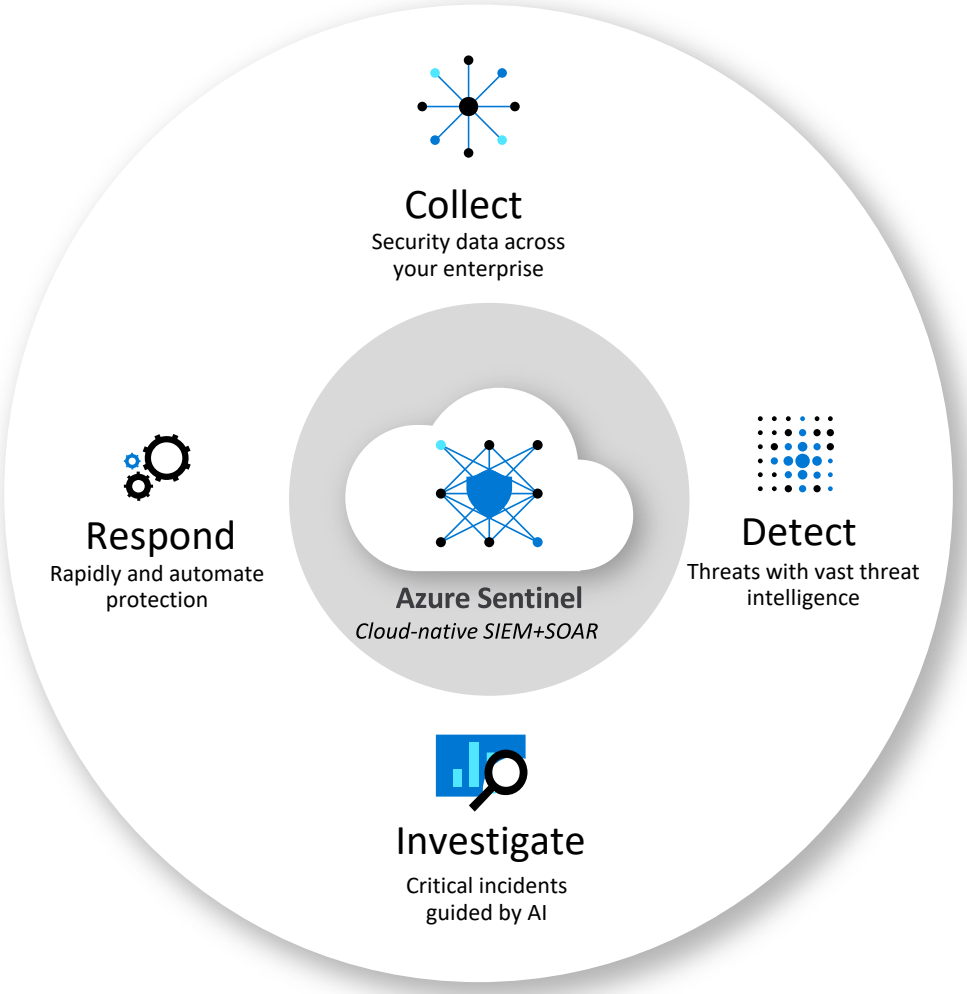
Cloud-natives SIEM für intelligente Security Analysen für die gesamte Organisation

Cloud-Speed und Skalierung ohne Limit

Kostenloser Office 365 Daten Import

Einfache Integration mit existierenden Tools

Schneller Schutz durch KI Unterstützung



https://azure.microsoft.com/en-us/blog/introducing-microsoft-azure-sentinel-intelligent-security-analytics-for-your-entire-enterprise/

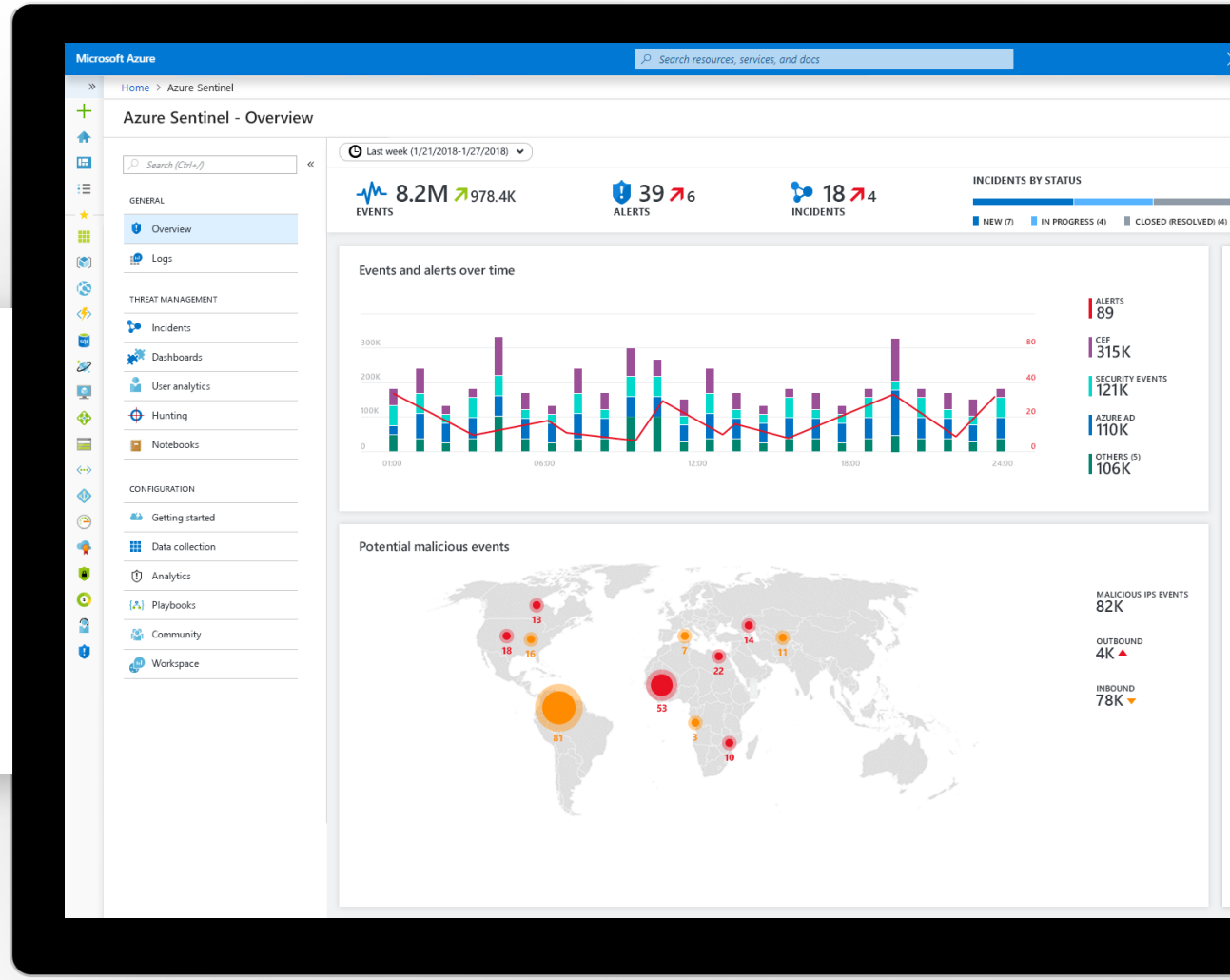
Fokus auf Security, Entlstung der SecOps von IT Tasks

Kein Infrastruktur Setup oder Wartung

SIEM Service über das Azure Portal verfügbar

Automatische Skalierung, ohne Ressourcen-Limitierung

Pay-per-Use Modell



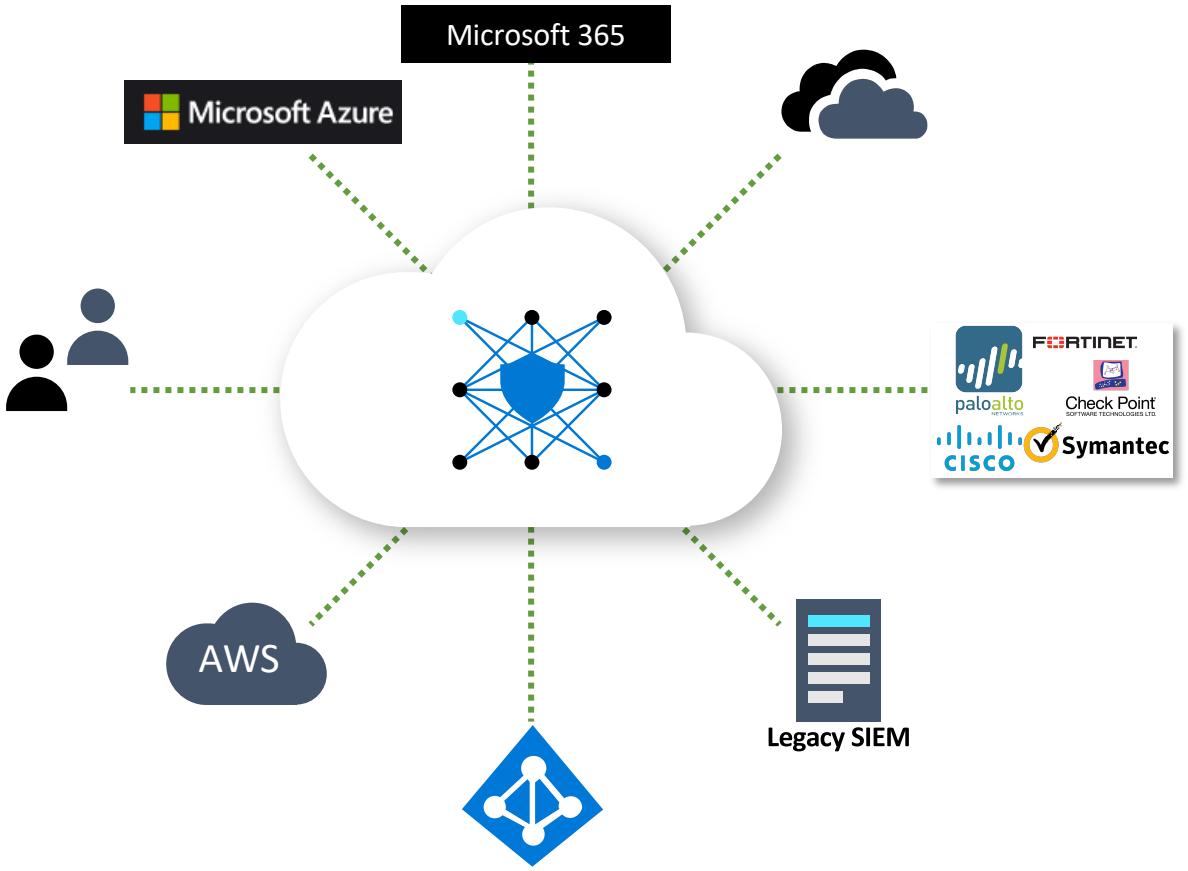
Erfassen von Security Daten aus allen Quellen der Organisation

Vorgefertigte Konfiguration mit Microsoft Lösungen

Connectorren für viele Dritthersteller-Lösungen

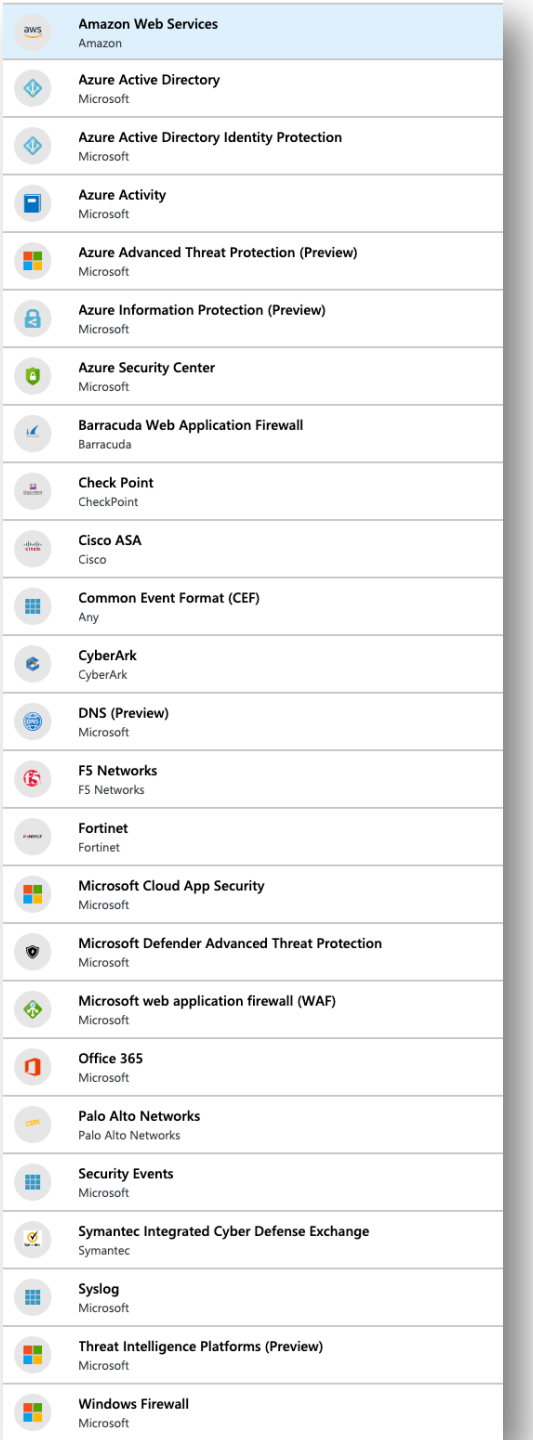
Standard Log Formate für die Einbindung aller Quellen

