Trump 2.0

KI als Sicherheitslücke?
Wie Sie die Kontrolle behalten – bevor andere es tun

Daniel Baumann, Insight
29. September 2025

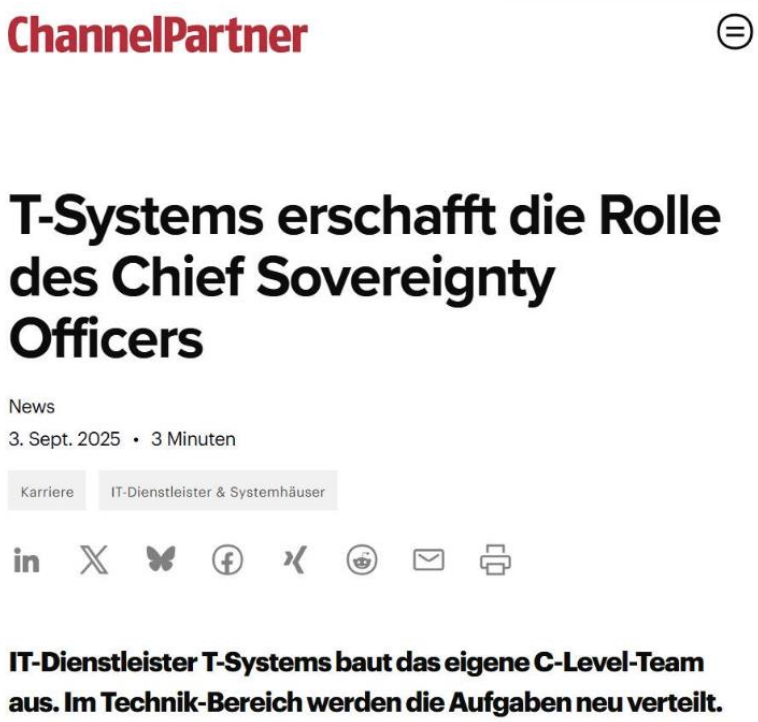
Von der Qualifikationslücke zur strategischen Notwendigkeit

Ein grundlegender Wandel in der Cybersicherheit

Der Fachkräftemangel im Bereich Cybersicherheit ist vorbei. Die Strategiekrise hat begonnen.

DIGITALE SOUVERÄNITÄT ALS GANZHEITLICHE AUFGABE

Bei T-Systems gibt es seit Kurzem nun erstmals die C-Level-Position eines "Chief Sovereignty Officers"



ChannelPartner

T-Systems erschafft die Rolle des Chief Sovereignty Officers

News

3. Sept. 2025 • 3 Minuten

Karriere | IT-Dienstleister & Systemhäuser

IT-Dienstleister T-Systems baut das eigene C-Level-Team aus. Im Technik-Bereich werden die Aufgaben neu verteilt.

Organisationen sind von der Qualifikationslücke im Bereich Cybersicherheit betroffen.

Dies ist nicht nur eine Statistik, sondern eine gemeinsame Realität, die Ressourcen einschränkt, Innovationen verlangsamt und das Risiko für Unternehmen überall erhöht.

- Fast die Hälfte **(47 %)** gibt an, dass **erhebliche oder schwerwiegende** betriebliche Auswirkungen zu verzeichnen sind.
- Dies wirkt sich direkt auf die geschäftliche Agilität und das Wachstumspotenzial aus.

Dies ist die gemeinsame Grundlage, von der aus wir alle handeln müssen.

Die strategische Bedeutung der Datensicherheit in der KI

1960 – 1970's

1

Erste Cyberangriffe

Die Anfänge der Computernetzwerke und die ersten Cyberangriffe

1980s

2

Erste Firewall-Technologie

Die erste Firewall-Technologie wird entwickelt. Sie ermöglicht es Unternehmen, den Zugriff auf ihre Computernetzwerke zu kontrollieren.

1990s

3

Aufstieg von Viren und Würmern

Der Aufstieg des Internets und die zunehmende Nutzung von Computernetzwerken führten zu einer Zunahme von Cyberangriffen.

2000s

4

Aufstieg WWW

Aufstieg des World Wide Web, das zu einem deutlichen Anstieg der Zahl der Cyberangriffe führte

2010s

5

Aufstieg von IoT, Mobilgeräten und Cloud

Fortgeschrittene Taktiken wie Phishing, Spear-Phishing und Ransomware, um sensible Informationen zu stehlen und Geld von Opfern zu erpressen.

2020s

6

Ausbreitung von COVID-19

Drastischer Anstieg der Nutzung von Videokonferenzen, Collaboration-Tools und Cloud-basierten Diensten, die von Cyberkriminellen ausgenutzt werden können

TODAY

7

Cybersicherheit nutzt KI

Die Entwicklung fortschrittlicher Technologien wie künstliche Intelligenz spielt eine wichtige Rolle im Kampf gegen Cyber-Bedrohungen.

Insight.

