LICENSA Empowered 2025 Wien

software one

Cyber-Resilienz neu gedacht – schnell, stark, smart.

Referent:

Radek Mrskos,
Senior Pre-Sales Security Consultant

Agenda

01 NIST Framework mit SoftwareOne

02 Professional Services

03 Compliance & Governance

04 MDR Services

Intro

Problemstellung

- Cyberangriffe sind heute nicht die Ausnahme, sondern der Normalfall.
- Geschwindigkeit und Professionalität der Angreifer nehmen ständig zu.
- Klassische Security reicht nicht mehr – es geht um **Resilienz**.

Warum Resilienz?

- Cyber-Resilienz bedeutet: **vorbereitet sein, Angriffe abwehren, schnell reagieren und sich erholen.**
- Es geht nicht nur um Technik, sondern um einen ganzheitlichen Ansatz: Prozesse, Menschen, Governance.
- Das Ziel: **schnell, stark, smart**.

Unser Weg

- Wir haben dafür ein eigenes **SOC mit MDR-Services** aufgebaut.
- Ergänzt durch Bausteine wie **Governance, NIS2-Compliance, IT-Grundschutz, Risiko- und Schwachstellen-management**.
- Damit begleiten wir unsere Kunden auf dem Weg zu **dauerhafter Widerstandskraft**.

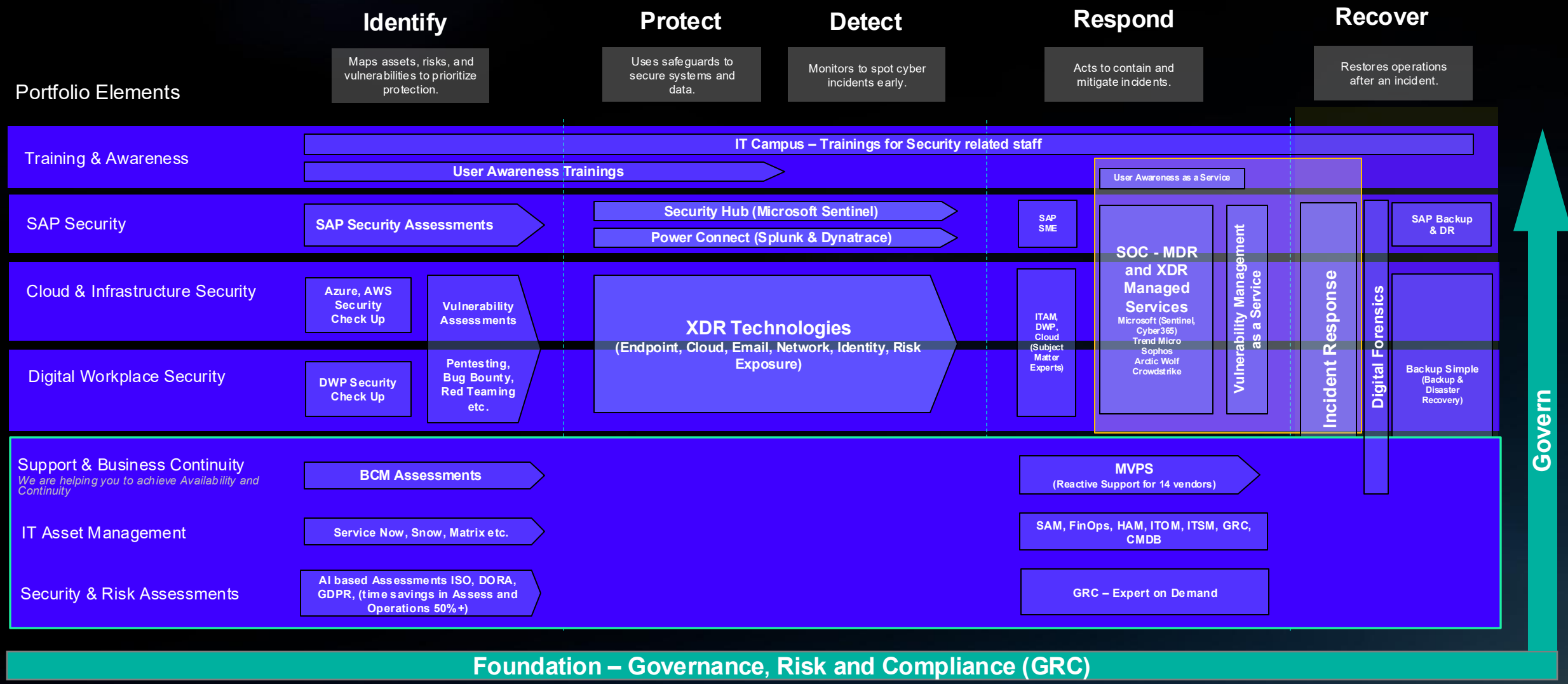
Strukturierung

- Doch wie strukturiert man diesen Weg?
- Dafür nutzen wir ein anerkanntes Modell: das **NIST Cybersecurity Framework**.
- Es bietet uns die fünf (bzw. sechs) Funktionen, mit denen wir Security **planbar und messbar** machen: *Identify, Protect, Detect, Respond, Recover, Govern*.

Alle 39 Sekunden passiert irgendwo auf der Welt ein Cyberangriff. Die Frage ist längst nicht mehr, **ob** es uns trifft, sondern **wie schnell und smart wir reagieren** können."

