IT-Sicherheit in Kliniken

Willkommen im unendlichen Spiel!

2025 Reimagine GERMANY

Sarah Wambach

Cybersecurity Specialists im Bereich Healthcare

IT-Grundschutz-Praktikerin

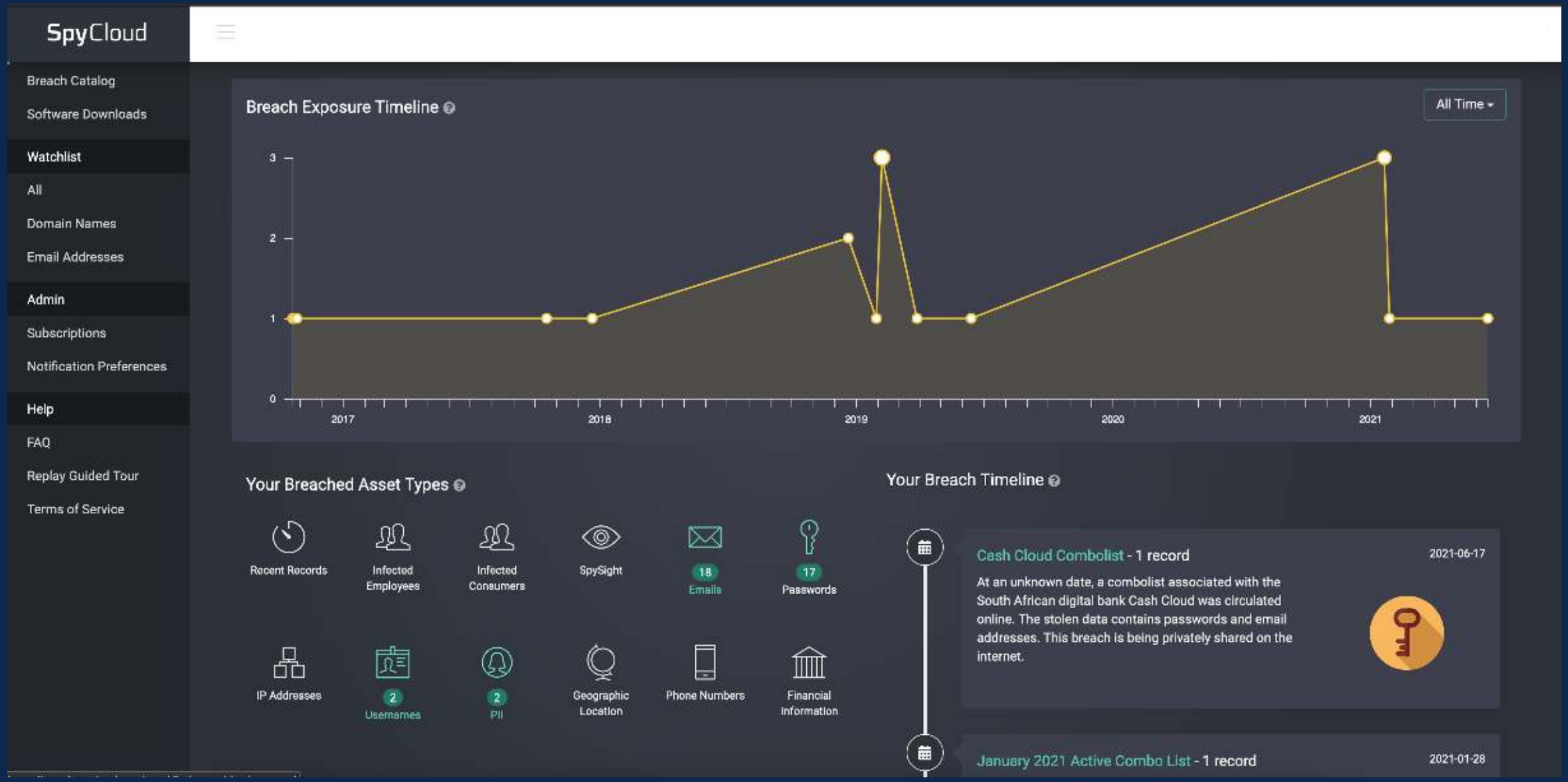
September 2022

Die bekannte Ausgangslage

Das unendliche Spiel der Cyber-Sicherheit und Resilienz

Ein volatiler Zustand als kontinuierlicher Prozess

“Keine Sorge,
die *Daten*
sind nicht weg
….sondern nur
verschlüsselt.”



https://spycloud.com/

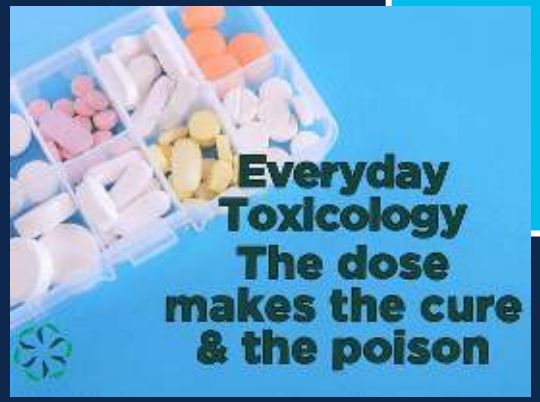
Patientendaten sind lukrativ.

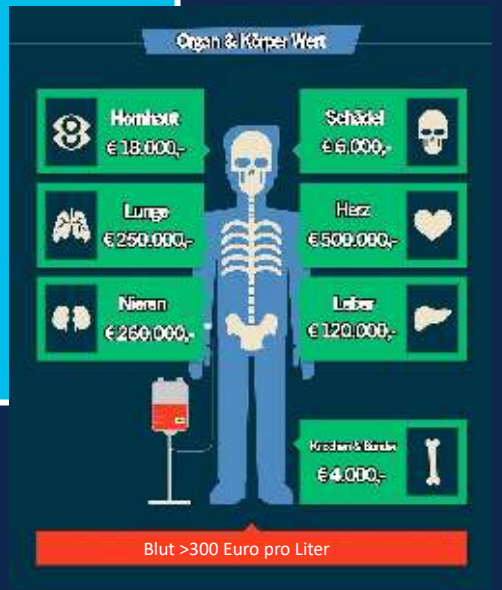
Preise im Darknet:

1000€ Patientendatensatz

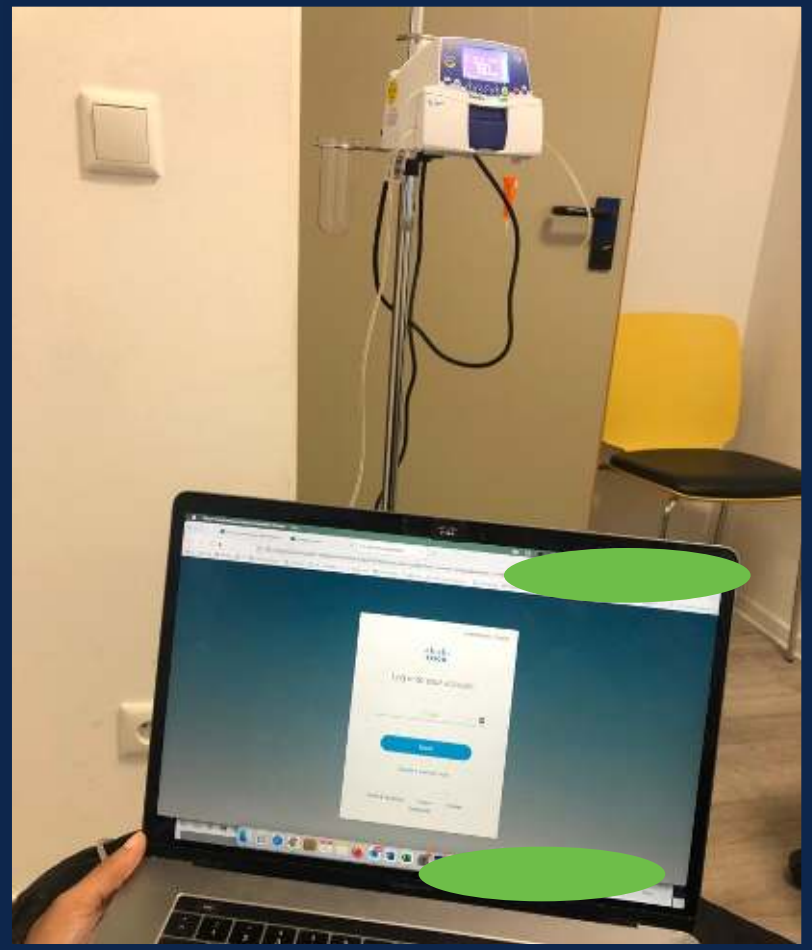
vs.

