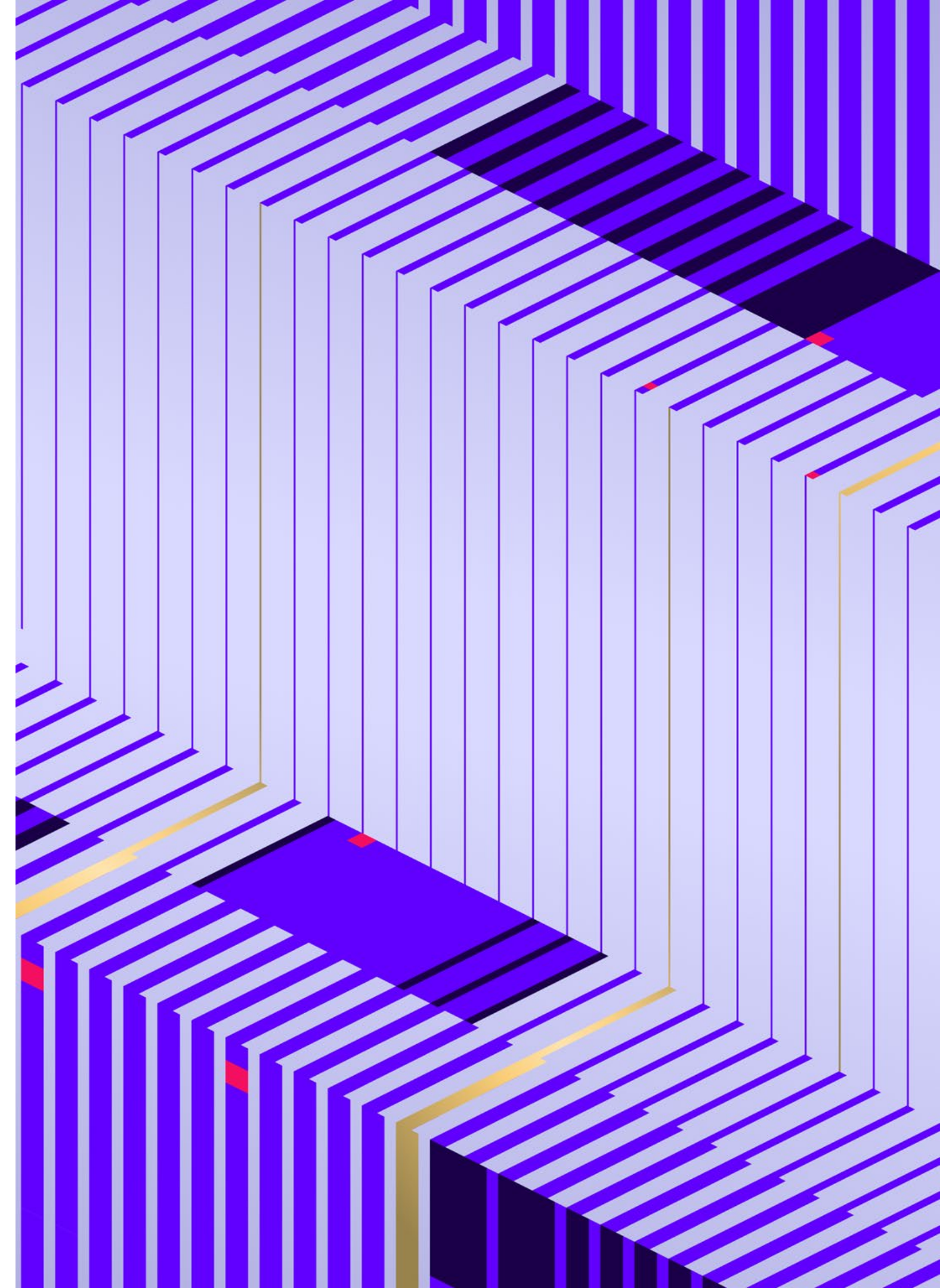




# Security mit KI beherrschbar machen

**Oliver Wenning**  
Regional Sales Manager



# Security Herausforderungen (“Evergreens”)



## Komplexität der Security Umgebung

---

Sicherheitsteams müssen Warnungen in vielen voneinander isolierten Tools hinweg manuell untersuchen und darauf reagieren



