CASE STUDY

CyFlare Builds Wholesale SOC-as-a-service Offering with Stellar Cyber's Starlight

Multi-tenant Solution Scales from Tiny MSPs to Large Enterprises

CyFlare is a top 100 global managed security services provider (MSSP) based outside of Rochester, New York. The company wholesales managed security services to small and mid-sized VARs, MSPs and MSSPs, and brings value to its customers by delivering Security Operations Center (SOC) as-a-service functionality that's comprehensive, cost-effective, and easy to deploy. CyFlare relies on Stellar Cyber's Starlight solution as the core of its SOC-as-a-service offering.

While many managed security providers cobble together complete solutions from a dozen or more different products, CyFlare CEO and co-founder Joe Morin thinks he has a better way.

"I'm hoping to be at the center of the transition from buying boxes to buying infrastructure as a service and become the premier provider of SOC-as-a-service to MSPs and MSSPs," says Morin. "Building your own SOC from scratch is wildly inefficient – it's the same as people building their own datacenters instead of using AWS. By offering SOC-as-a-service, we can accelerate our customers' time to value, make them more efficient, and improve reseller margins."

But not all SOC products make a good foundation for SOC-as-a-service. Some security providers are trying to expand their market profiles from firewalling or SIEM to a full-on SOC to provide what's known as Detection and Response for Anything (XDR), but these efforts typically involve buying all of that vendor's security systems, which means replacing systems the customer already has. CyFlare has chosen another path: Open-XDR.

> "Starlight enables our analysts to be very efficient in identifying real threats. Traditional SIEM solutions do not provide the many security engines that Starlight provides such as application ID, full packet capture, curated machine learning rules, file sandboxing and more than a dozen integrated commercial threat intelligence feeds."

"With the Starlight platform, we're product-agnostic," says Morin. "Customers don't want to rip out existing security systems and replace them with another vendor's products, and Open-XDR allows them to keep their existing equipment. In that way, Open-XDR makes it way easier for MSSPs to land an account."

"Starlight not only enables compliance and replaces incumbent SIEM solutions, but it we refer to it as a hyper-paranoid security platform that offers more sophisticated threat hunting than other solutions."

