

Don't just be protected. Be resilient.

*Schutz-, Erkennungs- und Reaktionsmaßnahmen optimieren -
mit Hilfe von Cisco CX Cybersecurity Services und TALOS Threat
Intelligence*

Manuel Beicht

Business Development Manager – Cyber Resilience & Breach Defense

Oktober 2022



Seit 2007 bei Cisco...

- Network Consulting Engineer
- Solution Integration Architect
- Business Development Manager

Technologien (chronologisch):

- Routing & Switching (CCIE #22457)
 - Collaboration
 - IoT & SmartCities
 - Security
-
- ✓ Zertifizierter CISO/ITSiBe & BSI IT Grundschutz Praktiker
 - ✓ Seit 2020 die deutsche Schnittstelle zu Cisco Talos

Schwerpunkt-Themen: **Cyber Risiko Management, Cyber Resilienz, Breach Defense, Incident Response**



Bedrohungslage 2022

Die größten Gefahren?

Ransomware & Commodity Malware

- Fokus auf Telekommunikations-Industrie, Bildungseinrichtungen und Behörden sowie Krankenhäuser
- Haupteinfallstor weiterhin E-Mail
- Lateralbewegungen ermöglichen tiefgreifende und dadurch längerfristige Infiltrierung, bedingt durch fehlende Netz-Segmentierung

Zunahme von Phishing & BEC

- Voice Phishing & MFA Fatigue (→ “Cisco Hack”)

Cyber Warfare (Ukraine Crisis)

- Unternehmen mit russischer Herkunft oder Beteiligung im Visier
- Erhöhte Alarmbereitschaft für KRITIS Betreiber

Potential Major Vulnerabilities (e.g. Log4j)

Häufige Fehler, die den Angreifer lächeln lassen

- 1) Keine oder unzureichende **E-Mail Security** → Gute oder böse E-Mail?
- 2) Keine oder unzureichende **Endpoint Protection** → Anti-Malware statt Anti-Virus
- 3) Keine oder unzureichende **DNS Security** → Wohin will mein Client?
- 4) Makro- statt **Mikro-Segmentierung** → Querbewegungen verhindern!
- 5) One-Time Trust statt **Zero Trust** → Überprüfe jede Art von Kommunikation / Zugriff
- 6) Zu wenig **Visibilität** → Ende-zu-Ende Sichtbarkeit, Baseline-Pattern vs. Anomalie, MTTD, initialer Vektor
- 7) Kein Risiko-basiertes **Schwachstellen-Management** → Wo sind meine kritischen Assets verwundbar?
- 8) Fokus auf Technologie – nicht auf **Prozesse & Expertise** → Anomalie erkannt...und dann?
- 9) Überschätztes **SOC/SecOps** → Ein SOC ohne 24x7 Abdeckung ist kein SOC -und SOC ist nicht gleich NOC!
- 10) Keine ausgereiften **Incident Response/CERT Prozesse** → RCA, Forensik und Threat Hunting sind keine SOC Aufgaben!
- 11) **Security Awareness** & Culture → Das erste Angriffsziel befindet sich auf Layer 8
- 12) Unzureichendes **Risiko-Management** – Streben nach 100% Schutz statt Risiko Akzeptanz

Wovon alle Hersteller sprechen: **Cyber Resilienz**

- "Die **Fähigkeit** eines Unternehmens, den **IT-Betrieb auf nahezu normalem Niveau aufrechtzuerhalten**, obwohl es Opfer eines erfolgreichen Cyber-Angriffs geworden ist."
- "Cyber-Resilienz ist ein **Indikator** dafür, wie gut Unternehmen sich auf einen Cyber-Angriff **vorbereiten**, ihn **überstehen** und wie schnell sie sich davon **erholen**."
- "Ein Unternehmen mit einem guten Cyber-Resilienz-**Konzept** kann den **Schaden im Optimalfall auf ein Minimum begrenzen**."
- "Cyber-Resilienz bedeutet auch, sich auf eine **adäquate** und nicht auf eine hundertprozentige Sicherheit zu fokussieren. Das Denken in den Kategorien der Resilienz ermöglicht es, **Gefahren bewusst zu akzeptieren** und zur Grundlage der Security-Strategie zu machen. "

Von Ransomware bis Cyber Warfare – *Was kann man tun?*

Kunden müssen sicherstellen, dass sie eine **24x7 Anomalie- und Angriffserkennung sowie Angriffsabwehr** gewährleisten können.

