Bringing cyber security to the next level at a large health care organization

The challenges

A Fortune 50 provider of health care products and services had developed a sound security information management environment and a capable cybersecurity team. However, they needed to improve operational efficiency, keep up with new threats, and better align their resources so that they can focus on more complex initiatives directly impacting the business.

Challenges included:

- Gaining an external perspective on the cybersecurity environment and its operational elements to add greater rigor and discipline to processes while improving their knowledge base
- Enhancing capabilities to proactively identify, monitor, and manage evolving security threats
- Bolstering their teams with specialized skills and reallocating resources to other higher-value initiatives
- Increasing the return on investment in its technology for application management, security, compliance, and analytics
The approach

Senior management turned to Deloitte’s Fusion Managed Services and its team of skilled practitioners to help them move beyond monitoring alerts and recommendations to advanced threat detection and response. The organization wanted to develop a strategic, collaborative relationship with a service provider that could scale and grow with them.

A new approach included:

- A flexible co-sourced model where Deloitte acted as members of the client’s team and integrated with the client’s 24x7 monitoring, ticketing, and escalation workflow tools. This enabled both the client and Deloitte to have full visibility into events, triage, and incident response.

- Proactive threat hunting and reconnaissance based on analysis of internal and external threat intelligence data and insights, open source information, and knowledge of the organization.

- Ramping up threat intelligence capabilities and identifying special scenarios. As an example, the company was involved in M&A activity that posed a risk. Deloitte developed custom Security Information and Event Management (SIEM) content and increased monitoring during the M&A period.

- Elevating the strategic importance of threats and investigations for the CIO and CISO and their senior leadership team.
The benefits achieved

The organization was able to significantly expand its capabilities and workflow while cost-effectively reallocating its resources. Specifically, the organization has been able to:

- **Redeploy skilled resources from work on lower-level issues to work on internal threat intelligence, architecture and development, analytical and automation projects, and broader enterprise security initiatives**
- **Cope efficiently with its stringent and evolving regulatory environment, including compliance with reports and expectations related to SOX and HIPAA**
- **Navigate a merger integration that presented a particularly complex set of cyber security risks**
- **Enhance its weekly operational and quarterly executive reporting to equip the CIO and CISO to have more strategic conversations with senior executives and business managers**
- **Drive more value from its SIEM through custom rulesets and content versus its previous reliance on out-of-the-box rulesets and modules**
- **Move its SIEM content and data sources from an on-premises environment to the cloud, in an efficient and secure manner**