SOPHOS

Cyberangriffe erkennen, bevor sie passieren:

HABAUs smarter Schutz mit SOC-Services

Ausgangsituation

- Vor ca. 7 Jahren wurden Endpoint Lösungen getestet.
  - Nextgen Endpoint wurde beschafft
    - Entscheidung fiel auf spezialisierten EDR Anbieter
- EDR Anbieter wurde von größerem Hersteller geschluckt
    - Seitdem war der Support nicht mehr zufriedenstellend
- Anforderungen an Lösung haben sich geändert
- Eine neue Gesamtlösung wurde beschafft

Challenges im Laufenden Betrieb

False Positives

PowerShell-Nutzung

PowerShell wird häufig für IT Operations genutzt. Dies führt zu Warnungen bei verwalteten Computern.

Auswirkungen von Fehlalarmen

False Positives erhöhen die Workload und führen zu Alert Fatigue.

Balance zwischen Sicherheit und Genauigkeit

Weit gefasste Ausnahmen reduzieren den Schutz und vergrößern somit die potenzielle Angriffsfläche.

COVID – Home Office

- Verlagerung des Arbeitsplatzes ins Homeoffice
  - Da viele Projekte stillstanden blieb den Administratoren mehr Zeit um sich mit der EDR Lösung zu beschäftigen

Was sind das für Alarme genau?

Ist das kritisch oder nicht?

Da hat sich jede Menge angesammelt!

SOPHOS

Aufarbeitung Events

- Große Anzahl Events werden kontinuierlich erzeugt
- Viele Erkennungen erfordern genauere Analyse durch Experten
- Ohne Automatisierung unmöglich zu bewältigen

Schlussfolgerung

Zu komplex

Expertise benötigt

Neuevaluierung vor Vertragsende

- Endpoint Schutz mit einfacher Handhabung
  - Best Practices Built-in
  - Möglichkeit einfache Ausnahmen zu erstellen
- Mehrwerte durch XDR
  - Automatisierte Erkennung von Gefahren
  - Größerer Focus (nicht nur Endpoint)
- Mehrwerte durch MDR
  - Unterstützung durch externe Expertise

