Die Rolle von KI in der modernen Cyber Abwehr

Chancen und Herausforderungen

Bastian Schmederer
Sales Manager Healthcare | Palo Alto Networks

Krankenhaus-IT JOURNAL

Die Rolle von KI in der modernen Cyber Abwehr

Teil I: *Schutz “vor” der KI*

paloalto NETWORKS

KI Nutzung erhöht die Produktivität unserer Mitarbeiter

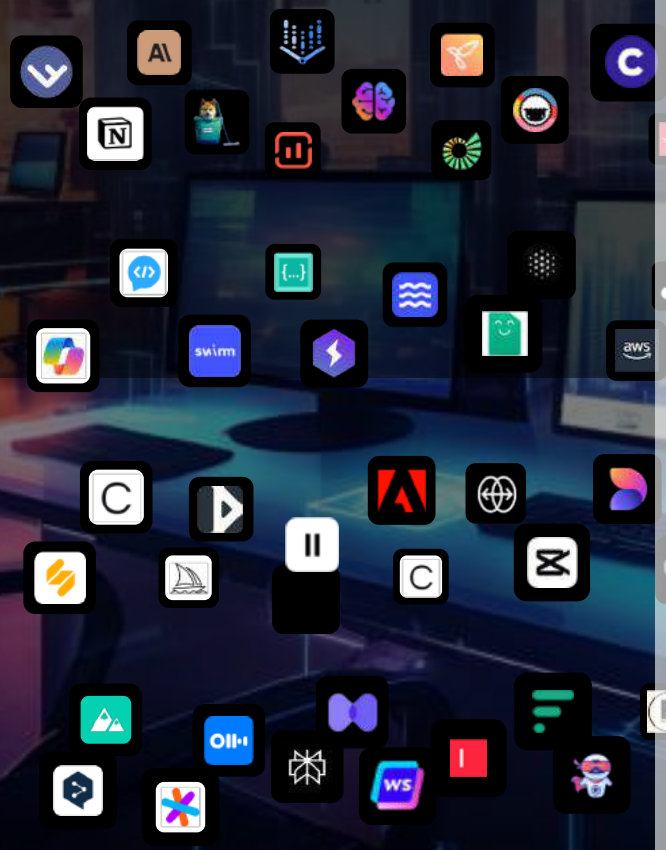
Conversational Chats

Code Assistants & Generators

Video & Image Generators

Writing Assistants

And **more...**



Native KI Apps auf dem Vormarsch

12,000+

Prognose für KI Apps bis **2030**.

Source: Pitchbook's Generative AI Emerging Space, Artificial Intelligence & Machine Learning Analyst Curated Vertical and SaaS Vertical

paloalto NETWORKS | PRISMA

Mit dem Anstieg der KI Nutzung, steigen auch die Sicherheitsrisiken

55%

…der Mitarbeiter nutzen **nicht freigegebene GenAI Tools** bei ihrer Arbeit.

Shadow AI apps
create security blind spots.

Sensitive data loss
stems from uninspected GenAI prompts and responses.

Malicious content
from GenAI responses poses risk to users.

CYBER SECURITY HUB

IOTW: Samsung employees allegedly leak proprietary information via ChatGPT

Three separate employees have allegedly leaked information to the AI chatbot

SC Media

US House forbids staff members from using AI chatbot Microsoft Copilot

House Office of Cybersecurity has deemed Microsoft Copilot a risk to users because of the threat of leaking House data to non-House approved cloud services.

siliconANGLE

Microsoft accidentally exposes 38TB of internal data via GitHub repository

38 terabytes of internal data, including passwords, publicly accessible through a GitHub repository that Microsoft's artificial intelligence research group uses

Source: Salesforce 2023

AI Access Security
- sichere Nutzung von KI Apps

Echtzeit-Sichtbarkeit von KI-Nutzung

View what AI apps are used and by whom.

Access control

Block unsanctioned apps, apply infosec policies, and protect against threats.

Comprehensive data protection

Scan what data, secrets, and IP are shared.