5€ Kreditkarteninformation

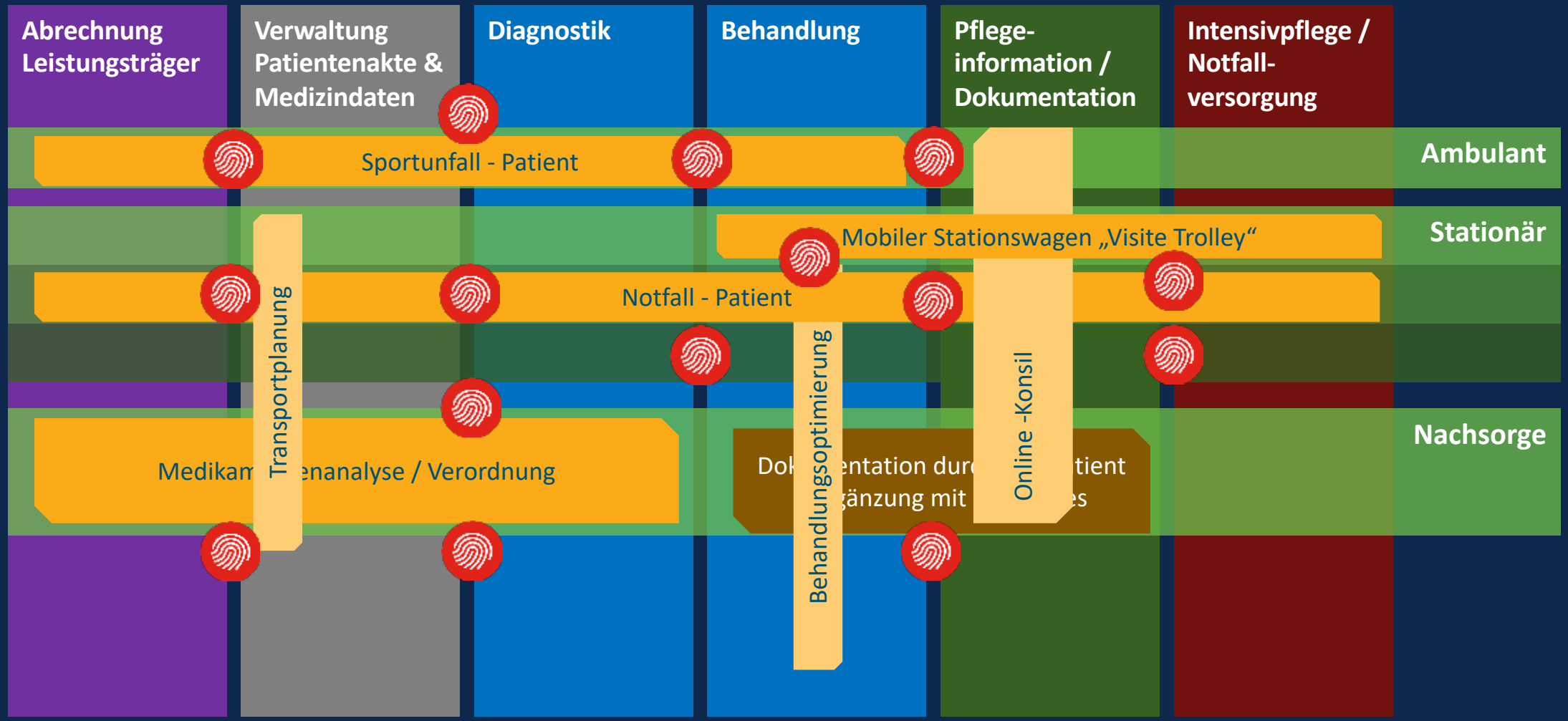




Patientendaten sind lukrativ.



