MANDIANT

CUSTOMER STORY

GLOBAL HEALTHCARE GIANT EXPEDITES SOC MERGER TO ENHANCE WORLDWIDE SECURITY POSTURE

Mandiant Cyber Defense Operations delivers blueprint for success

FACTS AT A GLANCE

Industry
Healthcare

Solution

- Mandiant Cyber Defense Operations

Benefits

- Expedited the merger of two disparate SOCs into a consolidated function without disruption to ongoing security operations
- Used existing strengths of both SOCs as foundation for world-class capabilities
- Complied with all pertinent regulatory, industry and contractual requirements
- Reduced SOC-related costs and increased capabilities and efficiencies
- Infrastructure designed to assimilate the security functions of future acquisitions

Customer Profile
The company is one of the biggest global health services providers in existence. It offers a broad range of insurance products—covering medical, dental, vision and significant life events— and also is a respected manufacturer of medical equipment.

The challenge

Mergers and acquisitions have become common occurrences across healthcare sectors around the world, frequently creating the need to combine or assimilate functions such as cyber security from previously disparate organizations into one unified body.

Following the high-profile acquisition of a complementary business, the company needed to quickly merge its existing SOC functions with those of the newly acquired entity.

The spokesperson for the new SOC described, "Although the combined security teams were highly skilled and experienced, because of the disparity in maturities and capabilities, it became apparent that bringing in external support would be the most expedient approach to ensuring a successful outcome to the SOC consolidation while simultaneously maintaining existing defenses."

> *The quality and comprehensiveness of the FireEye plan, combined with continuous guidance, ongoing customizations and hands-on implementation support enabled the rapid realization of meaningful improvements to our worldwide cyber defense capabilities.*
> — **SOC Spokesperson,** Global Health Services Provider

The solution

Having previously worked with the Mandiant Cyber Defense Center Development team on SOC enhancement initiatives for SOC blueprint and playbook development, the organization decided to engage the Mandiant Cyber Defense Operations team to help with the consolidation.

The Cyber Defense Operations team is comprised of expert consultants with unrivaled firsthand, frontline incident response experiences. The team use proven methodologies that reflect the knowledge acquired from designing and managing many of the world's largest cyber defense operations.

Phase 1

The team began by rigorously assessing the discrete capabilities of the two (original and acquired) SOCs to determine the maturity level of the individual components of each organization. With this snapshot of the SOC's legacy capabilities as a baseline, they constructed a detailed blueprint to architect a best-of-breed set of processes, competencies and technologies in a downstream phase.

Phase 2

The company's business model put it at the intersection of multiple exacting regulatory bodies—including healthcare, financial services and the payment card industry—making it imperative for the redesigned SOC to adhere to all relevant mandates. Regulatory requirements, both global and regional, were then merged with contractual and service-level obligations to create a highly detailed series of criteria that were subsequently integrated into the design blueprint.

Phase 3

The third phase was the development of a comprehensive blueprint for a consolidated SOC. This blueprint would embrace the findings from phases one and two and combine them with a rich set of operational elements and considerations, such as staffing, a unified SOC intake model and a future transformation roadmap with a unified taxonomy of terms, as well as a rearchitected technology stack.

The Cyber Defense Operations methodology prioritized focus areas for the blueprint: This enabled the team to expedite the launch of the transformation and minimize the duration of any ineffective duplication between the two legacy SOCs.

The new model took advantage of the strengths of both legacy centers and mapped a path a state-of-the-art security operations facility, that could protect the digital assets of a multi-billion-dollar enterprise. The design also considered streamlining the future absorption of new SOCs and security capabilities from upcoming acquisitions once the design was operationalized.

Becoming the trusted advisor

In this complex engagement, many nuances and challenges had to be considered. Once the optimal processes, procedures and technologies were defined, the ultimate success of the project depended on team members around the globe being aligned and united behind a common vision. The spokesperson for the new SOC reflected, "The intrinsic credibility of the FireEye consultants enabled them to quickly establish themselves as trusted advisors and operate as a single point of contact to unify all of the global groups that needed to collaborate and come together on this project."

The spokesperson for the new SOC concluded, "The quality and comprehensiveness of the FireEye plan, combined with continuous guidance, ongoing customizations and hands-on implementation support enabled the rapid realization of meaningful improvements to our worldwide cyber defense capabilities."

Learn more at **www.mandiant.com**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT