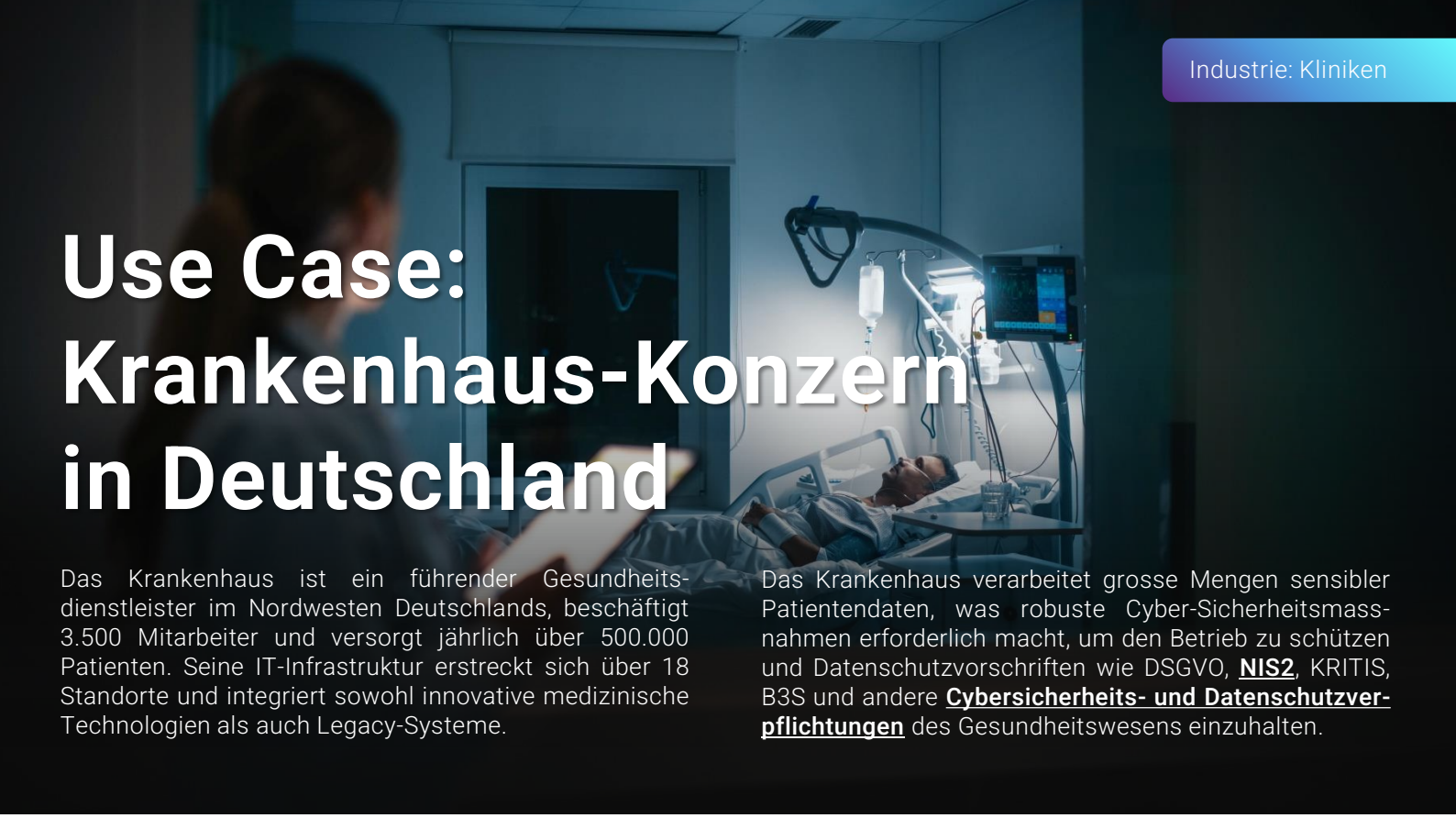


Industrie: Kliniken

Use Case: Krankenhaus-Konzern in Deutschland

Das Krankenhaus ist ein führender Gesundheitsdienstleister im Nordwesten Deutschlands, beschäftigt 3.500 Mitarbeiter und versorgt jährlich über 500.000 Patienten. Seine IT-Infrastruktur erstreckt sich über 18 Standorte und integriert sowohl innovative medizinische Technologien als auch Legacy-Systeme.

Das Krankenhaus verarbeitet grosse Mengen sensibler Patientendaten, was robuste Cyber-Sicherheitsmassnahmen erforderlich macht, um den Betrieb zu schützen und Datenschutzvorschriften wie DSGVO, **NIS2**, KRITIS, B3S und andere **Cybersicherheits- und Datenschutzverpflichtungen** des Gesundheitswesens einzuhalten.

Die aktuellen Trends der Cybersicherheit im Gesundheitswesen

Im Gesundheitswesen hat die digitale Transformation zu erweiterten Angriffsflächen geführt, insbesondere durch die Einführung von Telemedizin und elektronischen Patientenakten, die robuste Sicherheitsmassnahmen erfordern, um die Einhaltung von Vorschriften im Gesundheitswesen zu gewährleisten. Die Gewährleistung der betrieblichen Widerstandsfähigkeit ist von entscheidender Bedeutung, da Cybersicherheitsvorfälle die Leistungserbringung unterbrechen und die Sicherheit der Patienten und die Kontinuität der Versorgung gefährden können. Darüber hinaus erfordert die Einhaltung gesetzlicher Vorschriften einen umfassenden Ansatz, der Transparenz über die digitalen Bestände bietet und gleichzeitig die strengen Sicherheitsstandards im Gesundheitswesen erfüllt.

On-Premises-Lösung mit zentraler Sichtbarkeit und Überwachung gesucht

Die Lösung sollte einen vollständigen Überblick über hybride IT-Umgebungen bieten, einschliesslich Rechenzentren, IoT-Geräte und Remote-Systeme. Sie sollte Anomalien über eine zentralisierte Schnittstelle erkennen und wichtige medizinische Daten schützen.

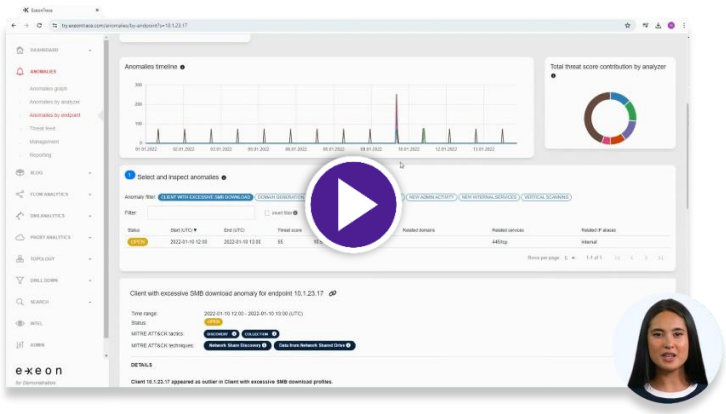
Die Herausforderungen im Einzelnen

1. Datenschutz und DSGVO-Compliance

Die On-Premises war zwingend erforderlich, um sicherzustellen, dass sensible Daten innerhalb des sicheren Netzwerks des Krankenhauses bleiben. Die Plattform verarbeitet pseudonymisierte Daten und erfüllt so die DSGVO Regulierungsstandards.

2. Schutz von medizinischen Geräten und Netzwerksegmentierung

Die Notwendigkeit, Aktivitäten auch innerhalb segmentierter Netzwerke zu überwachen, um ungewöhnliche Aktivitäten wie unbefugten Datenzugriff zu identifizieren, um die Sicherheit kritischer Systeme wie medizinischer IoT-Geräte zu gewährleisten.



Threat Detection in der OT

Zum Demo-Video

exeon
Smart Cyber Security.

3. Schutz vor fortgeschrittene, anhaltenden Bedrohungen (APT) und Ransomware

Ransomware, Zero-Day und Supply-Chain-Attacken, und Insider-Bedrohungen sollten sehr früh erkannt werden, um eine proaktive Schadensbegrenzung zu ermöglichen, bevor der Betrieb beeinträchtigt wird.

4. Sicherheit von Altsystemen

Ältere Diagnosegeräte sollen mit massgeschneiderten Überwachungsregeln gesichert werden. Die Lösung solle Anomalien in Kommunikationsmustern oder unbefugte Zugriffsversuche auch in Altsystemen erkennen.

5. Unterbrechungsfreie Implementierung

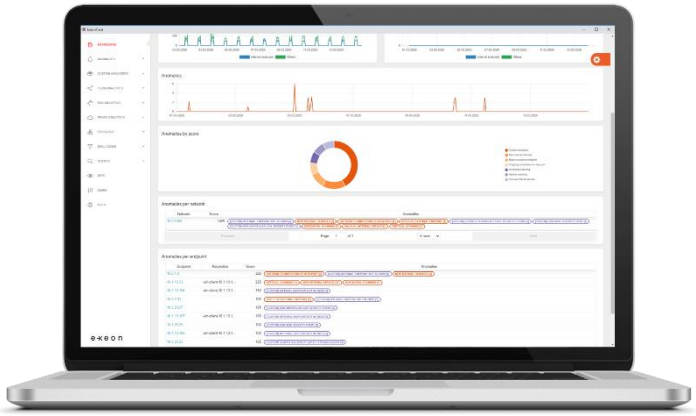
Eine, am besten, reine Softwarelösung sollte sehr schnell implementiert werden können, ideal ohne zusätzliche Hardware, da der kritische Krankenhausbetrieb auch während der Implementierungsphase ohne Unterbrechung weiterlaufen muss.