NIST Framework mit SoftwareOne

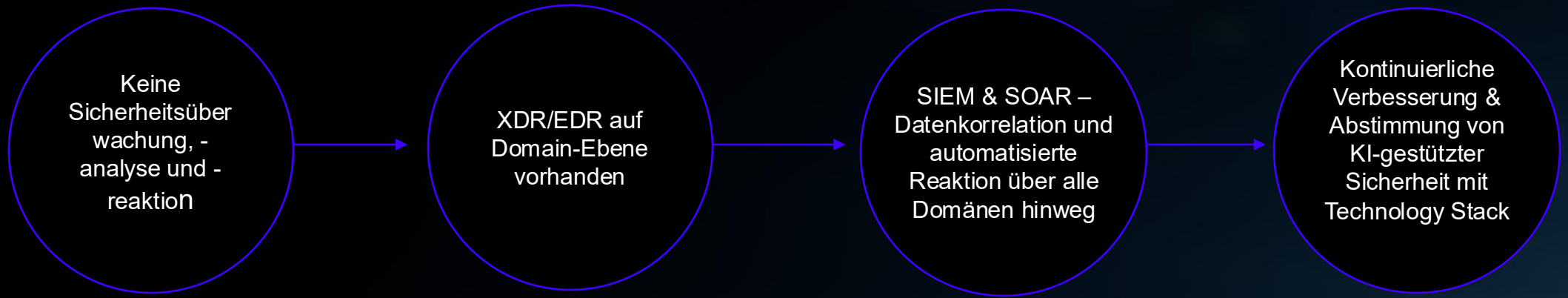
Kontinuierliche Verbesserung in SoftwareOne Services – wir führen Sie zu Tier 4 (Adaptive)



Unabhängige Hilfe für Ihre aktuelle Sicherheitslage

Wir beraten, liefern und managen

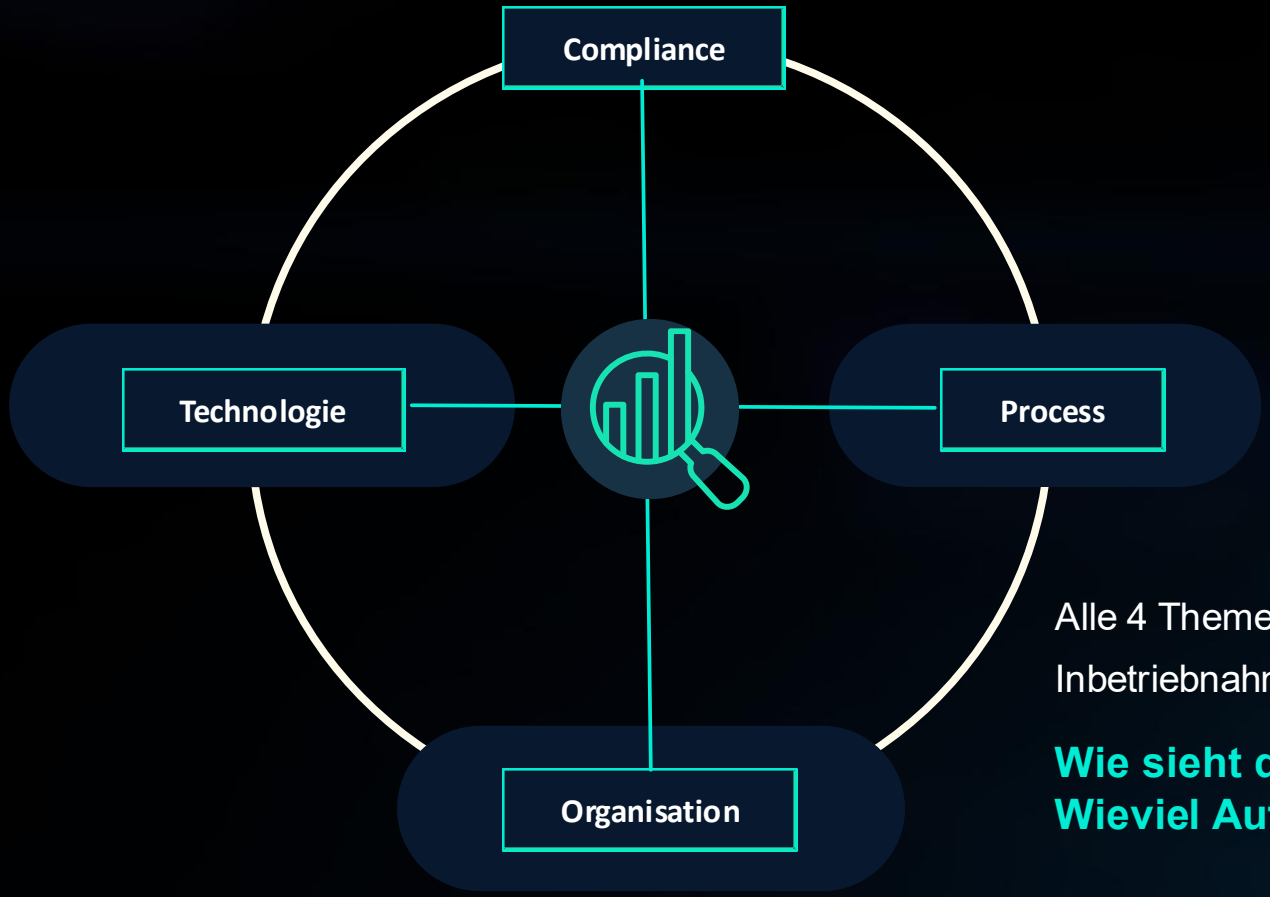
STEP 1	STEP 2	STEP 3	STEP 4
Kein Monitoring vorhanden	**XDR oder Best-of-Breed-Lösungen implementiert**	**Eingesetzte SIEM- und SOAR-Lösungen**	**Managed Detection & Response Services**
Wir ermöglichen es Ihnen, Bedrohungen zu erkennen, darauf zu reagieren und diese auf Basis von Frameworks wie ISO27001 oder NIST zu planen.	Wir bewerten und optimieren die XDR- oder Best-of-Breed-Lösungen nach Best Practices für die Sicherheit.	Wenn Sie über eine grundlegende Sicherheitsüberwachung verfügen, helfen wir Ihnen bei der Einrichtung einer automatisierten Reaktion auf Vorfälle.	Wir gewährleisten eine kontinuierliche Sicherheits-transparenz, -analyse und -reaktion über alle Unternehmensressourcen hinweg.



