



Ersetzt die KI
den Security Experten?



Was geht Ihnen durch den Kopf, wenn Sie hören:
“Ersetzt die KI den Security-Experten?”



WWW.MENTI.COM

2116 8190



WWW.MENTI.COM/ALX4CTOSPUX5

EINSATZ VON KI-ARTEN IN DER CYBERSECURITY



Aus Daten lernen und Vorhersagen treffen

- Potentielle Bedrohungen zu Geräte, Benutzer, Netzwerke erkennen und reagieren



Komplexe Datenstrukturen Big-Data analysieren

- Komplexe Bedrohungen erkennen und reagieren



Interaktionen in natürlicher Sprache

- Berichte erstellen
- Sicherheitsergebnisse zusammenfassen
- Untersuchung und Reaktion



Führt Security Aufgaben selbst aus

- Alarne triagieren
- Datenverlust verhindern (Insider Risiko)
- Optimieren von bedingten Zugriffen (Richtlinien)

KI IN DER CYBERRISIKO PROGNOSSE UND PRIORISIERUNG



SEQiFY

Menü verkleinern

Home

Risk Management

- Dashboard
- Risiko-Einblicke
- OS Einblicke
- MDM Einblicke
- Top
- Berichte
- Benchmark
- App Einblicke
- Integration Insights
- Key Insights
- Identity Insights

Compliance Management

- Compliance Insights
- Akzeptiertes Risiko
- SupplyChain Insights

Tenant: Test LLC

Endpoints: All

UPGRADE NOW

DAY MONTH YEAR

RISIKO-INDIKATOR

9.47

Risikoprognose und Priorisierung

ALLE EXPLOITS	KRITISCHE GERÄTE
3426	1827

HOCHRISIKO GERÄTE	MODERATE GERÄTE
1861	460

KRITISCHE APPS
55

User Insights

ACTIVE USERS	GHOST USER	AFFECTED CONNECTORS	ALL USERS
22	528	7	550

RISIKO-MONITOR

Geräte insgesamt ▾ Letzte 30 Tage ▾

4000
3000
2000

RISK GAME CHANGER

Critical Issues	
CVE-2015-0313	179 Devices 4%
ch-internet-new	151 Issue 3%

CHAT

DAS NEUE KI CYBERRISIKO

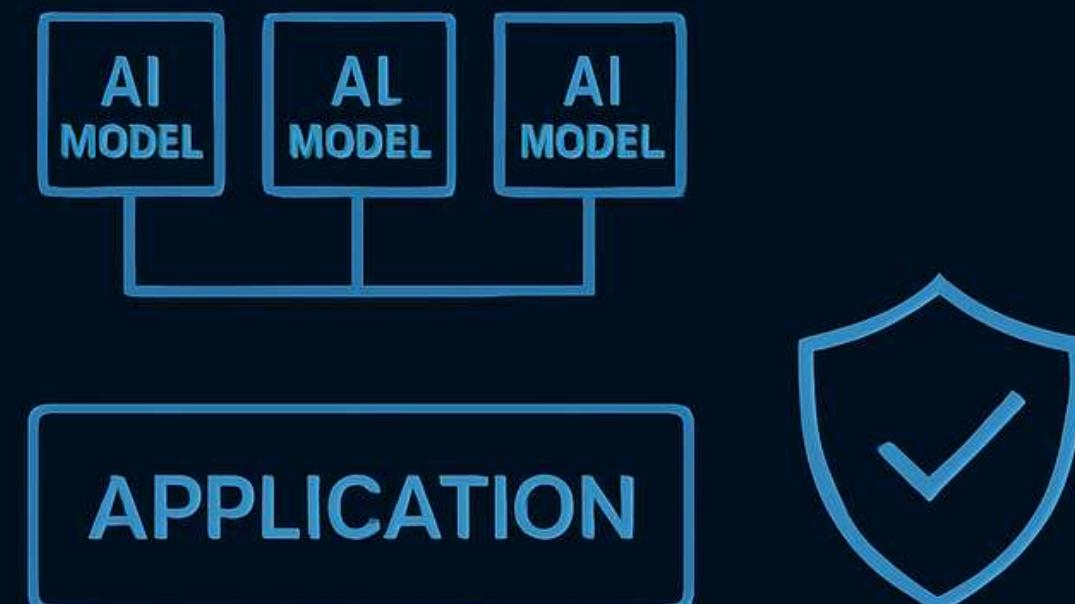


CYBERSECURITY + KI



Security Tools für
Angreifer und Verteidiger

KI SECURITY



APPLICATION

Security zu KI Apps für
Unternehmen und Nutzer

KI für die Cybersecurity



ANWENDUNG: KI IN DER CYBERSECURITY



- Anomalien bei Anmeldungen
- Zwei-Faktor-Authentifizierung
- Kompromitierte Konten



- Prozesse beschleunigen
- Vertrauliche Daten kennzeichnen
- Datenabfluss blockieren, melden



- Erweiterte Threat Intelligence
- Angriffe blockieren
- Schnellere Security Event auswerten



- Bedrohungen reagieren
- Verborgende Angriffsmuster entdecken

- Cyberangriff entdecken
- Vereinfachte Berichterstellung
- Reduktion Falsch Positiver

- Security Experten entlasten
- Korrelation von Volumsdaten
- Gen AI verinfacht Untersuchung durch natürliche Fragen



EINSATZ VON KI IN DER CYBERSECURITY



Effektiver durch KI

Erweiterung der Kompetenzen

Skalierbarkeit

KI: automatisiert Aufgaben, verarbeitet große Datenmengen in Echtzeit und lernt kontinuierlich.

KI stellt in der zunehmenden Komplexität von Cyberbedrohungen sicher, dass Cybersicherheitssysteme resilenter werden.

DAS KI MINDSET EINES SECURITY HERSTELLERS



Nicht die Technologie ist der Startpunkt – sondern
“Where is the customer value?”

Safety by Design – Drei zentrale Prinzipien:



1. Minimierung der Interaktionen
zwischen Nutzer & KI-Modell
weniger Angriffsfläche, mehr Kontrolle



2. Isolierung der Daten
Schutz sensibler Unternehmensdaten



3. Datensicherheit bei Foundation Models
Sicherstellen, dass keine Unternehmensdaten zum
Training genutzt werden

Warum ist das relevant?

- **Vermeidung von Datenlecks** durch Dritte (z.B. via Prompt Injection)
- **Reduktion von Halluzinationen** durch kontrollierte Promterstellung (maintain the prompts)
- **Vertrauen durch Kontrolle**: Unternehmen behalten ihre Datenhoheit



INTEGRATION VON KI IN CYBERSECURITY LÖSUNGEN

The screenshot shows a software interface for cybersecurity monitoring. The left sidebar includes sections like 'Start', 'UMGEBUNG', 'Geräte', 'Cloud', 'Netzwerk', 'Gerätesicherheitsstatus', 'Gefährdung', 'Identitäten', 'Patchverwaltung', 'Software-Reputation', 'EREIGNISSE' (selected), 'Sicherheitereignisse', 'Broad Context Detections' (selected), 'Reaktion', 'SICHERHEITSKONFIGURATION', 'Berichte', 'VERWALTUNG', 'Sicherheitsservices', 'Support', and 'COLLABORATION PROTECTION'. The main panel displays a 'Broad Context Detection' entry with ID 183720731-4549, categorized as 'Lateral Movement'. It shows a timeline from 21.05.2025 16:16:32 UTC-03:00 to 21.05.2025 16:57:59 UTC-03:00. The interface includes tabs for 'Zusammenfassung', 'Prozessstruktur', 'Zeitleiste', 'Analyse', 'Gerätedetails', 'Kommentare', and 'Protokoll'. A summary table lists three detections: 'Erkennung 2/4: Https connection to non standard port' (Info, 21.05.2025 16:11:09 UTC-03:00), 'Erkennung 3/4: Http connection by rundll32.exe' (Info, 21.05.2025 16:11:09 UTC-03:00), and 'Erkennung 4/4: Rundll32 no arguments making netconn' (Kritisch, 21.05.2025 16:11:09 UTC-03:00). The 'Details' section provides a description of the rundll32.exe process and its network connections. The 'Aktivitätskontext' section shows a network connection between Desktop01 and 10.99.1.77.

WithSecure: Security Events and Broad Context Detections™

GenAI analysiert

- komplexe Security Information
- stellt die Zusammenfassung
- in **natürlicher Sprache** bereit.

„Es unterstützt IT-Teams, indem es Anwendern **jeglicher Erfahrungsstufe** hilft, den Kontext und die Auswirkungen von BCDs **besser** zu verstehen, so dass sie sich auf das Wesentliche konzentrieren können.“

SECURITY SUMMARY IN LANDESSPRACHE DES USERS



European Operations
WithElements Inc

Events / Security Events

We're eager to get your feedback.

Security Events

+ Generate summary

Stars symbol stands for LLM generated content

You can export Security Events to MS Excel. See the guide in the community

Select field Equals Select value

456 events

Time	Severity	Source	Target
23 minutes ago May 22, 2024, 12:29:07	! Action needed	EDR	ADServer
23 minutes ago May 22, 2024, 12:29:07	! Action needed	EDR	Desktop0
23 minutes ago May 22, 2024, 12:29:07	Information	EDR	Desktop0
23 minutes ago May 22, 2024, 12:29:07	Information	EDR	Server
23 minutes ago May 22, 2024, 12:29:05	Action needed	EDR	Desktop0
23 minutes ago May 22, 2024, 12:29:05	Action needed	EDR	Desktop0
23 minutes ago May 22, 2024, 12:29:04	Action needed	EDR	ADServer
23 minutes ago May 22, 2024, 12:29:02	Action needed	EDR	ADServer
24 minutes ago May 22, 2024, 12:27:56	Attention	File scanning Real-time scanning	ADServer
25 minutes ago May 22, 2024, 12:27:29	Action needed	System Events	ADServer
25 minutes ago May 22, 2024, 12:27:20	Attention	File scanning Real-time scanning	Desktop0
4 hours ago		Collaboration	

Kontrolle der Ergebnisse durch nachvollziehbare Quellangaben.

Security events summary

Please note that this summary is AI generated and should be treated with caution. Further investigation and professional consultation may be required to fully address all threats.

Below is a summary of security events for the company WithElements Inc generated on May 22, 2024, for the measurement period between May 15, 2024 to May 22, 2024 with 3 devices and 116 total events.

- On 2024-05-20, the edr engine detected a severe lateral movement incident with the ID 183720731-1037 on device DESKTOP01.

Recommendation: Analyze the incident and update the resolution. If help is needed, the incident can be elevated to WithSecure for further analysis.

- Between 2024-05-17 and 2024-05-20, the DeepGuard engine blocked several rare applications on devices DESKTOP01, Desktop03, and ADServer. The blocked applications include Tr-DGg.exe, DG_Malware.exe, Tr-DGr.exe, Malicious_DG.exe, DemoMalware1.exe, DG_TEST_Tr-DGr.exe, MaliciousFile.exe, and WINWORD.EXE.

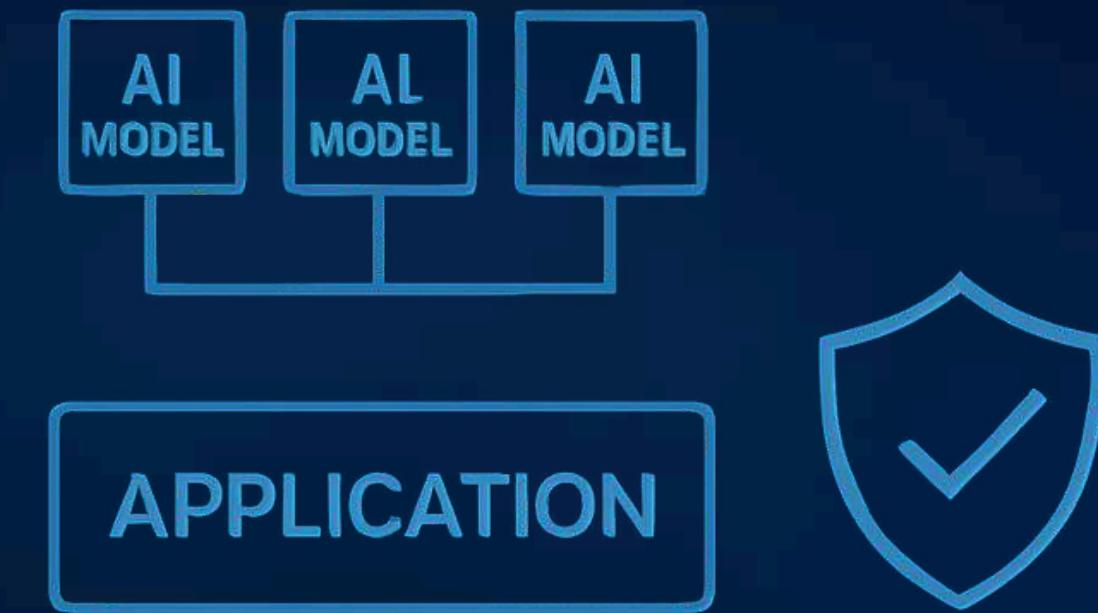
Recommendation: Analyze the processes that triggered the DeepGuard detections. If necessary, create exclusions in the device profiles.

- On 2024-05-15 and 2024-05-16, the systemEventsLog engine reported events on device ADServer.
- Between 2024-05-15 and 2024-05-16, the fileScanning engine quarantined the EICAR_Test_File on devices ADServer and DESKTOP01. On 2024-05-16, the fileScanning engine also quarantined a file identified as Heuristic.HEUR/Macro.Agent on device DESKTOP01.
- On 2024-05-17, the fileScanning engine blocked two files identified as PotentiallyUnwanted:W32/App.b283067a37!Online on device DESKTOP01.
- On 2024-05-21, the fileScanning engine blocked a file identified as PotentiallyUnwanted:W32/App.b283067a37!Online on device Desktop03. The applicationControl engine also blocked a rule named "Test SHA256 block" on the same device.
- On 2024-05-16 and 2024-05-22, the collaborationProtectionEmailScan engine detected events categorized as "harmfulContent".

Executive Summary: The report highlights several security events detected by various security engines on different devices. The edr engine detected a severe lateral movement incident on device DESKTOP01. The DeepGuard engine blocked several rare applications on devices DESKTOP01, Desktop03, and ADServer. The fileScanning engine quarantined or blocked potentially unwanted files on devices ADServer, DESKTOP01, and Desktop03. The collaborationProtectionEmailScan engine also detected events categorized as "harmfulContent". Overall, the report indicates that multiple security engines have been actively monitoring and responding to various security events across the organization's devices.

