CASE STUDY

Preventing Breaches, Preserving Care

Swiss Regional Hospital Achieves 30% Risk Reduction and Secures IoMT Environment

Overview

Spital Region Oberaargau (SRO) is a growing hospital centre focused on high-quality patient care. The leadership team, application team, and systems engineer knew the risks of unmanaged, insecure cyber-physical systems (CPS). They sought to improve visibility of their connected devices and associated business risks. In addition, SRO leaders wanted a data-driven approach to device procurement decisions. SRO found the platform and partnership they were looking for with Claroty.

Challenges

SRO faced an all-too-common challenge. The IT and CPS security team lacked visibility into the status of connected medical devices and had no direct access to them. The medical device team that owns the assets is not in the same team as the IT staff but leaves the security team with a tough road to securing the hospital's critical systems.

- **Limited Visibility:** A significant challenge remains as MedTech devices were not integrated into the Configuration Management Database (CMDB). Due to their proprietary nature, the inability to deploy inventory agents on these machines left them 'unmanaged' in the traditional IT sense. Consequently, without a reliable database of medical assets, the team lacked the necessary visibility to identify assets requiring protection, the specific risks involved, their network behaviour, or the active threats targeting them

About Spital Region Oberaargau (SRO AG)

SRO AG is the regional hospital centre in the Oberaargau region of the Canton of Bern. The Langenthal Hospital and its two health centres in Huttwil and Niederbipp, as well as the PanoramaPark in Herzogenbuchsee, offer comprehensive and high-quality medical care for the region's population. The satisfaction of their patients and employees is their top priority.

- **Unable to Segment the Network:** The team had no visibility into what devices were communicating, from which VLAN, and to which devices–or which devices were open to internet communication.
- **Operational Inefficiency:** Without data on device utilisation, SRO lacked the necessary metrics to make data-driven decisions on purchasing new, costly medical equipment and had no means to capitalise on operational data for process improvements.
- **Regulatory Risk:** An external security audit confirmed the existence of major vulnerabilities, specifically highlighting critical unpatched legacy systems, which created significant risk exposure for patient data and operational continuity.

Solution

Claroty xDome provided the solution to SRO's challenges. The team quickly gained complete asset visibility, learning exactly what devices have vulnerabilities, legacy firmware, internet communications, and more. They set out with four goals: Reduce their risk score, segment the medical devices, document all IoMT assets, and inform leadership on device utilisation.

> **"With Claroty, we have a super inventory of all devices that are not managed directly by IT. We were able to use Claroty very effectively for segmentation. This was the only way we could restrict all network communication for medical devices in just a year and a half. Without Claroty, this would have taken much longer and would probably have caused more operational interruptions."**
>
> **Martin Herrmann,** IT Security Officer for SRO AG

A Path to Segmentation

The Systems Engineering Team can now use real-time communication mapping to create precise Access Control Lists (ACLs) and enforce network segmentation policies across all connected medical devices, even for devices they do not directly manage.

Maintain a "Super Inventory"

The Information Security Officer and IT team are now able to instantly discover, categorise, and document all IoMT and unmanaged devices, resulting in a comprehensive and constantly maintained inventory where none previously existed.

Data-Driven Device Utilisation

Department Heads and Leadership can now extract and report accurate device utilisation rates for all major medical assets, enabling data-driven decision-making for capital expenditure (CapEx) and procurement.

Tangible Risk Reduction

The security team can now continuously track vulnerabilities, unpatched firmware, and exposed services, providing a measurable metric for security progress and justifying continued investment to SRO Leadership.

Benefits

The implementation of Claroty xDome immediately empowered the SRO IT and security teams, including Information Security Officer Martin and Systems Engineer Silvan, to transition from reactive firefighting to proactive risk management.

> **"Everything is in one place. I can see which devices are not segmented and get through the entire segmentation process in 30 minutes, ensuring there is no risk of unexpected or malicious communications that could disrupt any medical devices."**
>
> **Silvan Kohler,** IT System Engineer for SRO AG

- **Valid, Non-Disruptive Segmentation:** The team was able to restrict network communication for all medical technology devices in an unprecedented short time. They now trust the segmentation policies because Claroty provides a clear view of communication flows, obviating the need for complex queries or disruptive network monitoring.
- **Massive Resource Savings:** Segmentation time was reduced by up to 75% for routine devices. Before Claroty, the task was nearly impossible to achieve reliably. Now, the time required for securing a device type has dropped to just 30 minutes, offering significant resource savings for the IT team.
- **Accelerated Regulatory Compliance:** Claroty's immediate visibility provided critical, verifiable information that helped SRO successfully navigate its medical security device audit. SRO is now positioned to demonstrate substantial progress in future audit cycles.
- **Executive Buy-in and Validation:** The platform provides clear, quantitative metrics that allow the team to justify project scope and show measurable progress to management, such as tracking the reduction of risk devices.

Conclusion

By leveraging Claroty xDome, SRO fundamentally shifted its security strategy from reactive to proactive. They not only closed critical security gaps, such as achieving a 30% reduction in their risk score and containing internet exposure but also gained a powerful tool for operational management. The platform's ability to provide a complete, trusted inventory and enable quick, validated segmentation has proven to be the key to maintaining both a high standard of patient care and a leading security posture in the healthcare sector.