Govern: Wer hat das Ruder in der Hand?

Digitalisierung / Regulatorik

Die Herausforderung – “Das Bürokratie-Monster”



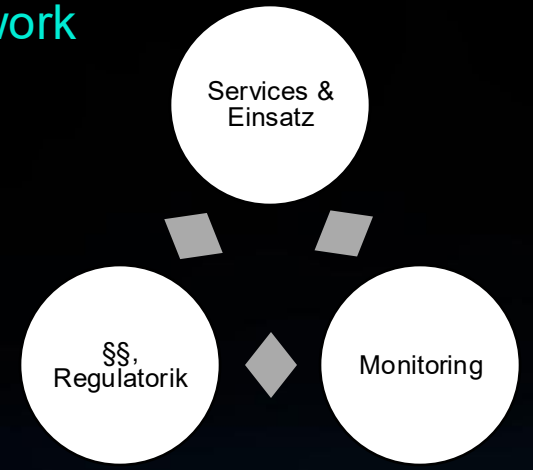
Alle 4 Themenfelder müssen vor einer Inbetriebnahme geklärt sein.

Wie sieht die Praxis aus?
Wieviel Aufwand ist es?

Govern | Identify | Protect | Detect | Respond | Recover

LEO – Legal and Organisation IT – Services & Compliance Framework

Wir sichern Ihre Qualität durch ein ganzheitliches Führungs- und Steuerungsinstrument.



Strategie
Ausrichtung
Geltungsbereich
Risiken

U1: Unternehmensausrichtung

- Unternehmensstrategie
- Unternehmensprozessmodell (Kernprozesse)
- Compliance (Externe Anforderungen)
- Governance (Interne Umsetzung)
- Risk Management Unternehmen (BCM)
- Lieferantenmanagement (u.a. Outsourcing)

S1: Ausrichtung

- IT-Leitlinie
- IT-und Cloud-Strategie
- IT-Sicherheitskonzept
- Datenschutz

Management
Steuerung
Anforderungen
& Reporting

M1: Anforderungen

- IT-Service: MS, SAP Risikomanagement
- Geltungsbereich
- Datenklassifizierung

M2: Reporting

- Monitoring
- Servicebericht
- IT-Sicherheitsbericht
- Investitionsplan
- Datenschutzbericht

M3: Prozesse/Verfahren

- Kapazitätenplanung
- On-/Offboarding
- prüfbare Prozesse
- Lizenzmanagement
- Vertragsmanagement
- Datenschutz (formell)

M4: Outsourcing

- Auslagerungs-management
- Auftragsverarbeitung
- Monitoring Partner
- Managed-Services

Operativer
IT-Betrieb
Leistungen
und Services

O1: Betrieb / Prävention

- Betrieb Services TEAMS, SAP, AI
- Verfügbarkeiten und Sicherheit pro Service
- techn. Notfallvorsorge
- Richtlinien IT
- Datenkontrolle/-qualität
- IAM (Berechtigungen)
- Datenschutz pro Service