Close

Security für die KI



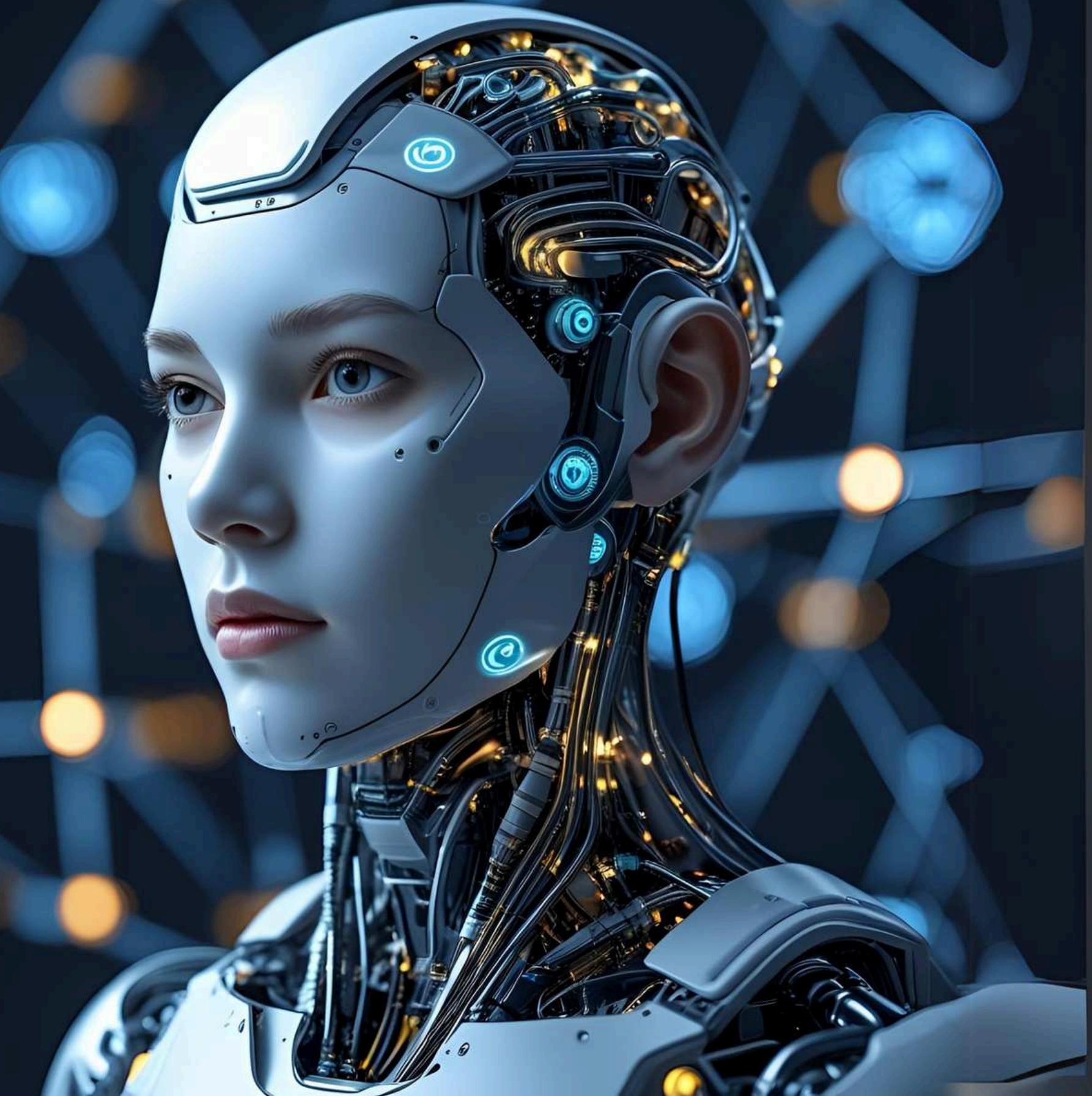
DIE KI HAT DIE WELT VERÄNDERT

KI FÜR ALLE

SUPER KI

2022 ChatGPT
Schneller

Macht Dinge
BESSER



DIE KI ERMÖGLICHT EIN NEUES DENKEN IN DER BUSINESS WELT



10X MEHR LEISTUNG DURCH KI IN DER BUSINESS WELT



AI Agents



AI Apps



Roboter



Humanoide



DIE KI BRINGT NEUE RISIKOKLASSEN IN DIE BUSINESS WELT

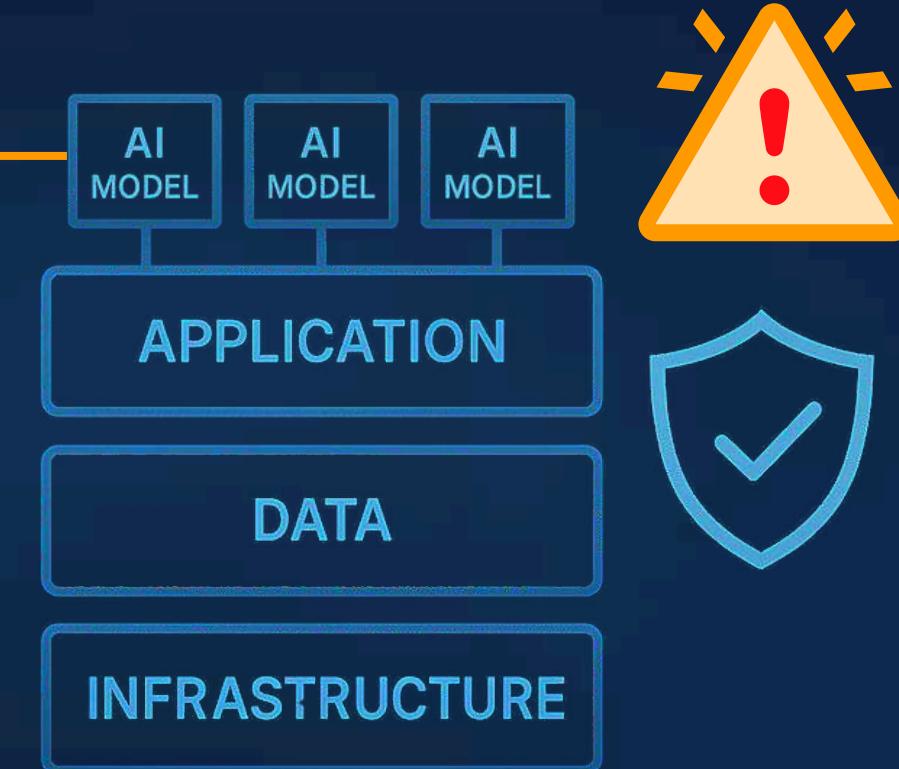


DAS NEUE RISIKO DURCH KI APPS



Modelle haben keine Grenzen
sind also nicht deterministisch

ChatGPT: Gleiche Frage, aber
unterschiedliche Antworten.



KI MODELLE IN KRITISCHEN WORKFLOWS



Sicherheit

z.B. Halluzination

Toxisch

Verharmlosung



Security

z.B. Manipulation von Trainingsdaten

Promt Injection

Datenexfiltration

WIE SCHÜTZEN WIR UNS BEI KI?

HERAUSFORDERUNG: IN HIGH SPEED FÜR SICHERHEIT & SECURITY



Mistral
CoPilot OpenAi



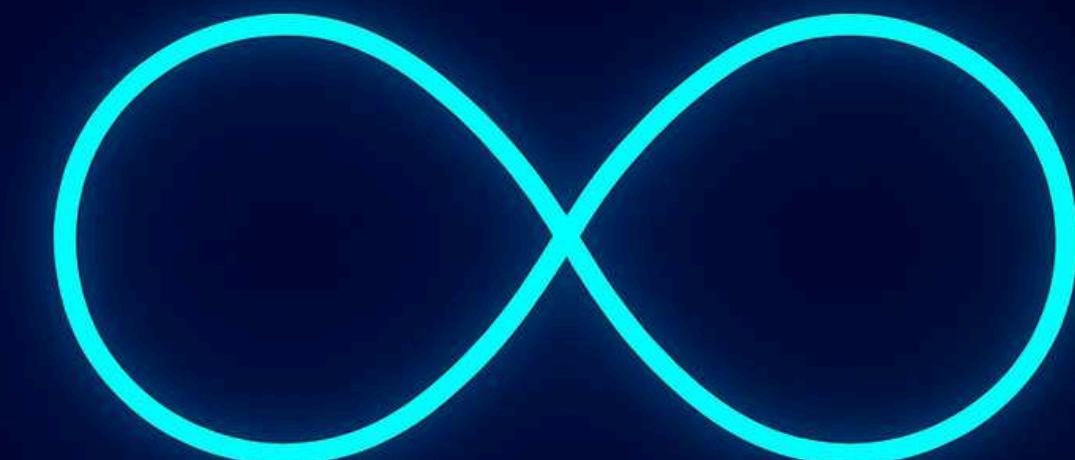
Nutzung
AI Apps

KI Agent
Modell KI App



Entwicklung
AI Apps

Es gibt **keine**
“Vulnerability” Datenbank für KI



AI Algorithm Red Teaming

Es braucht “**Visibility**” für die Nutzung

- Umsetzung von Richtlinien (Compliance)
z.B. Copy/Paste vertrauliche Infos
- Prompt Request und Responses
- im Traffic (z.B. Cisco)

Es braucht “**Visibility**” für die KI Apps

- KI Modell Validierung (Privat, Public Cloud)
- Korridor und Vorschläge



Risikoklassifizierung



Hohes Risiko

Begrenztes Risiko

Minimales Risiko



z.B. Social Scoring

z.B. Bewerbungsprozesse

z.B. Chatbots

z.B. Übersetzungs-KI

COMPLIANCE & KI - DER NEUE ORDNUNGSRAHMEN



BIN ICH BEREIT FÜR KI IN DER SECURITY?

DIE 5 WICHTIGSTEN FRAGEN FÜR ENTSCHEIDER



1. Welche **Sicherheitsdaten** darf ich der KI anvertrauen?
2. Welche **Vorgaben** gelten für den sicheren KI-Einsatz?
3. Wie **kontrolliere** ich KI im Security-Kontext?
4. Wie **betreibe** ich KI sicher & Compliance-konform?
5. Welchen konkreten **Mehrwert** liefert KI – und wo?

CONCLUSIO - KI VERÄNDERT DIE CYBERSECURITY STATUS “HEUTE”



HUMAN
IN THE LOOP



DATEN
SIND ALLES



MÄCHTIGES TOOL ZUR
SKALIERUNG

CONCLUSIO - KI UND SECURITY EXPERTEN “NEXT STEP”



