CyberProof®
A UST Company

Better Security,
Together.

CASE STUDY:

How a healthcare payment processor went from 3 SOCs and 3 SIEMs to a single, global, threat-led SOC

INDUSTRY: HEALTHCARE

About the client

As a healthcare payment processor, our client solves complex operational challenges across all lines of business, including Medicare, Medicaid, Commercial, Individual and Self-funded employer health plans. By acting as a one-stop-shop for all health plan technology needs, the business aims to create meaningful operational cost savings for its customers.

Its security program is built on four key pillars, which are risk compliance governance and audit, security operations, application security/data security, and identity and access management, all of which form the foundation of its threat exposure management strategy. By leaning on best-of-breed vendors for each area of the business, the client has historically been able to rely on the right Subject Matter Experts for each project.

Client challenge

The client's existing infrastructure consisted of many disjointed systems and databases, which led to inefficiencies and inconsistencies. Due to an uncoordinated approach, the business found it hard to adapt to market needs as they evolved. Teams found that without true visibility into their work and systems, they were duplicating efforts and spend on the same tasks and tools, and limiting their ability to understand and prioritize threats based on exposure.

The business had three SIEM tools and three Security Operations Centers (SOCs) and knew it was time to move to a single unified SOC. “With three entities, and three different tech stacks, operational inefficiencies were rife, which increased our susceptibility to human error,” the CIO said. “We had almost no real-time visibility, and I, myself, had an ID in three different places, with each system working in a silo. The business couldn’t respond to real-time events or proactively manage threat exposure, which had a direct impact on duplication of effort and rising costs.”

Goals for the project included:

- **Increasing efficiency:** By automating tasks that were traditionally performed by human analysts, the company could address the ongoing talent shortage.
- **Lowering costs:** First, everyday operational spend was excessive, and second - the potential costs of a major incident due to poor processes were significant.
- **Improving accuracy:** The client wanted to be able to identify and prioritize potential threats based on risk exposure, reducing false positives and enabling more efficient incident response.
- **Reducing technical footprint:** Another goal was to adopt one unified SOC that had robust threat visibility and response capabilities, rather than lean on multiple disparate tools.

Benefits

Establishing a unified, threat-led SOC: From three disparate SOCs and SIEMs, the client transitioned out multiple service providers and was able to onboard a single global SOC in just 6 weeks.

Leveraging Gemini’s Advanced Language Capabilities: Gemini makes it easy to search for information and to train both technicians and the SOC team. It also has a direct impact on improving incident response, reducing MTTR.

Adopting a threat-led SecOps focus for the business: Automation has made operations far simpler, with 30+ log sources connected and parsed, from AWS and Azure to SaaS and on-prem.

Custom playbooks: Implementation of 120+ custom detection rules and a single contextual best-of-breed playbook consolidating CyberProof’s experience and Google’s security playbooks.

Why CyberProof?

The client's overarching goal was to transition from working with multiple service providers, Microsoft, SumoLogic and SecureWorks, into a single effective SOC. By partnering with CyberProof, the business could benefit from a strong partnership with Google and complete a Google SecOps implementation for correlating and ingesting data sources. This created unified threat visibility and exposure reduction by consolidating their existing three SOCs into a single pane of glass.

Another differentiator was CyberProof's extensive playbooks, all customizable to meet specific business needs. "One of the main benefits of working with CyberProof was the ability to create more than 120 custom detection rules," the CIO said. "We started with a set of playbooks out of the box, created from CyberProof's wealth of experience, and then augmented with our existing playbooks as well as Google's security playbooks to consolidate and find the best-of-breed rules — making a single playbook, a single set of threat-led use cases for our needs."

Our solution

Within six weeks, the client had migrated from three SOCs and three SIEMs to leverage CyberProof's global SOC, and Google SecOps Enterprise Plus. They had 35 log sources to connect including AWS, Azure, SaaS solutions and on-premises logs, and around seven thousand devices. Together this was 20TB per month — billions in logs every day to correlate and parse. Some parsers were unavailable and were therefore built from the ground up.

To ensure business continuity and maintain continuous threat visibility, CyberProof worked with the client to implement a phased migration. After the six-week onboarding, both systems worked in tandem for six months — the previous three SOCS, and the new unified CyberProof SOC. Within this period of time, the client was able ensure everything was working as intended, and was also able to leverage the advice and insights of HITRUST during its recertification process. Being a certified HITRUST entity is an important part of its business model, ensuring compliance while advancing a threat-led, risk-based security posture. This was critical alongside meeting wider regulations in Healthcare such as HIPAA. It was crucial for the client to feel confident that any redesigned or modernized security operations wouldn't cause compliance issues. After six months of working without any issues, they were able to cut off the previous solutions entirely.

By leveraging CyberProof's partnership with Google, the business has been able to gain a tremendous amount of functionality, flexibility and power as the driving force behind its security operations. For example, they can now leverage Mandiant for Threat Intelligence, VirusTotal for malware scanning, and Gemini for advanced language capabilities, providing real-time context for threat exposure and reducing Mean Time to Respond (MTTR), critical for incident response. Everything works together seamlessly, providing that much-needed single pane of glass.

Working with CyberProof, the team has been guided through a threat-led exposure management process, identifying, prioritizing, and remediating the most critical risks to the business.

CyberProof®
A UST Company

Better Security,
Together.

About CyberProof

CyberProof, a UST company, delivers better security operations and drives superior experiences for enterprise customers. Our cloud-first, AI-powered approach to security delivers industry-leading services to drive real business results. We believe that working closely with our customers and partners through a 'better security, together' services model jointly empowers us to defend against the greatest of threats. See: www.cyberproof.com.

Barcelona | California | London | Singapore | Tel Aviv | Trivandrum