Erprobte Log Plattform mit mehr als 10 Petabyte am Tag

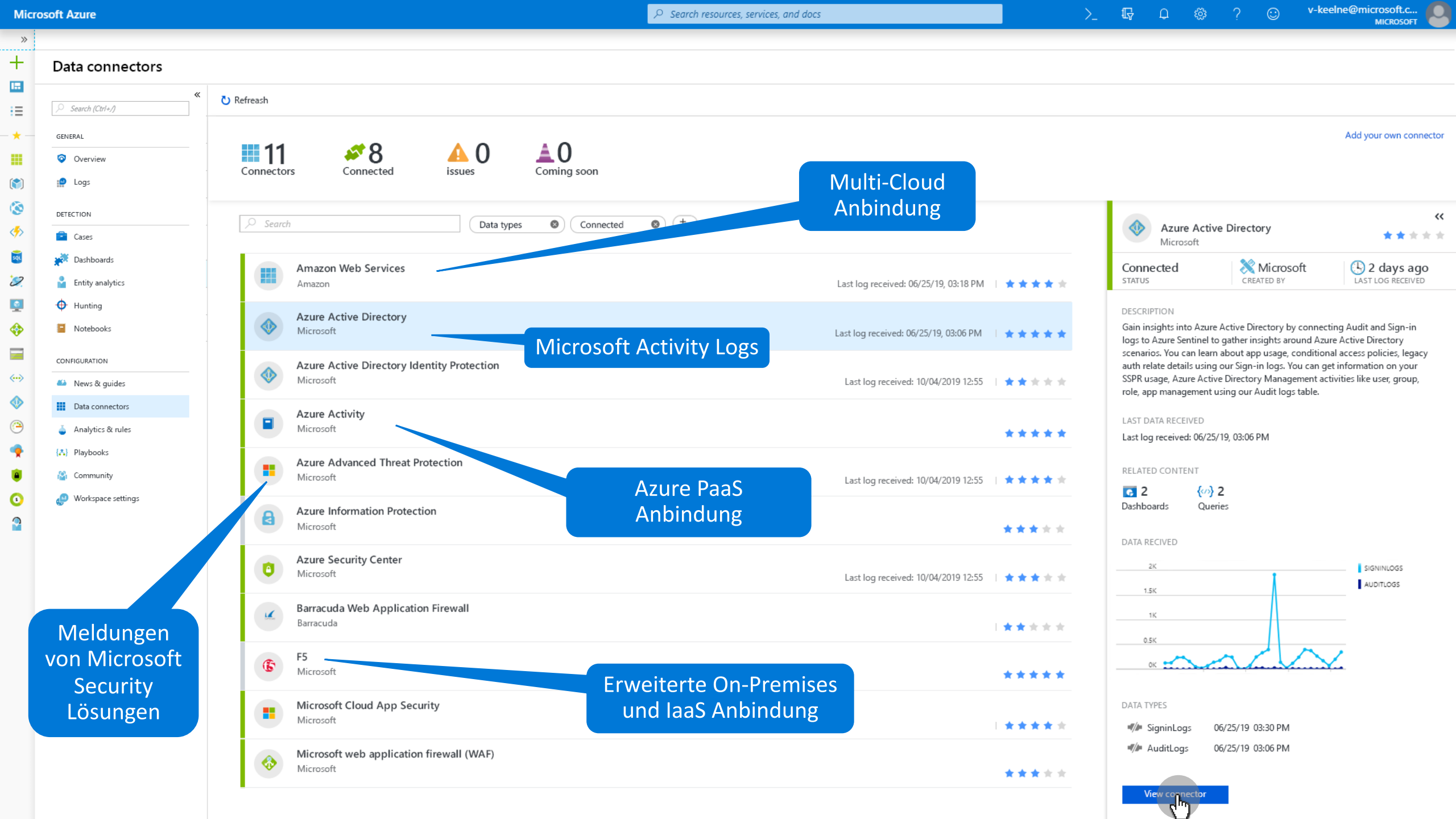


Integration mit Daten-Konnektoren

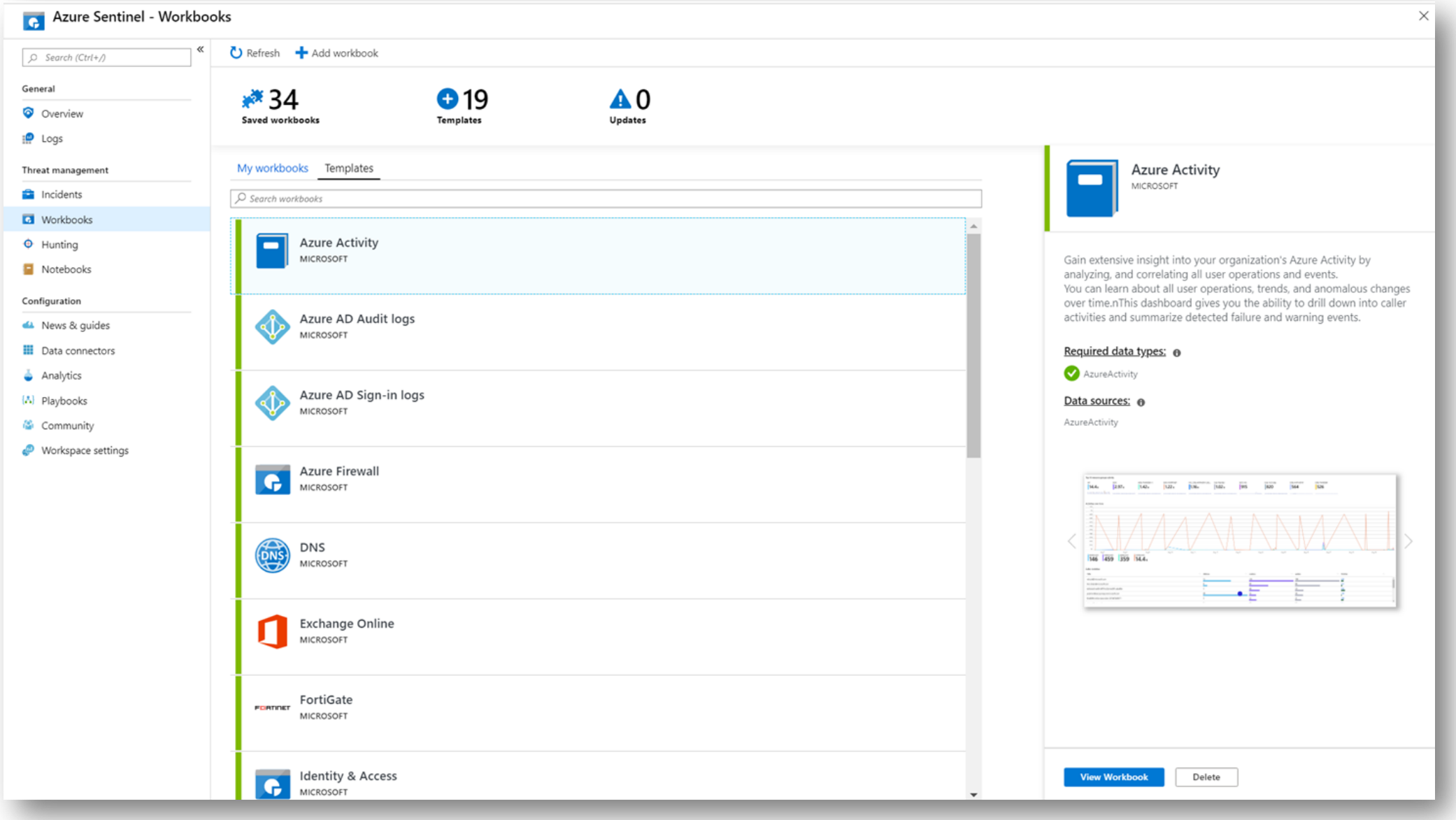
Integration mit Daten-Konnektoren wird ständig erweitert – Microsoft und Drittanbieter