KI INTEGRIERT IN ALLEN
SERVICES & LÖSUNGEN



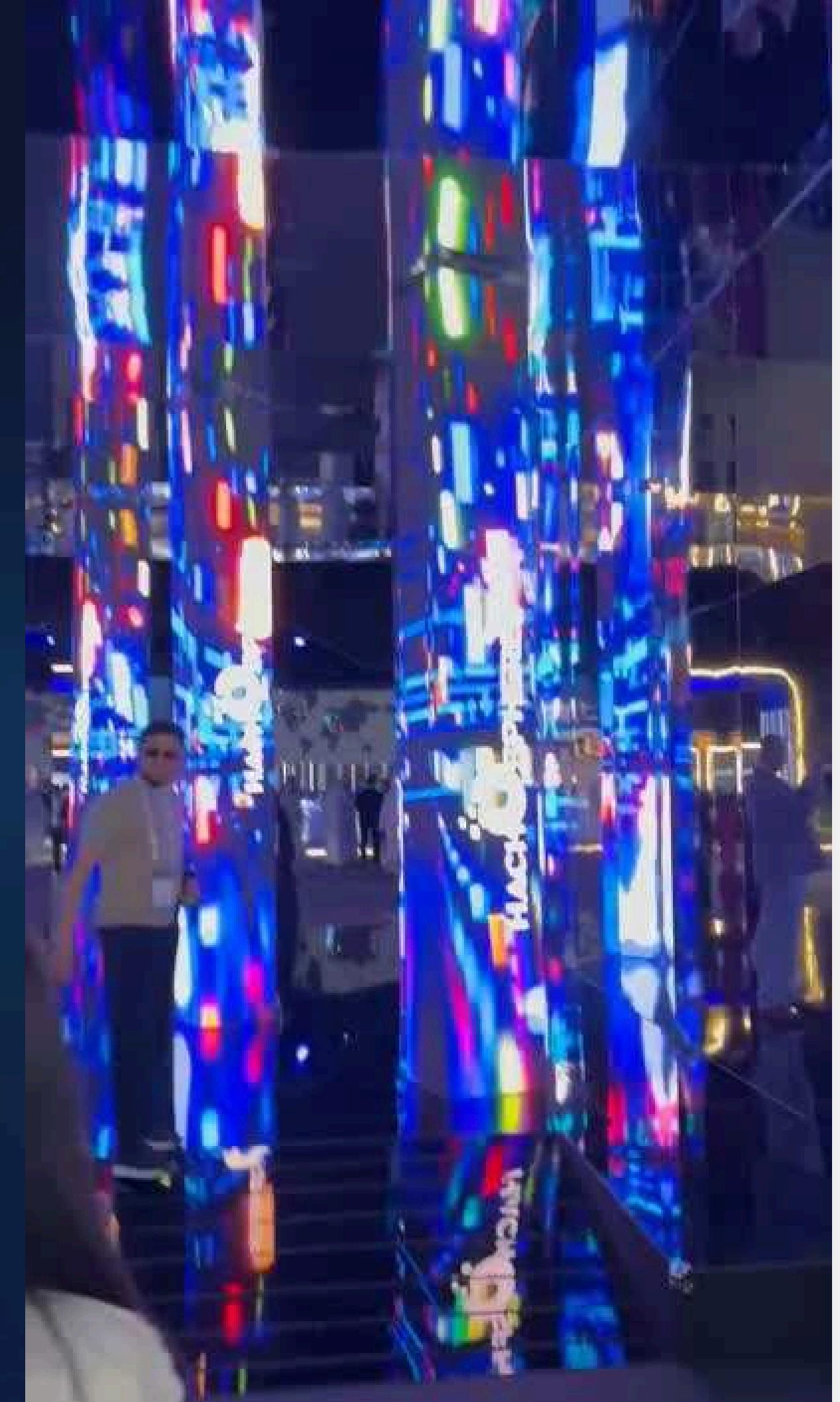
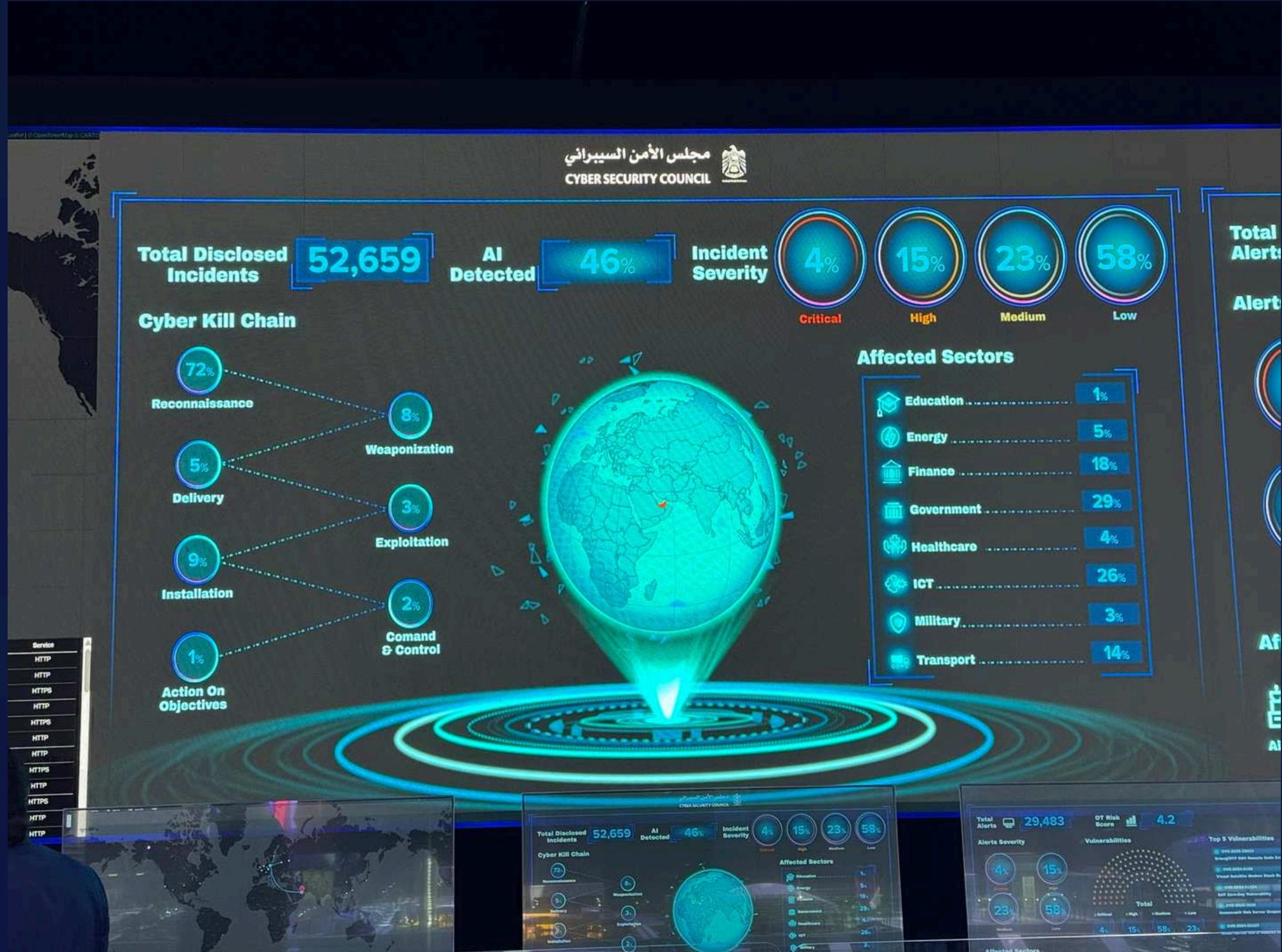
CHANCE UND RISIKO
KI MODELLE SIND
GRENZENLOS



EXPERTEN WERDEN ZU
KI-SPARRINGPARTNER

KI VERÄNDERT
UNSER ROLLENBILD

LIVE: CYBERSECURITY UND KI GISEC 2025 DUBAI / VAE



EMPFEHLUNGEN

KI **steigert** die **Leistungsfähigkeit** von Unternehmen **massiv** – und wird international längst als **unverzichtbar** angesehen (USA, VAE, CN, Nordics)

Gleichzeitig entsteht mit **KI ein zusätzliches (Cyber)Risiko** und muss überwacht und gesteuert werden.

