Wie schützt ein SOC die Spitäler?

Herausforderungen aus der Praxis

Kundennähe

SOC-Einsatzteam

Security Analyst | Security Engineer | Threat Hunter | Incident Manager | Service Manager

Security Operations Center in der Schweiz

Über 90 SOC Kunden
3/4 Umsatz mit SOC Services

Unsere Server stehen in der Schweiz

Insgesamt 600 Jahre Berufserfahrung der 90 Mitarbeiter

Nah beim Kunden und schnell erreichbar

Schweizer Wurzeln
1996 gegründet

Vorstellung

Wer bin ich

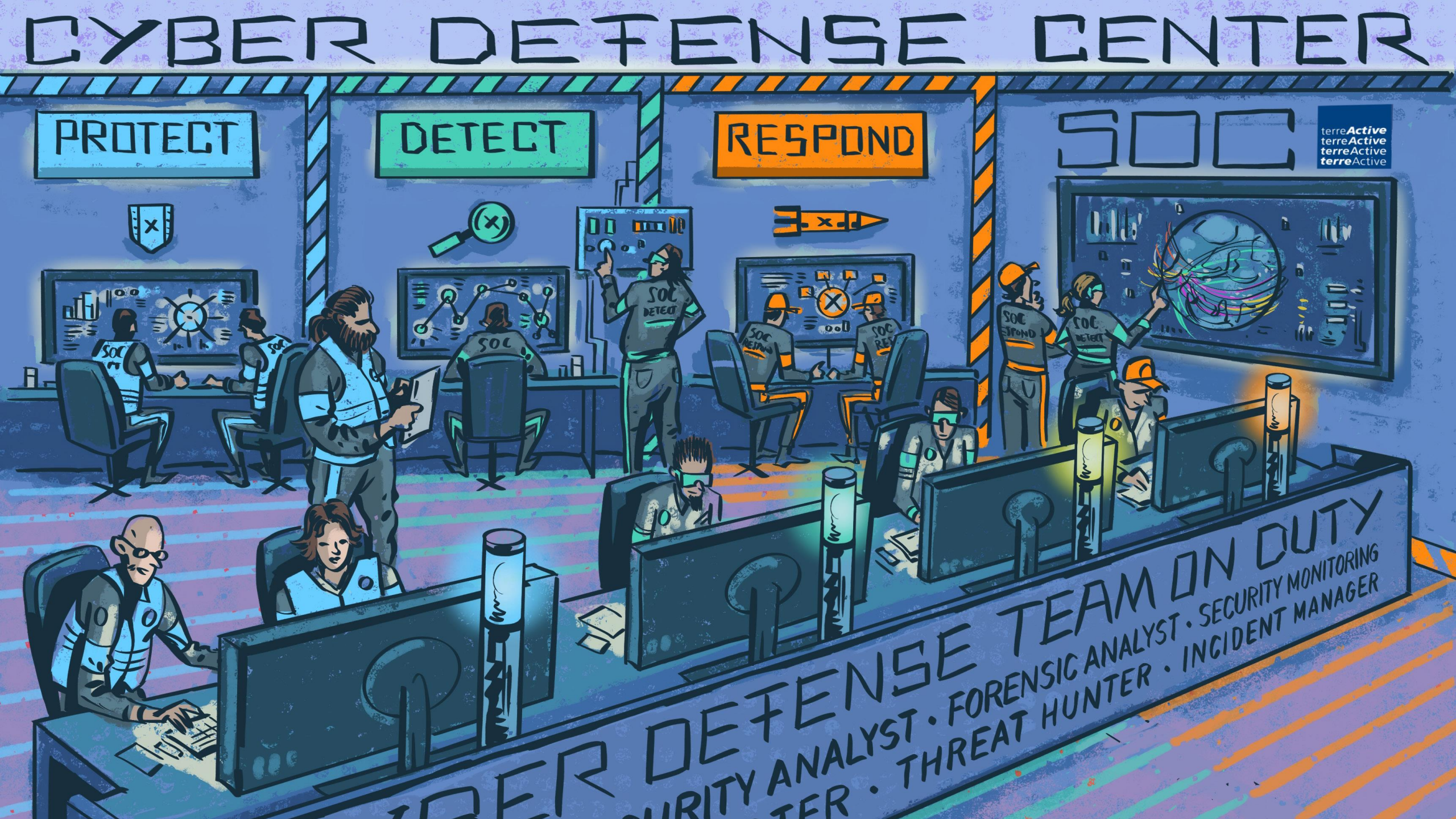
Rolf Hefti

