STELLAR CYBER®

CASE STUDY

5iron Implements an Automated, Multi-Tenant Security System to Expand Services

Automates Security Responses to Boost Analyst Productivity

5iron is an advanced managed security service provider focused on serving financial institutions. Based in Nashville, Tennessee, the company serves banks and credit unions throughout the United States with a variety of services, including secure e-mail protection, intrusion detection (IDS), security information and event management (SIEM), firewall, as well as advanced endpoint, all managed around the clock from the 5iron security operations center (SOC).

"We provide managed security operations – SOC as a service," says Jeremy Hopwood, CEO of 5iron. "Often the focus is on buying another box which adds layers of security, but the CISOs know that just means more to manage. 5iron managed solutions ease the client's internal burden and increase their security posture by providing around the clock management, detection, verification and response."

SIEM WOES

5iron's managed SIEM services are built on best-in-class platforms to ensure its clients have the most actionable intelligence possible. The company had been primarily using a platform from one of the largest SIEM providers, but it wasn't getting the service or support it needed. Because of the size of the major SIEM provider, 5iron often had to wait in a queue for answers to product questions or issues, no matter how large the problem. As a company that prides itself on rapid-response services to its own clients, 5iron grew frustrated with slow response times from the provider.

In addition, while the existing SIEM was good at detection and reporting, 5iron wanted a platform that would automate the collection, detection, investigation and response processes in order to make its security analysts more effective and the response to threats quicker.

> "Starlight gives us the ability to expand our own service offerings. We can now offer security analytics as part of our Managed Security Operations offering."

Multi-tenancy was another key issue. 5iron needed to be able to manage all of its clients efficiently from a single interface, but the existing SIEM required expensive and complex add-ons to support multi-tenancy. The company wanted a platform that delivered multi-tenancy natively, simplifying operations and client management.

A final issue was the cost. The existing SIEM's pricing proved to be a barrier to entry for many organizations. Small and mid-sized customers in particular were balking at the cost of the service, and even large enterprises were concerned about the cost. As a result, 5iron could not provide the quality of tools necessary to effectively manage

> "Starlight makes our analyst teams more efficient, and continually improves our services day after day. That's something we could never have done with our existing SIEM."

security operations in these organizations. The Starlight pricing model enabled 5iron to provide both a more robust platform and a competitive pricing model to their clients.

SWITCHING TO STARLIGHT

On seeing a demonstration of Starlight at the RSA show in 2018, 5iron saw an opportunity. Starlight offered automated incident response, multi-tenancy and an agile support team, all at a fixed cost that provided more value for a lower cost than the existing SIEM.

"As a strategically-focused service provider, we didn't have the level of partnership we needed from our existing SIEM vendor," says Hopwood. "Stellar Cyber gives us both the platform and the support we need to effectively support our clients. The company is much more nimble with requested features and faster to respond to support requests—that's a tremendous value. When we're trying to be as agile as possible with our own customers, we need a vendor that is acting as a real partner."

It was the robustness of the platform that really motivated 5iron to adopt Starlight. "The clincher was that Starlight does so much more than we originally thought," says Hopwood. "Starlight gives us the ability to expand our own service offerings. We can offer security analytics as part of our

Managed Security Operations offerings. With Starlight's built-in IDS, threat intelligence, threat hunting and other functions, it gives us significantly more capability than a traditional SIEM."

Starlight's industry-leading ability to collect the right information, detect anomalies, investigate the causes, and respond to threats automatically sets it apart from other security analytics and SIEM platforms.

"Starlight isn't just an alerting engine—it can take action," says Hopwood. "We don't have to see the same alert a thousand times; we can see it once and work with the system to block it. Traditional SIEMs create a ton of alerting noise, and filtering through this noise can cause analysts to be less effective. Instead, they should be focused on actionable intelligence and tightening the security posture. With a traditional SIEM for example, thousands or even millions of alerts can occur each day, and analysts responding to this many alerts are not efficient and cause responses to take hours rather than minutes or seconds. Starlight more effectively correlates and addresses those alerts before they are presented to the analyst. As a result, analyst effectiveness is increased because they are responding to fewer but more specific alerts. Starlight has enabled us to continually tighten the security posture of our clients, and that's worth the price."

Moreover, Starlight's pricing was aligned with 5iron's business strategy. Stellar Cyber's pricing model enabled 5iron to get its services into the hands of people who couldn't have purchased the competition. In reality, Starlight lowered 5iron's spend on SIEM solutions enough to pay for the product, so what was originally seen as a product that would refine its current SIEM became a new and highly cost-effective platform for expanded services.

"I can take this product out to many more people than I could approach before," says Hopwood. "It's become a core platform for all of our customers."

As 5iron rolls out Starlight-based services to its financial industry customers, it is developing new ways to deliver services. "We see expanded platform and service possibilities," says Hopwood. "Starlight makes our analyst teams more efficient, and actually improves our services from day to day. That's something we could never have done with our existing SIEM."