Das KI Risiko ist **Teil** des gesamten Cyberrisikobildes.

Wer ein **klares** Bild und eine unternehmensspezifische KI-Strategie hat, kann richtige Schritte setzen.



SEQiFY

1

CyberRisiko Bild

automatisiert

verknüpfte
Innen- und Außensicht

Globale Datenquellen

Development
Schutz vor Bedrohungen



KI Risiko
3rd Party Risk



People Management
Compliance





STAKEHOLDER



“ist unser CyberRisiko Layer über der bestehenden Security Infrastruktur.”



SEQiFY zeigt, welche technischen Risiken für unser Geschäft relevant sind.

Strategisch und operativ
CyberRisiko steuern.

in Echtzeit

- automatisiert
- systemübergreifend
- unternehmensweit



ERGEBNISSE

Geschäftsrelevante Risiken in Echtzeit

strategische Steuerung

Risikobewertung & Priorisierung

Entscheidungsgrundlage für IT Operations

Compliance - Nachweis für u.a. NIS2, Dora, Tisax, ISO 27001

Klarheit im CyberRisiko in 30 Min



WAS SAGT DIE KI DAZU?

STAND 30.05.2025



ChatGPT 4.0

Welche Potentiale siehst Du für den KI Einsatz in der CyberSecurity und im Risikomanagement?

Der Einsatz von KI in der Cybersecurity und im Risikomanagement bietet enorme Potenziale – sowohl zur Effizienzsteigerung als auch zur Qualitätssicherung in sicherheitskritischen Prozessen.

Hier sind die zentralen Potenziale, unterteilt in operative, strategische und transformative Ebenen:

1. Operative Potentiale (Automatisierung & Effizienz)

Früherkennung & Prävention

- Anomalieerkennung in Echtzeit durch Machine Learning (z. B. Login-Verhalten, Datenzugriffe, Netzwerkverkehr).
- Predictive Threat Intelligence: KI kann Muster aus früheren Angriffen erkennen und präventiv blockieren.

Reaktionsgeschwindigkeit

- Automatisierte Incident Response: KI triagiert Alarne, priorisiert sie und stößt Gegenmaßnahmen an (z. B. Isolierung eines Endpunkts).
- KI-basierte Playbooks in SOAR-Systemen.

Entlastung von Security-Teams

- KI übernimmt Routineaufgaben wie Log-Analysen, False-Positive-Filterung oder Compliance-Checks.
- Natural Language Interfaces machen Analysen zugänglich für Nicht-Techniker (z. B. via Generative KI).

2. Strategische Potentiale (Qualität & Governance)

Risikoanalyse & Priorisierung

- KI-gestützte Risikobewertungen (z. B. Asset-Bewertungen im Kontext von Bedrohungslage und Schwachstellen).
- Priorisierung von Maßnahmen auf Basis von tatsächlichem Geschäftsnutzen und Gefahrenlage.

Compliance & Audits

- Automatische Kontrolle von Richtlinien & Standards (ISO 27001, NIS2, DSGVO).
- KI kann Dokumente analysieren, Abweichungen erkennen und Audit-Vorbereitung beschleunigen.

Erkennung von Insider-Risiken

- Verhaltensanalysen über KI decken schleichende oder verdeckte Bedrohungen durch interne Akteure auf.

3. Transformative Potentiale (neue Paradigmen)

Continuous Risk Management

- Weg von punktuellen Kontrollen hin zu dynamischem, kontinuierlichem Risikomanagement durch KI-gestützte Analyse-Engines.

Mensch-KI-Kollaboration

- KI wird zum Sicherheits-Co-Piloten, der Empfehlungen gibt, aber immer noch durch Menschen gesteuert wird.

Adaptive Security Architectures

- KI ermöglicht adaptive Zugriffskontrolle und Sicherheitsrichtlinien basierend auf Kontext (Ort, Zeit, Verhalten).

Beispielhafte Use Cases mit hohem Potenzial

Bereich	KI-Einsatz
IAM	Adaptive MFA, Risikobewertung bei Login
XDR	Korrelieren von Angriffsmustern über E-Mail, Endpoint, Cloud
Cloud Security	Automatische Sichtbarkeit & Bewertung von Ressourcen
Awareness	Generative KI für personalisierte Schulungen

Aber: Grenzen & Herausforderungen

- Bias & Blackbox-Probleme** → Entscheidungen müssen nachvollziehbar bleiben (Explainable AI).
- Datenschutz** → Welche Daten analysiert werden dürfen, ist kritisch.
- Falsches Vertrauen in KI** → Menschliche Kontrolle ist unerlässlich.
- Komplexität** → Der Aufbau eines sinnvollen KI-Stacks erfordert Know-how und Ressourcen.



WIRD KI UNSERE CYBERSECURITY EXPERTEN ERSETZEN?



SEQIFY CYBERRISIKO MANAGEMENT

**Special Guest:
Internationaler Experte
Einzigartiger Erfahrungsschatz
Anerkannt & Renommiert**

LIVE



WIRD KI UNSERE CYBERSECURITY EXPERTEN ERSETZEN? BEFRAGUNG VON CHATGPT



KURZ UND DIREKT: NEIN –
ABER KI WIRD DIE ROLLE VON
CYBERSECURITY-EXPERTEN
RADIKAL VERÄNDERN.

💡 Warum KI den Security-Experten nicht ersetzt:

1. Kontextverständnis

KI erkennt Muster, aber versteht keine Geschäftslogik oder geopolitischen Kontext.

Beispiel: Ein Zugriff aus einem neuen Land ist für ein globales Unternehmen ggf. harmlos – für ein Behördennetzwerk ein Alarm.

2. Verantwortung und Ethik

KI kann Entscheidungen vorschlagen, aber keine Verantwortung übernehmen.

In kritischen Situationen (z.B. Incident Response, Datenschutzverstöße) braucht es menschliche Entscheidungen.

3. Interpretation und Kommunikation

Security ist nicht nur Technik, sondern auch Risikokommunikation, Awareness und Priorisierung – etwas, das Menschen mit Fach-, Kultur- und Geschäftswissen besser leisten.

📌 Fazit:

KI ersetzt keine Menschen. Sie ersetzt Aufgaben.

Die neuen Security-Experten arbeiten **mit** KI, nicht **gegen** sie – und das macht sie wertvoller als je zuvor.