Warum ein übergreifendes Verständnis nötig ist



Der richtige Ausgangspunkt entscheidet

Sichtbarkeit & Transparenz erlangen

Sichtbarkeit aller Geräte, Nutzer und Kommunikations-beziehungen

„Normales“ Verhalten verstehen

Erkennen von realen Risiken

Analyse

Risiko- und Compliance Bewertung

Richtlinien etablieren

Kontrolle

Kontinuierliche, Risiko-orientierte und organisations-übergreifende Kontrollen

Detektions- und Reaktionsmaßnahmen

Security als integrative Architektur: *erleichtert den Betrieb*

Kritische Sicherheits-kontrollen zur Prävention

Nutzer

Endgeräte

Netzwerk

Apps & Daten

Anomalie- und Angriffserkennung

Ganzheitliches, proaktives & automatisiertes Security Monitoring, Analysen und Reaktionsmaßnahmen

Sichtbarkeit ermöglicht Transparenz. Transparenz ermöglicht Kontrolle.

Seriennummer: 3GJH471FGaLw1E

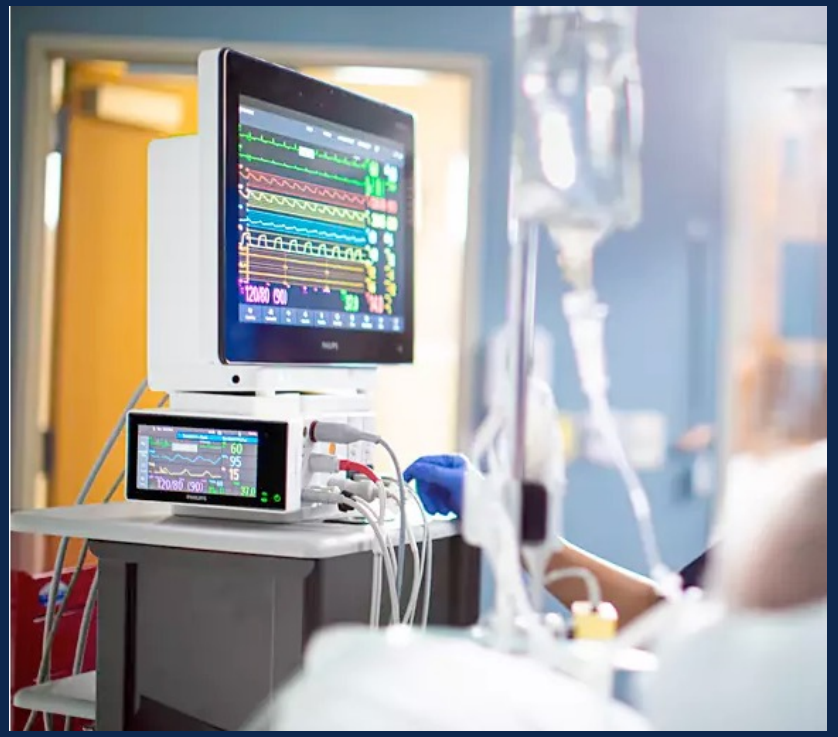
Gerät? Phillips mobiler Patienten Monitor

User Login? Generic User Station 14

Wo? Station 14, Zimmer 102

Was? Überwachung Vitalwerte

→ Policy: Richtlinienkonform, normales Verhalten



Sichtbarkeit ermöglicht Transparenz. Transparenz ermöglicht Kontrolle.

Datenkorrelation aus Sicht der IT:

