Lake Regional Achieves Cybersecurity Boardroom Alignment Using Sensato's Nightingale Solution

The Customer: Lake Regional Health System ("LRHS") is a not-for-profit community-based hospital in Osage Beach, Missouri. Lake Regional's mission is simple: Provide exceptional health care.

The Challenge: Lake Regional Health System relied on what is commonly considered traditional cybersecurity practices. Traditional cybersecurity practices often hamper the ability of an organization, especially those supporting critical infrastructure, to adequately address the challenges posed by the current threat landscape and evolving regulatory requirements.

As they evaluated their needs of what cybersecurity should be, it became apparent that traditional approaches to cybersecurity no longer addressed their vision. They also realized that most cybersecurity organizations could only solve one or two specific challenges. The cost and complexity of managing multiple tools were not sustainable, and Lake Regional had spent time and money on the implementation, training, and maintaining various tools. Because it was so cumbersome to manage, many purchased solutions were never fully implemented.

The Solution: As Lake Regional evaluated various cybersecurity solutions from well-known vendors (Alien Vault, Symantec, and others), they came across the term "full-stack cybersecurity platform" by Sensato. The Sensato Full-Stack Solution was built on Sensato Nightingale (a fully integrated cybersecurity software platform that combines deep packet inspection, host intrusion detection, honeypots, honeytokens, vulnerability scanning, compliance tools, log analysis, incident response, and security orchestration). Integrated with Nightingale is the Sensato Cybersecurity Tactical Operations Center (CTOC) that is specifically crafted to address the needs of critical infrastructure organizations, especially those who must protect human life.

The Full-Stack Solution includes Sensato Widgets. Widgets are a library of policy and procedure templates, cross-walked to NIST 800-53, NIST-CSF, HIPAA, and PCI, which can be used to support compliance and regulatory requirements. The solution was deployed by Lake Regional in a matter of weeks, replacing their traditional approaches and several single-point solutions with a fully integrated cybersecurity program.

The Process of Identifying Cybersecurity Priorities

Lake Regional was initially focused on meeting HIPAA requirements, but their cybersecurity vision was much grander; they wanted a program based on the current threat landscape and holistic. They didn't want to buy multiple software solutions and try to get them all talking together. Lake Regional's CIO, Patrick Neece, wanted to replicate the best healthcare information technology ("HIT") practices to support patient care and safety. HIT best practices demonstrate that you reduce costs and improve patient outcomes when you use integrated technology solutions, coupled with consistent patient monitoring and documented evidence-based methods. Lake Regional wanted to achieve the same level of confidence in their cybersecurity program as they had achieved in supporting patient care through technology.

To start, Lake Regional decided to adopt NIST CSF as their foundational framework. This first step is what prompted them down a path to assure that; however their cybersecurity program evolved, the tools, policies, and procedures would need to support NIST CSF. The organization also wanted to ensure that they could articulate cybersecurity priorities and current versus future state to their board members, executive leadership, and across the organization.

"To me, we needed to start with a foundation of understanding and alignment when it comes to cybersecurity from boardroom to basement," shared Patrick. "The majority of current offerings are a roll your own mentality. You buy software from one vendor, more from another, and then you turn to consultants to provide expertise. Followed by contracting or building a security operations center, you try to get all your infrastructure to share logs with something else. You then need to add more software and consultants to get it all to work. Then you end up with a system that generates different alerts in various systems, and if you are lucky, you can maybe make sense of it all. It reminded me of where healthcare information technology was ten years ago."

This classical approach to cybersecurity is something that Gartner has identified as a risk. On average, organizations across all industries deploy between twenty and thirty different cybersecurity tools. Yet only 23% of organizations fully deploy the tools purchased in a manner that reduces risks and improves defenses against today's threat landscape.

> *"Working with Sensato is more like working as part of a team than a typical vendor/client relationship."*
>
> *~ Patrick Neece*
> *CIO, Lake Regional Health System*

Deploying the Solution

After evaluating solutions and recommendations from various vendors, Lake Regional learned about Sensato Cybersecurity Solutions. Sensato offered a fully integrated platform that supports compliance, detection, and incident response. The platform can be deployed in less than a day and provides advanced technologies (deception technologies, active countermeasures, deep packet inspection, machine learning) backed by a robust managed detection and response program based on the military's tactical operation centers (TOC). It also provides best practices, procedural and policy templates, and an annual tabletop simulation. More importantly, for Lake Regional's requirements, the Sensato full-stack solution offered the medical device cybersecurity program that meets or exceeds the FDA suggestions for hospital medical device cybersecurity. Sensato's solution is designed to help detect and respond to IoT, OT, and IT threats holistically, making it a robust single platform solution for many environments.

Upon deploying the full-stack solution, Lake Regional took advantage of the Nightingale Compliance module. Specifically, the Cybersecurity Capability Maturity Modeling (C2M2) tool. C2M2 is a proven methodology for evaluating the current state of cybersecurity maturity and providing a roadmap of priorities. In Patrick's own words, "Having the C2M2 assessment gave me a way to finally align the Board Members and Executive team with our cybersecurity strategy. We could visualize what we were trying to explain in a manner we couldn't do before deploying the Sensato solution. We went from having little to no knowledge of where our cybersecurity gaps were to, within a week, the board members were asking how much budget we needed to fix the gaps."

Patrick went on to disclose that, "The entire C2M2 process is fairly easy. It's a series of questions within ten domains, assessing your maturity level and reports if you are green, yellow, or red in each area. We were quickly able to determine where we needed to focus our attention. We can also track progress, reassess and compare results side by side."

Lake Regional used the C2M2 dashboard to communicate their needs to the board in 15 minutes resulting in funding approval to put cybersecurity measures in place.

Medical Device Cybersecurity

Lake Regional faced another challenge in making sure their medical devices were secure. Lake Regional had no visibility into what was occurring with their medical devices because they didn't have a way to monitor them. Monitoring and protecting medical devices was a high priority for Lake Regional. Patrick states, "Being able to monitor all devices on our network is like the golden egg."

With the implementation of Nightingale, they can fingerprint and inventory devices and monitor medical devices and IT, OT, and IoT devices on the network. Patrick comments, "Working with Sensato is more like working as part of a team than a typical vendor/client relationship."

Summary

Patrick's advice for other hospitals is to rethink their whole cybersecurity program, starting with risk assessments. He suggests asking, "how valuable is your current process to you?" Most risk assessments produce lengthy documents that focus on the technical aspects instead of improving processes and procedures that can help stop a cyberattack. Patrick recommends defining a longer-term strategy that takes you into the next three years—utilizing C2M2 to turn your assessment process on its head and focus on getting boardroom alignment by using a tool to illustrate gaps and priorities.

Patrick states: "I had looked at a lot of products over the last two years trying to find the right partner, and everything was too complex; even negotiating contracts was taking months. Working with Sensato was a simplified approach to get a comprehensive solution implemented quickly. We feel very fortunate that we ran across the Sensato application".

To learn more about how to advance your cybersecurity strategy, contact us at info@sensato.co