Head of Product Management
Cyber Defense

Mitglied Management Team

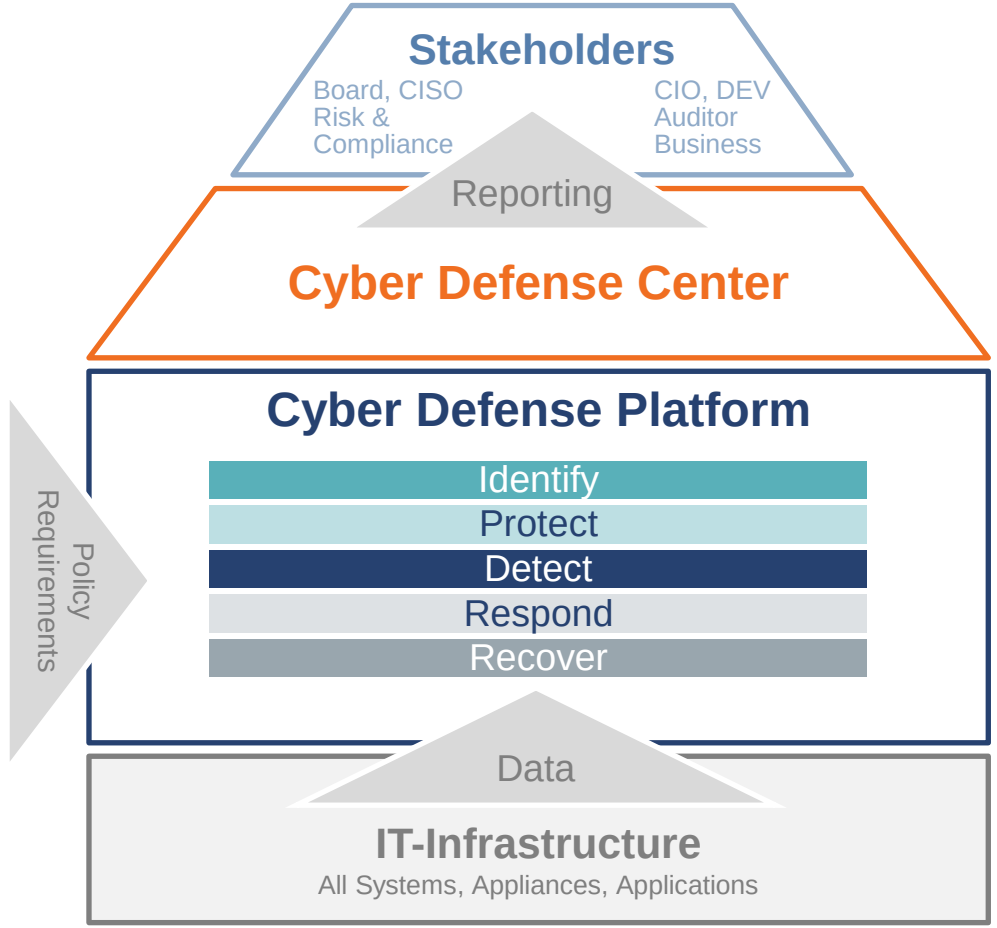
Rolf Hefti verfügt über 25 Jahre Erfahrung in der Cyber Security mit ausgewiesenem Know-how in Themen wie Security Monitoring und SOC Services. Er berät Unternehmen im Aufbau und dem effizienten Betrieb von Security Operations Centern.

Rolf Hefti baut auf einem langjährigen IT-Background auf. Bevor er 2002 zur terreActive wechselte, war er Leiter Internet Hosting bei Swisscom und Head of Engineering bei Aspectra.