14:31 Uhr: Verbindung zu IP 123.456.789 **unterbunden**

14:28 Uhr: **Zugriff** auf „Da Vinci **VLAN_3“ gewährt**

14:26 Uhr: **Zugriff** auf Klinik Backup Server **fehlgeschlagen**

14:25 Uhr: Login **User Sarah W.** Station 16

14:23 Uhr: C: \ windows\system32>**net user / add Sarah W.**

14:19 Uhr: **Alarm Temperaturkontrolle** Insulin Kühlschrank

14:18 Uhr: Überwachungskamera Medikammer **ausgefallen**

14:16 Uhr: **St. 14 Generic User Zugang** zu St. 16 **gewährt**

14:15 Uhr: **Unbekannter Prozess** auf dem Stations-PC

Seriennummer: 3GJH471FGaLw1E

Gerät? Phillips mobiler Patienten Monitor

User Login? Generic User Station 14

Wo? Station 16, Zimmer 907

Was? Datei-Upload zu unbekanntem Server

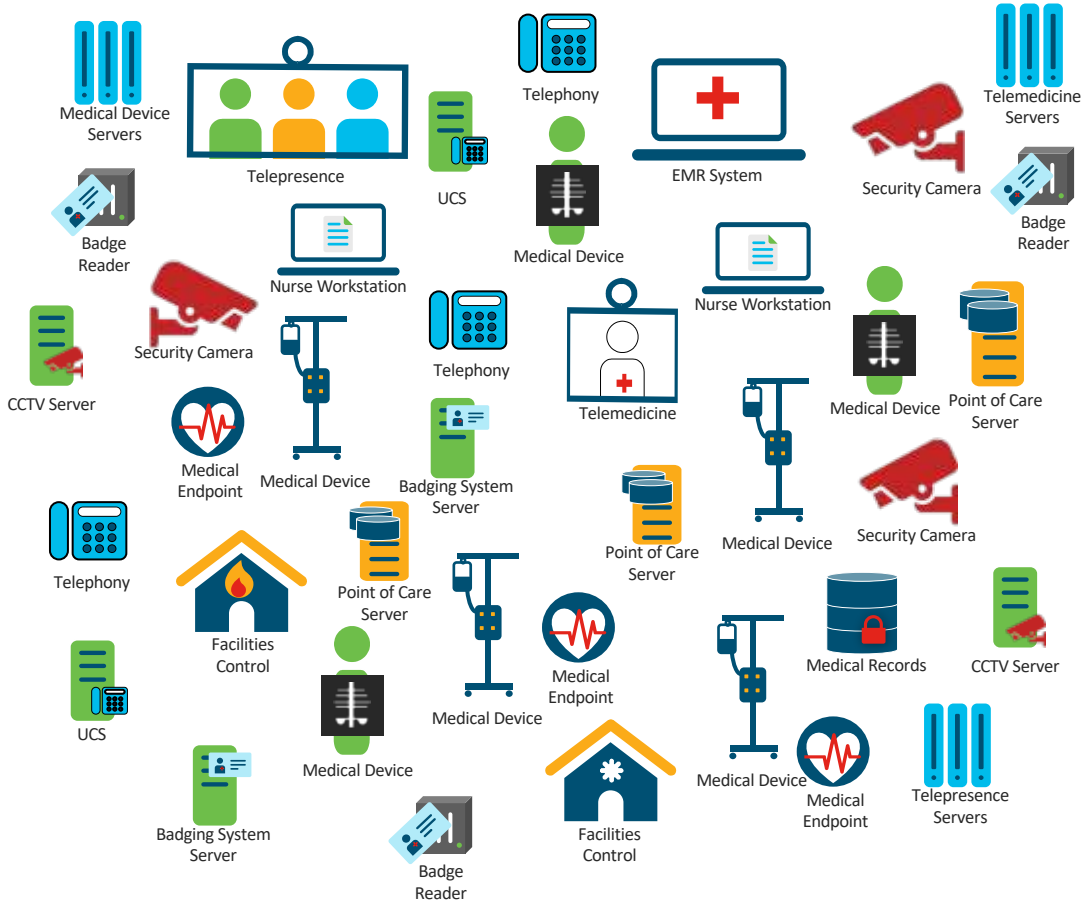
→ **Policy: Dynamische Änderung, temporärer Zugang**