Krankenhaus-IT JOURNAL

Die Rolle von KI in der modernen Cyber Abwehr

Teil II: *Mehr Schutz “durch” KI*

paloalto NETWORKS

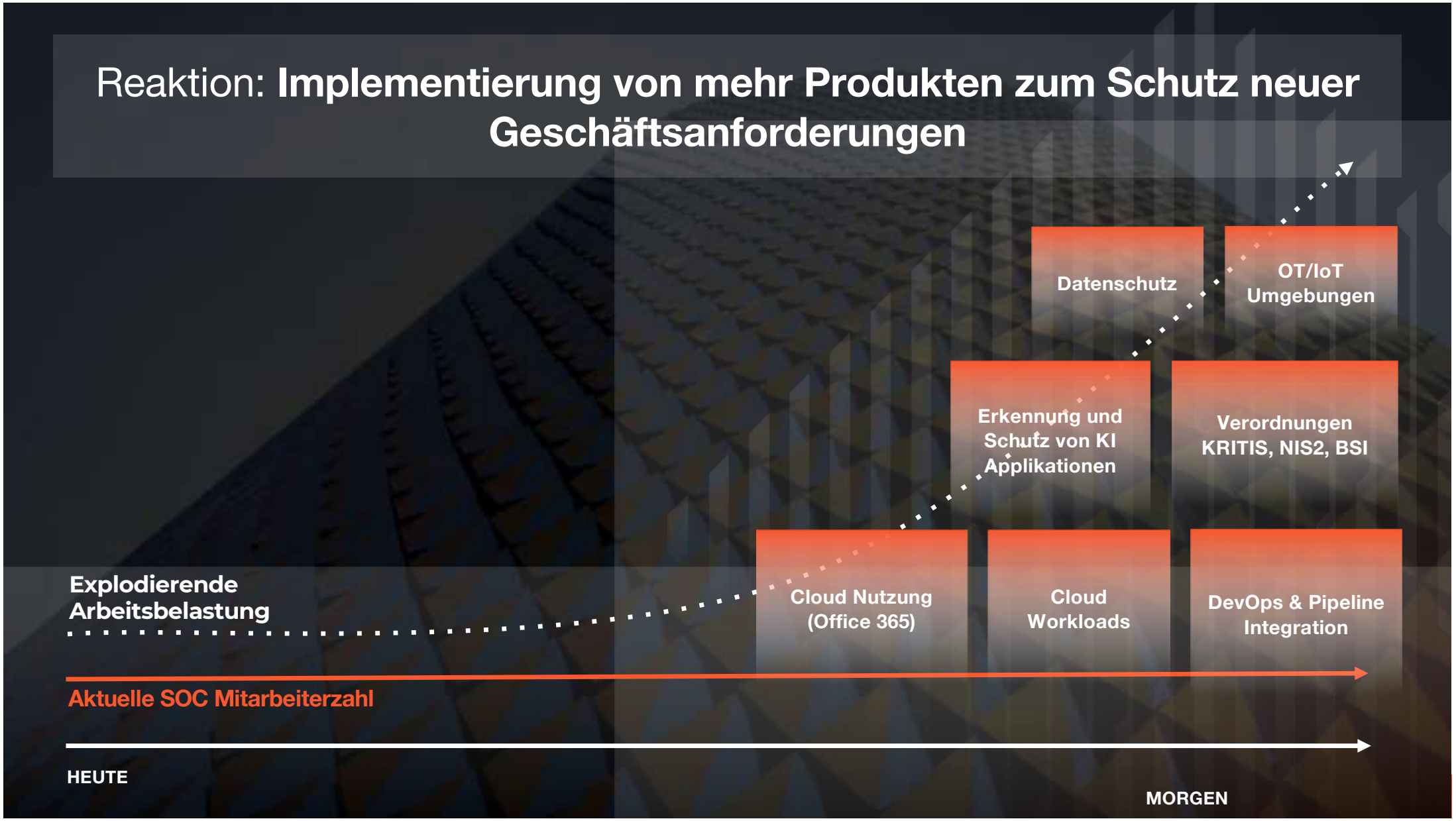
Herausforderung: **Erhöhte Sicherheitsanforderungen durch Digitalisierung und Compliance**

Compliance Anforderungen
KRITIS, NIS 2

Digitale Transformation

paloalto NETWORKS

Reaktion: **Implementierung von mehr Produkten zum Schutz neuer Geschäftsanforderungen**



Problem: **Zu viele Tools, Zu viele Silos, Zu viele Alarme und zu wenig geschultes Personal**

Viele Tools in Silos

Viel manuelle Arbeit

Falsches Sicherheitsgefühl
(es passiert ja so viel)

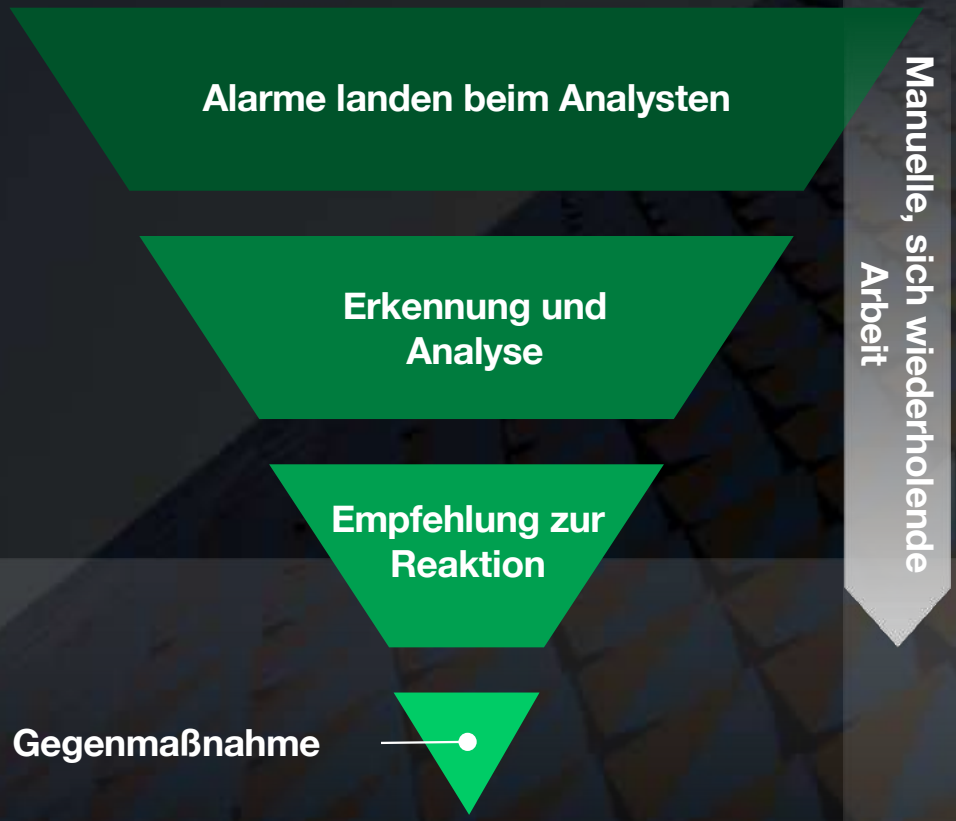
Im Durchschnitt **11k** Alarme pro Tag, über **30%** bleiben unberührt