6. Unterstützung von Zero-Trust-Strategien

Die kontinuierliche Authentifizierung und Überwachung aller Benutzer und Geräte, Granulare Zugriffskontrollen sollen die Integration in zukünftige Zero-Trust-Architekturen unterstützen.

Ergebnisse und Vorteile

- **Umfassende, zentralisierte Netzwerkvisibilität:** Mithilfe von NetFlow-Daten überwacht das Krankenhaus den gesamten Netzwerkverkehr und identifiziert Anomalien effizient über eine zentrale Benutzeroberfläche. Das ermöglicht End-to-End-Transparenz über medizinische Geräte, Patientensysteme und administrative Netzwerke.
- **Schutz von sensiblen Daten:** Eine on-premises, pseudonymisierte Datenverarbeitung gewährleistet die Einhaltung von DSGVO und schützt gleichzeitig sensible Patientendaten.



- **IoT- und medizinischen, cyber-physischen Geräten:** Sichert IoT-Geräte und medizinische Geräte durch Verhaltensanalyse und Metadatenüberwachung.
- **Integration von Legacy-Systemen:** Spezielle Überwachungsregeln sichern Legacy-Systeme, die für die Patientenversorgung wichtig sind.
- **Agentenlose Erkennung:** Die KI-gesteuerte Metadatenanalyse sichert Geräte, ohne dass Agenten auf medizinischen Geräten installiert werden müssen.
- **Erkennung von Bedrohungen in Echtzeit:** Erkennt und meldet Anomalien schnell, um Unterbrechungen in der Patientenversorgung zu verhindern.
- **Compliance:** Eine erweiterte Berichterstellung und Ereignisverwaltung erfüllen die strengen gesetzlichen Anforderungen im Gesundheitswesen.
- **Insider-Bedrohungen:** Identifiziert ungewöhnliche Zugriffsmuster, um sensible Informationen auch vor internen Bedrohungen zu schützen.
- **Nahtlose Integration:** Einfache Integration in die bestehende IT-Infrastruktur zur Minimierung von Betriebsunterbrechungen.
- **Skalierbarkeit:** Das System passt sich an wachsende und komplexe Krankenhausnetzwerke an und gewährleistet eine flexible Bereitstellung.
- **Verbesserte SOC-Unterstützung:** Ergänzt Tools wie SIEM, SOAR und EDR und verbessert die Sicherheitsabläufe und Reaktionszeiten.
- **Minimale Unterbrechung:** Durch die nicht-intrusive Integration werden Ausfallzeiten vermieden und ein kontinuierlicher Krankenhausbetrieb gewährleistet.

exeon
Smart Cyber Security.

Andere kritische Infrastrukturen, die auf ExeonTrace vertrauen:

solothurner spitäler soH

Bonn Netz

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

ExeonTrace: Sichere Krankenhäuser, nahtlose Versorgung

ExeonTrace bietet dem Kunden eine umfassende, skalierbare und DSGO-konforme Cyber-Sicherheitslösung, die auf die besonderen Herausforderungen von Krankenhäusern zugeschnitten ist.

Die Fähigkeit von ExeonTrace, verteilte Netzwerke zu sichern, Altsysteme zu schützen und fortschrittliche Bedrohungen zu erkennen, gewährleistet die kontinuierliche Sicherheit kritischer medizinischer Abläufe. Durch die Einführung von ExeonTrace können Krankenhäuser die digitale Transformation ohne Kompromisse bei der Sicherheit oder Compliance angehen.

Warum Spitäler uns wählen

In diesem Testimonial erklärt Patrick Käppeli, Netzwerkingenieur bei unserem geschätzten Kunden Solothurner Spitäler, wie ExeonTrace den Betrieb sichert.

Allianz für Cyber-Sicherheit

CYBERSECURITY MADE IN EUROPE

ATTESTA ISO 27001 CERTIFIED

Exeon Analytics AG
contact@exeon.com
exeon.com

Grubenstrasse 12
8045 Zürich
Switzerland

LinkedIn

YouTube