securITe
Intelligence meets care.

Verteidigung Nach Dem Einbruch

Gesundheitswesen unter Beschuss

Manuel Nedbal | August 2025

securITe

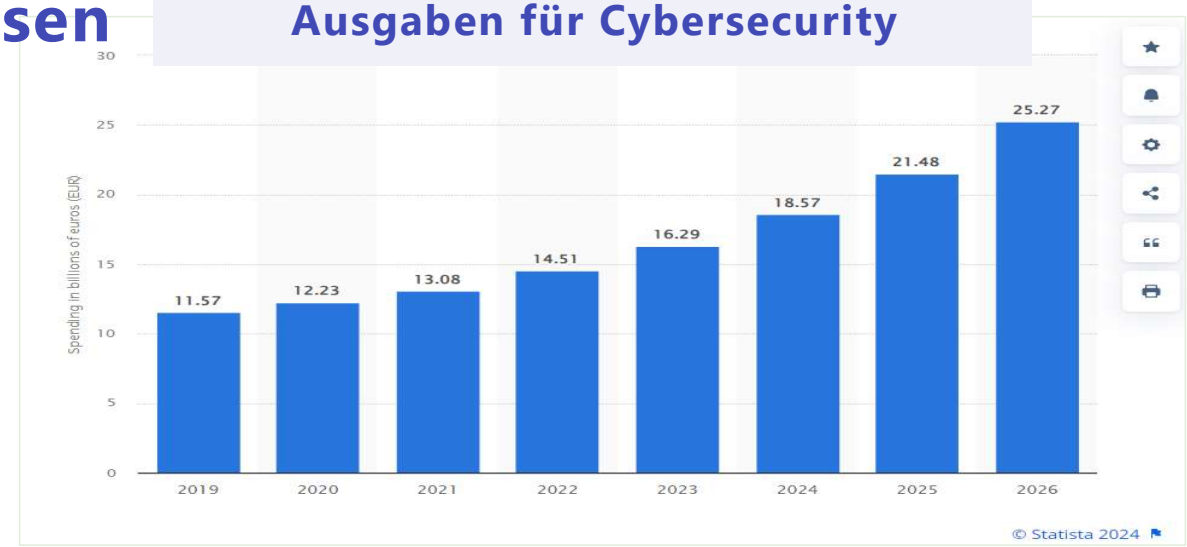
Angriff auf Gesundheitswesen

Trends die gegenläufig sein sollten...

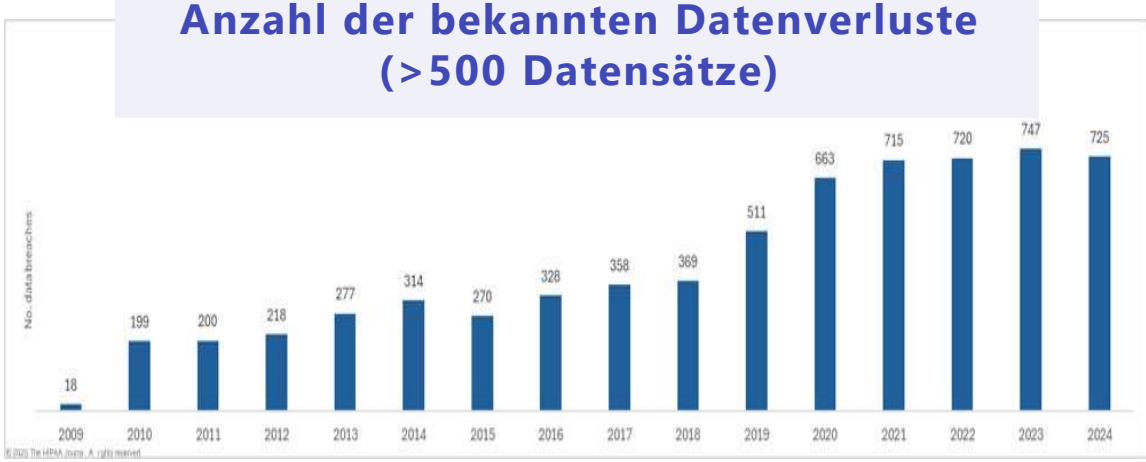
- Jedes Jahr **erhöhen** sich das **Budget** und die Ausgaben für Cybersecurity im Gesundheitssektor
- Diese Spitzenausgaben treffen jährlich auf neue **Rekorde** in Volumina an **verlorenen Daten**

→ Warum kann durch erhöhtes Investment keine Umkehr dieses Trends herbeigeführt werden ?

Ausgaben für Cybersecurity



Anzahl der bekannten Datenverluste (>500 Datensätze)



Healthcare Data Breach Statistics

securITe

Angriff auf Gesundheitswesen

Warum ist der Gesundheitssektor stark von Attacken betroffen ?

Attraktivität der Daten

- Persönliche, medizinische und finanzielle **Daten** sind unglaublich **wertvoll**
- Können für weitere Attacken benutzt werden
- Phishing, Kreditvergabe, Raub, Betrug, Erpressung, **Beeinflussung in Beruf** & **Privatleben**,...

Dringlichkeit der Wiederherstellung

- Untersuchungen, Eingriffe, **Behandlungen**, Notfälle können **nicht durchgeführt** werden
- Potentiell lebensbedrohliche Situationen entstehen
- **4x Belastung** durch: Systemausfall, Patienten, Wiederherstellung, Verhandlungen

Fragmentierte Infrastruktur

- **Cloud Applikationen** öffnen neue Kommunikationspfade
- Labore, Partner, Mitarbeiter, Kunden, mit verschiedenen Geräten und Lokationen
- Gesetzgebung erschwert rasche Updates bei **Schwachstellen**
- **Spezielle** medizinische **Protokolle** zwischen Geräten

securITe

Vergleich: Verteidigung Nach Einbruch

Keine Kontrollen
Nach Einbruch

1. Patches können nicht installiert werden
2. Proprietäre Protokolle werden nicht verstanden
3. Endpunkt-Sicherheit kann nicht ausgerollt werden

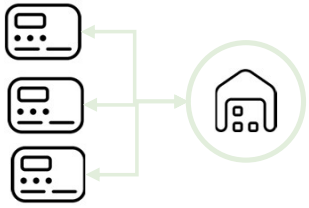
Starke Kontrollen
Nach Einbruch

IT im Gesundheitswesen

Perimeter Sicherheit

Krankenhaus Informations-System

Medizinische Geräte



Identäts-Management

Healthcare Provider

IT in Unternehmen

Perimeter Sicherheit

Schwachstellen Management

Netzwerk Sicherheit

Endpunkt Sicherheit

Desktop

Laptop

Tablet

Telefon

securITe

Vergleich: Verteidigung Nach Einbruch

Fehlende Sicherheitskontrollen im Gesundheitswesen

MITRE ATT&ACK [1)]	State
Deliver	✓
Exploit	✓
Control	✓
Execute	✓
Maintain	✓

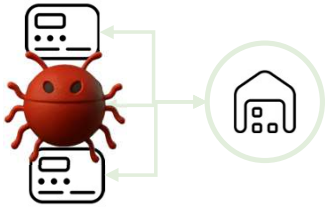
IT im Gesundheitswesen

Perimeter Sicherheit

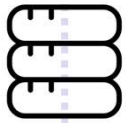
Krankenhaus Informations-System

Healthcare Provider

Medizinische Geräte



Identitäts-Management



IT in Unternehmen

Perimeter Sicherheit

Schwachstellen Management

Netzwerk Sicherheit

Endpunkt Sicherheit

Desktop

Laptop

Tablet

Telefon

[1)] A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations, https://attack.mitre.org/