🚀 Was sich verändern wird:

Der Security-Experte wird zum KI-Kurator

- Steuert KI-basierte Security-Systeme
- Bewertet Empfehlungen und trennt "Noise" von echten Risiken
- Trainiert KI mit realen Fällen und Policy-Wissen

Fokus verschiebt sich

- Weg von manuellen Tasks (Log-Analyse, Regelpflege)
- Hin zu strategischer Risikoanalyse, Governance, Kommunikation

Cybersecurity wird produktiver

- Mit KI sind Experten 10x schneller bei Analyse, Dokumentation, Reporting.
- Teams skalieren besser – besonders relevant bei Fachkräftemangel.

LIVE

EXPERTE - CYBERRISIKO IM MANAGEMENT



WITH EASE.
Elmar Jilka



ELMAR JILKA

CEO & FOUNDER SEQiFY

elmar.jilka@genoa.at



LinkedIn

SEQIFY

**CyberRisiko Management
Plattform**

www.seqify.net

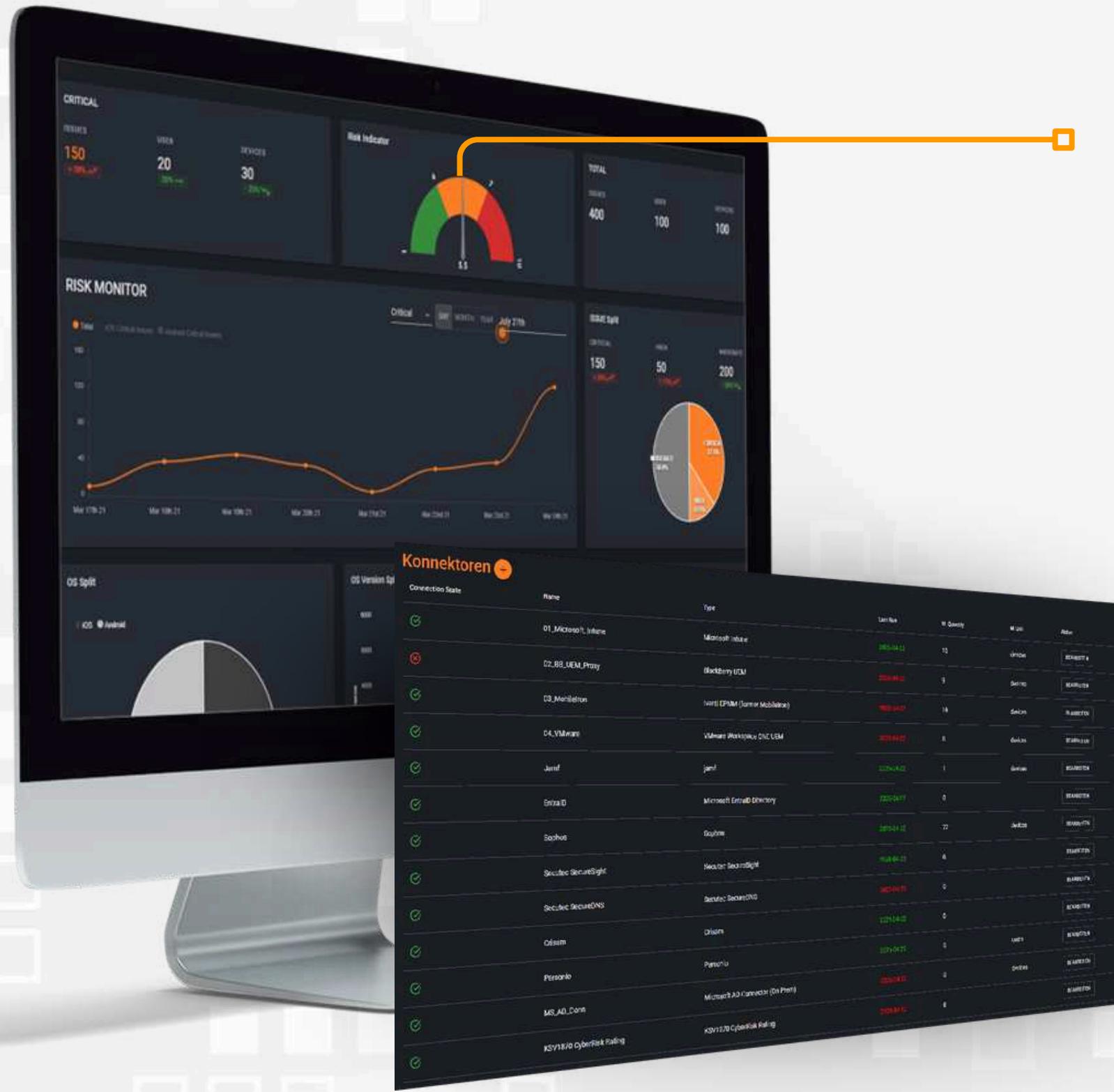


STEUERN SIE IHR CYBERRISKO

SEQIFY

DIE CYBERRISIKO MANAGEMENT PLATTFORM

WWW.SEQIFY.NET



Automatisierte Risikoanalyse in Echtzeit

Systemübergreifendes Risikobild
mit mehr als 30 Konnektoren

Verständlich und klar in Sekunden
für Vorstand, Geschäftsführer, CEO, CFO,
CIO, CISO, IT-Leiter, das IT-Team, Prüfer und
Auditoren.

Steuern Sie Ihr CyberRisiko
Wie in der Finanz.



Objektiver Compliance-Nachweis

Messbare Wirkung und Erfolgsnachweis
von Sicherheitsmaßnahmen in Echtzeit.

Unterstützung bei regulatorischen Vorgaben
(NIS2, DORA, Tisax, ISO 27001) zur **Erfüllung von
Audit-Anforderungen**.

Steuern Sie Ihr CyberRisiko
automatisch und aktuell.



Priorisierte Handlungsempfehlungen

Die Plattform schlägt **automatisiert Maßnahmen zur Risikominimierung** vor.

4 Kritische Server mit 27% Impact.

Steuern Sie Ihr CyberRisiko vorausschauend.

Wie funktioniert SEQiFY?

DAS HERZ UNSERER LÖSUNG.

**Systemübergreifend
mit 30+ Konnektoren.**

- Endpoint Security
- Thread & Detection
- Vulnerability Management
- Unified Device Management
- Identity Management
- HR-Systeme
- GRC / ISMS
- Development
- Lieferketten
- Darknet & Secure DNS
- Awareness
- Case Management



Verknüpfte Innen- und Außensicht

SEQiFY integriert sich in die IT-Systeme und externe Datenquellen für ein umfassendes Risikobild.

Integrationen



SEQIFY CYBERRISIKO MANAGEMENT

CRISAM

INFORMATION
Security

IDENTITY
Management

DEVICE
Management

BlackBerry

jamf Microsoft
ivanti **vmware**
by Broadcom

SentinelOne Microsoft Defender
W / T H secure **sophos** **paloalto**
NETWORKS

W / T H secure Microsoft Defender

CASE Management

PEOPLE
Management

DEVELOPMENT

AWARENESS

SUPPLY CHAIN

DARKNET

ERP Systeme

EOL

NIST

Secutec

Supply Chain

Darknet

ERP Systeme

EOL

NIST

Secutec

Supply Chain

Darknet

ERP Systeme

EOL

NIST

Secutec

Supply Chain

Darknet

ERP Systeme

EOL

NIST

Supply Chain



Key Features



ONE PLATFORM

Klares Cyberrisikobild für das Management



SYSTEM-ÜBERGREIFENDE RISK INSIGHTS

mit 30+ Konnektoren



AKZEPTIERTES RISIKO

Risiken aktiv steuern und dokumentieren



AUTOMATISIERTE RISIKOANALYSE

tagesaktuell



COMPLIANCE

Automatisierte Zuordnung von ISMS-Anforderungen



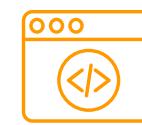
HANDLUNGS-EMPFEHLUNGEN

zur sofortigen Umsetzung



RISK FORECASTING

Priorisierung entlang von Eintrittswahrscheinlichkeit



SUPPLY CHAIN RISIKEN

Cyberrisiken in der Lieferkette erkennen

SOFTWARE-DEVELOPMENT

Risiken bei SW-Entwicklung monitoren

Erklärung in 30 Sek für den CEO

Steuern wie in der Finanz

Energie

Industrie

Finance

Handel



Public Sector

Health Care

IT & Technology

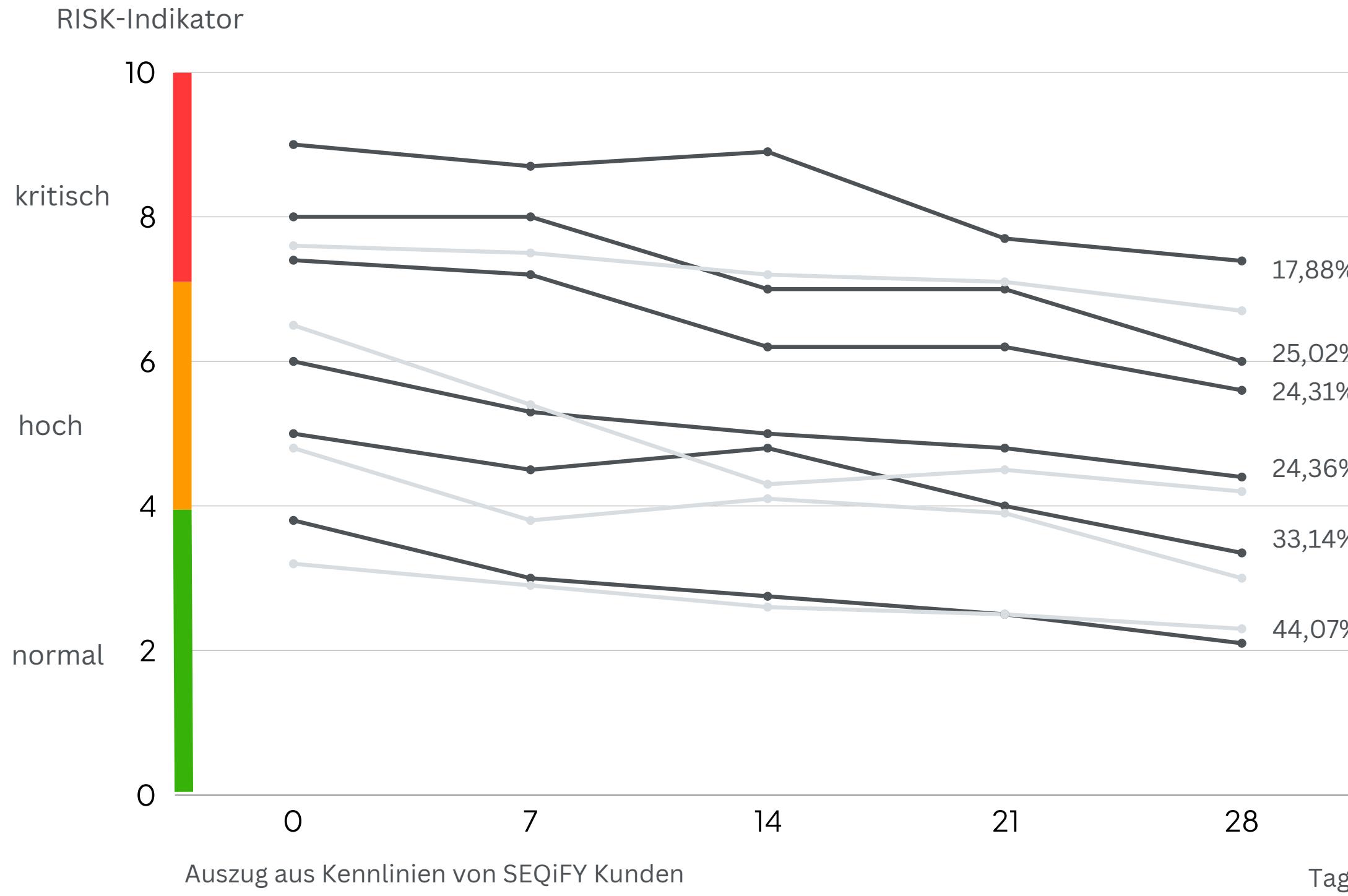
Pharma

Welcher Anwendungsfall interessiert Sie am meisten ?



SEQiFY

Gemessene Risikosenkung nach 30 Tagen.





The European Way.



2

Aus Europa –
für Europa.



Entwicklung



Cloud / Daten



Support

100% MADE IN EUROPE

Unsere Lösung wird in
Europa entwickelt,
gestaltet und betrieben –
für maximale Sicherheit und
unter Einhaltung höchster
Standards.

Trusted EU Cloud Service | DSGVO-konform | ISO 27001



SEQiFY | One Small Step.



Gemeinsame Aktivierung

Anbindung der
relevanten Systeme -
ohne Clients, Agents
oder Server.

1h

Cyberrisiko in Echtzeit

Automatisch



24h

Guidance: Das Cyberrisiko im Griff.

Kontinuierlich:
Interpretation & Analyse
Ihrer Risikodaten
durch SEQiFY Experten

365

3

Einfach loslegen.

Nach der Aktivierung
erhalten Sie bereits nach
24 Stunden erste
Risikodaten und danach
ein laufendes Cyber-
Risikobild.



SEQiFY

WWW.SEQIFY.NET

[HTTPS://WWW.SEQIFY.NET/LP/SEQIFY-DEMO-BUCHEN/](https://www.seqify.net/lp/seqify-demo-buchen/)

DEMO BUCHEN