exeon

Use Case: Healthcare

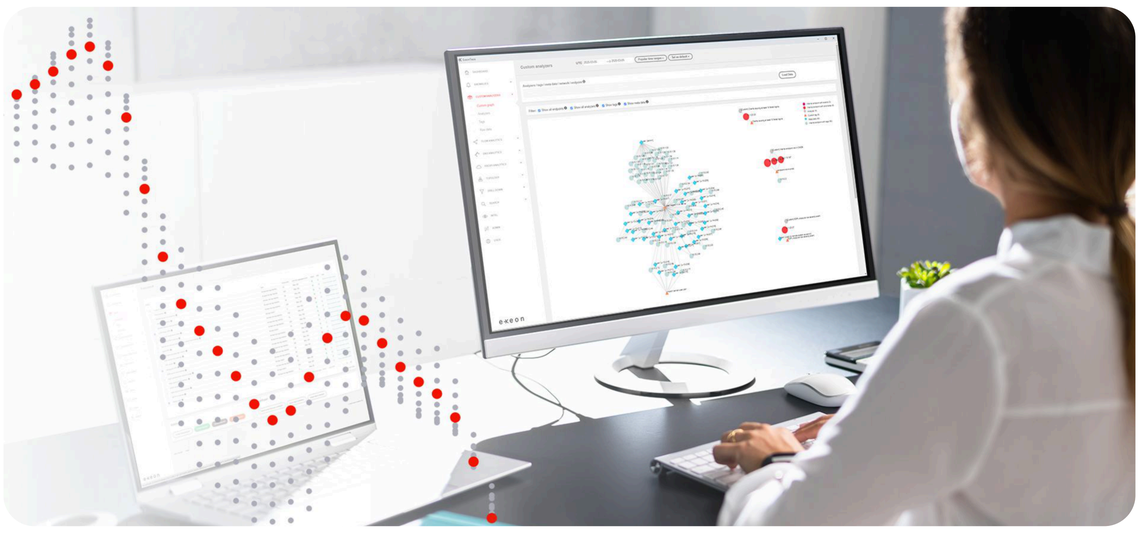
Cyber Resilience in a German Hospital Group

Strategic Insights for **Healthcare Security**

The healthcare sector is at a strategic inflection point: rapid digitization, IoT-enabled care, and regulatory mandates demand a proactive, risk-based security posture that anticipates threats before they materialize. Security leaders must shift from siloed, reactive defenses to integrated, context-aware frameworks that support operational resilience and protect patient safety.

Case Overview

A leading hospital group in North-West Germany—with 3,500 employees across 18 sites and 500,000+ patients annually—needed unified visibility over a complex IT/OT ecosystem of data centers, medical IoT, and legacy systems. The goal was to bolster regulatory compliance and enable real-time threat anticipation without disrupting critical care.



Want a closer look? Discover how it works in our **on-demand demos**.

Core Challenges

Challenge	Strategic Impact
(Patient) Data Privacy (GDPR, NIS2)	Requires on-premises processing and pseudonymization
OT/IoT Availability	Demands passive monitoring that won't interrupt millisecond control
Advanced Threats (Ransomware, APT)	Necessitates early anomaly detection & containment
Legacy Medical Devices	Needs tailored analytics to uncover hidden communication anomalies

Adaptive Monitoring Approach

Rather than layering yet another agent, the hospital adopted a metadata-centric monitoring layer that passively captures network flow and behavioral indicators. This approach complements existing firewalls and endpoint solutions, enhancing signal fidelity without increasing device footprint.

Key elements

Holistic Telemetry
Continuous collection of NetFlow, DNS, and control-plane logs across IT and OT networks.

Behavioral Modeling
Dynamic baselining of device and user activity to spot deviations indicative of compromise.

Contextual Alerts
Rich session metadata empowers SOC analysts to prioritize incidents with surgical precision.

Outcomes & Metrics

Within six months, the hospital achieved:

50%
faster detection cycles through unified visibility.

Zero downtime during deployment—critical for uninterrupted patient care.

40%
reduction in false positives by correlating behavior and flow analytics.

Streamlined compliance reporting aligned with GDPR and healthcare regulations.

Recommendations for Healthcare Leaders

Build an **open-architecture telemetry layer** that spans both IT and OT without impeding operations.

Incorporate behavioral analytics early to detect subtle, pre-attack reconnaissance in medical networks.

Align monitoring initiatives with broader Zero Trust roadmaps: enforce continuous verification, least privilege, and micro-segmentation

Conclusion

Gartner Peer Insights™

Learn more

By embracing an integrated telemetry strategy underpinned by advanced analytics, healthcare organizations can proactively anticipate threats, safeguard patient safety, and maintain compliance—ushering in a new era of cyber resilience that places operational continuity and risk management at its core.