## Attacken mit und auf Identitäten

---

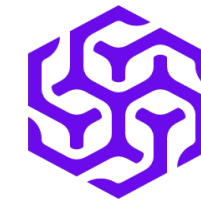
Missbrauch von Zugangsdaten und Angriffe auf die Infrastruktur als primärer Angriffsvektor



## Bedrohungen der Cloud Infrastruktur

---

Public- und Private- Cloud-Umgebungen sind zunehmend attraktive Ziele für Angreifer



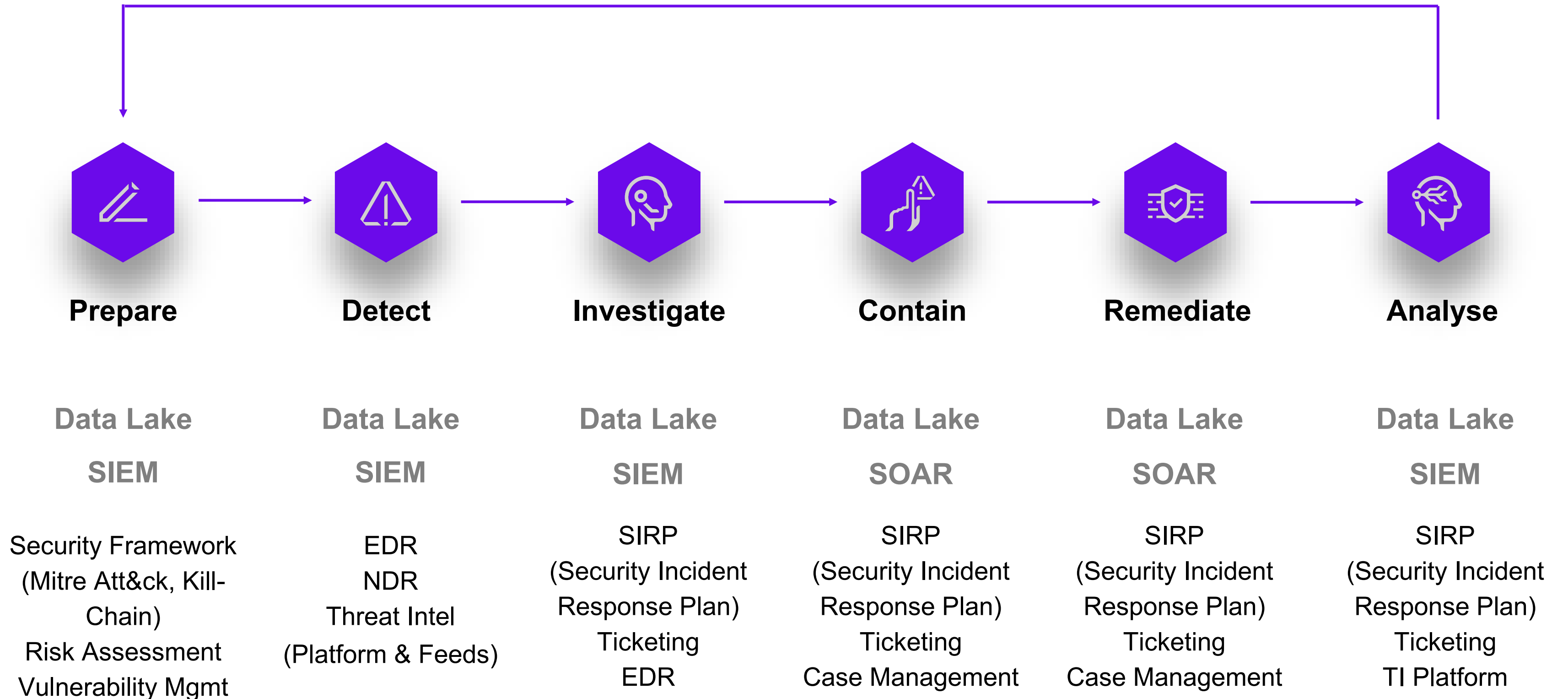
## Security ist ein Datenproblem

---

Eine Masse von verschiedenen Daten muss erfasst und miteinander korreliert werden, um sinnvolle Entscheidungen treffen zu können

# Warum ist eine Security Plattform sinnvoll?

Lernen, Anpassen & Verbessern



# KI in der Security - Definitionen

---

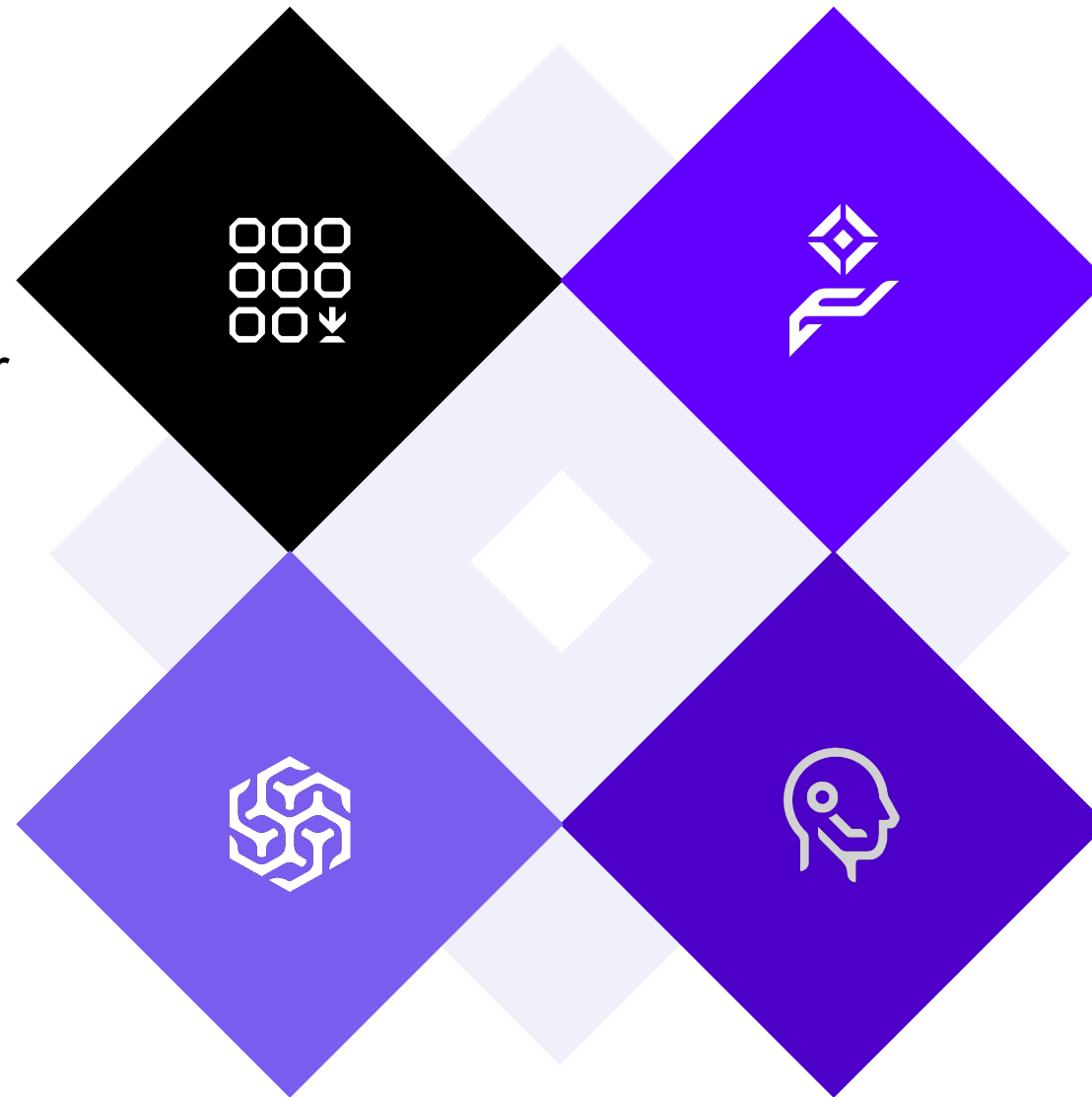
## Machine Learning

Ein Bereich der KI, bei dem Algorithmen aus Daten **lernen**, um **Vorhersagen** oder **Entscheidungen** zu **treffen**, ohne dabei explizit programmiert zu sein

---

## Large Language Module (LLM)

Große KI-Modelle, die menschliche **Sprache verstehen und generieren** können



---

## Generative KI

Modelle, die **neue Inhalte** wie Texte, Bilder oder Musik basierend auf gelernten Mustern **erstellen** können

---

## Agentische KI

Modelle, die **autonom handeln**, Ziele verfolgen, Schritte planen, Entscheidungen treffen und **Aufgaben eigenständig** über längere Zeiträume **ausführen**