CYBER DEFENSE CENTER
PROTECT
DETECT
RESPOND
SOC
terreActive
terreActive
terreActive
terreActive
SOC
SOC DETECT
SOC RESPOND
SOC DETECT
SOC RESPOND
SOC
CYBER DEFENSE TEAM ON DUTY
SECURITY ANALYST · FORENSIC ANALYST · SECURITY MONITORING
THREAT HUNTER · INCIDENT MANAGER

Cyber Defense

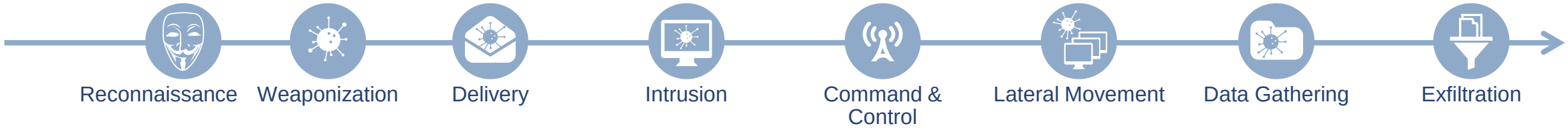
Zielbild für die SOC-Organisation



Cyber Defense Platform

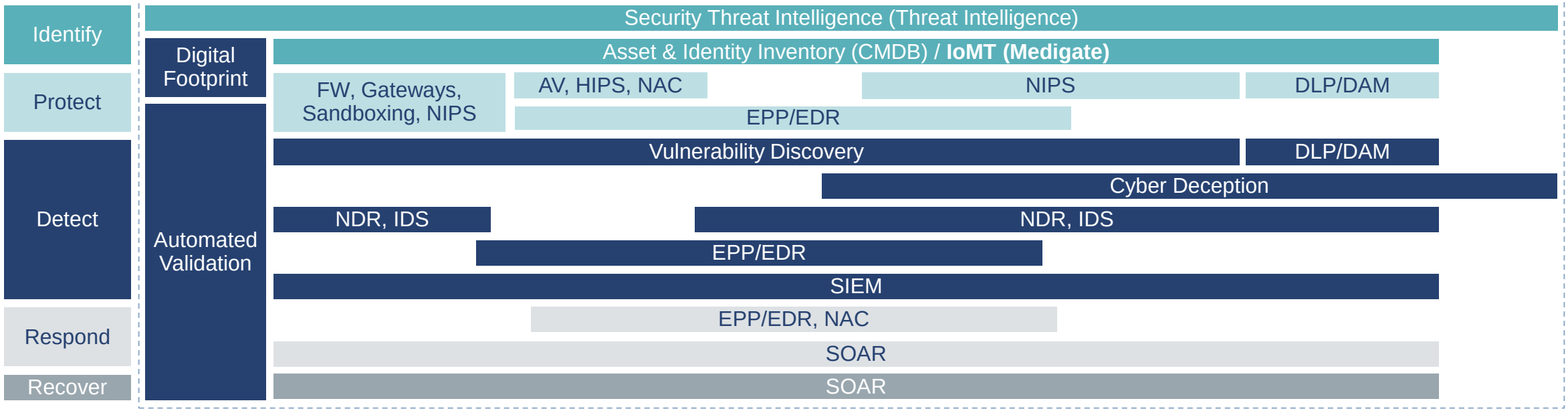
Welche Komponenten braucht Ihre Cyber Defense Platform (CDP)?

Attack Phases (Cyber Kill Chain)