SOPHOS

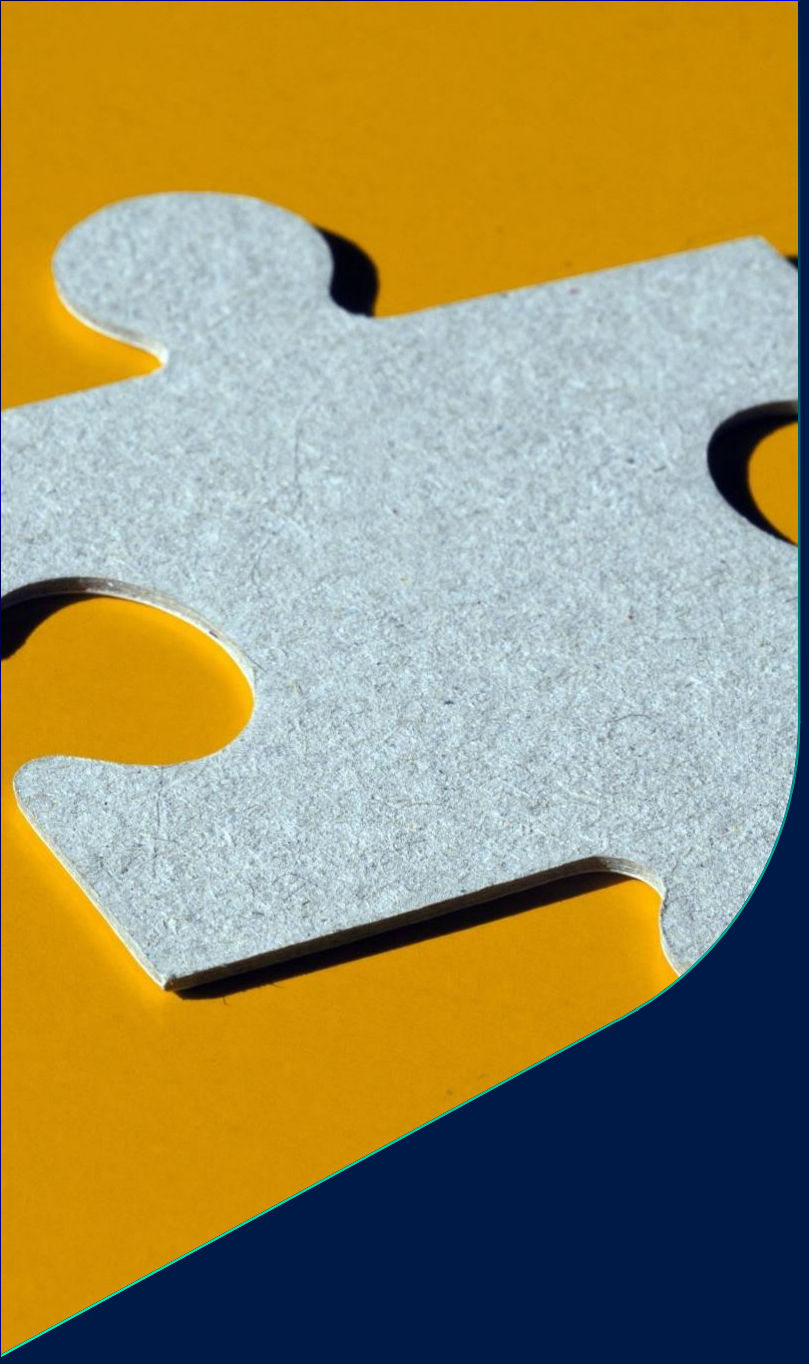
Neue Anforderungen

- Next Gen EP
  - Verhaltenserkennung
  - Control Features
- KI gestützte Erkennung
  - Kein reiner Signaturen Basierter Scanner
  - Weniger False Positives und Negatives
- Schnelle Unterstützung durch externes SOC
- Zuverlässiger Support

Ergebnis

- Neue Lösung wurde eingeführt die
  - Weniger False Positives und Negatives liefert
  - Schnelle Reaktionszeiten ermöglicht
  - Service der uns als Kunden ernst nimmt
- Kontinuierlicher Ansprechpartner
  - Security wird stetig verbessert