O2: Notfallmanagement

- Wiederanlaufpläne
- Meldewege
- Notbetrieb/Krise
- Notfallhandbuch

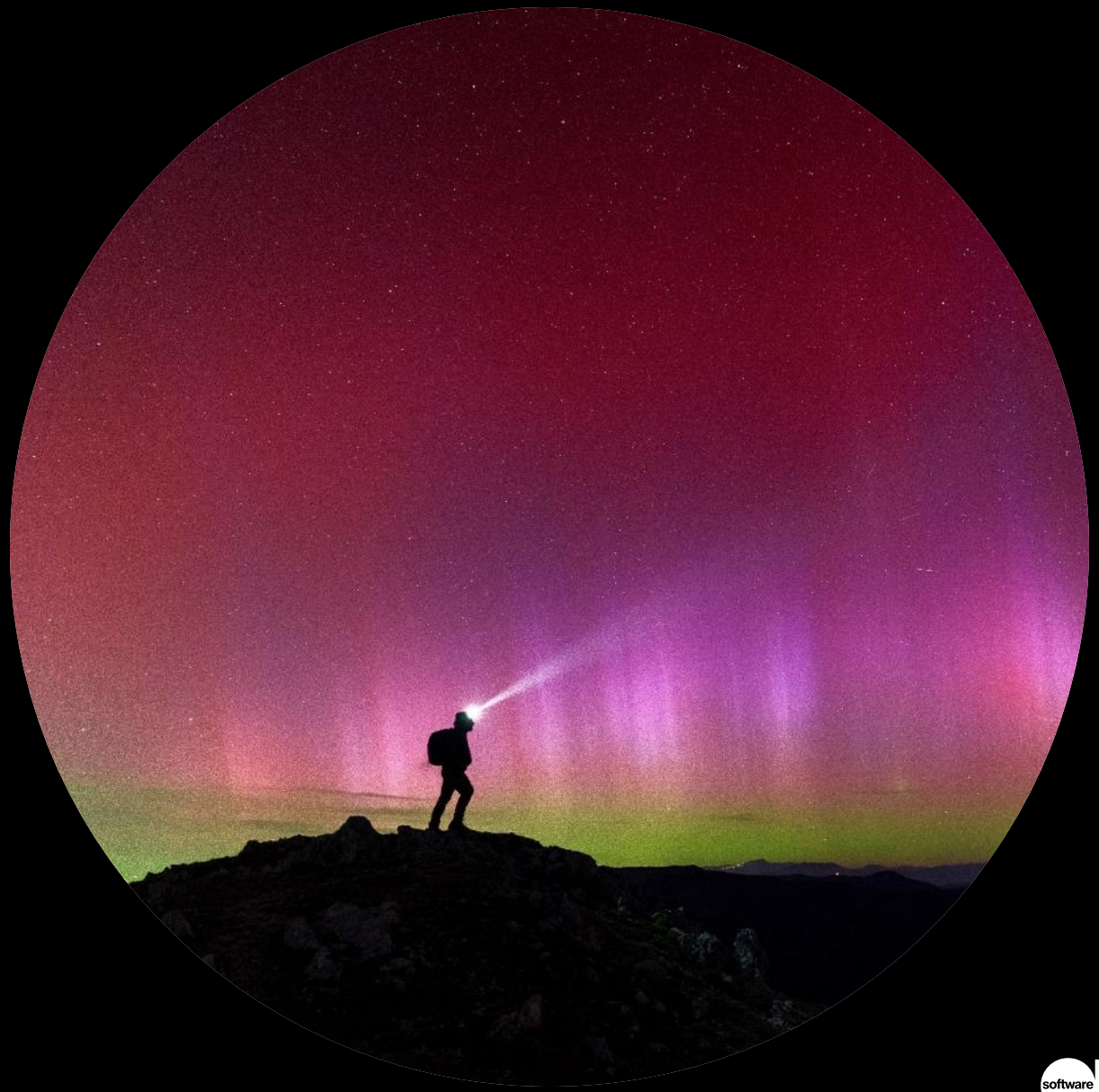
O3: Aufrechterhaltung

- IKS - Internes Kontrollsystem
- Sensibilisierungsmaßnahmen
- Audits, Testläufe Notfall
- Stand der Technik (Cybersecurity, Pentests)
- IT Revision

O4: Betriebs-Doku

- Betriebsdokumentation pro Service
- Sonstige Dokumente (VV, Risk, Auditberichte)

Identify: Assessments / GAP-Analyse



Outlook: GAP Analyse

Priorisierung von Handlungsvorschlägen – Ergebnis einer GAP Analyse

Phase 1 (Assessment) → **Phase 2** (Implementierung) → **Phase 3** (CIM)

Projektmanagement

Gap-Analyse

Erfassung und Auswertung der Daten gemäß Security-Standards
(ISO, DORA, NIS 2 etc.)

Organisatorische Umsetzung
ISMS + BCM

Adoption- und Change-Management (ACM)

Technische Umsetzung
Branchenführenden Sicherheitslösungen

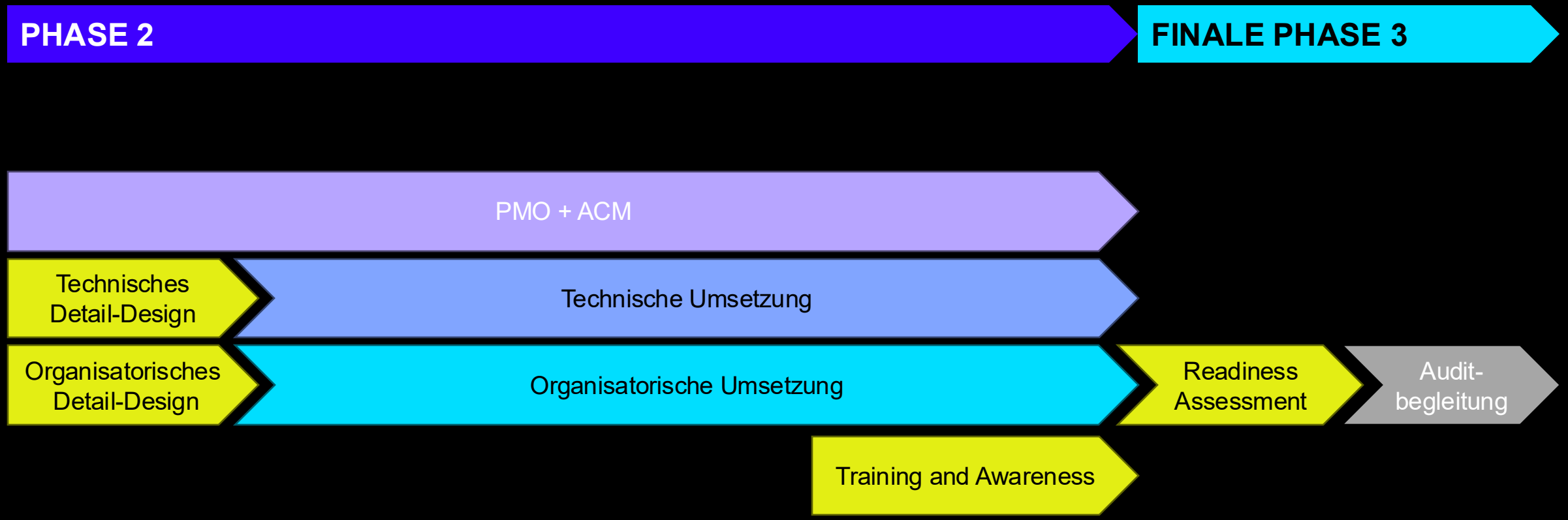
Erfüllung der Frameworks

Continuous Improvement Management (CIM)

Unterstützungsleistungen durch Expert on Demand und Managed Dienstleistungen

Phase 2 und 3 im Detail

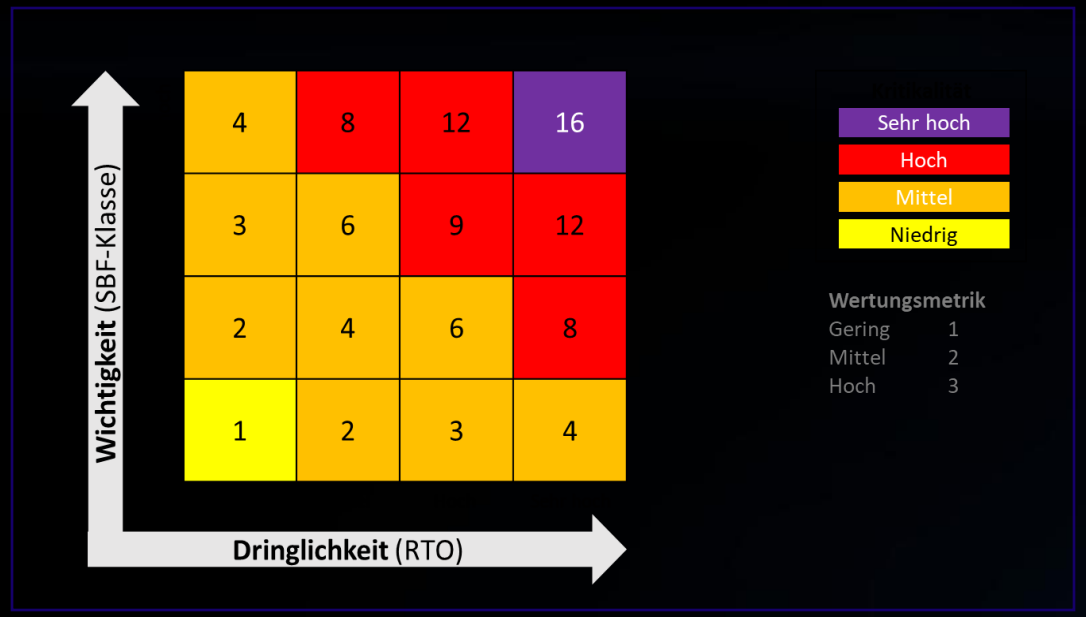
Govern | Identify | Protect | Detect | Respond | Recover



Outlook: GAP Analyse

Priorisierung von Handlungsvorschlägen – Ergebnis einer GAP Analyse

Alle im Workshop erfassten Handlungsvorschläge werden in ihrer Kritikalität durch eine einheitliche Metrik bewertet.



Kritikalitätsbewertung von Maßnahmen

	Jan `21	Feb	Mär	Apr	Mai	Juni	Juli	Aug	Sep	Okt	Nov
1.	Thema #1										
2.			#2								
3.	Thema #3										
4.	Thema #4										
5.	Parallel-Projekt X										
6.		Thema #5									
7.	#6										
8.	Thema #7										
9.				Thema #8							
10.	Thema #9			Thema #10							
11.										#11	
12.	Thema #12										

Mittelfristige Umsetzungsplanung

Im Anschluss wird ein Umsetzungsplan der einzelnen Maßnahmen erarbeitet.

Umfrage

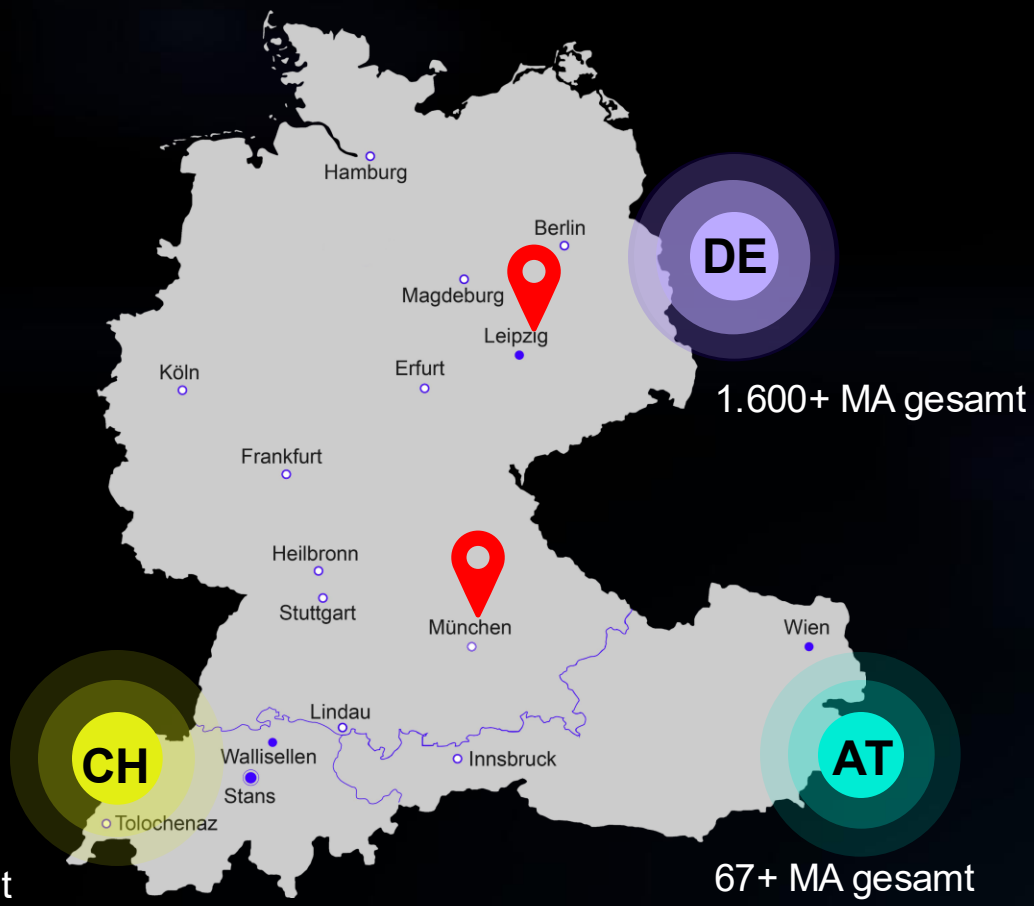
Wie erleben Sie aktuell den Aufwand rund um Compliance und regulatorische Anforderungen in Ihrem Unternehmen?