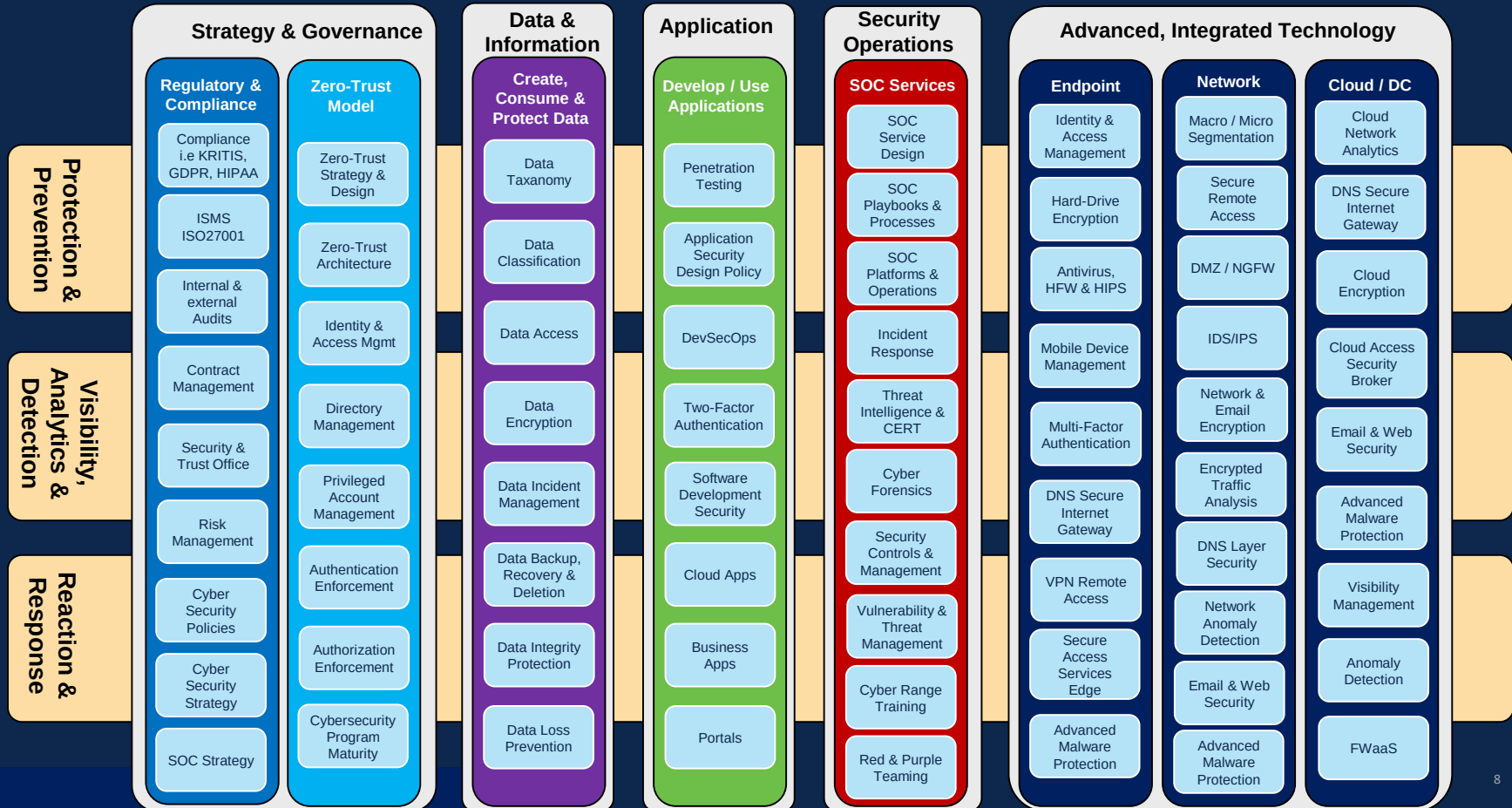
Hierzu braucht es drei Dinge:

- 1) **Technologie** → Visibilität auf allen Endgeräten, Monitoring von internen und externen Datenbewegungen & Kommunikation
- 2) **Prozesse** → Wie wird mit Technologie-Informationen verfahren? Welche Log-Informationen werden wo konsolidiert, korreliert und ausgewertet? Was ist im Falle von erkannten Anomalien und Kompromittierungen zu tun?
- 3) **Expertise** → SecOps Know How um Alarme zu analysieren und auszuwerten, Maßnahmen zur forensischen Untersuchung von Incidents durchzuführen, Angreifer zurückzuverfolgen und zu isolieren.

Nicht direkt über Technologie reden – erst über **Fähigkeiten!**

Eine Strategie für Informationssicherheit bedeutet, die erforderlichen Fähigkeiten zu etablieren, um das Unternehmen zu **schützen**, Angriffe zu **erkennen** und angemessen darauf zu **reagieren**.

Enterprise Architecture Fähigkeiten für Informationssicherheit



Cisco Cybersecurity Services Portfolio – Powered by Talos

Bestmöglicher Schutz von kritischen Geschäftsprozessen, durch Etablierung wichtiger Sicherheitskontrollmaßnahmen, schneller Erkennung von Anomalien sowie Abwehr von Angriffen.

FY23 Priorities

Strategie für Zero Trust & Segmentierung

Unternehmensweite
Asset-Identifizierung
& Klassifizierung, als
Basis für eine Mikro-
segmentierung.

SOC & CDC Aufbau, Entwicklung, Bewertung & Optimierung

Weiterentwicklung
vorhandener
SecOps Prozesse,
Fähigkeiten und
Technologien.

Managed Detection & Response

Talos-gestützte
SOCs für 24x7x365
Erkennung von
Anomalien und
Abwehr von
Angriffen

Incident Response Retainer

Proaktive und reaktive
24x7x365 Unterstützung
durch Talos Threat
Intelligence.

Threat Modeling, PenTesting, Red & Purple Teaming

Identifizieren von
Risiken,
Schwachstellen und
Einfallstoren für
Angriffe.

SASE & Multicloud

Planung und Design von
SASE & Multicloud
UseCases sowie
Implementierung
entsprechender Lösungen

Security Expertise für den Betrieb (Business Critical Services)

Optimale
Unterstützung des
täglichen Betriebs
durch dedizierte
Experten

120 TB

Daten täglich gesammelt
und analysiert



Millionen

von Telemetrie Agenten



Mehr als 350+ Threat
Intelligence Analysten



Mehr als 100

Threat Intelligence Partner



Milliarden

von Malware-, E-mail-,
DNS-, Web-, IPS- und
Flow Meta Daten

**4x Data-Center
weltweit
(incl. Malware Labs)**

Blocken von
20 Milliarden
Angriffen täglich

Analyse von
1.5 Millionen Malware-
Samples pro Tag

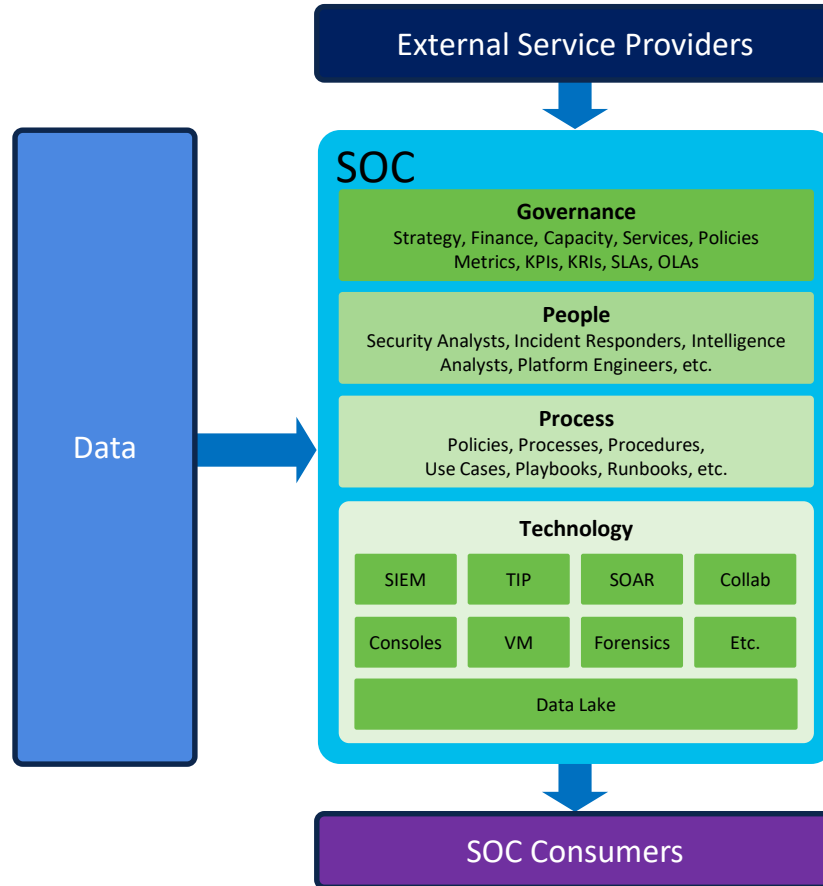
Verifizierung von **16
Milliarden**
URLs täglich