→ **Alarm: Verbindungsaufbau unterbunden**

→ **Alarm: Keine Freigabe zum Datei-Upload**

→ **Policy: Einschränkung der Zugangsrechte**

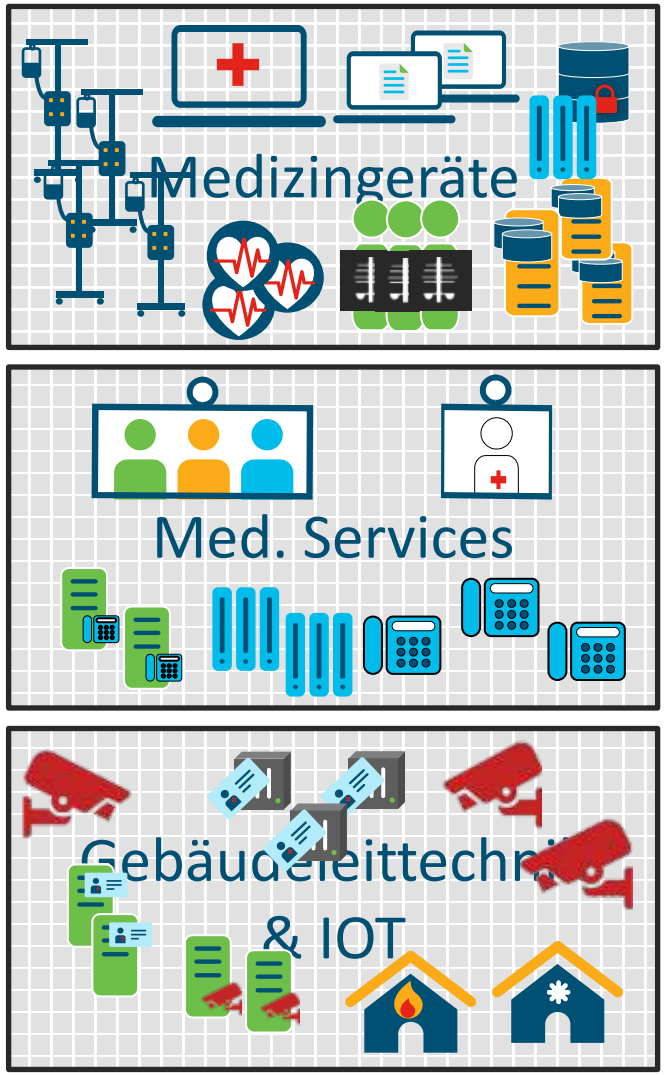
Klassifizierung



Bildung logischer Segmente

- Medizingeräte
- Med. Services
- Gebäudeleittechnik & IOT

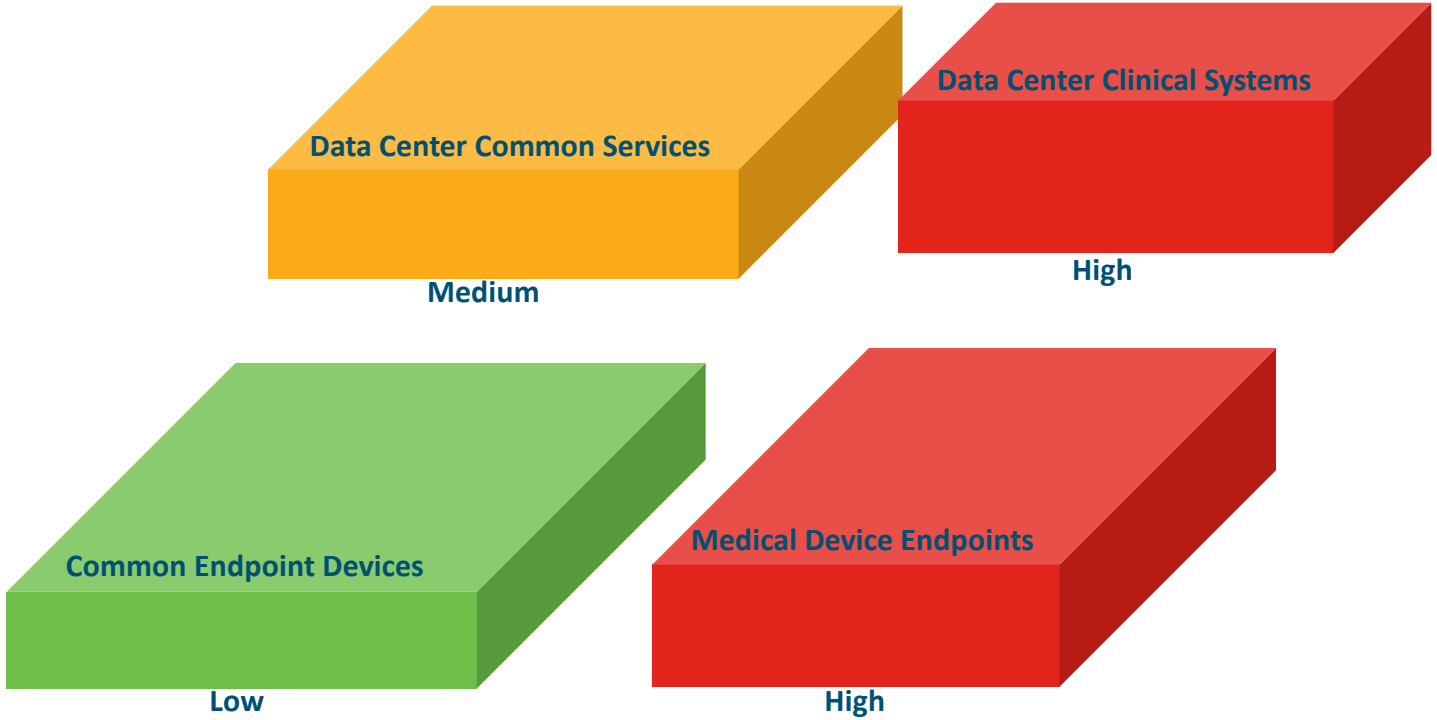
Bewertung



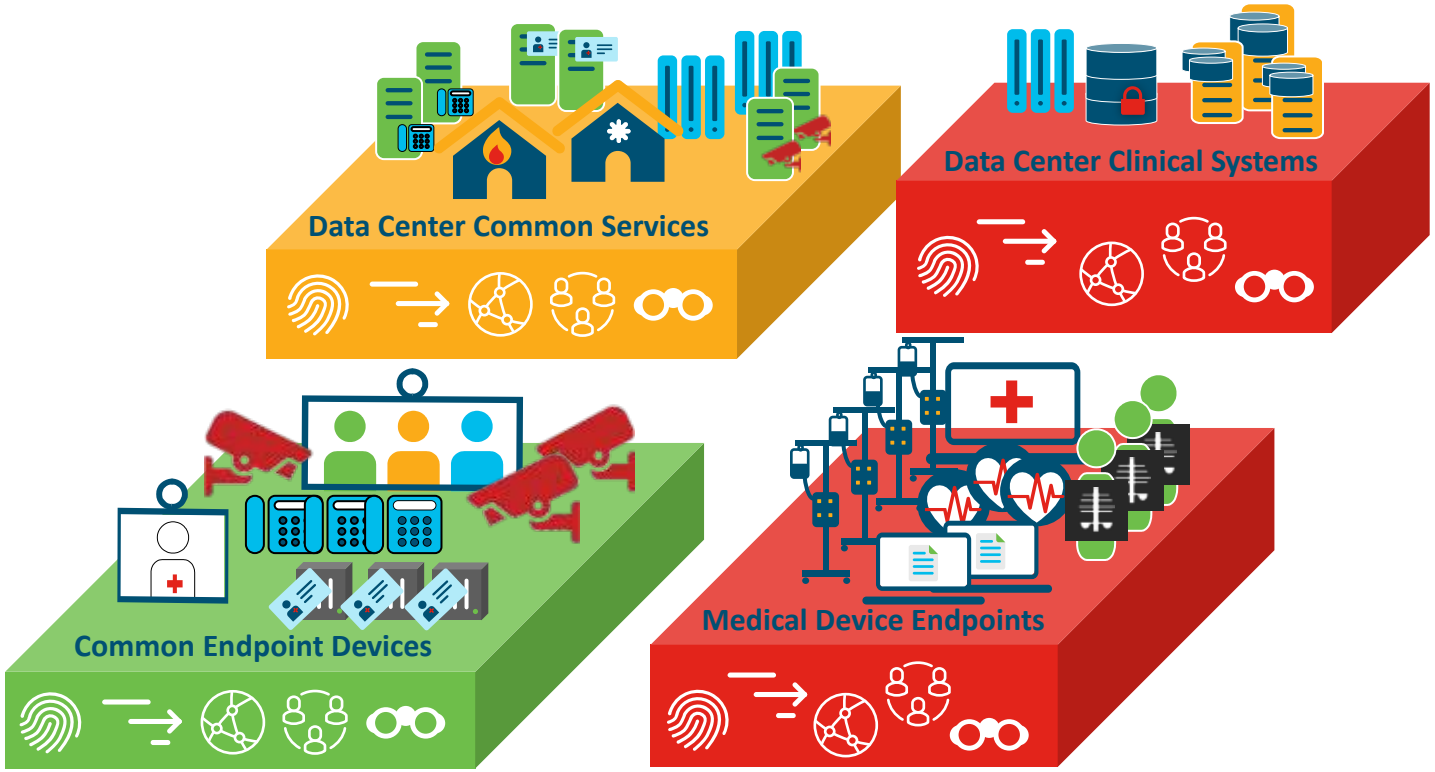
Mapping der Schutzziele / Richtlinien

Vertraulichkeit	Integrität	Verfügbarkeit

Enklaven definieren und Assets zuordnen



Richtlinien & Kontrollen



- Identitäts- und Vertrauensbildung
- Durchsetzung von Richtlinien
- Isolation
- Verfügbarkeit
- Sichtbarkeit

Sicherheit im Klinikum


Wir begleiten Sie
sicher durch die Winterzeit
- Erhöhung der IT-Sicherheit in wenigen Minuten -
cisco
SECURE

Status Quo ermitteln

Was zeigt das Umbrella Assessment auf?

- ✓ Schatten-IT: es werden alle mit dem Web kommunizierende Applikationen visibel
- ✓ Identifizierung kompromittierter Systeme mittels Sicherheitsaktivitätsberichten in Echtzeit
