crothall healthcare

asimily

ST LAWRENCE HEALTH

An Affiliate of
Rochester Regional Health

St. Lawrence Health Reduces IoT and IoMT Device Security Risk Through Prioritization and Mitigation

3 Hospitals	144 Beds	3,450+ Connected Devices	20k+ Employees

CHALLENGES

After a ransomware attack in 2019, St. Lawrence Health knew it needed to gain visibility into the protections it had and the ones it was missing. Although they have a managed detection and response (MDR) vendor with the ability to actively monitor medical devices, the provider advised them against using the service since it was unclear of the impact its monitoring would have on the devices.

The health system lacked clear ownership over medical device identification, threat detection, vulnerability remediation, and attack containment. **While the security team focused on defending against attacks, the vulnerability management capabilities remained siloed under the IT team's duties.**

St. Lawrence Health recognized that it had a gap in monitoring its medical device fleet, especially its lack of threat intelligence in the space.

Further, they were concerned about the inherent security issues that medical devices and other types of mission-critical equipment have. These technologies often lack built-in security, using default usernames and passwords that increase the risks to its environment.

The organization sought a cost-effective solution that could:

- Integrate with its outsourced healthcare technology management (HTM) partner, Crothall Healthcare
- Identify all medical devices connected to its networks
- Passively monitor the environment for known vulnerabilities
- Provide threat intelligence for visibility into real-world attacks leveraging vulnerabilities on devices within their environment
- Prioritize the devices that require remediation
- Offer real-time threat detection and incident response workflows
- Offer actionable clinically approved remediation

> "Crothall's CyberHUB powered by Asimily's AI-based risk management technology gives us visibility and insights into our environment we didn't have before. It notifies us of issues and prioritizes vulnerabilities efficiently – time savings equivalent to at least one full-time employee."
>
> — **Richard Ingersoll, Director of IS St. Lawrence Health**

> "We were on the bleeding-edge of a ransomware attack in 2019, and my biggest goal with onboarding CyberHUB was to get back to sleeping at night."
>
> — **Aaron Scott, Information Security Engineer, St. Lawrence Health**

APPROACH

While the cybersecurity talent gap impacts all HDOs, St. Lawrence Health's geographic location makes finding and hiring people with the right skills even more challenging, especially as employees must be on-site regularly.

They needed a solution that would help it achieve compliance objectives across various regulations and frameworks, including:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- HiTRUST CSF Framework
- DNV Standards with an annual audit

After reviewing the CyberHUB offering, St. Lawrence Health selected our platform for its ability to:

- Gain full visibility into IoT and IoMT device inventory
- Filter out false vulnerability positives
- Identify exploitable vulnerabilities per device
- Detect and capture anomalies and threats for automated Incident Response
- Reduce medical device cybersecurity risk
- Prioritize remediation and streamline mitigation by collaborating with Crothall's onsite HTS team
- Drive the development of a holistic ongoing security program with deep expertise
- Create benchmark reports that apply to each healthcare entity to communicate risk reduction and NIST coverage to the board

OUTCOMES

St. Lawrence Health found the CyberHUB deployment a straightforward process that required little beyond incorporating the appliance into its environment in order to begin passively monitoring the network.

The discovery that some connected medical devices were communicating with servers in other countries led to a comprehensive investigation. The team took effective measures to secure the devices properly.

Additionally, the system uses the platform for:

- Reviewing various reports, including the Banned FCC report to ensure none of its vendors are selling technologies that could lead to compliance violations.
- Identifying devices that have default usernames and passwords that create unauthorized access risks, including security cameras and medical devices
- Monitoring and investigating device communications to mitigate risks arising from undetected command and control communications
- Leveraging vulnerability reports to identify and prioritize remediation activities
- Tracking risk scores to provide key performance indicators over the organization's medical device security posture

St. Lawrence realized significant value by leveraging CyberHUB to offset its need for at least one full-time employee. Current staff can easily review dashboards and reports to gather the information they need, freeing them up to focus on other critical tasks.

FUTURE PLANS

Having achieved its initial baseline objectives, St. Lawrence Health can move forward to mature its security posture.

The organization plans to create a single pane of glass for the network infrastructure connecting it to Rochester Regional Health. **As it moves toward a zero-trust model, it plans to implement additional network technologies, to mitigate unauthorized access risks** and review technology risks prior to implementing them in its environment.

Take control of your connected medical and IoT devices with Crothall's CyberHUB, powered by Asimily's AI-based risk management technology. Visit **crothall.com** or call **1-877-4CROTHALL**.