  - Bessere Zukunftsplanungen
- „Es schläft sich viel besser, wenn jemand da ist, der reagiert, sollte etwas sein..“
- „Es ist jemand da, der mit seiner Expertise unterstützt!“

SOPHOS



Lösung

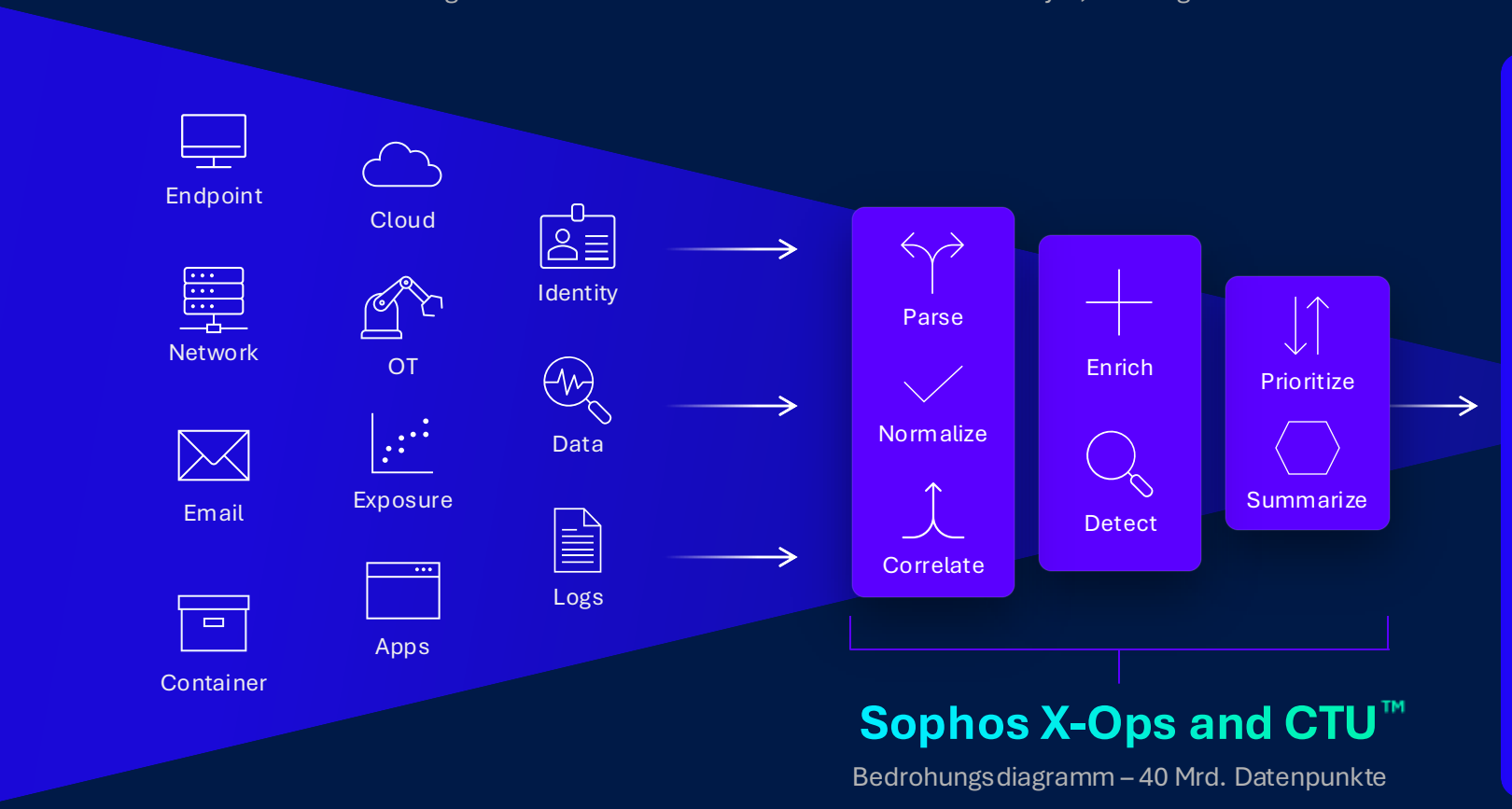
- Sophos Next Generation Endpoint Agent
  - Einfache Ausrollung
  - Schutz Module können einfach per Knopfdruck ausgerollt werden
  - App Control einfach Umzusetzen
  - Web Control
  - Device Control
- Sophos XDR/MDR Service
  - Mehrwert: XDR filtert vor…
  - 24/7 Monitoring und Reaktion
  - Ausrollen ist sehr einfach: sehr schnell…