Warum Data Security jetzt strategisch ist

Regulatorik: NIS2, DORA, ISO 27001 – Datenklassifizierung wird Pflicht

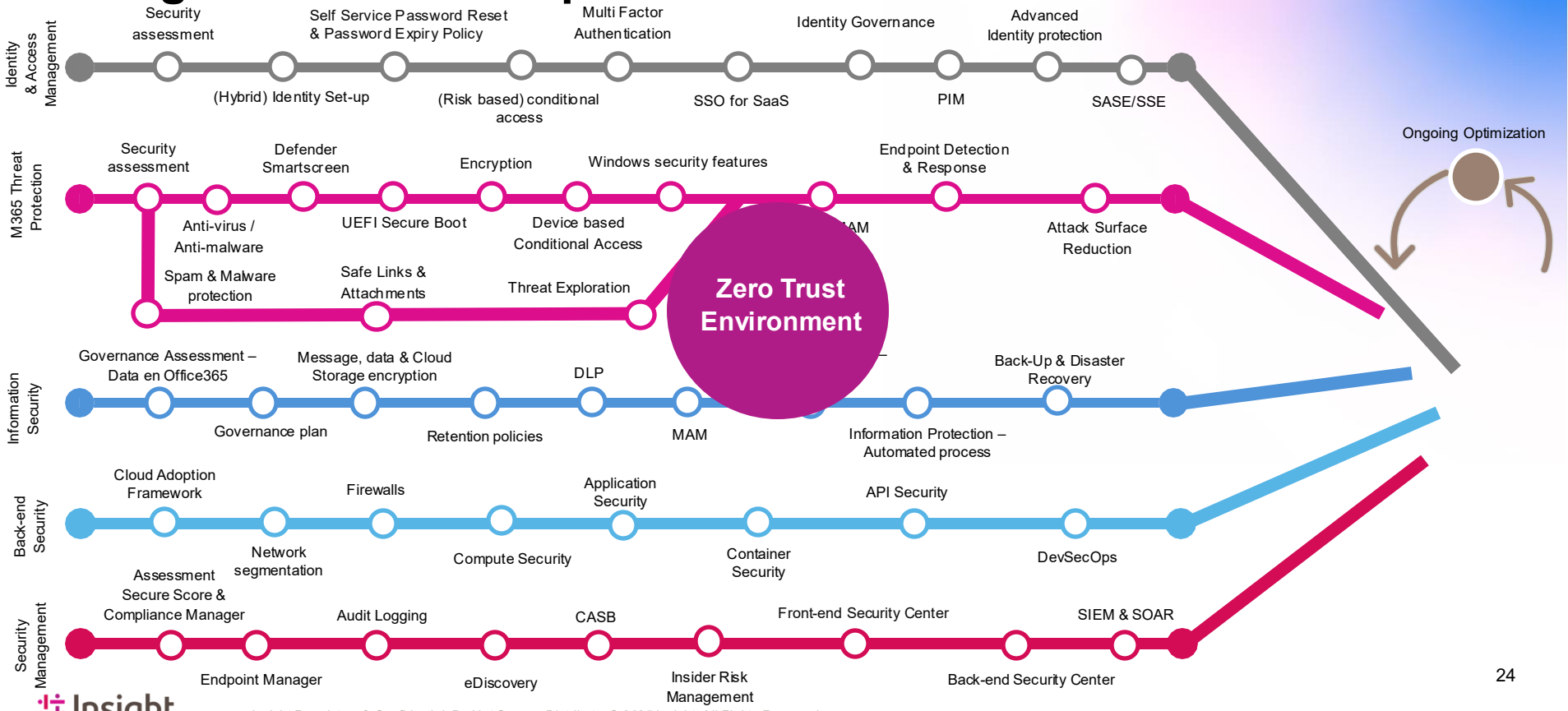
KI: Ohne geschützte Daten keine sichere Copilot-Einführung

Multi-Cloud & hybride Szenarien: Daten bewegen sich, Sicherheit muss folgen

Die strategische Bedeutung der Datensicherheit in der KI

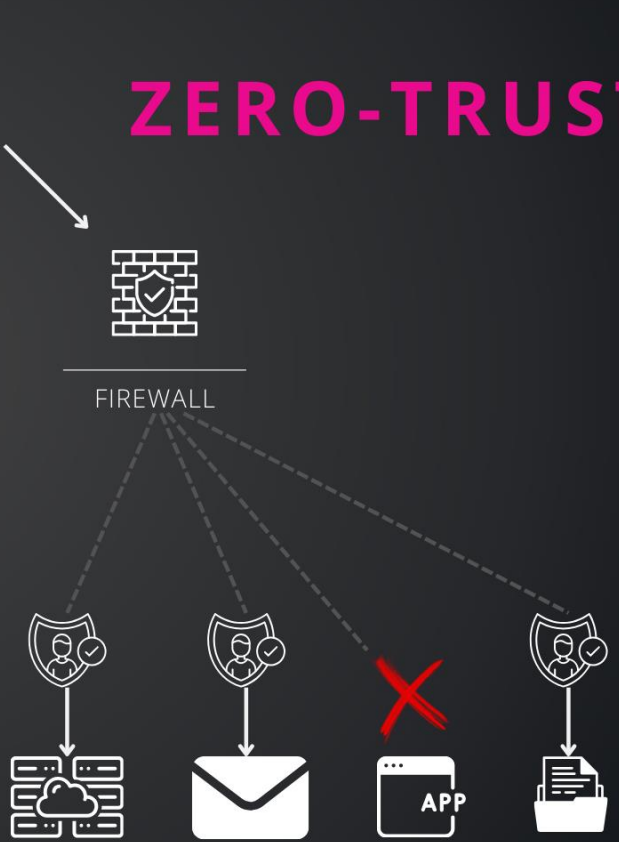
ZERO TRUST

Managed Secure & Compliant IT environment



TRADITIONAL NETWORK:

ZERO-TRUST:



Data Security Journey

Verstehen Sie Ihre Datenlandschaft und identifizieren Sie wichtige Daten in Ihrer hybriden Umgebung.

Erkennen Sie riskantes Verhalten und verhindern Sie die versehentliche Weitergabe sensibler Informationen.

Flexible Schutzmaßnahmen wie Verschlüsselung, Zugriffsbeschränkungen und visuelle Markierungen anwenden

Daten und Aufzeichnungen automatisch auf konforme Weise aufbewahren, löschen und speichern.

Angetrieben von einer intelligenten Plattform

Einheitlicher Ansatz für automatische Datenklassifizierung, Richtlinienverwaltung, Analysen und APIs

DER CYBER RESILIENCE ACT (CRA) IST DA

Was Unternehmen jetzt umsetzen müssen

WIP Format

Wichtige Aspekte des Cyber Resilience Act:

- **Geltungsbereich:**
  Der CRA betrifft alle Produkte, die mit anderen Geräten oder Netzwerken verbunden sind, was Hardware wie Router, IoT-Geräte, aber auch Software wie Betriebssysteme und Anwendungen einschließt.
- **Verpflichtungen für Hersteller:**
  Hersteller müssen sicherstellen, dass ihre Produkte von vornherein sicher sind und nicht erst nachträglich geschützt werden müssen. Sie müssen Sicherheitsupdates bereitstellen, Schwachstellen dokumentieren und melden sowie Sicherheitsinformationen für Kunden bereithalten.
- **Pflichten für Händler und Importeure:**
  Diese Akteure müssen sicherstellen, dass nur Produkte in Verkehr gebracht werden, die den CRA-Anforderungen entsprechen, und dass die erforderliche Dokumentation und Kennzeichnung vorliegt.
- **Ziele:**
  Der CRA will die Cyberresilienz entlang des gesamten Produktlebenszyklus erhöhen, das Vertrauen in digitale Produkte stärken und ein einheitliches Sicherheitsniveau im europäischen Binnenmarkt gewährleisten.
- **Vollzug:**
  Die Verordnung ist am 11. Dezember 2025 in Kraft getreten und wird ab dem 11. Dezember 2027 vollumfänglich anwendbar sein.