- **Wir haben Prozesse etabliert und empfinden den Aufwand als gut handhabbar.**
- **Wir sind gut aufgestellt, aber der Aufwand wächst spürbar.**
- **Regulatorische Anforderungen bremsen uns – wir suchen nach pragmatischen Lösungen.**
- **Wir sind noch dabei, unsere Compliance-Prozesse zu strukturieren.**

Managed Detection and Response mit deutschem SOC

SoftwareOne DACH in Zahlen

24x7 OnCall SOC
DACH (Leipzig, Munich)



1.600+ MA gesamt

248+ MA gesamt

67+ MA gesamt

Standorte Head Offices Headquarter SoftwareOne Group

16
Standorte in DACH

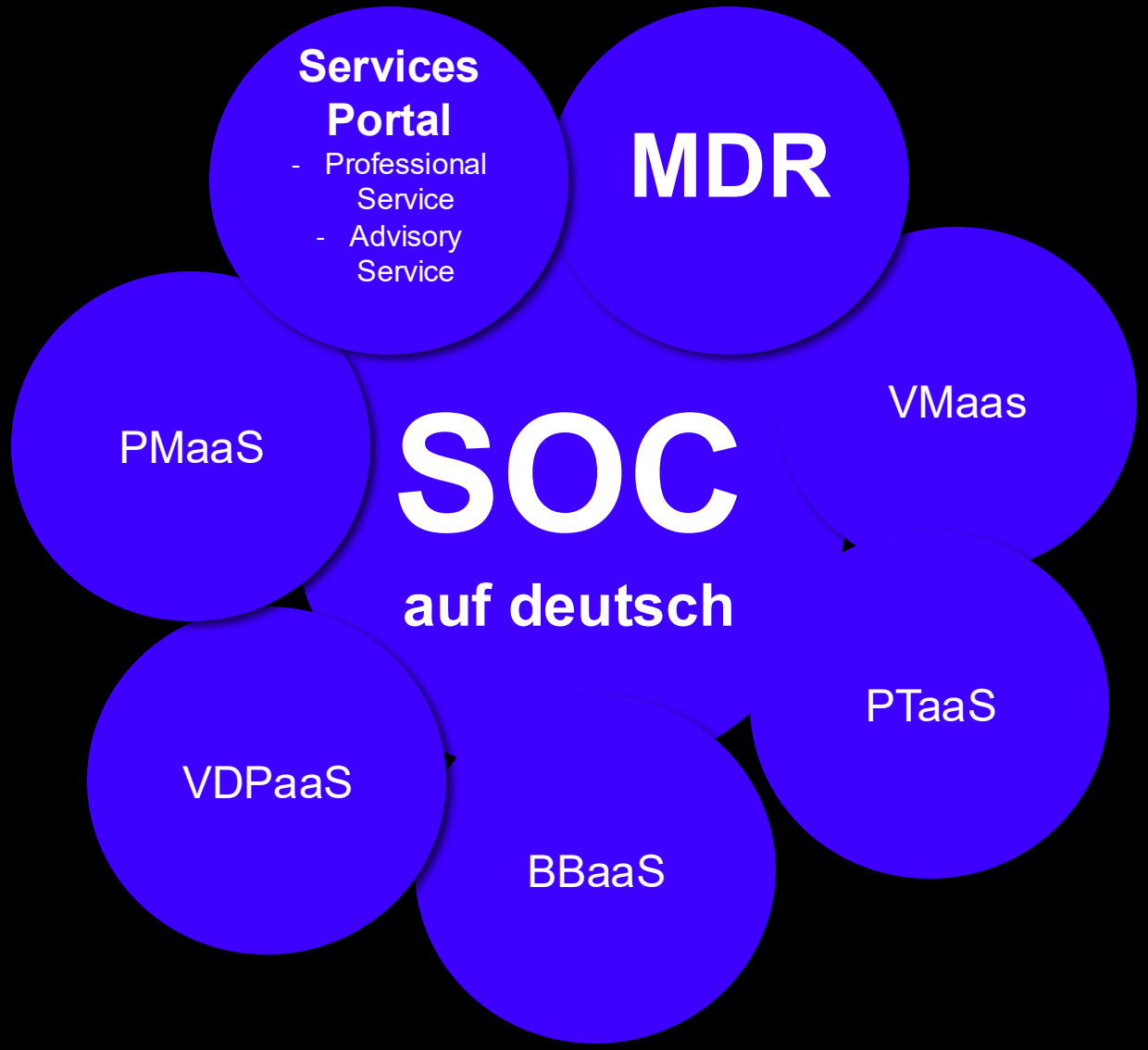
1.915+
Mitarbeiter und Mitarbeiterinnen in DACH