SOPHOS

Plattform für Sicherheitsoperationen

Umfassender Input

350+ Integrationen



Erkennen und Korrelieren

223 Terabyte; 34M Tägliche Detektionen

Untersuchen und reagieren

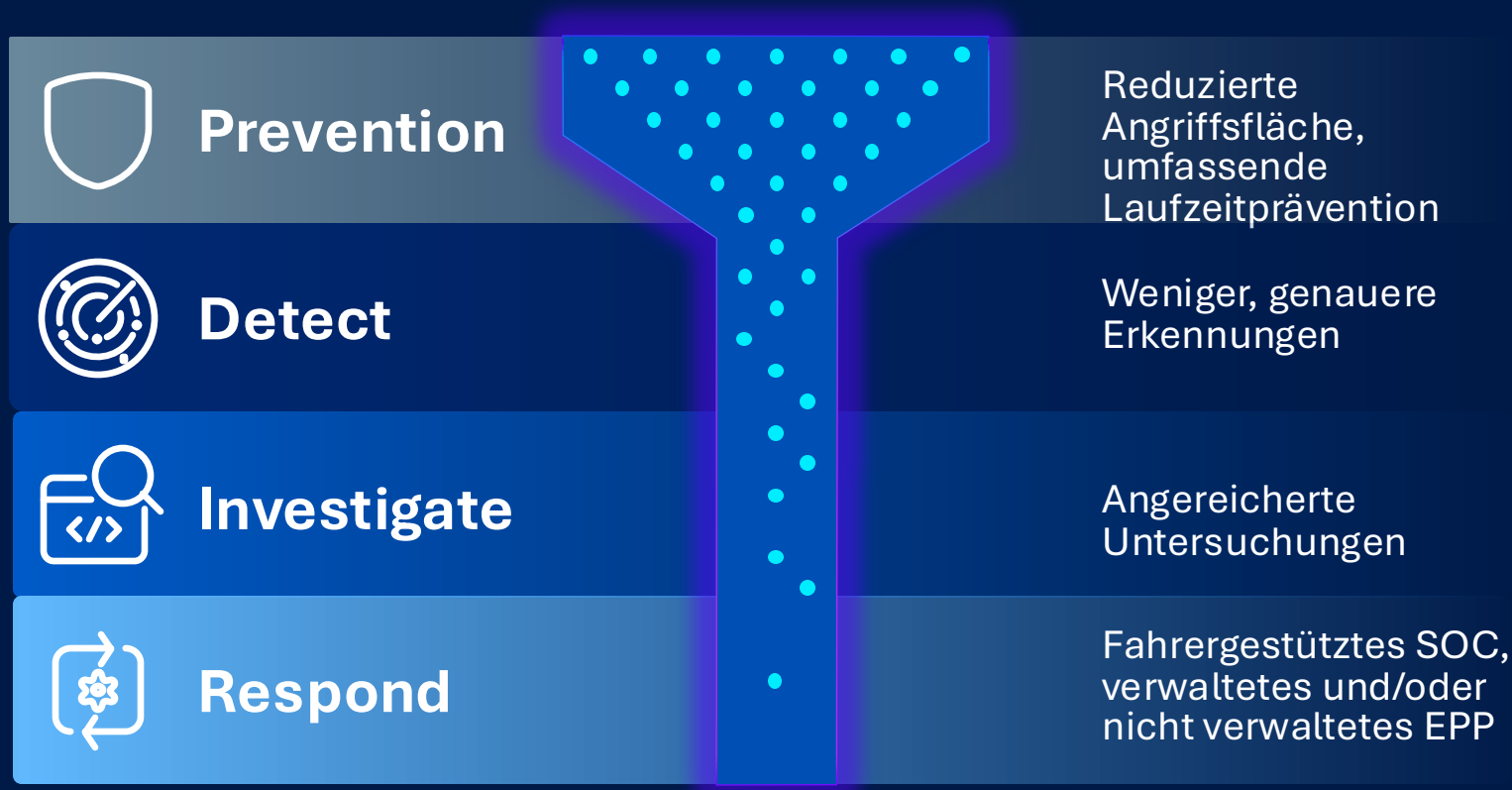
1.100+ Untersuchungen; 230+ Angriffe täglich gestoppt