SOC SOLUTION REQUIREMENTS

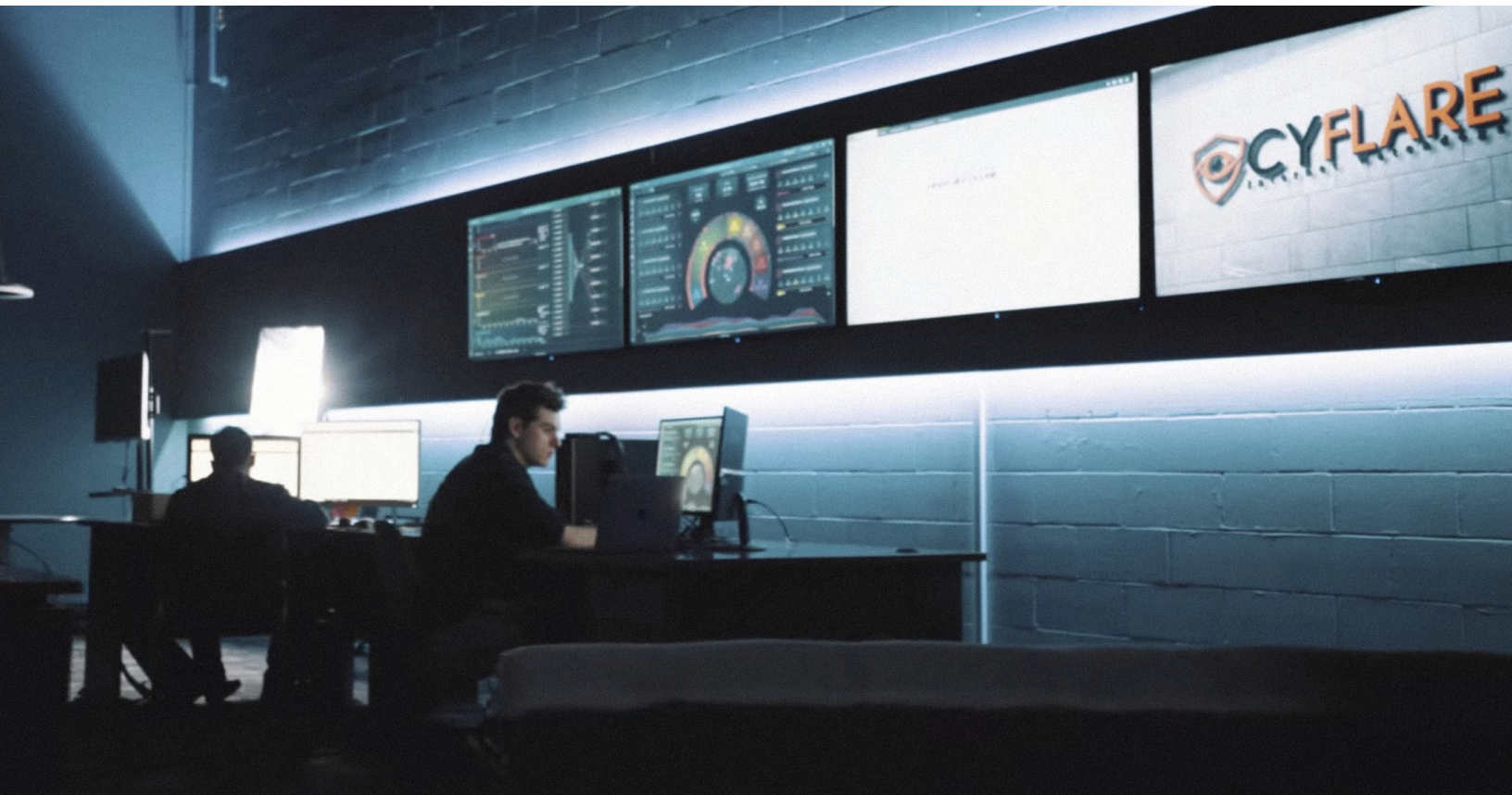
In searching for a platform on which to base their SOC-as-a-service offering, CyFlare considered several alternatives, including the typical market-leading SIEM solutions, but none proved feasible due to the significant cost, lack of capabilities or solution extensibility. That's when Morin got in touch with John Peterson, Chief Product Officer at Stellar Cyber.

First off, Stellar Cyber's Starlight solution is the only Open-XDR offering on the market. It deploys as software in the cloud, edge or via a turnkey appliance, and it does not require customers to swap out any of their existing security hardware. Secondly, Starlight scales easily from very small to very large customer accounts, and it does so cost-effectively.

"What was compelling with Stellar Cyber was that it was possible to put it into small clients with a simple hardware device, and yet it could scale all the way up to large enterprise deployments. This strategic alliance enables us to provide a complete SOC-as-a-service solution including the hardware and software that every organization on the planet can afford."

TRIALS AND RESULTS

To test Starlight, Morin's team put it on the company's internal network and also deployed it with some friendly clients. "There were immediately a lot of threats we could visualize very easily," says Morin. "Starlight has made things better for our analysts by making them more efficient at spotting real threats. It is far more paranoid and advanced than most traditional SIEM vendor solutions. Getting all the data through the analytical engines in the cloud happens a lot faster compared to other products."



Another advantage is Starlight's multi-tiered security approach. "The App Store and its security apps are very impressive," says Morin. "With the number of apps and the layered engines, the platform is very accurate, and it's an approach that works very well for us."

In addition, Stellar Cyber's security dashboard presents all relevant security information on one screen, so it makes analysts more efficient. "The dashboard enables highly engaging customer demos," says Morin. "A lot of our clients aren't really educated in cybersecurity, and the dashboard looks really cool while adding immediate value."

Stellar Cyber was also much more responsive than other vendors with whom Morin had worked. "We were evolving our service as Stellar Cyber was evolving its product, and their ability to listen and respond with new features was outstanding," says Morin. "They were very responsive and fast, and that's what I need in a partner."

Currently, CyFlare is serving over 50 active customers with the Starlight solution, and expects that to accelerate to over 100 within the next three months. In addition, CyFlare plans to integrate the data from Starlight into its security orchestration, automation and response (SOAR) platform so it can produce metrics that prove Starlight's effectiveness to non-technical managers such as boards of directors.

For this SOC-as-a-service wholesaler, Starlight proved to be the ideal platform for offering services to its MSP and MSSP customers.