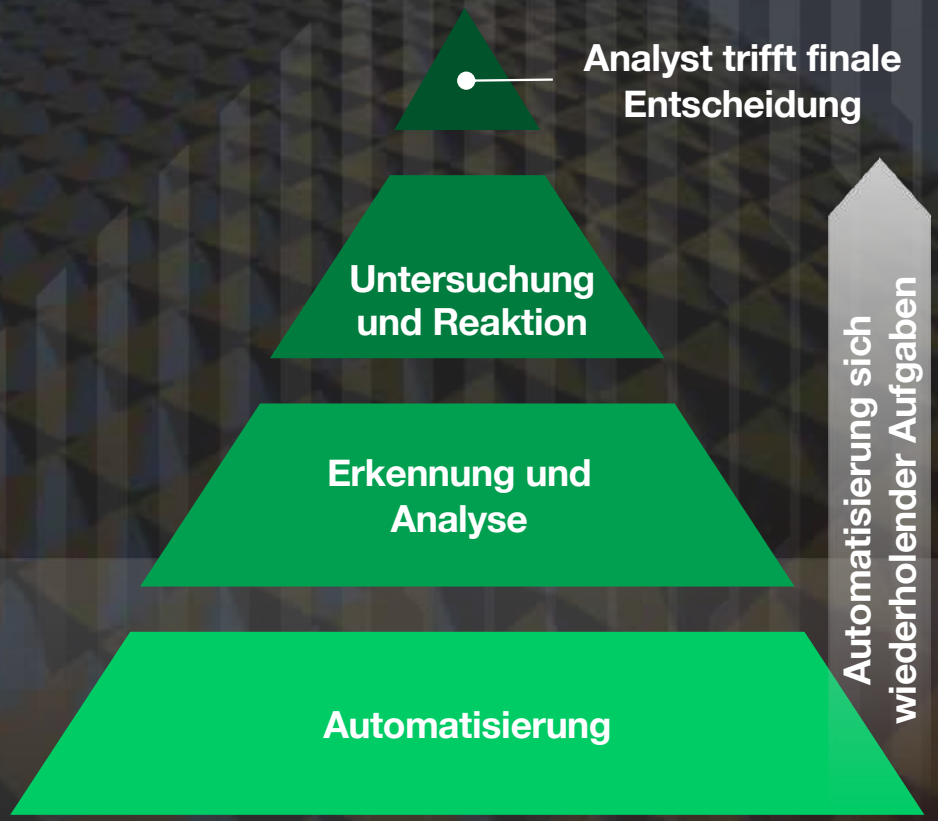
paloalto NETWORKS

Künstliche Intelligenz (KI) sinnvoll nutzen

Mensch + KI = Perfektes Team

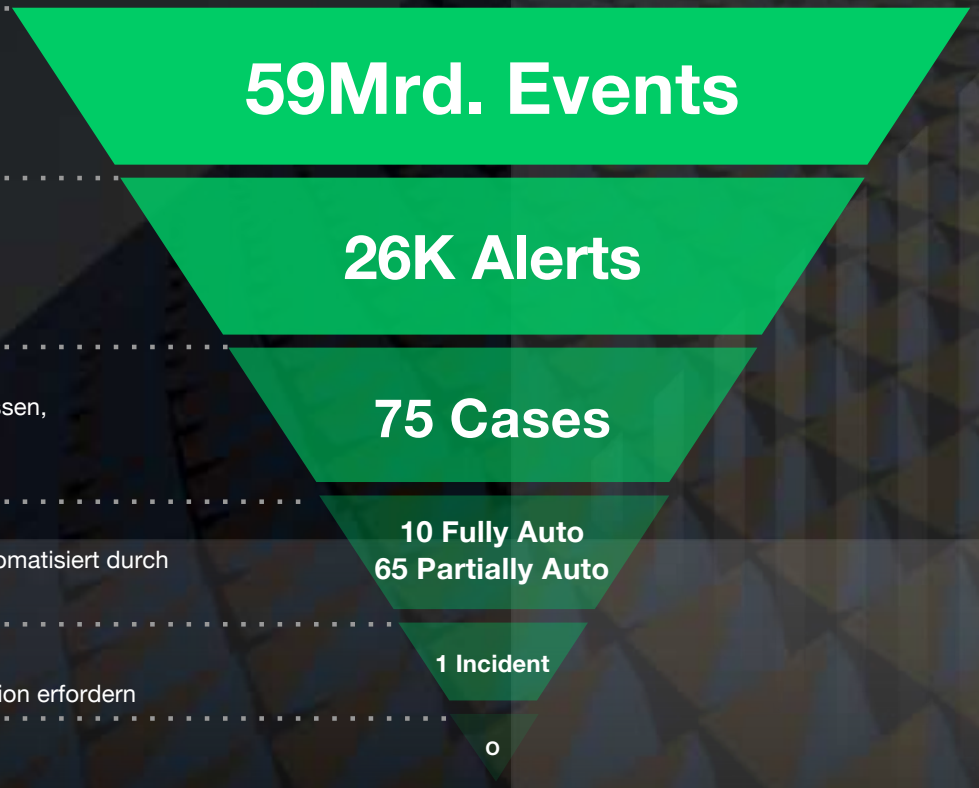
Perspektive ändern: **KI zur automatisierten Abarbeitung wiederkehrender Aufgaben im SOC Prozess**





paloalto NETWORKS

Ein Tag im SOC von Palo Alto Networks



Log Events
Beinhaltet alle Log Events, die in XSIAM aufgenommen wurden

Raw Alerts
Nach KI-gesteuerter Datenanalyse durch XSIAM

Alerts
Nach Gruppierung, Ausschlüssen, Deduplizierung durch XSIAM

Analysis
Vollständig oder teilweise automatisiert durch Playbooks

Incidents
Alle Alarme, die eine SOC-Aktion erfordern

Major Incidents

7
Minuten
Mean Time to Detect

1
MINUTE
Mean Time to Respond
(Hohe Priorität)

65
FTE
Plattform Effizienz durch Automatisierung
(pro Jahr)

paloalto NETWORKS

paloalto NETWORKS

Krankenhaus-IT JOURNAL

Vielen Dank

paloaltonetworks.com

Bastian Schmederer
0160 / 9630 9328

Halle 3.2, E-108-a