Prüfung von **150
Milliarden** DNS
Anfragen täglich

Scannen von **600
Milliarden E-Mails**
täglich

Fokus 1: Kunden brauchen ein SOC

...aber ein SOC braucht
Governance, Personal,
Prozesse und
Technologien





Fokus 2: Incident Response Retainer – Proaktiv & Reaktiv

Reaktiv

Proaktiv



Ich benötige
jetzt Hilfe!
(24x7x365)



Ich benötige
einen Plan für
wenn es passiert.



Bin ich im
Krisenfall gut
aufgestellt?



Ich möchte
Gewissheit,
dass wir richtig
reagieren.



Bin ich aktuell
kompromittiert?
(Breites Bild)



Bin ich aktuell
kompromittiert?
(Fokussiert)



Ich möchte Wissen
aufbauen, um mich
zu verteidigen



Habe ich ausreichend
Logs zur Verfügung
im Falle eines
Incidents?

**Emergency
Incident
Response**

**IR Plans
& Playbooks**

**IR Readiness
Assessments**

**Tabletop
Exercises**

**Compromise
Assessments**

**Threat
Hunting**

**Cyber Range
Training**

**Log
Architecture
Assessment**



Penetration Testing

Ich möchte spezielle Anwendungen, Systeme (IT, OT, IoT) oder Infrastruktur Komponenten auf Schwachstellen überprüfen.



Red Teaming

Ich möchte ein realistisches Angriffsszenario simulieren, welches *Advanced Persistent Threat (APT)* Taktiken verwendet.



Purple Teaming

Ich möchte meine Fähigkeiten auf der Verteidigungs-Seite (Blue-Team) verbessern, mittels Durchführung & Analyse von *Threat Actor Tactics, Techniques and Procedures (TTPs)*.



Fokus 3: Segmentierung – Strategy first!

- Identifizierung von Assets
 - Klassifizierung von Assets
 - Definieren von Enklaven und Zuordnung von Assets
 - Zuordnung von Security Kontrollen
 - Festlegen von Kommunikations- und Vertrauensbeziehungen
- 

- Inventory Erstellung aller Systeme, Dienste und Anwendungen: Platforms, Apps, Servers, Machines, PLCs, Cameras, Scanner, Phones, ...
 - ➔ Ggfs. durch Einsatz eines Asset Scanning Tools
- Inventory Erstellung aller Endgeräte Typen: Workstations, Laptops, Tablets, Mobiles, IoT, ...
- Asset Identifier sowie dazugehörige Domains erstellen
- Datenpfade identifizieren: Wer/Was nutzt ein Asset und greift von wo aus worauf zu
- Asset Data Klassifizierung basierend auf Risiko = Geschäftsnutzen + Auswirkung Verfügbarkeit
- Definition der Kritikalität aller Assets für die operative Prozesse unter Berücksichtigung der Sicherheitsrichtlinien
- Zuordnung von Privilegien zu Rollen und Profilen

CISCO
SECURE

Secure your

resilience.



CISCO

The bridge to possible