https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources


Microsoft Azure
Search resources, services, and docs
v-keelne@microsoft.c...
MICROSOFT
Data connectors
Search (Ctrl+/)
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
Add your own connector
Search
Data types
Connected
Amazon Web Services
Amazon
Last log received: 06/25/19, 03:18 PM
Azure Active Directory
Microsoft
Last log received: 06/25/19, 03:06 PM
Azure Active Directory Identity Protection
Microsoft
Last log received: 10/04/2019 12:55
Azure Activity
Microsoft
Azure Advanced Threat Protection
Microsoft
Last log received: 10/04/2019 12:55
Azure Information Protection
Microsoft
Azure Security Center
Microsoft
Last log received: 10/04/2019 12:55
Barracuda Web Application Firewall
Barracuda
F5
Microsoft
Microsoft Cloud App Security
Microsoft
Microsoft web application firewall (WAF)
Microsoft
Multi-Cloud Anbindung
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 RECIVED
2K
1.5K
1K
0.5K
0K
SIGNINLOGS
AUDITLOGS
DATA TYPES
SigninLogs
06/25/19 03:30 PM
AuditLogs
06/25/19 03:06 PM
View connector

Monitoring mit Workbooks



https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data

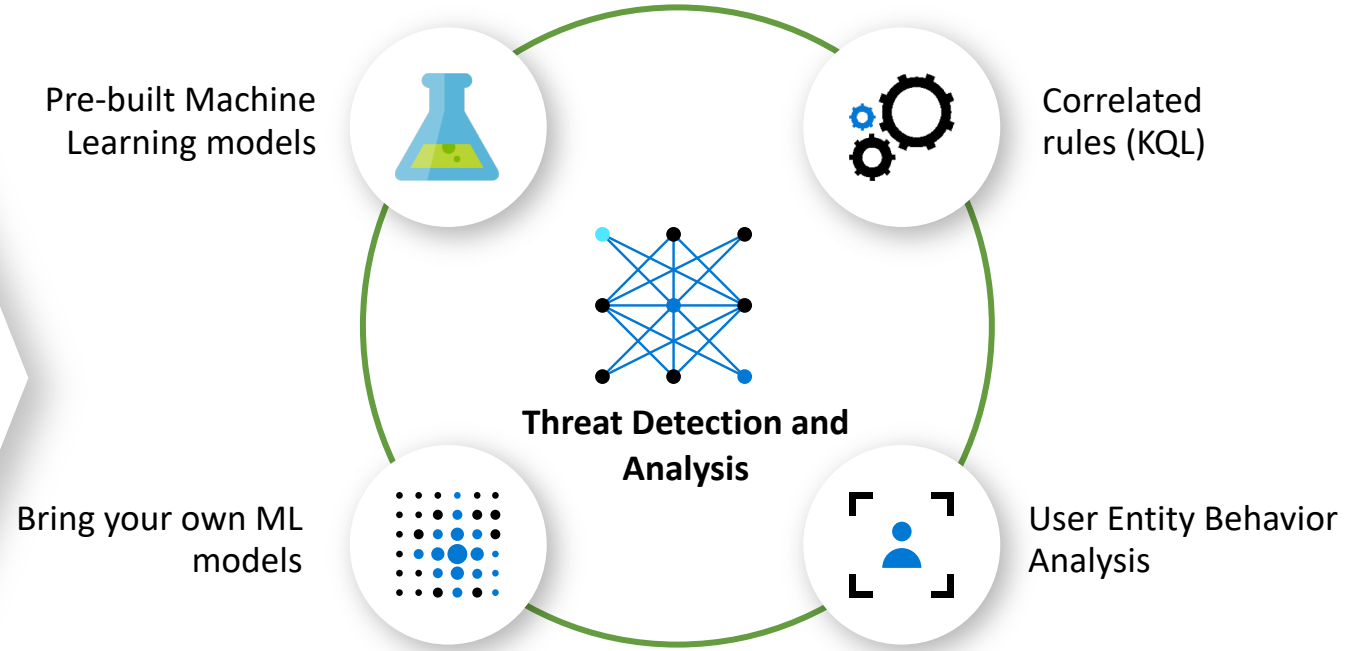
Ermitteln von Bedrohungen und schnelle Analyse von Security Data mit der KI

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 Billiarden Signalen am Tag

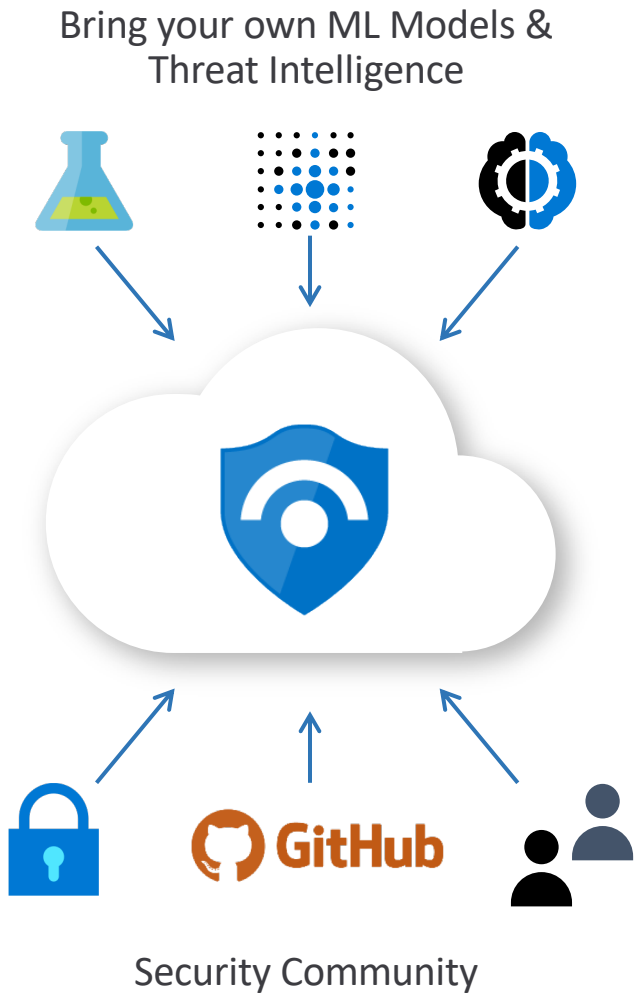
Reduziert “Alert Fatigue” bis zu 90%



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.