DER CYBER RESILIENCE ACT (CRA) IST DA

Was Unternehmen jetzt umsetzen müssen

WIP Format

Erstens:

Aufbau eines Schnelleinsatzteams für den Ernstfall

Zweitens:

Bedrohungs- und Risikoanalysen als zentrales Instrument

Drittens:

Überblick durch Ist-Stand-Analyse

WIP Format

DER CYBER RESILIENCE ACT (CRA) IST DA

IT der Zukunft ohne „Security by Design“: absolut undenkbar!

Warum Security by Design immer wichtiger wird

- Secure-by-Design ist ein proaktiver, sicherheitsorientierter Ansatz für digitale Produkte und Dienstleistungen, der auf die Cybersicherheitsziele eines Unternehmens abgestimmt ist.

- Er erfordert, dass Sicherheitsbedrohungen bereits bei der Entwicklung eines Produkts oder einer Dienstleistung berücksichtigt werden, und fördert verstärkte Sicherheitsmaßnahmen während des gesamten Entwurfs- und Bereitstellungsprozesses. Sein Grundprinzip besteht darin, Daten und Privatsphäre durch verbesserte Konzeption, Implementierung und Bereitstellung zu schützen und letztendlich dazu beizutragen, dass digitale Produkte und Dienstleistungen mit weniger oder gar keinen Sicherheitslücken existieren.

Die wahre Kluft: Führung und strategische Ausrichtung

Der kritischste Mangel besteht im Bereich der strategischen Führung.

Die Herausforderung besteht nicht nur darin, Analysten zu finden, sondern auch darin, die für die Steuerung, Planung und Abstimmung der Sicherheit mit den Geschäftsergebnissen erforderliche Fachkompetenz auf Führungsebene zu finden.

Kritische Qualifikationslücken auf Führungsebene:

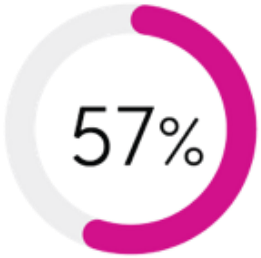
- **Strategische Fähigkeiten und Governance: 46 %**
- **Compliance und Vorschriften: 42 %**
- **Sicherheit durch Design und Implementierung: 41 %**

Ohne diese Führung können selbst die besten Teams und Werkzeuge die Orientierung verlieren.

Die Folge: Ein Kreislauf der Kompromisse

Die Strategielücke zwingt zu riskanten Kompromissen, die Unternehmen zurückhalten.

Ohne strategische Ausrichtung sind Unternehmen gezwungen, sich in einem Kreislauf kurzfristiger Lösungen zu bewegen, die die langfristige Sicherheit und Innovation untergraben.



haben wichtige Sicherheitsinitiativen verzögert oder zurückgestellt.

haben sich auf vorübergehende Workarounds verlassen und dadurch technische Schulden verursachen.

haben sich bemüht, komplexe Compliance-Vorgaben zu erfüllen.

Das ist die Strategiekrise in Aktion.

Führungskräfte setzen auf strategische Partnerschaften, um wieder an Schwung zu gewinnen.

Die Komplexität moderner Sicherheit führt zu einem klaren Markttrend: Weg vom rein internen Modellhin zur Nutzung externen Fachwissens für strategische Vorteile.

- **74%** der Unternehmen arbeiten mittlerweile mit einem MSSP zusammen.
- **51%** haben allein im letzten Jahr den Einsatz von MSSPs erhöht.
- **59%** nennen die Verfügbarkeit rund um die Uhr und die schnelle Reaktion als wichtigsten Grund – ein Leistungsfaktor, nicht nur eine Kostenersparnis.

Strategische Partnerschaften sorgen für spürbare Verbesserungen in den Bereichen Ausfallsicherheit, Transparenz und Compliance.

Für diejenigen, die sich für eine Partnerschaft entschieden haben, sind die Ergebnisse eindeutig. Es geht nicht darum, die Kontrolle zu verlieren, sondern darum, Fähigkeiten zu gewinnen.

Unternehmen, die mit MSSPs zusammenarbeiten, berichten:

74%

haben ihre Widerstandsfähigkeit im Bereich Cybersicherheit gestärkt.

72%

haben ihre Compliance-Ergebnisse verbessert.

77%

sorgen für klare Sichtbarkeit und Kontrolle.

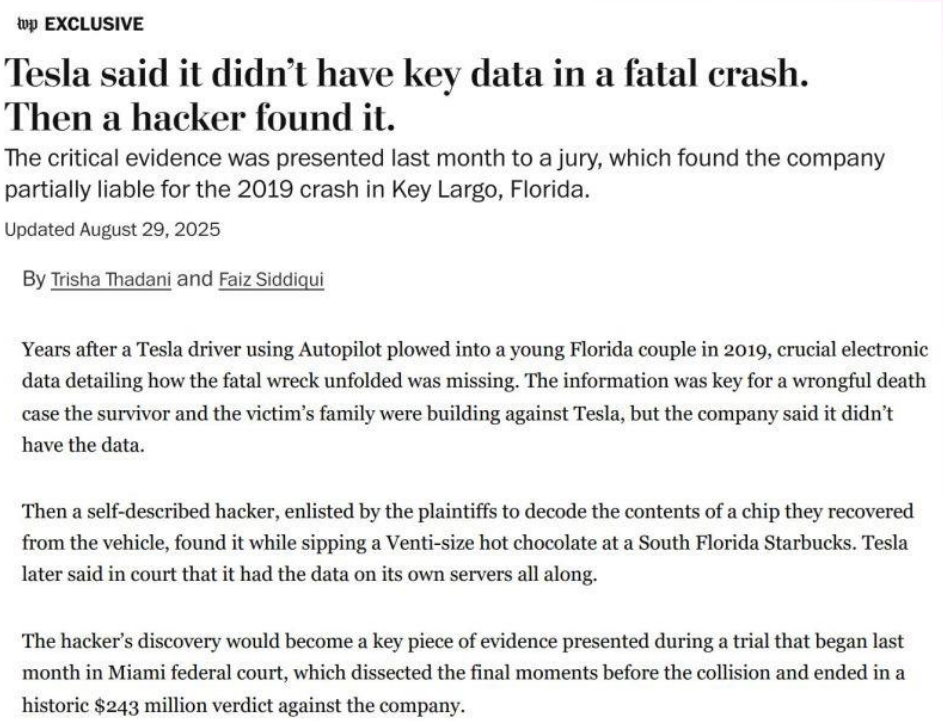
KI wird die Cyberabwehr neu definieren, erfordert jedoch einen strategischen Ansatz.