24.000+
Kunden

560
zertifizierte Service-Spezialisten

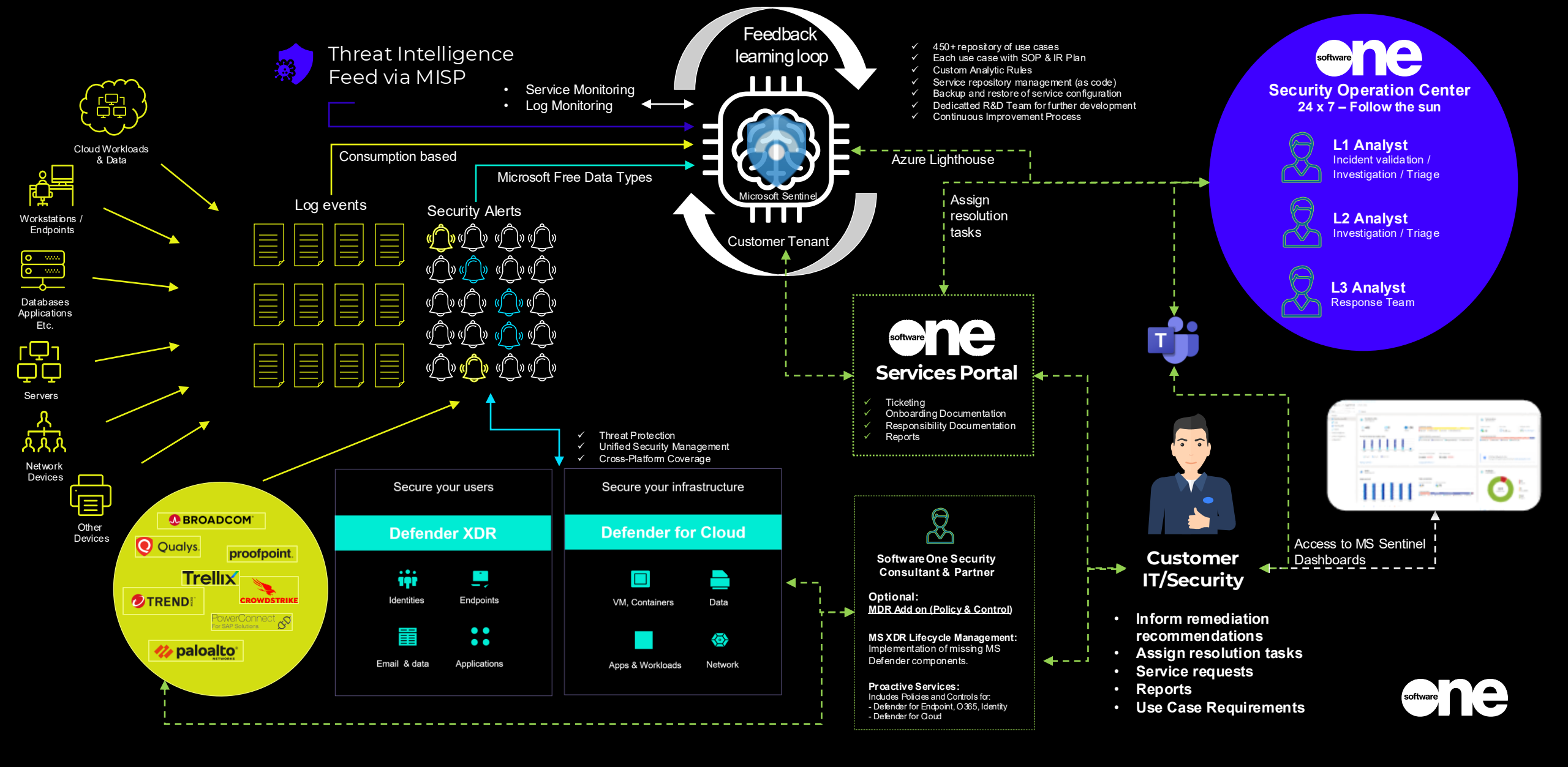
End-to-End-Schutz für jeden das Richtige.

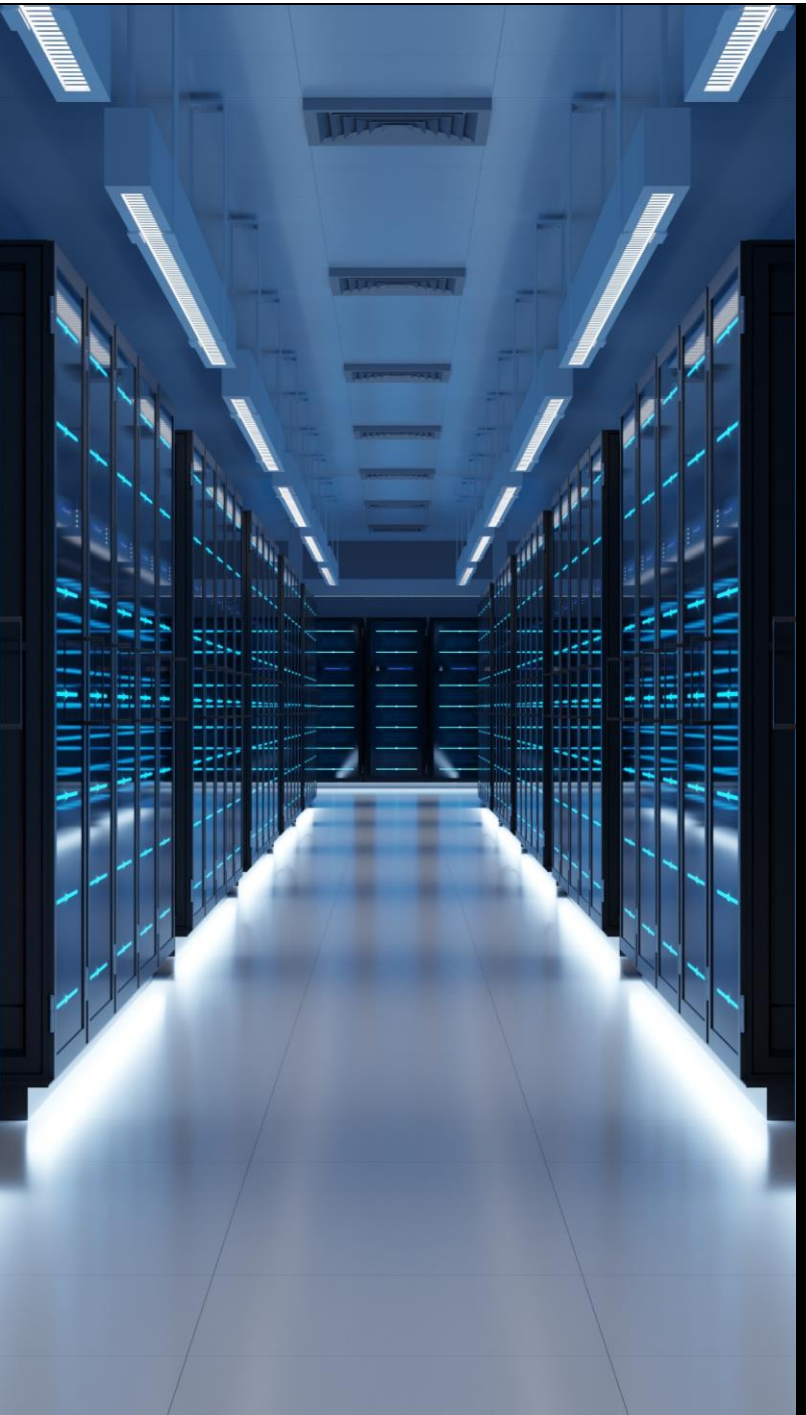
End-to-End-Schutz für alles Wichtige.