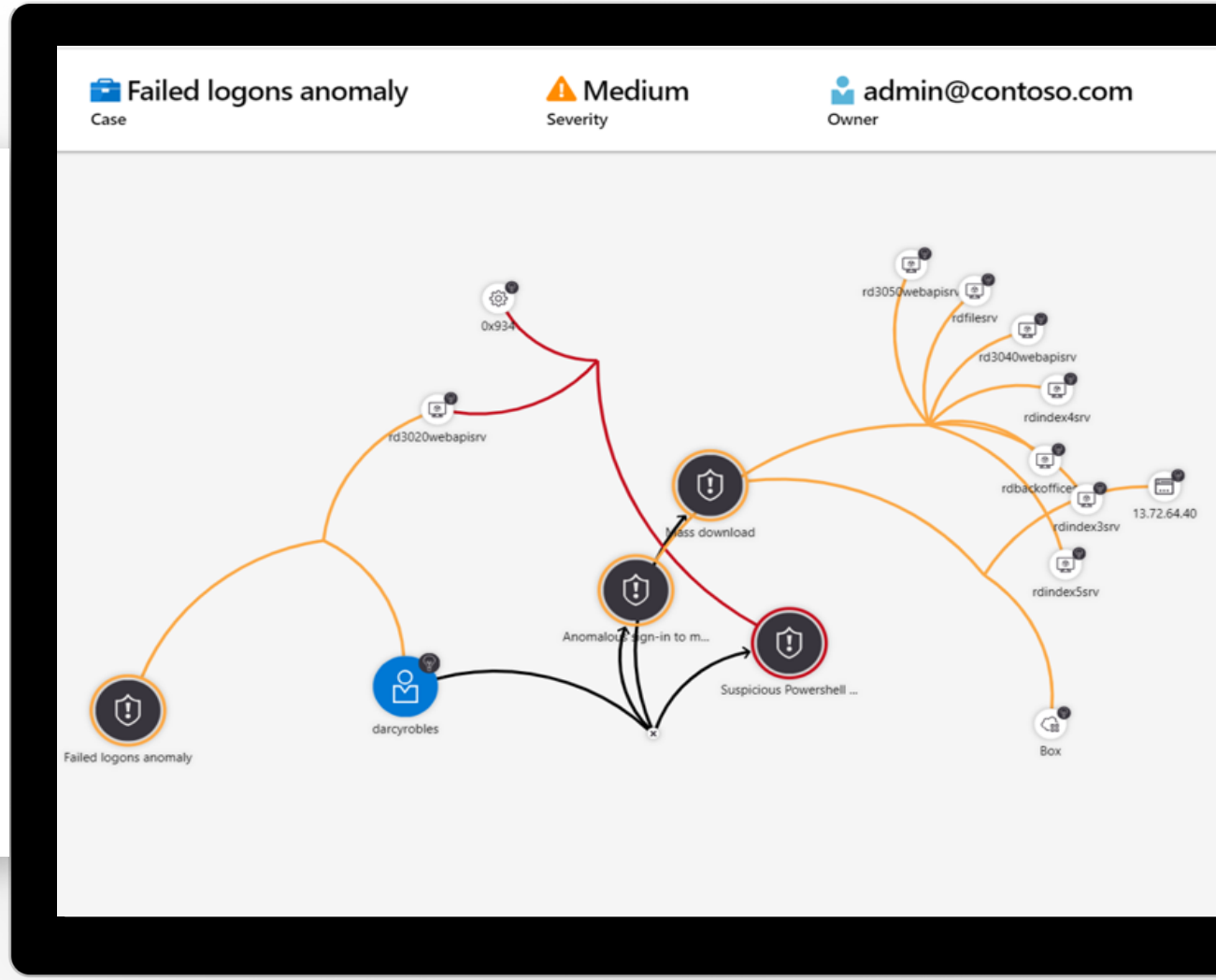


Untersuchen von Bedrohungen mit KI und nachverfolgen von auffälligen Ältivitäten, Verwendung der Microsoft Cybersecurity Arbeit von Jahren