KI bietet eine enorme Chance, unsere Teams zu verstärken und die Verteidigung zu beschleunigen. Vertrauen und Governance sind jedoch zentrale Hindernisse, die mit Fachwissen überwunden werden müssen.

- Nur **15%** haben KI in großem Umfang eingesetzt, was zeigt, dass die Reise gerade erst begonnen hat.
- **52 %** nennen die **Angst vor ungenauen Ergebnissen** als größtes Vertrauenshindernis.

Das Potenzial der KI sicher zu erschließen, ist die nächste große strategische Herausforderung.

Rechts- und oder Ethikfrage?



wp EXCLUSIVE

Tesla said it didn't have key data in a fatal crash. Then a hacker found it.

The critical evidence was presented last month to a jury, which found the company partially liable for the 2019 crash in Key Largo, Florida.

Updated August 29, 2025

By Trisha Thadani and Faiz Siddiqui

Years after a Tesla driver using Autopilot plowed into a young Florida couple in 2019, crucial electronic data detailing how the fatal wreck unfolded was missing. The information was key for a wrongful death case the survivor and the victim's family were building against Tesla, but the company said it didn't have the data.

Then a self-described hacker, enlisted by the plaintiffs to decode the contents of a chip they recovered from the vehicle, found it while sipping a Venti-size hot chocolate at a South Florida Starbucks. Tesla later said in court that it had the data on its own servers all along.

The hacker's discovery would become a key piece of evidence presented during a trial that began last month in Miami federal court, which dissected the final moments before the collision and ended in a historic $243 million verdict against the company.

„Das traditionelle Modell, die Cybersicherheit vollständig intern zu verwalten, wird zunehmend unhaltbar. Die Landschaft ist zu schnelllebig, zu fragmentiert und zu spezialisiert.“

Rob O’Connor
Chief Information Security Officer für EMEA

LIEBER GEMEINSAM ALS ALLEIN

Healthcare Cyber Security Center (H-CSC)

28. August 2025

18 Schweizer Spitäler gründen ein nationales Cybersicherheits-Zentrum

Schweizer Spitäler ziehen gemeinsamen Schutzschirm auf: 18 führende Gesundheitseinrichtungen haben das «Healthcare Cyber Security Center» (H-CSC) gegründet. Der neue Verein soll Cyberangriffe auf Spitäler gemeinsam abwehren.

News

Spitäler sind attraktive Angriffsziele für Cyberkriminelle, da Gesundheitseinrichtungen mit einer grossen Menge sensibler Daten arbeiten. Solche Angriffe können den Betrieb erheblich beeinträchtigen: Operationen müssten verschoben werden, Patientendaten wären nicht verfügbar, lebensrettende Geräte könnten ausfallen.

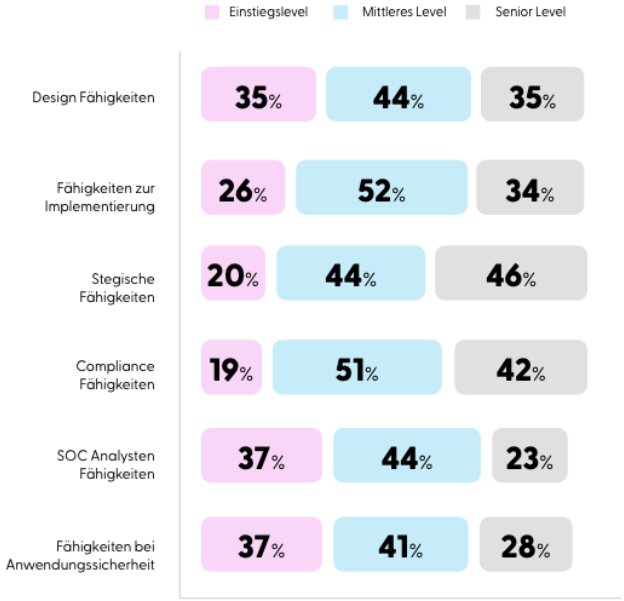
Der heute in der Spital Thurgau AG gegründete Verein funktioniert wie ein Frühwarnsystem: Die Spitäler tauschen Informationen über Angriffe aus, entwickeln gemeinsame Schutzstandards und helfen sich bei Cyberattacken. Ziel ist es, die Reaktionsfähigkeit zu verbessern und gemeinsam auf digitale Bedrohungen zu reagieren.

WIP Format

DAS CYBERSICHERHEIT-TALENT-PARADOXON

Mehr Technologie erfordert mehr (erweiterte) Menschlichkeit

Der rasche Fortschritt bei innovativen Technologien wie KI verringert nicht den Bedarf an qualifizierten Menschen; sondern verändert ihn.



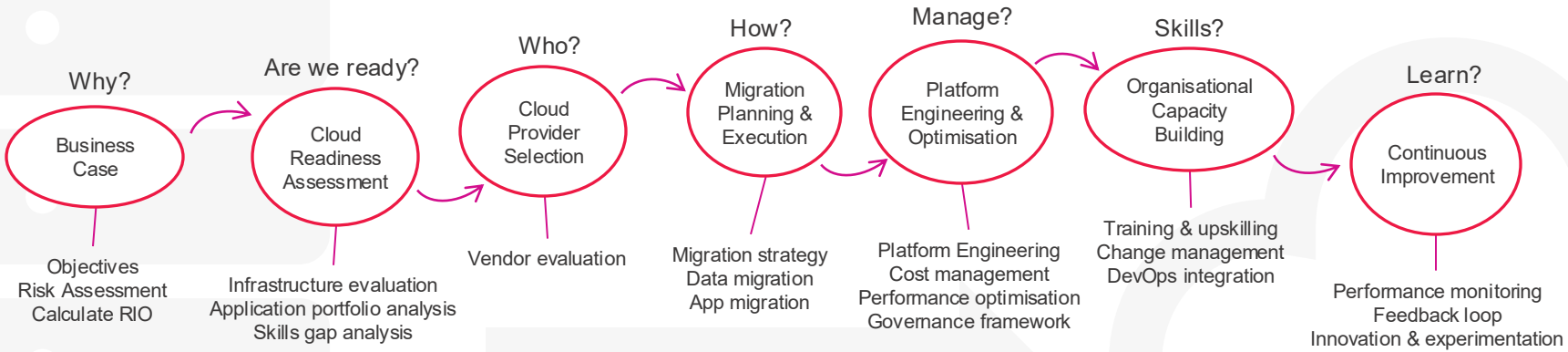
Kompetenzbereiche, auf welchem Level Ihre Organisation eine Lücke bei den Cybersicherheitskompetenzen aufweist