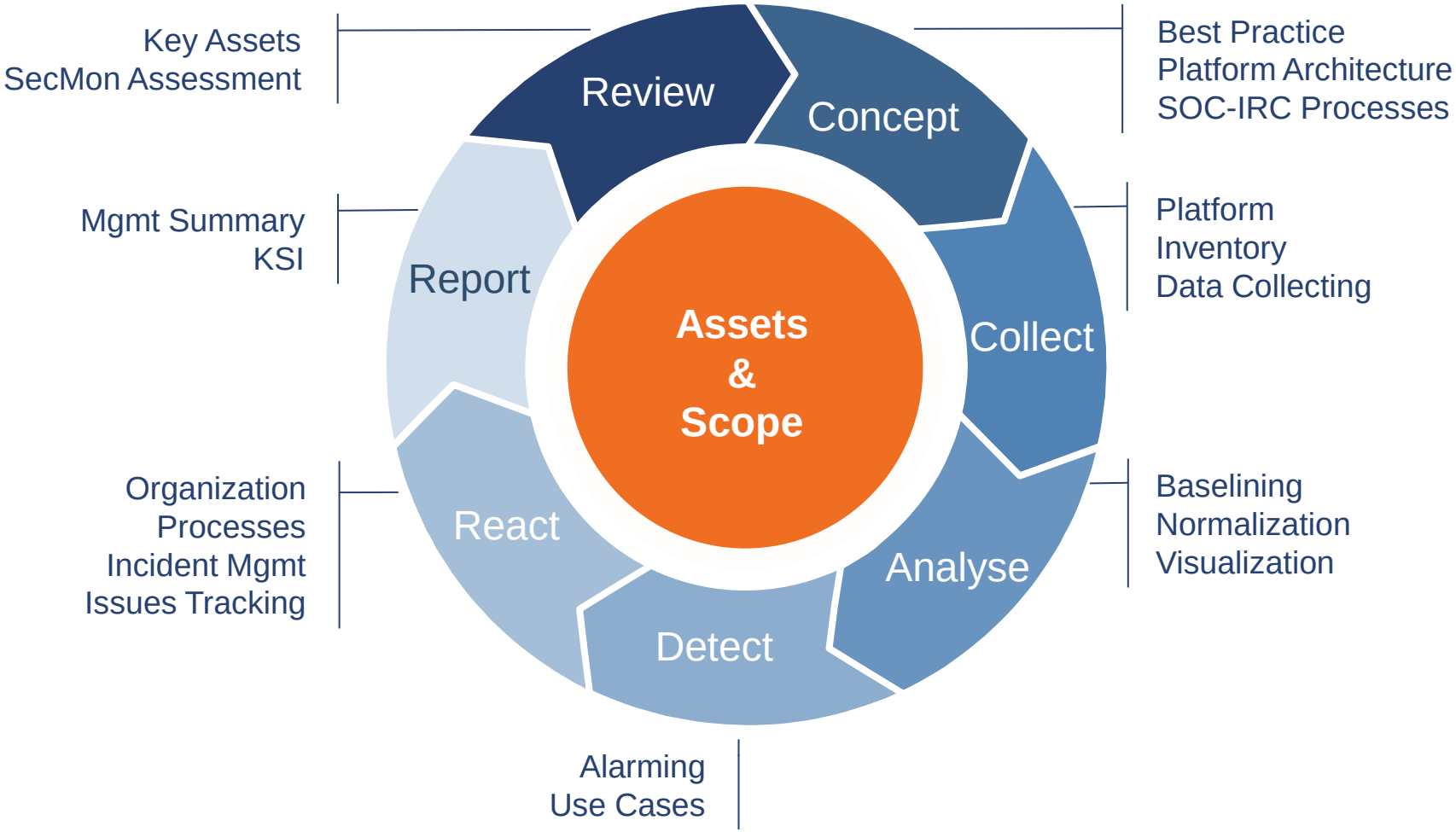
NIST

TOOLS FOR CYBER DEFENSE PLATFORM



Cyber Defense Project

Wir bauen nach dem Standardvorgehen der 7-Steps-Methodik



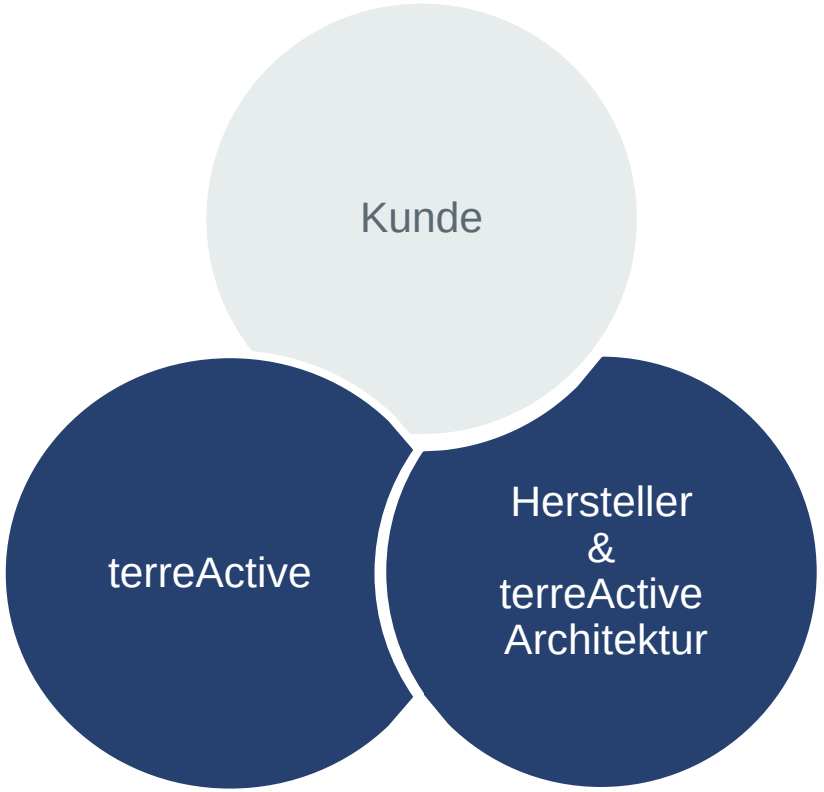
Cyber Defense Project

Bestimmen Sie Schützenswertes und Umfang (Assets & Scope)

Client & Server	Core Processes	Core Application	Perimeter: Firewalls & Proxies	Network
Critical Customer Data	Operation Technology Medical Things IoMT / IoHT	Security Components	Managed Service Provider	Top-Down Bottom-Up

Zusammenspiel