- ✓ Blockierung von Domänen im Zusammenhang mit Phishing, Malware, Botnets und anderen Kategorien mit hohem Risiko (z. B. Krypto-Mining, neu erkannte Domänen)
- ✓ Schutz vor Malware und Phishing- Versuchen von schädlichen Websites
- ✓ Blockierung von webbasierten und nicht-webbasierten Callbacks von kompromittierten Systemen
- ✓ Proxy und Entschlüsselung riskanter Domänen zur genaueren Überprüfung der URLs und Dateien
- ✓ Möglichkeit zur Webfilterung mit mehr als 85 Domäneninhaltskategorien
- ✓ Inklusive deutschem Jugendschutzfilter (BPjM)

Hier finden Sie einen Cisco Umbrella Beispiel-Report

Sicherer Zugriff auf alle Applikationen

Secure Access by Duo liefert Ihnen eine schnelle Möglichkeit, um sowohl für alle Mitarbeiter als auch besonders privilegierten Zugängen für Geschäftsführung und Admins eine zusätzliche Sicherheitsstufe einzuführen.

- Die Lösung sorgt dafür, dass nur die richtigen Mitarbeiter mit den von Ihnen freigegebenen Geräten auf Ihre Applikationen zugreifen können.
- Flexible Überprüfung der jeweiligen Mitarbeiter-Identität mittels Multifkator-Authentifizierung
- Sie erhalten während des Netzwerkzugriffs einen detaillierten Überblick über die Geräte Ihrer Benutzer um Risiko zu minimieren und Compliance Richtlinien durchzusetzen
- Health Check: Verhindern Sie den Netzwerkzugriff für risikobehaftete Gräte, damit kein Zugriff auf sensible Daten erfolgen kann.

Secure Access by Duo für den sicheren Zugriff auf Ihre Anwendungen

Duo schützt Organisationen durch Überprüfung der Identität von Benutzern und der Konformität ihrer Geräte, BEVOR Sie eine Verbindung zur jeweiligen Anwendungen herstellen.

Möglichkeiten zur Authentifizierung:

Bundesamt für Sicherheit in der Informationstechnik

BSI Typ 1 C5 Testat

Darf der User auf die Anwendung zugreifen?

Ist der Mitarbeiter wer er vorgibt zu sein?

Ist das Gerät vertrauenswürdig?


CISCO
SECURE
Sichtbarkeit ermöglicht Transparenz.
Transparenz ermöglicht Kontrolle.
sloehlei@cisco.com / +49 160 84 727 07
Sarah Wambach, Cisco Cybersecurity Specialist, Healthcare