Cloudification der IT-Infrastruktur

Der Weg zu einer modernen Infrastruktur

DER WEG ZU EINER MODERNEN INFRASTRUKTUR

Cloudification der IT-Infrastruktur



Business Drivers

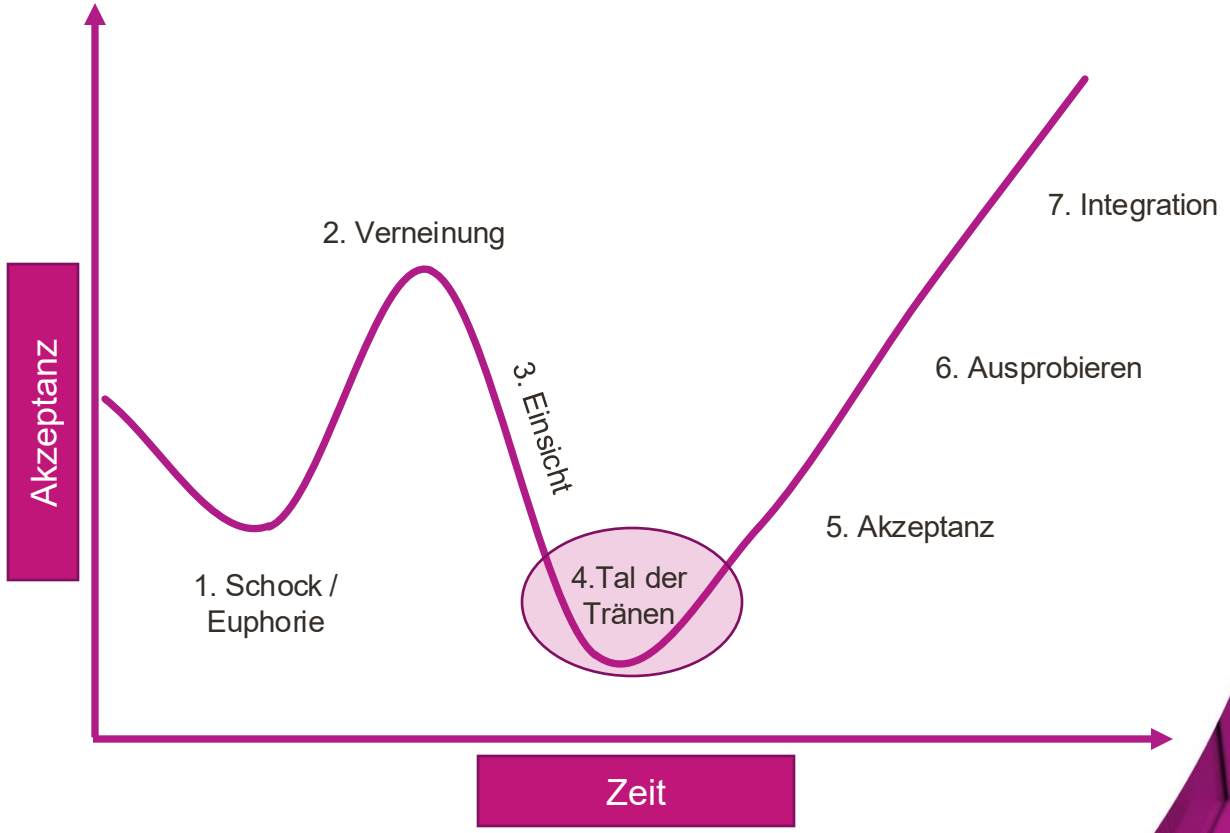
- Infrastructure & Software Obsolescence
- Cashflow (Capex to Opex)
- App Modernisation
- Data Modernisation
- Accelerate Test & Innovation