Jeder hat seine Stärken



SIEM: Security Information and Event Management

Zusammenspiel

Tools für die Cyber Defense Platform (CDP)

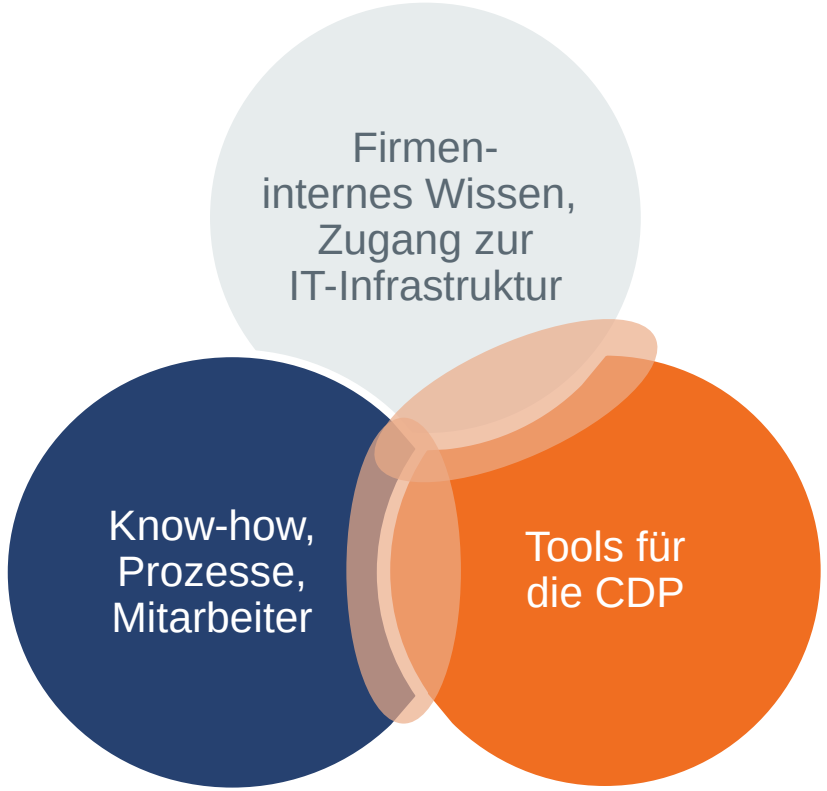
Schnittstellen:

- Das Gefährdungspotential Kernprozesse ist dokumentiert und verstanden.
- Gemeinsame Analysen mit Kunde oder Partner sind möglich.
- Vorgaben und Compliance Richtlinien sind bekannt und abgebildet.

Plattform:

- Komponenten (Tools) der CDP sind optimal integriert.
- Alle NIST Phasen werden unterstützt.

→ Trend geht zu Plattformen eines Anbieters.



