Deloitte.

Together makes progress

Deloitte Cyber Operate
A life sciences company's journey

A medical device maker turns fragmented cybersecurity efforts into an integrated strategy

The challenge

It's not unusual for companies to drift into a state of subpar cybersecurity hygiene. Patchwork infrastructure, inconsistent practices, and process bottlenecks often stay under the radar, where they can build up over time.

However, to the new chief information security officer of a global medical device manufacturer, the situation presented some immediate concerns. The security team was managing several Priority 1 incidents each month, many stemming from long-standing infrastructure vulnerabilities that were yet to be addressed. In addition, there was limited visibility into whether existing security controls were fully aligned with live environmental data, making it difficult to assess overall effectiveness. Taken together, these gaps underscored the importance of strengthening oversight and assurance processes to ensure devices continued to meet the high standards required for use in critical surgical settings.

A disparate global environment

What the company's cybersecurity organization needed was a coherent strategy. However, IT operations were fragmented into three global regions with no unifying vision. On top of that, the infrastructure teams owned the assets. This meant the cybersecurity team was unable to carry out many of the tasks they were responsible for, such as applying security patches. What they could do was recommend a course of action and encourage the asset owner to follow through.

To make matters even more challenging, many of the assets under the infrastructure team's purview were physically controlled by a variety of IT service providers. The same was true for cybersecurity—a given region might have as many as three different security operations centers (SOCs) running

in parallel. Although the vendors were meeting their service-level agreements, it wasn't enough to maintain accountability due to the lack of coordination or visibility between the different coverage areas.

Pivot to consolidation

With those circumstances in mind, Deloitte's Cyber Operate team set up a workshop with the client to identify ways to consolidate the three regional IT operations into an integrated, next-generation global SOC. A year later, the client issued a request for proposal (RFP) for global consolidation services. The RFP contained some of our suggested approaches and leading practices, including three principles to guide day-to-day operations:

- Standardization of tools, practices, datasets, and dashboards
- Modernization by leveraging the benefits of new technologies
- Operational excellence via automation and a focus on business objectives
- To simplify the cybersecurity operating model, we proposed organizing the SOC across six domains, each consisting of a defined set of workstreams. For example, the application security domain's workstreams ranged from security scanning to threat modeling. Each domain would be plugged into an ongoing governance cycle to drive consistency, improve efficiency, and be able to uphold compliance with industry standards and leading practices.

This was a competitive bid. In the end, the client selected Deloitte for the depth of our skills and access to global capabilities across the Deloitte Touche Tohmatsu Limited network of member firms.

Results

Although one of the goals was to reduce fragmentation across a multiregion, multivendor environment, our proposed approach didn't preclude outsourcing. What it did was provide a way for the client to gain ownership over their security information management and allow consistency to govern. The tools and data would continue to belong to the company while Deloitte managed the company's global security operations.

By helping the client redesign its approach to cybersecurity, the Deloitte team shifted their perspective on what a managed service could be. It doesn't have to entail a binary decision between the managed service provider owning all the equipment or the company owning all the work. A well-thought-out strategy can bring creative solutions into focus, while positioning the organization for greater insight, efficiency, and effectiveness.

About Deloitte's Cyber Operate

Deloitte's Cyber Operate managed security services bring cloud-based threat hunting, detection, response, and remediation capabilities to your cybersecurity environment. Specialists pursue threats before they become attacks and respond to help limit business impact. Example services include:

- Cyber threat intelligence
- Incident readiness and response
- Zero Trust identity prevention, detection, and response
- Enterprise prevention, detection, and response
- Attack surface management and vulnerability management
- Multicloud security

Contact us today to see how Deloitte's ***Operate*** services can deliver for you.

Contact us:

Paul J. Kim
Managing Director
Deloitte & Touche LLP
Email: pjkim@deloitte.com

Akhilesh Bhangepatil
Senior Manager
Deloitte & Touche LLP
Email:abhangepatil@deloitte.com