Govern | Identify | Protect | Detect | Respond | Recover

Einheitliche Sicherheitsabläufe mit MDR (Bsp. MS Sentinel)





Govern | Identify | Protect | Detect | Respond | Recover

450+ vordefinierte Sicherheits-Anwendungsfälle

Wir arbeiten aktiv sowohl mit manuellen Maßnahmen, die von SWO-SOC-Analysten ausgeführt werden, als auch mit automatisierten Lösungen, die auf einer Bibliothek vordefinierter Anwendungsfälle für Bedrohungsreaktionspläne basieren.

Azure DevOps Integration

Azure DevOps-Integration und Lösungsbereitstellung über CI/CD-Pipelines. Diese Fähigkeit steigert die betriebliche Effizienz und stärkt die Cybersicherheit unserer Kunden.

Globales SOC-Management 24x7

Dies gewährleistet unseren Kunden weltweit einen kontinuierlichen Zugang zu fachkundiger Sicherheitsüberwachung, unabhängig von ihrem Standort und ihrer Zeitzone.

In wenigen Tagen einsatzbereit

Durch die Nutzung von Automatisierung, intelligenten Datenanalysetools und einer Bibliothek vordefinierter Szenarien sowie unserem optimierten Onboarding-Prozess können wir unseren Kunden einen schnellen Übergang von der Einrichtung zur Umsetzung ermöglichen.

software one

Kosten optimieren

Kosten senken

Rationalisieren Sie Ihre Sicherheitsausgaben für fragmentierte Sicherheitslösungen. Unser Service bietet Sicherheit auf Unternehmensniveau zu einem überschaubaren Budget und in jeder Größenordnung.

Maximiert den ROI

Verschaffen Sie sich mit branchenführender Technologie einen vollständigen Überblick über Ihre Sicherheitslage und Bedrohungslandschaft.

Senken Sie Ihre Gesamtbetriebskosten

Beschleunigen Sie den Einstieg und reduzieren Sie gleichzeitig Infrastruktur und Wartung mit der Pay-as-you-go-Cloud-Technologie, und maximieren Sie Ihre vorhandenen Microsoft-Investitionen.

Arbeitsplatzbasierte, vorhersehbare Kosten

Sie zahlen nur für das, was Sie benötigen und ohne Ihnen Gebühren auf der Grundlage der aufgenommenen Protokolldaten in Rechnung stellen. Sie werden in der Lage sein, die Servicekosten im Voraus vorherzusagen.

Beispiel für ein Kunden-Dashboard (monatliche Statistik)

Kundengröße: 8000 Mitarbeiter
17 Datenquellen, die in Microsoft Sentinel integriert sind

Alerts and incidents	Number of alerts
Events summarised by Sentinel tables	**1 461 000 000**
Security alerts	15 600
Security incidents	**6 900**
Auto-incident enrichment and false positives auto closure	4 000
Manual investigation (by SoftwareOne Blue Team)	**2 900**
True positives	**320**
Incidents resolved by SoftwareOne and reported to the client (incl. remediation)	180
Handover to client [manual actions]	**10**

MDR für Microsoft Sentinel – Serviceangebot

Core Services:

- **Onboarding (Einmalige Gebühr)**
  - Inklusive 5 Datenquellen, kann der Client bis zu 300 weitere Datenquellen als Add-on hinzufügen
- **Alert Monitoring and Incident Response (monatlich)**
  - (Gebühr für den verwalteten Dienst für die Anzahl der Identitäten, die der Kunde verwendet)

Add-Ons (Einmalige Gebühr):

- Standardmäßiges Onboarding von Datenquellen/Konnektoren
- Onboarding von benutzerdefinierten Datenquellen/Konnektoren
- Onboarding von benutzerdefinierten Anwendungsfällen
- Forensische Dienstleistungen (jeder Block dauert 50 Stunden)
- Integration von EDR-Lösungen von Drittanbietern
- Integration von ITSM-Tools

Key Takeaways

Compliance Neu Denken

Holen Sie sich schon heute die Zukunft ins Haus – mit KI und erprobten Methoden beschleunigen wir gemeinsam Ihre Verfahren und bändigen das Bürokratiemonster Regularien.

Best of Breed vs. XDR

Nicht jede Architektur passt zu jedem Unternehmen. Orientieren Sie sich an anerkannten Standards, um herauszufinden, ob ein spezialisierter Ansatz oder eine integrierte XDR-Lösung besser zu Ihrer Sicherheitsstrategie passt.

Managed Services

Sie können mit SoftwareOne technologieunabhängige MDR Dienste aus unserem SOC in Leipzig und München erwerben.

SoftwareOne IT Campus

SoftwareOne Security Operations Center Training – Basic

Besuchen Sie unser Training zum Thema!

Menschliches Versagen ist die Hauptursache für Fehler bei Cybervorfällen.

In der „Cyber Training Range“ trainieren Teilnehmer Erkennung, Abwehr und Management solcher Angriffe.

Kurs: SEC-SOCL1

Jetzt anmelden →


Q&A


Thank you

Get in Touch

Radek Mrskos
Senior Cybersecurity Pre-Sales Consultant

Radek.Mrskos@softwareone.com
www.softwareone.com/de-at

Disclaimer