# Wie kann uns KI helfen?



Entscheidungen treffen

(Hund oder Hähnchen)



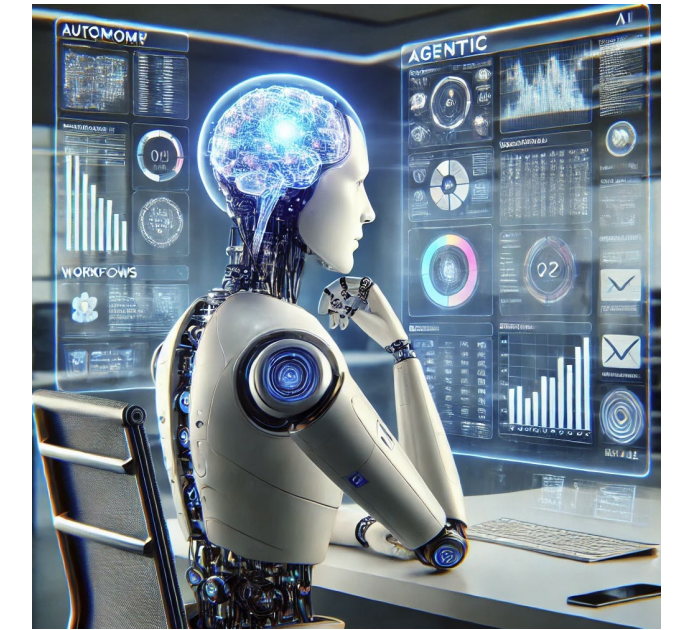
Finden, Beschreiben,  
Bewerten von großen  
Datenmengen

(ChatGPT)



(neue) DINGE erstellen

(deepfake Pope Francis)



Ziele verfolgen, Planen,  
autonom Aufgaben über  
mehrere Schritte hinweg  
ausführen

(booking.com)

# Singularity Platform



Purple AI

HYPERAUTOMATION

SECURITY OPERATIONS  
Singularity AI SIEM



DATA LAKE



Gartner  
A LEADER

**ENDPOINT**  
Singularity Endpoint

**CLOUD**  
Singularity Cloud Security

#1 IN G2



CROWDSTRIKE FALCON

WIZ WIZ (CODE, CLOUD, DEFEND)

MICROSOFT DEFENDER

PRISMA CLOUD

DATA INGEST

**IDENTITY**  
Singularity Identity

**EMAIL**

**NETWORK**  
CISCO

**UNSTRUCTURED DATA & LOGS**

# SentinelOne: KI Evolution

**Singularity** Platform  
Solving the Data Problem

**EDR**  
Solving the Breach

Analytics & Automation

Business Resilience

**NGAV**  
Solving the AV Problem

Detect & Respond  
Recover Faster

 **Purple**<sup>ai</sup>

Prevent  
Reduce Device Impact

Device Focused

Incident Focused

Outcome Focused

# SentinelOne: KI Evolution

**Singularity Platform**  
Solving the Data Problem

**EDR**  
Solving the Breach

Analytics & Automation  
Business Resilience

**NGAV**  
Solving the AV Problem

Detect & Respond  
Recover Faster

Prevent  
Reduce Device Impact

Device Focused

Incident Focused

Outcome Focused

# SentinelOne: KI Evolution

Singularity Platform  
Solving the Data Problem

**EDR**

Solving the Breach

Analytics & Automation

Business Resilience

**NGAV**

Solving the AV Problem

Detect & Respond

Recover Faster

Prevent

Reduce Device Impact

Device Focused

Incident Focused

Outcome Focused

# SentinelOne: KI Evolution

**Singularity** Platform  
Solving the Data Problem

**EDR**  
Solving the Breach

**Analytics & Automation**

**Business Resilience**

**NGAV**  
Solving the AV Problem

**Detect & Respond**  
Recover Faster

 **Purple**<sup>ai</sup>

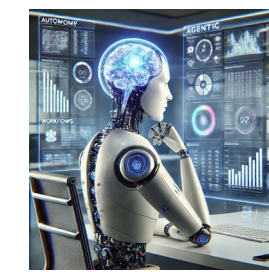
**Prevent**  
Reduce Device Impact

Device Focused

Incident Focused

Outcome Focused

# Singularity Platform



Purple AI

HYPERAUTOMATION

SECURITY OPERATIONS  
Singularity AI SIEM



DATA LAKE



Gartner  
A LEADER

ENDPOINT  
Singularity Endpoint

CLOUD  
Singularity Cloud Security

#1 IN G2



CROWDSTRIKE FALCON

WIZ WIZ (CODE, CLOUD, DEFEND)

MICROSOFT DEFENDER

PRISMA CLOUD

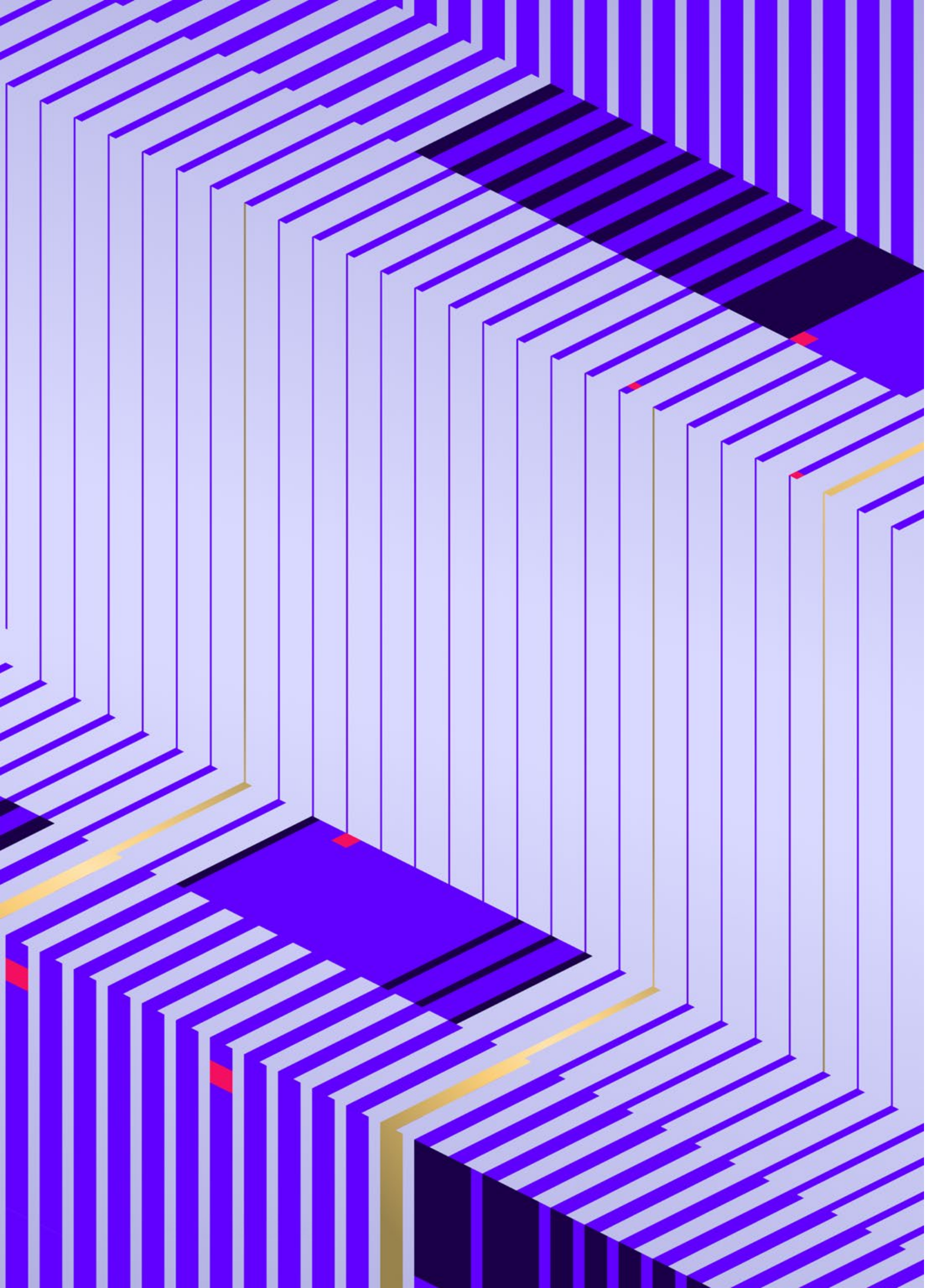
DATA INGEST

IDENTITY  
Singularity Identity

EMAIL

NETWORK  
CISCO

UNSTRUCTURED DATA & LOGS



**Danke.**

[Sentinelone.com](https://Sentinelone.com)