Sophos X-Ops and CTU™

Bedrohungsdiagramm – 40 Mrd. Datenpunkte

SOPHOS

Optimierter Schutz und reduzierte Reaktionszeiten



Reduzierte Angriffsfläche, umfassende Laufzeitprävention

Weniger, genauere Erkennungen

Angereicherte Untersuchungen

Fahrergestütztes SOC, verwaltetes und/oder nicht verwaltetes EPP

99,98 % der Bedrohungen automatisch blockiert

MTTD <1 Min

MTTI <25 Min

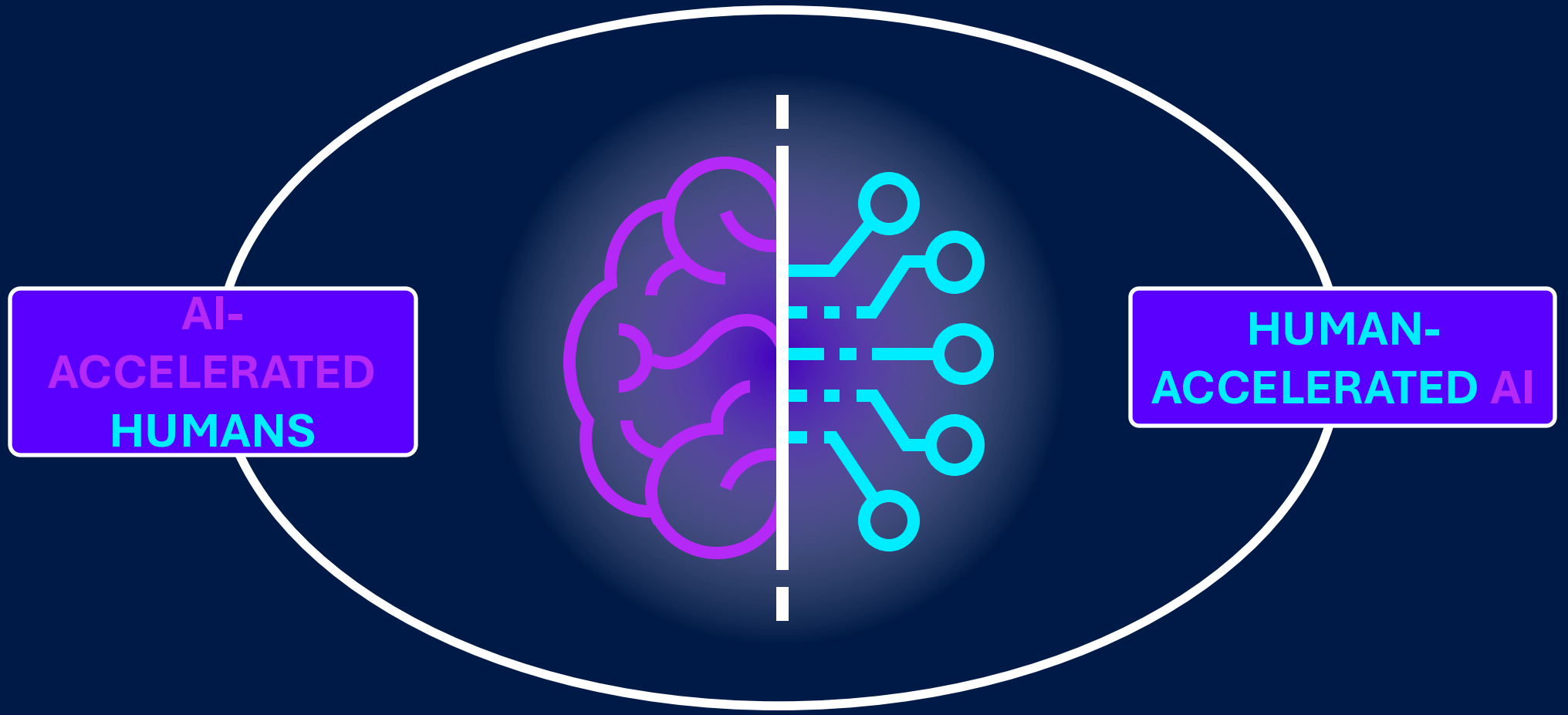
MTTR <12 Min

Überragendes Ergebnis

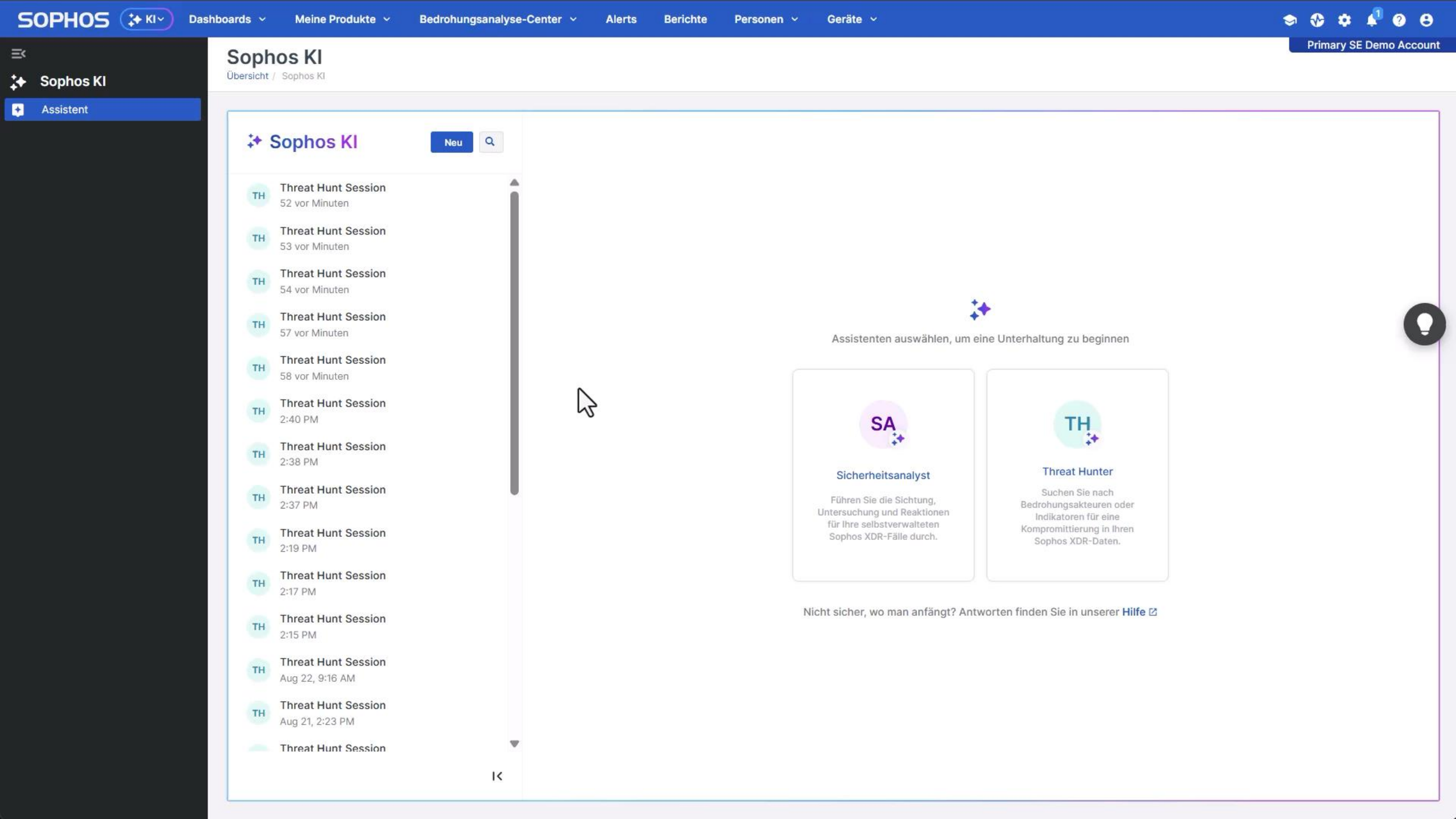
(Weniger Risiko, höhere Effizienz, geringere Kosten)

