# Continuous Visibility:
# How XM Cyber Protects Patient Trust Across Sana Kliniken's Network

Thomas Lemke,
Chairman of the Board of Sana Kliniken AG
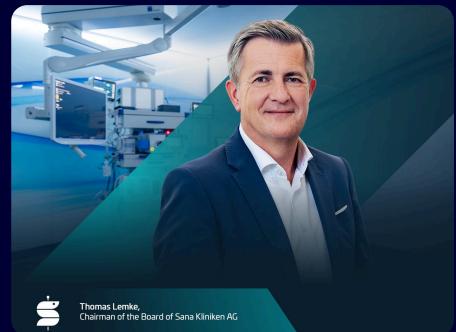
## The Challenge

### Protecting Patient Trust in a Tightly Regulated Digital Landscape

Sana Kliniken AG is one of Germany's largest healthcare providers, operating a vast network that includes about 50 clinics, 58 outpatient facilities, and related health services. With over 40,000 employees, the company's nationwide network connects hospitals, supply stores, and physiotherapy centers, all critically dependent on constant access to accurate and secure patient data.

The healthcare sector in Europe operates under one of the world's most demanding regulatory frameworks. Strict data laws, fixed pricing, and complex compliance rules make modernization and IT investment particularly challenging. Consequently, many hospitals still rely on isolated, legacy systems that struggle to share data or grow efficiently. CEO Thomas Lemke described a key industry challenge: "In terms of the degree of digitization and the use of modern and networked tools, the health care sector has a lot of catching up to do."

To modernize safely, Sana Kliniken needed to overcome these limitations and build a resilient, compliant IT foundation that both protects sensitive patient data and keeps every facility operating smoothly.

## The Solution

### Continuous, Pragmatic Cybersecurity Across Critical Systems

Sana Kliniken chose the XM Cyber Continuous Exposure Management platform, running on the sovereign STACKIT cloud, to significantly strengthen visibility and resilience across its complex clinical and IT environments. The platform continuously maps potential exposure paths and detects weak points that could connect internal systems to external threats. "No single paper, no guideline and no IT certificate really helps us to minimize cyber risks and protect us." Anyone who relies solely on the fulfillment of formalities as a minimum standard is not acting in the interests of the community. Sana therefore takes the clear stance that security must be actively and continuously lived in the very heart of the IT infrastructure.

XM Cyber's attack graph uncovers critical exposures in Sana Kliniken's ecosystem in real time, focusing especially on risks related to medical device networks and mandatory remote maintenance connections. Crucially, the solution allows Sana's teams to prioritize the fixes that matter most—the ones with the highest impact—without interrupting essential patient care.

---

**sana**

---

**Customer**
Sana Kliniken AG

**Industry**
Healthcare

**Location**
Germany

**Challenge**
Protecting sensitive health data and ensuring continuity across a complex, highly-regulated clinical network.

**Solution**
XM Cyber exposure management platform on STACKIT infrastructure.

**Results**
Continuous visibility, proactive prevention, and a sovereign framework for secure digital transformation.

# Benefits and Outcomes

### Resilience, Visibility, and Readiness for Critical Incidents

XM Cyber gives Sana Kliniken a live, integrated view of threats across its nationwide network. By highlighting high-impact exposures, it helps the IT organization proactively prevent costly shutdowns and maintain operational continuity across over 200 operational units. Thomas Lemke framed XM Cyber not as an add-on, but as an essential infrastructure: "You don't have to see it as a cost factor. It's a vital vein that we need to keep the system going."

The platform enables faster identification of weak points, supports coordinated incident responses across facilities, and delivers measurable reductions in overall exposure risks. Sana's teams can now act before exposures escalate into full-scale incidents, protecting both patients and critical operations.

# Outlook:

### Digital Sovereignty as a Condition for Innovation

Thomas Lemke views sovereignty not as an add-on but as a fundamental requirement for progress in the healthcare sector. Operating XM Cyber on STACKIT ensures that sensitive patient data remains strictly under German jurisdiction, supporting Sana's strategic goal of secure digital independence. "It is not only a sufficient, but a necessary condition to find partners who take up this basic need and offer solutions and thus, somewhat patriotically speaking, to anchor independence in this original service again here in Germany", says CEO Thomas Lemke.

With this foundation, Sana Kliniken can continue to expand digital care safely, successfully combining innovation with full control over its systems, data, and patient trust.

## Key Outcomes

> **Continuous monitoring across clinical and IT systems**

> **Early detection and prioritization of high-risk exposures**

> **Compliance with European data protection and sovereignty standards**

> **Stronger resilience and operational continuity across 200 sites**

> **Secure foundation for ongoing digital transformation**