Migration Strategy

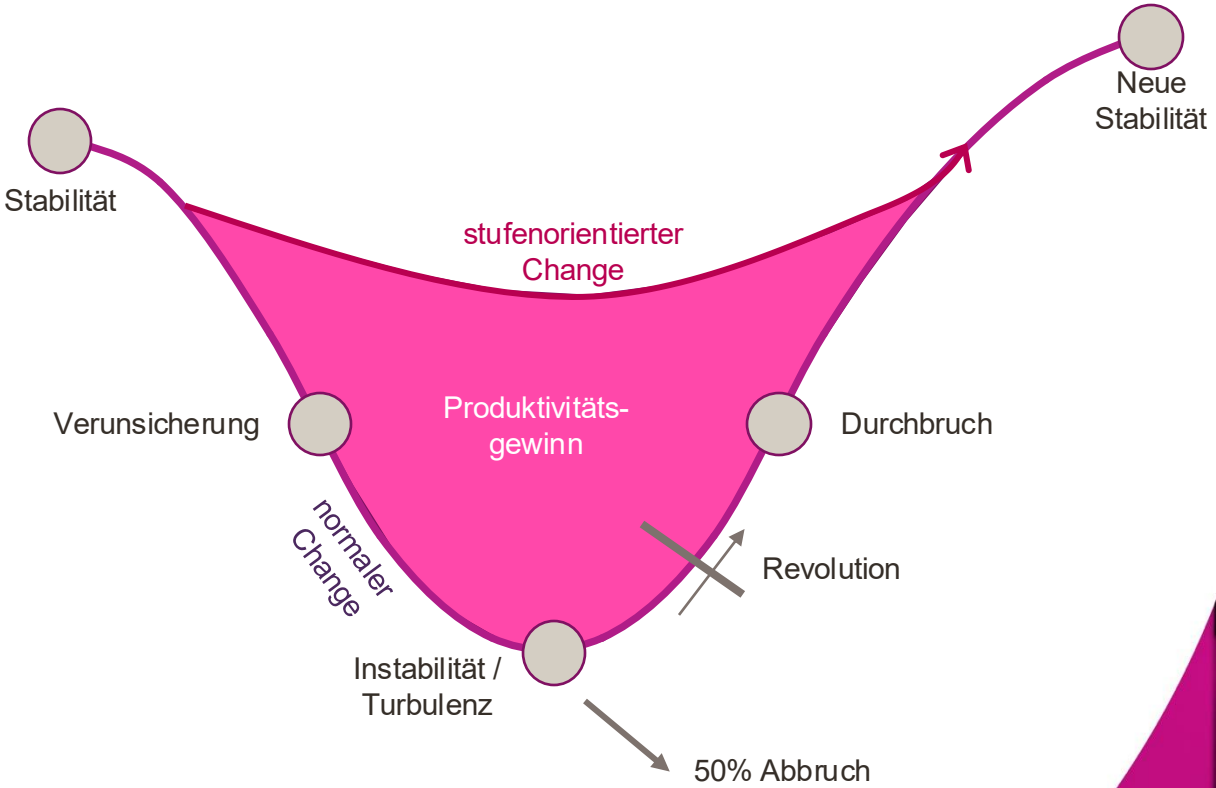
6 R model

- Rehost
- Replatform
- Refactor
- Retain
- Retire
- Repurchase (SaaS)

Phasen der (Cloud) Transformation



Das „Tal der Tränen“ / Change während einer Transformation

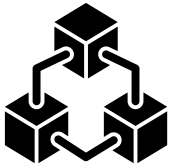


Cloud als marktdurchdringendes Geschäftsmodell ohne einheitliche Sicherheitsstandards?

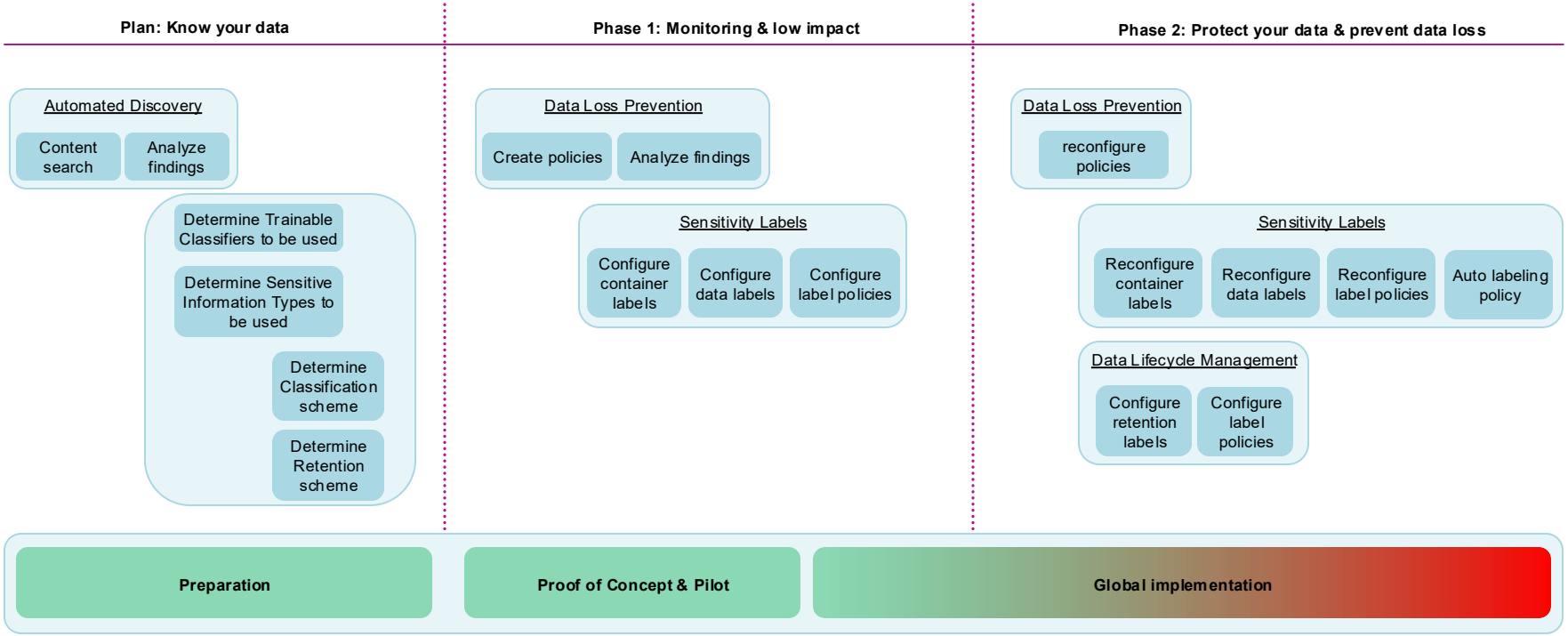
Implementierungsphasen und Timelines zur Datenklassifizierung

Data Security Customer Value Journey

PLAN Assess	BUILD Design/PoC	BUILD Implement	MANAGE
Security Baseline	**Microsoft Purview**		Continual Adoption
CSI Data Security Engagement			Managed Services Agreement
ISO 27001 Assessment	Remediation Consultation		