SOPHOS

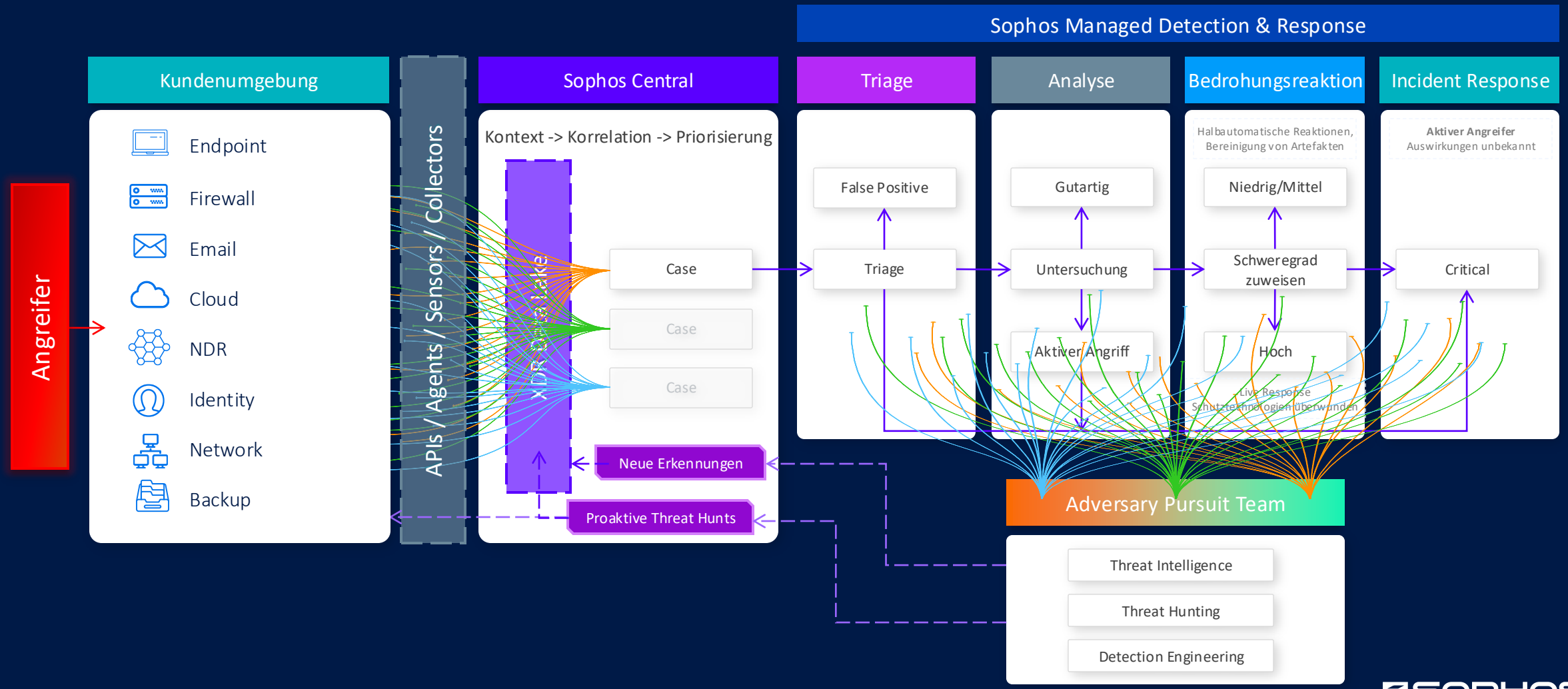
Automatisieren Sie mit Mensch-Maschine-Kollaboration