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

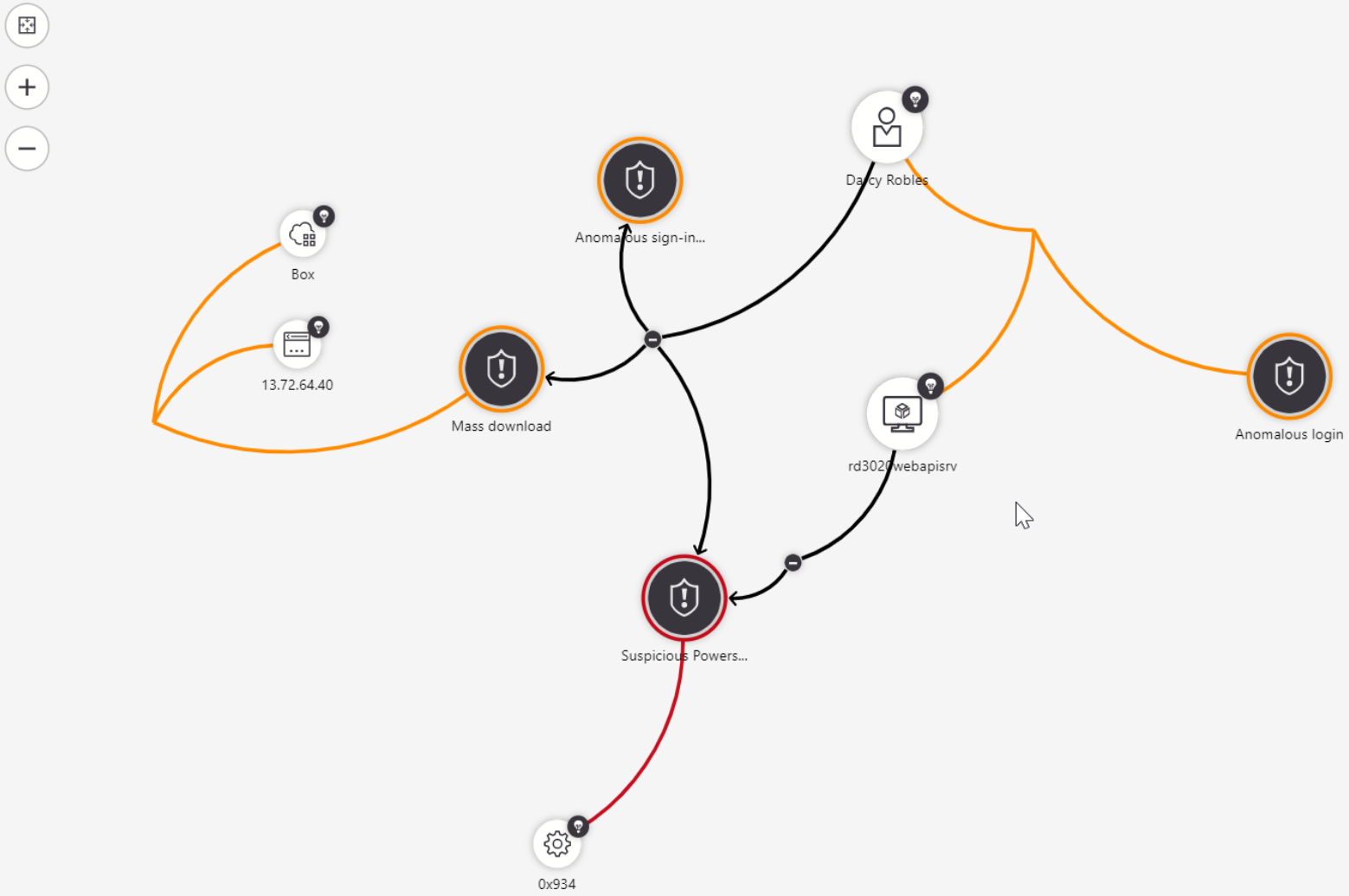
Anomalous login
Case

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 ...

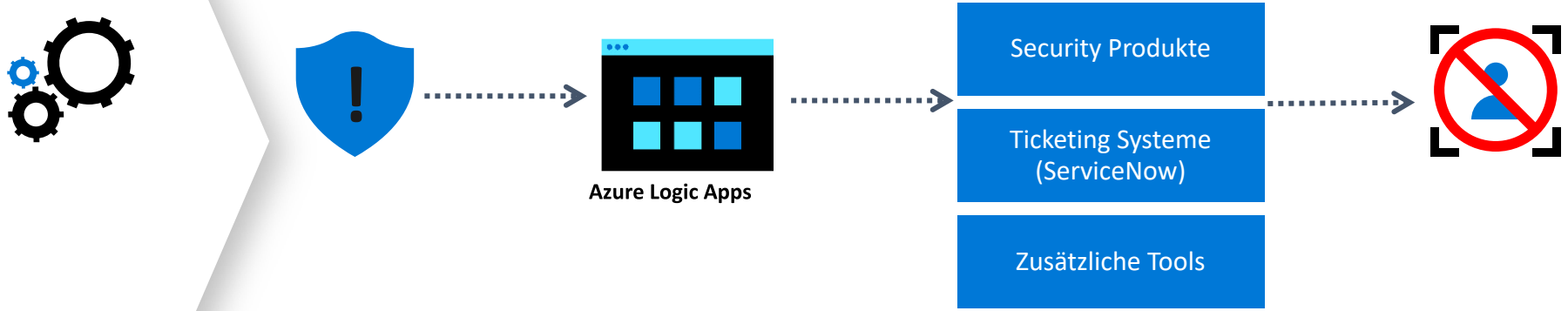
Anomalous sign-in to multiple comp...
3/13/2019, 1:51:00 PM
Account sign-in activity indicates numerous sign-ins to mu...

Mass download
3/13/2019, 2:48:00 PM
The user 'Darcy Robles (darcyrobles@contoso.com)' down...