securITe

Cybersecurity - Technologiebereiche

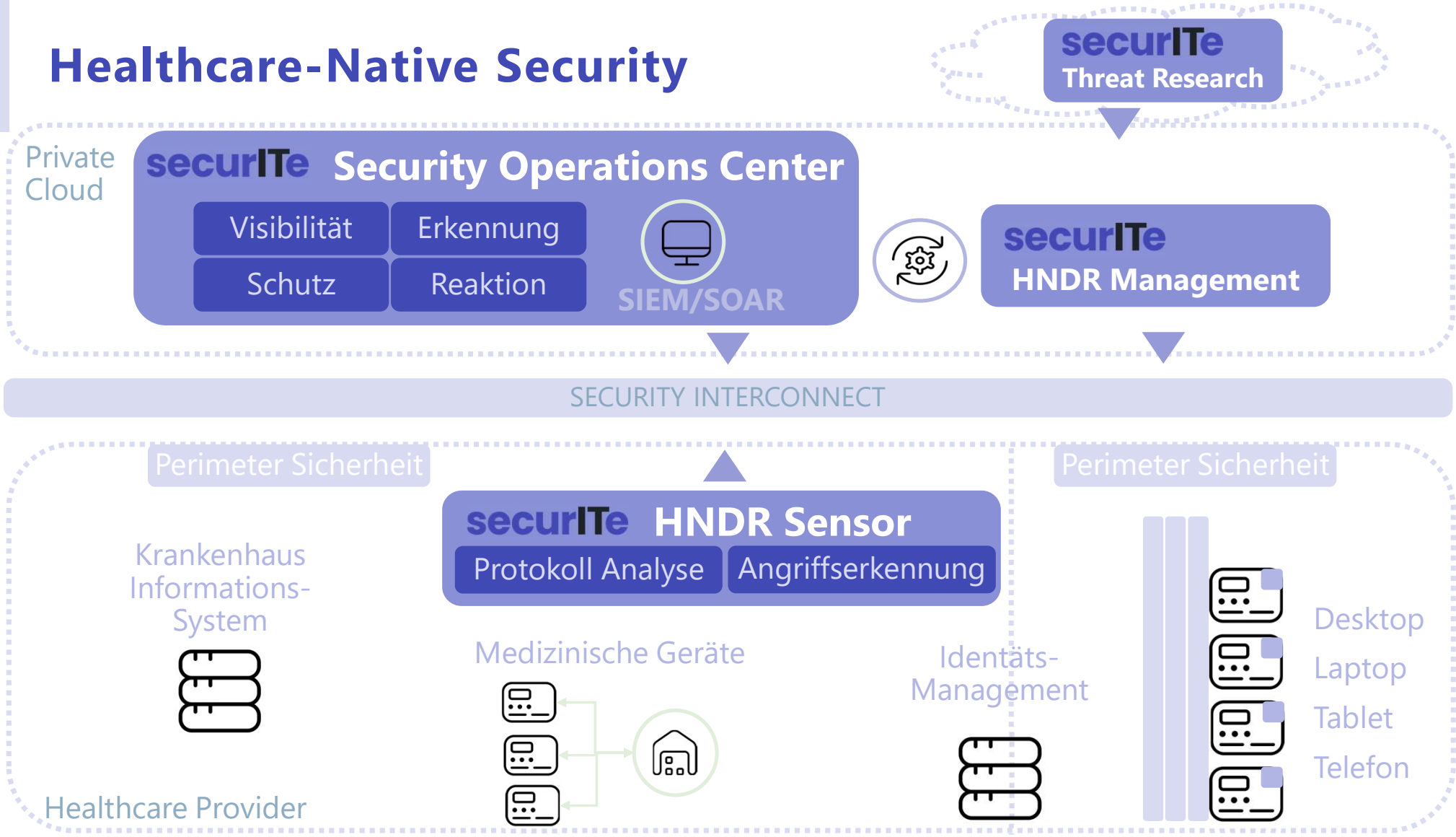
>3000 Sicherheitslösungen

Netzwerksicherheit	Endpunktsicherheit	Network Detection & Response (NDR)	Anwendungssicherheit	Datensicherheit
• Firewalls (NGFW) • VPN & Remote Access • IDS/IPS • Web Application Firewall (WAF) • Traffic Inspection & Filtering	• Virenschutz (AV) • Endpoint Detection & Response (EDR/XDR) • Gerätekontrolle (USB,...) • Application Control • Verhaltensanalyse	• Deep Packet Inspection • Anomalieerkennung (ML-basiert) • East-West Traffic Monitoring • Lateral Movement Detection	• Static Code Analysis (SAST) • Dynamic Analysis (DAST) • RASP (Runtime Protection) • Software Composition Analysis • Application Control	• Datenklassifikation • DLP (Data Loss Prevention) • Verschlüsselung (at rest / in transit) • Backup & Recovery • Datenmaskierung / Tokenisierung

IAM & PAM	Cloud-Sicherheit	Überwachung & Reaktion	Awareness & Schulung	Physische Sicherheit
• Single Sign-On (SSO) • Multi-Factor Authentication (MFA) • Privileged Access Management (PAM) • Identity Lifecycle Management • Just-in-Time Access (JIT)	• Cloud Security Posture Management (CSPM) • Cloud Workload Protection (CWPP) • Cloud Access Security Broker (CASB) • Cloud IAM & Compliance Monitoring	• Security Information & Event Management (SIEM) • Security Orchestration & Automation (SOAR) • XDR-Plattformen • Log Aggregation & Correlation • SOC & IR Playbooks	• Phishing-Simulationen • Security Awareness • Benutzerverhaltenstraining • Gamified Learning • Compliance-Training	• Zutrittskontrollsysteme • CCTV • Biometrische Auth. / MFA • Physische Sicherheit

securITe

Healthcare-Native Security



Healthcare-Native Network Detection & Response (HNDR)

Zusammenfassung

- HNDR gehört zu den netzwerkbasierten Sicherheitssystemen (NDR)
- HNDR ist eine spezialisierte Form von NDR-Systemen
- HNDR **versteht** die spezifischen Protokolle des Gesundheitswesens durch Tiefprotokollanalyse (DICOM, HL7 / FIHR*, OpenEHR, …)
- Erkennung von Bedrohungen, Angriffen und Anomalien im medizinischen Netzwerk durch Fortschritte in KI

securITe
Intelligence meets care.

thank you

SecurITe Offices

Friedhofstr. 57
Wels, 4600, Austria

2445 Augustine Dr., Suite 150
Santa Clara, 95054, CA, USA

Green Park, Exeter Park Road
Bournemouth BH2 5BD, UK

www.securite.world
office@securite.world