Zusammenspiel

Know-how, Prozesse, Mitarbeiter

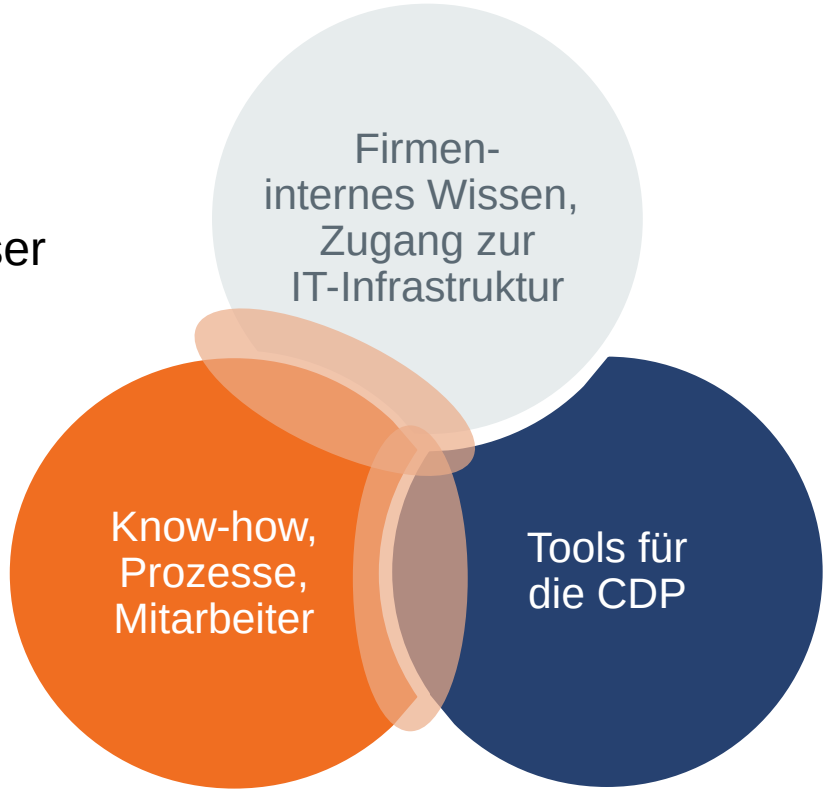
Schnittstellen:

- Die Verbindung von Alarmierung mit Prozessen und Ressourcen aller Parteien steht im Mittelpunkt.
- Je mehr firmeninternes Wissen im externen SOC liegt, umso grösser die Entlastung des Kunden.

SOC-Organisation:

- Das SOC bietet alle notwendigen Rollen als Service.
- Die Services richten sich an NIST aus und entwickeln sich gemäss der aktuellen Bedrohungslage.

→ Trend geht Richtung Schutz gegen konkrete Angriffsgruppen. (MITRE ATT&CK)



Zusammenspiel

Firmeninternes Wissen, Zugang zur IT-Infrastruktur

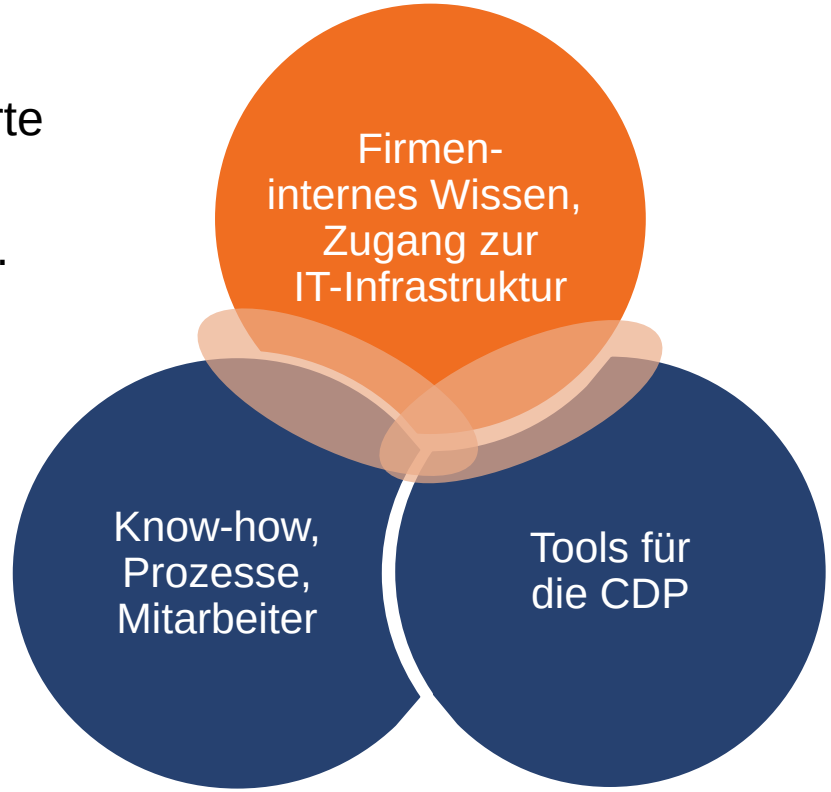
Schnittstellen:

- Der Kunde muss alle relevanten Informationen erhalten um fundierte Entscheide fällen zu können.
- Die Prozesse müssen für den Notfall aufeinander abgestimmt sein.
- Bei jedem Vorfall sind schnelle Antworten beider Seiten Pflicht.

Organisation des Kunden:

- Redundanter SPOC mit gutem internen Wissen und Zugang zu den Know-how-Trägern.
- Viele Aufgaben wie Kommunikation, Wiederherstellung und Verbesserung der IT-Infrastruktur bleiben beim Kunden.

→ Trend bei den Kunden: Weg von «selber Tools evaluieren», hin zu den internen Kernprozessen.



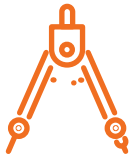
Häufige Fallstricke im Projekt

Aus der Praxis

Es ist wichtig, den Umfang des Projekts nicht zu unterschätzen. Um ein erfolgreiches Ergebnis zu erzielen, ist eine enge Zusammenarbeit unerlässlich.

Es wird zu viel über Produkte gesprochen und zu wenig über Prozesse, Aufgaben und Resultate.

Kernapplikationen & Daten: Nur wer weiss *was* zu schützen ist, kann auch die richtigen Massnahmen und Entscheide fällen.



Die eigenen Ressourcen und Prozesse kennen und auf die der Partner und Provider abstimmen.

Herausforderungen

Was bedeutet es für die Spitäler?

Besonderheiten:

- Ein Universitätsspital ist auch eine Ausbildungsstätte.
- Spitäler haben sehr viele Partner, die das «Supply-Chain-Risiko» erhöhen.

→ Anstelle eines hohen und flächendeckenden Schutzes, fokussiert Schutz der Kernsysteme ausbauen.

- Die Angreifer erwarten eine höhere Zahlungsbereitschaft bei einem Spital.
- Die Gesundheitsbranche ist weniger geschützt als andere Branchen, was einen Angriff einfach macht.

→ Neue Ansätze und Techniken schneller einführen, um den Rückstand zu kompensieren.

- Medtech Systeme (viele Anbieter, wenig Standards) belasten IT und Cyber Security zusätzlich.

→ Zuerst die Standard-IT sichern und danach die Medtech Systeme mit dem gleichen Ansatz in Angriff nehmen.

Zusammenfassung

Drei Grundsätze

1. **Jeder konzentriert sich auf seine Stärken.**
   Der Kunde kennt seine IT im Detail während das SOC die nötigen Cyber-Defense-Fähigkeiten einbringt.
   Ständige Diskussionen über Tools bringen keinen Fortschritt.

2. **Nur wer gut vorbereitet ist kennt seine Schwächen.**
   Systematisch und schrittweise die Cyber Defense etablieren und ausbauen führt zum Ziel. Nur wenn die involvierten Parteien ständig üben und daraus lernen, sind sie im Notfall bereit.

3. **Immer einen Schritt voraus sein.**
   Nur wer sich ständig weiterentwickelt, kann dem Angreifer einen Schritt voraus sein.
   Wenn der Aufwand zu hoch ist, sucht sich der Hacker ein anderes Opfer.

Besser immer einen Schritt voraus zu sein!

Kontakt

Wir sichern Ihren Erfolg

Rolf Hefti

rolf.hefti@terreActive.ch

terreActive AG
Kasinostrasse 30
CH-5001 Aarau

www.security.ch

+41 62 834 00 55
info@terreActive.ch