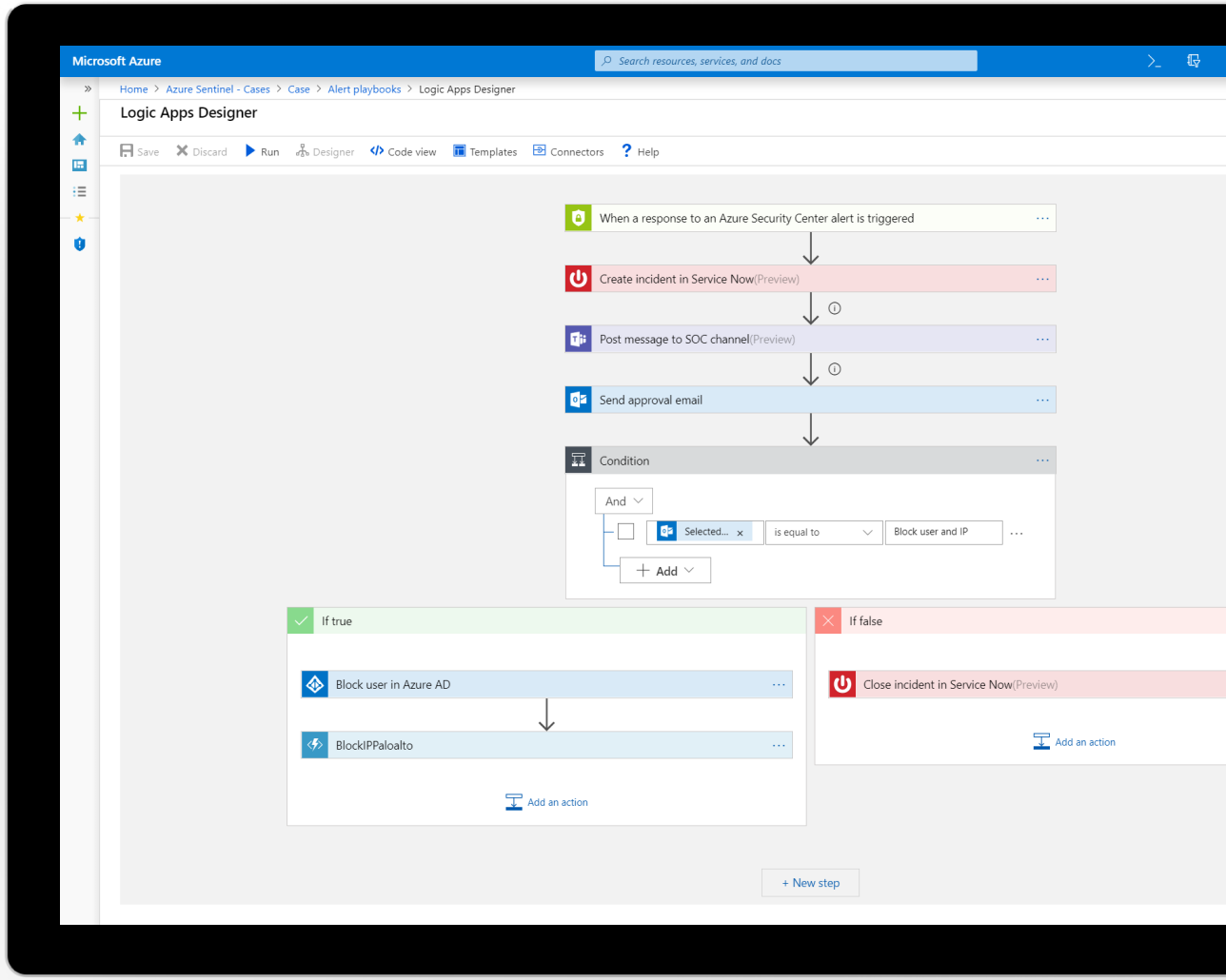
Timeline
Info
Entities

Schnelle Reaktion mit eingebautert Orchestrierung und Automatisierung

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



Orchestrierung von Bedrohungserkennung, Überprüfung und Reaktion



Azure Sentinel - Cases

Selected workspace: 'CyberSecurityDemo' - PREVIEW

Refresh | Last 24 hours

8 OPEN CASES

8 NEW CASES

0 IN PROGRESS

Open Cases By Severity

CRITICAL (0) | HIGH (2) | MEDIUM (5) | LOW (0) | INFORMATIONAL (1)