SOPHOS


SOPHOS
KI
Dashboards
Meine Produkte
Bedrohungsanalyse-Center
Alerts
Berichte
Personen
Geräte
Primary SE Demo Account
Sophos KI
Assistent
Sophos KI
Übersicht / Sophos KI
Sophos KI
Neu
TH Threat Hunt Session 52 vor Minuten
TH Threat Hunt Session 53 vor Minuten
TH Threat Hunt Session 54 vor Minuten
TH Threat Hunt Session 57 vor Minuten
TH Threat Hunt Session 58 vor Minuten
TH Threat Hunt Session 2:40 PM
TH Threat Hunt Session 2:38 PM
TH Threat Hunt Session 2:37 PM
TH Threat Hunt Session 2:19 PM
TH Threat Hunt Session 2:17 PM
TH Threat Hunt Session 2:15 PM
TH Threat Hunt Session Aug 22, 9:16 AM
TH Threat Hunt Session Aug 21, 2:23 PM
Threat Hunt Session
Assistenten auswählen, um eine Unterhaltung zu beginnen
SA
Sicherheitsanalyst
Führen Sie die Sichtung, Untersuchung und Reaktionen für Ihre selbstverwalteten Sophos XDR-Fälle durch.
TH
Threat Hunter
Suchen Sie nach Bedrohungsakteuren oder Indikatoren für eine Kompromittierung in Ihren Sophos XDR-Daten.
Nicht sicher, wo man anfängt? Antworten finden Sie in unserer Hilfe

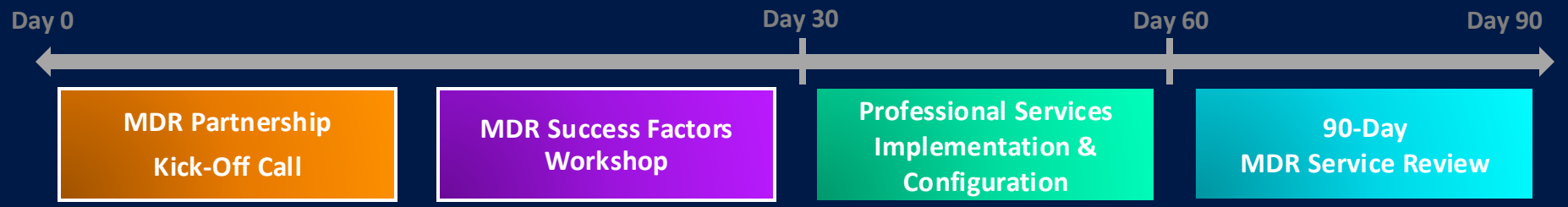
MDR Detection & Response Prozess



Umsetzung

- MDR Service wurde bestellt.
- Sophos Central wurde schnell eingerichtet
- Agents über Software Deployment ausgerollt

MDR Onboarding

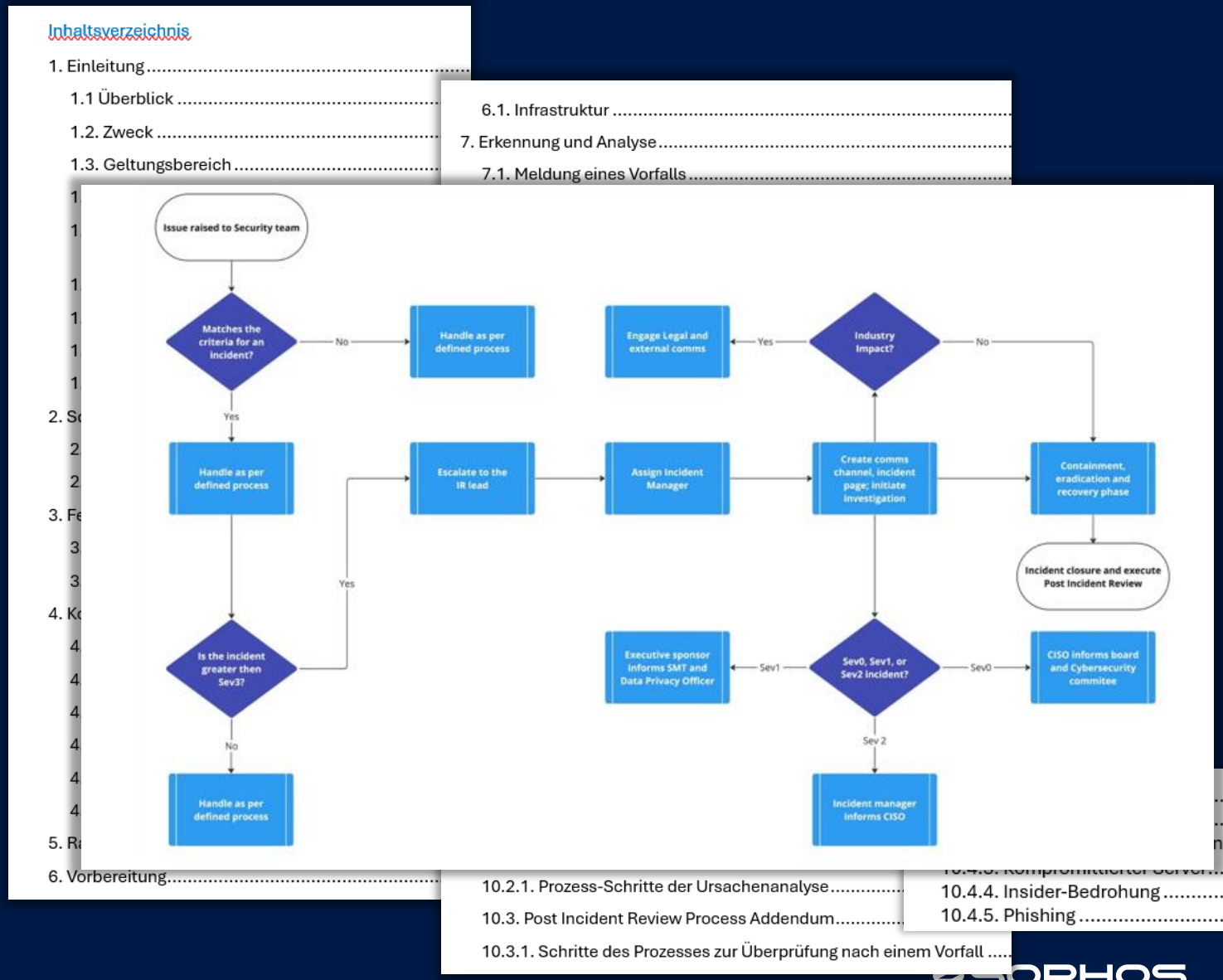


Business as usual...

SOPHOS

Sophos Incident Response Planner

- Kostenloses Sophos Tool zum **Erstellen** eines **Incident Response Plans**
- Basierend auf **Richtlinien** und **Empfehlungen** von **NIST** und **CISA**
- Dient als wesentliches **Instrument** zur effektiven **Bewältigung** und **Eindämmung** von **Sicherheitsvorfällen**
- Durch einen strukturierten Ansatz hilft dieser Plan, **Ausfallzeiten** zu **reduzieren** und **Schäden** zu **minimieren**



Penetration Tests

Service	Ziel
External Penetration Testing	Was kann ein Angreifer vom Internet aus sehen und worauf kann er zugreifen?
Internal Penetration Testing	Was könnte ein Angreifer tun, wenn er Zugriff auf unser Netzwerk erhält? Könnten wir ihn erkennen?
Wireless Network Penetration Testing	Ist unser drahtloses Netzwerk sicher? Gibt es unautorisierte oder versteckte Geräte?
Web Application Security Assessment	Sind unsere Webanwendungen sicher? Werden sensible Daten offengelegt? Wie können wir Schwachstellen beheben?

SOPHOS

Direkter Ansprechpartner

- MDR Customer Success
  - Stellt sicher, dass
    - die gewünschten Ergebnisse erreicht werden.
    - Technologie im vollen Umfang genutzt wird.
    - Risiken identifiziert und proaktiv behoben werden.
    - langfristige Beziehung aufgebaut wird.
  - Fungiert als Eskalationsstelle und strategische Berater.

SOPHOS

Blick in die Zukunft...

Sophos MDR + Sophos ITDR

Ein ganzheitlicher Ansatz zur Reduzierung des Identitätsrisikos Ihres Unternehmens

Schützt Gegen Identity Threats

Sophos untersucht in Ihrem Auftrag identitätsbasierte Bedrohungen mit hohem Risiko und reagiert darauf

Reduziert die Angriffsfläche für Identitäten

Kontinuierliches Scannen der Microsoft Entra ID auf Identität Sicherheitslücken

Minimiert das Risiko gestohlener Anmeldeinformationen

Warnungen, wenn Anmeldeinformationen im Dark Web offengelegt werden und Datenbanken verletzt werden

Identifiziert riskantes Benutzerverhalten

Überwacht auf abnormale Aktivitäten im Zusammenhang mit gestohlenen Anmeldeinformationen

Sophos MDR

Sophos ITDR (Add-on)

SOPHOS

Wer hilft im Notfall?

Im Notfall

Sophos Emergency Incident Response Hotline

Wir sind 24/7 für Unternehmen da, die einen Cyberangriff erleben

Australia	+61 272084454	**Italy**	+39 02 94752 897
Austria	+43 73265575520	**Switzerland**	+41 445152286
Canada	+1 7785897255	**United Kingdom**	+44 1235635329
France	+33 186539880	**United States**	+1 4087461064
Germany	+49 61171186766	**Email:** EmergencyIR@sophos.com	

SOPHOS


SOPHOS