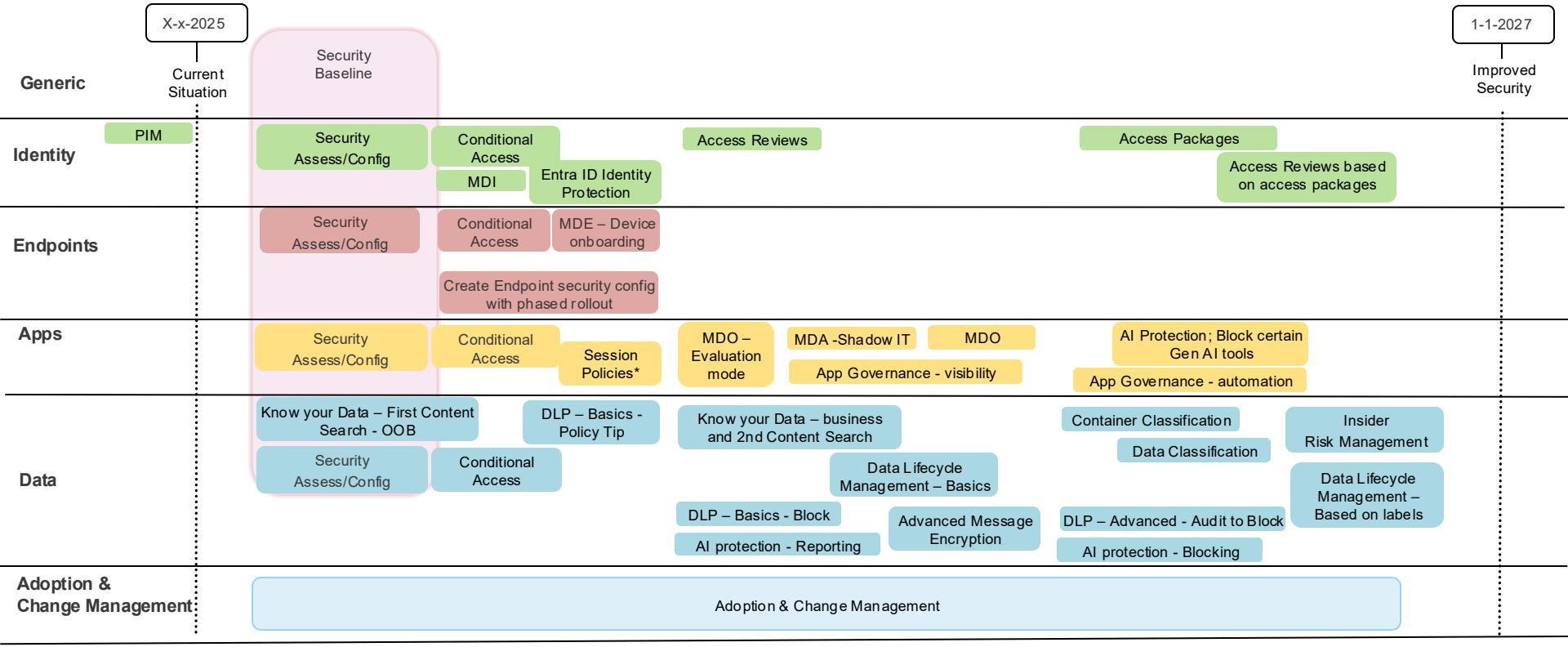


Implementation schedule



Roadmap

- **MDO**: Microsoft Defender for Office
- **MDI**: Microsoft Defender for Identity
- **MDE**: Microsoft Defender for Endpoint
- **MDA**: Microsoft Defender for Cloud Apps
- **PIM**: Privileged Identity Management
- **DLP**: Data Loss Prevention
- *: Phased Rollout



Interaktive Diskussion

Themenbereiche

- [A] – Aktuelle Situation
- [B] – Use Case Cluster
- [C] – Interaktive Diskussion

[A] Status Quo

Wer von Ihnen hat bereits Data Classification oder Labeling (in bspw. Microsoft 365) im Einsatz?

Was hindert Sie aktuell daran, (bswp.) Microsoft Purview vollständig zu nutzen?

[B] Use Case Cluster

In Projekten sehen wir diese Top-3-Szenarien:		
IP-Schutz (z.B. CAD-Dateien, F&E-Dokumente)	**(DSGVO-) Compliance** (HR, Legal, Finanzdaten)	**Enablement von Microsoft Copilot** (Sensitivitätslabels als Voraussetzung)

Frage: *„Wo sehen Sie sich aktuell auf dieser Reise? – Was sind Ihre Use Cases?“*

[C] Vertiefte Diskussion

Ziel der vertieften Diskussion
In dieser Session möchten wir gemeinsam ein praxisnahes Verständnis für Datenklassifizierung im Kontext moderner Data Security entwickeln.

Im Fokus stehen der organisatorische und technologische Reifegrad der teilnehmenden Unternehmen sowie zentrale Herausforderungen bei der Umsetzung. Ziel ist es, Erfahrungen auszutauschen, strategische Zielbilder zu diskutieren und konkrete nächste Schritte zu identifizieren, um Data Security als Enabler für Compliance, Innovationsfähigkeit und KI-Nutzung zu etablieren.

[C.1]
Organisation

Wer treibt das Thema intern: IT, Legal, CISO?

[C.2]
Technologie & Integration

Welche Tools sind im Einsatz? Wie gut sind Datenquellen integriert?

[C.3]
Nächste Schritte

Was bräuchte es, um bei Ihnen mehr aus den Tools zu machen?

[C.1]
Phase 1 – Organisatorischer Reifegrad

Wie ist Data Security bei Ihnen organisatorisch verankert – wer trägt Verantwortung?

- IT, CISO, Datenschutz, Legal, Betriebsrat?

Gibt es eine übergreifende Data-Governance-Strategie in Ihrem Unternehmen?

Wie gelingt die Abstimmung zwischen IT und Fachbereichen bei Klassifizierungen?

[C.2]
Phase 2 – Technologischer Reifegrad & Tool-Einsatz

Welche Tools setzen Sie aktuell zur Datenklassifizierung und -sicherung ein?	Nutzen Sie Purview bereits produktiv? In welchen Bereichen?	Wie viele Ihrer Datenquellen (M365, Exchange, SharePoint, File Shares, Azure, SAP…) sind eingebunden?
• (z. B. MIP - Microsoft Purview, 3rd Party)		

[C.3] Phase 3 – Strategische Ziele & „Next Steps“

Was wäre für Sie ein realistisches Ziel für die nächsten 6–12 Monate im Bereich Data Security?“

- z. B. vollständige Klassifizierung aller M365-Daten, DLP auf Top-Use-Cases, Copilot-Fähigkeit

Was hindert Sie aktuell an einer breiteren Umsetzung – Ressourcen, Know-how, Tool-Komplexität?

Wenn Sie Unterstützung bei der strategischen Planung Ihrer Security Roadmap benötigen - Wäre ein gemeinsamer Readiness-Workshop für Sie hilfreich? → kommen Sie gerne auf uns zu.