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

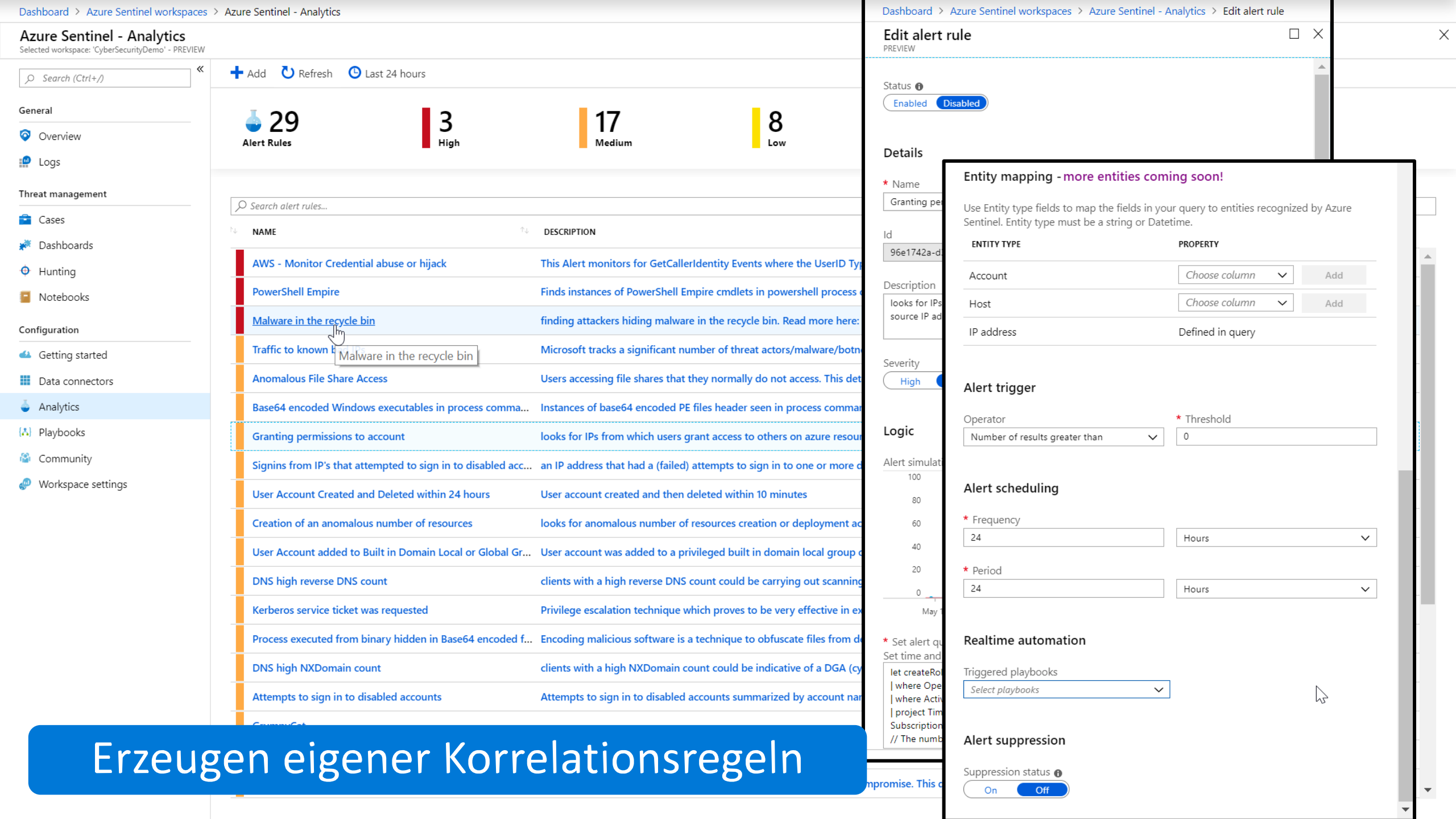
CREATION TIME
03/14/19, 11:32 AM

EVIDENCE
1 Alerts

ENTITIES
1 Account | 1 Host | 0 IP

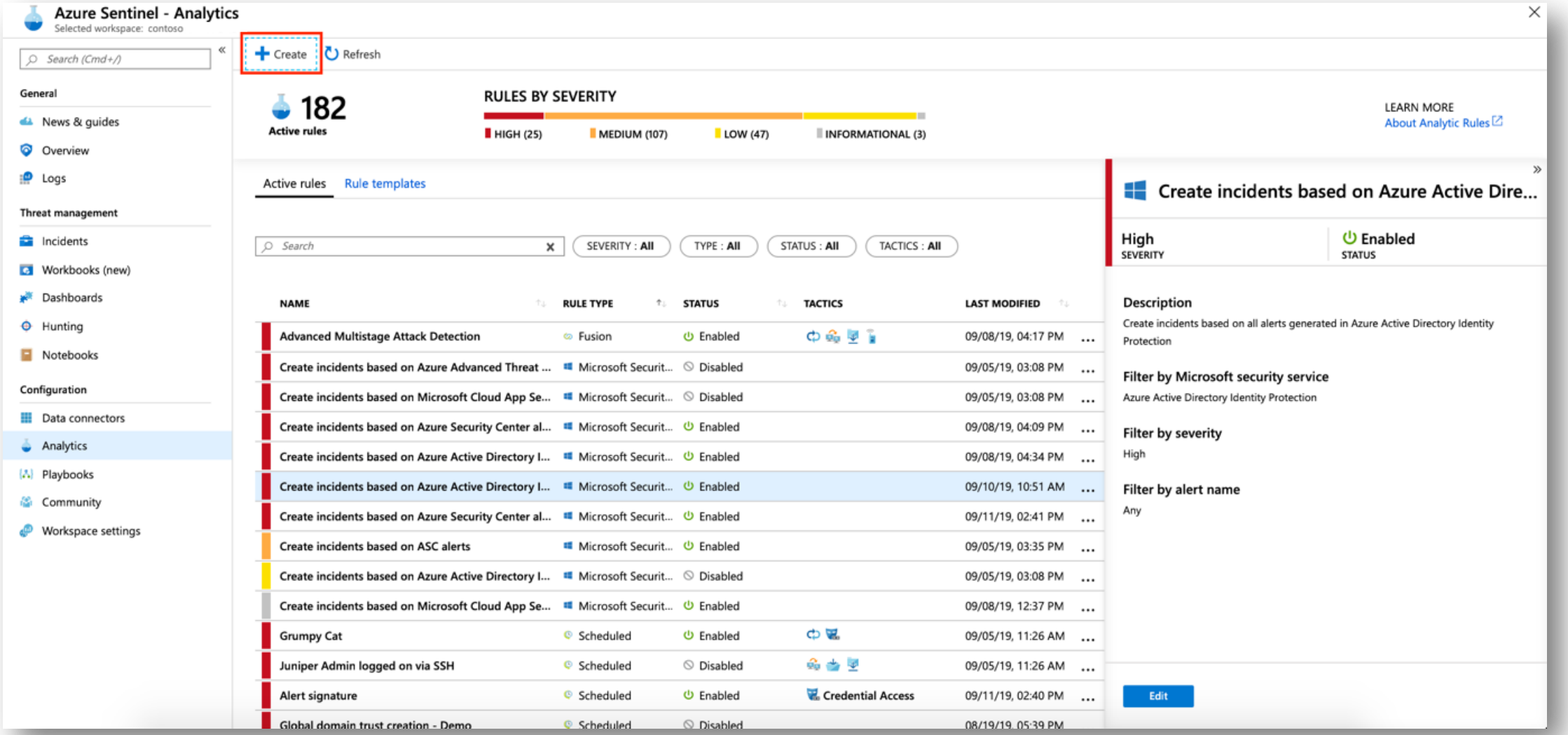
Investigate | View full details

Cases und Meldungen



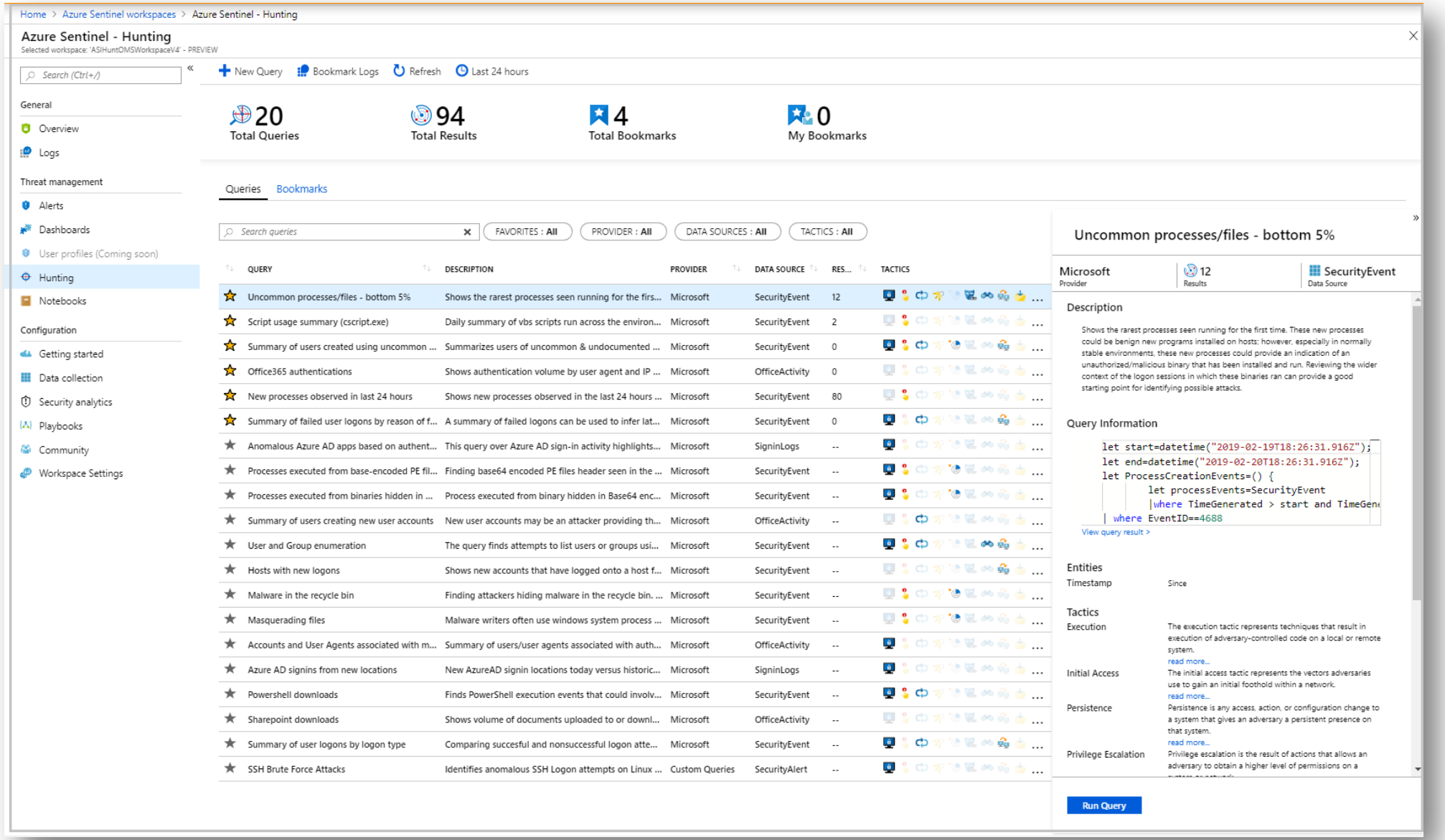
Erzeugen eigener Korrelationsregeln

Automatische Erzeugung von Incidents durch die Integration von Microsoft Security Meldungen



https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts

Threat Hunting



https://docs.microsoft.com/en-us/azure/sentinel/hunting

Übersicht

Collect

Microsoft Services

Apps, users, infrastructure

Public Clouds

Security solutions

Visibility

Dashboard

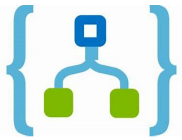
Analyze & Detect

Machine learning, UEBA

Investigate & Hunt

Pre-defined Queries, Azure Notebook

Automate & Orchestrate Response



Playbooks

Enrichment

Data Ingestion

Data Repository

Data Search

Azure Monitor

Integrate

ServiceNow

Other tools

Community

https://aka.ms/AzureSentinel

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

https://azure.microsoft.com/de-de/pricing/details/azure-sentinel/

Jens Lorenz
Strategic Consultant, CISSP, CCSP

fon: +49-170-4516565
mail: jens.lorenz@expertcircle.de

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