[C.3] Phase 3 – Strategische Ziele & „Next Steps“

Reifegradmatrix:	Welchen Reifegrad haben Sie aktuell?
1. Initial	**keine Klassifizierung**
2. Pilot	**einzelne Labels manuell**
3. Standardisiert	**Auto-Labeling & Policies**
4. Integriert	**Unternehmensweite Governance**
5. Optimiert	**Nutzung für KI, Audits, Proaktive Sicherheit**

[C] Trigger Themen für Security

Copilot Readiness: „Welche Rolle spielt Data Security in Ihrer KI-Strategie?“

Industrie-Use-Cases: „Wie gehen Sie mit IP-Daten, Produktionsdaten oder Kundenverträgen um?“

Audit & Reporting: „Wie auditierbar sind Ihre Data Security Maßnahmen gegenüber Regulatoren heute?“ – EU AI Act etc.

The Insight Way

Um echte Resilienz aufzubauen, ist ein vernetzter, strategischer Ansatz erforderlich. Das ist unser Versprechen an Sie.

People:

Wir helfen Ihnen dabei, Ihre Teams zu stärken und zu erweitern, damit sie zu einer strategischen Kraft werden.

Partners:

Als Ihr Partner bieten wir Ihnen fundiertes Fachwissen und strategische Beratung, damit Sie komplexe Herausforderungen meistern und kritische Lücken schließen können.

Platforms:

Wir arbeiten mit Ihnen zusammen, um eine integrierte, moderne Technologieplattform aufzubauen und zu verwalten; jene die Sicherheit, Transparenz und Anpassungsfähigkeit bietet.

Insight Cybersecurity
Wie wir Ihnen helfen

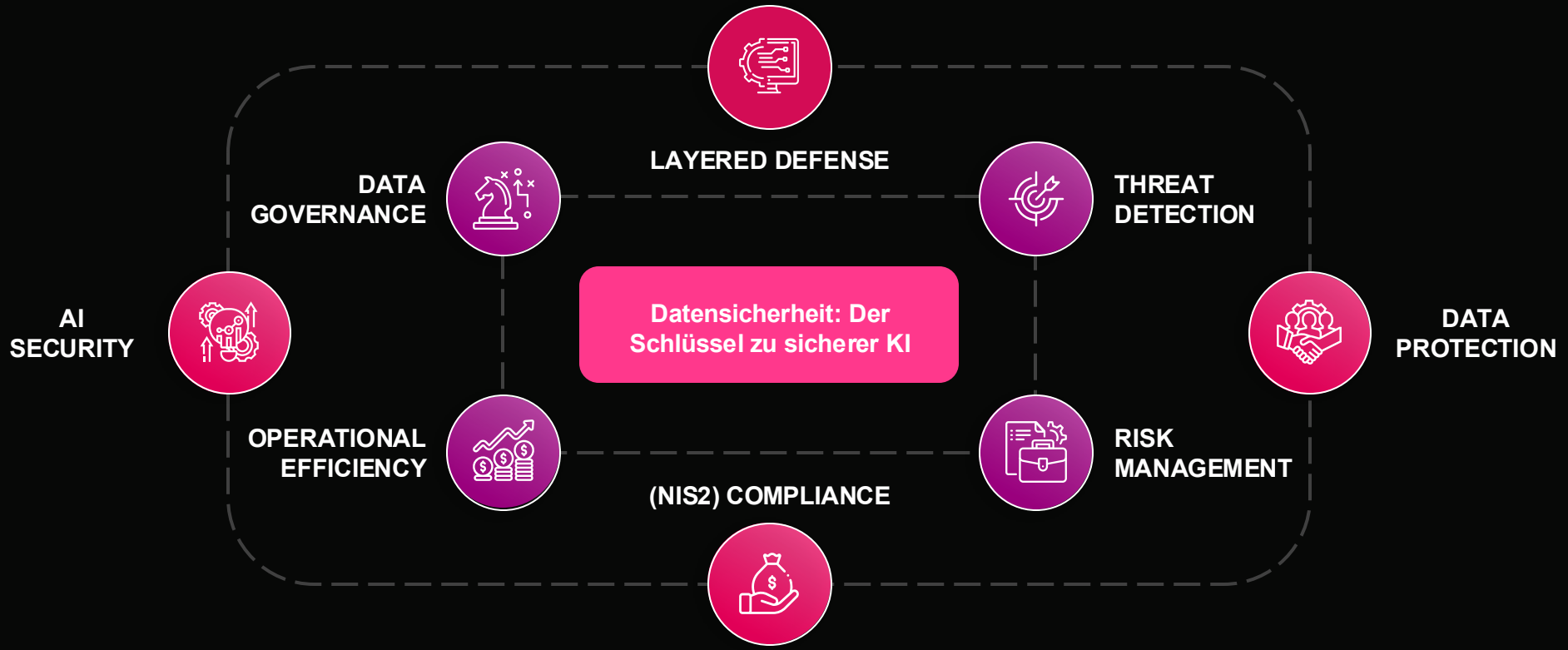
Assessment
- Unterstützung bei der Akkreditierung nach Branchenstandards wie ISO27001 oder NIS2
- Überprüfung Ihrer bestehenden Sicherheitskontrollen und Identifizierung von Restrisiken
- Erstellung einer priorisierten Roadmap, um Ihr gewünschtes Level an Sicherheit zu erreichen

Planung & Design
- Unterstützung bei der Umsetzung der Herausforderungen Ihres Unternehmens in Projekte zur Sicherheit
- Support und Anleitung bei der Auswahl der richtigen Anbieter, Produkte und Dienstleistungen
- Vorstellung von Workshops und technischem Design

Aufbau und Implementierung
- IMachen Sie Pläne Wirklichkeit – vom Entwurf bis hin zu vollständig gebauten und dokumentierten Sicherheitskontrollen
- Insight betrachtet jedes Projekt im Kontext Ihrer gesamten Roadmap
- Übergabe an Ihre internen Teams zum Management oder Übergang zu unseren Managed Services

IT Operations Management
- Support-Services sorgen für optimale Sicherheit
- Managed Services, bei denen Insight die Verantwortung für Ihre Sicherheitskontrollen übernimmt

Key Takeaways - Datensicherheit: Eine strategische Notwendigkeit für KI-Innovationen



Be ambitious.

Insight

#LSZGraz25

Daniel Baumann

DACH Technical Design Authority
EMEA ELT Board Member

Nächste Events:

IT-SA Home of Cybersecurity 2025 - Strategiekrise & KI @ Nürnberg vom 7.10 – 9.10

CIO Kongress @ Loipersdorf vom 12.10 – 14.10

Cybercrime Forum Wien @ Marriott Hotel am 22.10