inSOC

inSOC Brings Enterprise-level Solution to the MSP Market with Stellar Cyber Open XDR NIST 800 Cybersecurity Framework-based Toolset

AI-Driven Technology Exposes the XDR Killchain: Combines All Key Security Technologies Under A Single Pane of Glass with 24/7 SOC Wraproundto Give MSPS A Major Productivity Boost

inSOC provides a security operations center (SOC) as a service to Manged Security Providers (MSPs) and Managed Security Service Providers (MSSPs). inSOC is based in Los Angeles, with international offices in London, UK and Sydney, Australia. The company relies on Stellar Cyber's Open XDR technology to underpin its offering. inSOC had initially used AT&T Cybersecurity to provide security information and event management (SIEM) functionality for its service, but the product's complexity made it difficult for the company to maintain profitability.

inSOC

> It took months to turn up a new client and tune the deployment until we were looking at real information rather than just noise," says Eric Rockwell, CEO of inSOC. "Our goal was to find the right security partner that would let us turn up a new client in less than an hour."

Before:

Alert Fatigue
Too many false positives

Cost Wasted
Manpower was spent sorting through a deluge of false threats

Limited Options
Other SIEMs didn't offer deployment on hardware

With Stellar Cyber:

Streamlined
Spot real threats

Multi-Tenancy
Makes it simple to onboard new clients

Easy to Deploy
Hardware option allows users to plug in and begin use immediately

Open XDR
Delivers comprehensive visibility and pieces complex attacks together

Consolidated Tools
Make analyst's job easier

> I liked how Stellar Cyber presented information on the dashboard, it was very clear, and it made it easy to bring our team up to speed."

> “I can dive into brute force attacks…all of this is possible because of how Stellar Cyber’s Open XDR delivers comprehensive visibility and pieces complex attacks together…”

When the inSOC team investigated alternatives, however, it mostly saw more of the same. The key problem was that other solutions presented too many false positives, didn’t offer all the needed security functions, and required laborious tuning to work properly at identifying breaches. “That’s when the team discovered the sorts of things that we weren’t getting from our current solution.”

Stellar Cyber’s thinking on everything detection and response (XDR) also stood out because unlike other products, it curates collected data and correlates what may seem like random events to discover the difference between false positive noise and real alerts. Stellar Cyber made it easy for the inSOC team to focus immediately on the most important information based on the Cyber Security framework, its policies, and the top 20 security controls from CERT. The team created a template so that all it needed to do to onboard a new client was ask some simple questions about their environment, provision a simple hardware sensor and ship it to them, and be up and running in less than an hour from the time the box was plugged into the client’s network.

Naturally, Stellar Cyber’s RBAC multi-tenant capabilities were a must for inSOC. “I wouldn’t have even considered Stellar Cyber if it didn’t have multi-tenancy,” says Jeff Gulick, CIO at inSOC. “We have to be able to onboard dozens of clients, and other solutions made it difficult or expensive to do that.”

In addition, Gulick adds, “I liked how Stellar Cyber presented information on the dashboard, it was very clear, and it made it easy to bring our team up to speed.”

Stellar Cyber also offered the option to deploy on hardware. “I liked the option to deploy with a piece of hardware,” Gulick says, “because a lot of other tools were based on virtualization, and we wanted to get out of virtualized environments. We were walking into environments with different virtualization platforms; people couldn’t configure them correctly. We’ve had a much better experience with the hardware deployments, because the client can just plug them in, and we can start working immediately.”

Open XDR Simplifies Security Analysis

To trial Stellar Cyber, the inSOC team onboarded a new client and started reviewing their activity. Stellar Cyber’s Open XDR correlation ability immediately showed that the client had unauthorized remote accesses, unauthorized remote control tools, people trying to break in through a default administrator name, and an open port in their firewall. Stellar Cyber alerted on these important threats and just as importantly, it didn’t alert on false positives.

> “If we need to pay a lot of money for a bunch of different tools, we can only compete in the enterprise space. Our mission goes well beyond that – we’re trying to bring this down to everyone – we don’t want anyone to say no because of money. Stellar Cyber makes that possible.”

“I can dive into brute force attacks – Windows logon failures, privilege escalations – all of this is possible because of how Stellar Cyber’s Open XDR delivers comprehensive visibility and pieces complex attacks together across cloud, endpoints, users and network—helping to parse through logs and what it hears on the network to create a concise report on the information,” says Gulick. “I couldn’t do that with AT&T Cybersecurity.”

The product’s native applications made it easy to consolidate the number of tools in order to make inSOC’s analysts’ jobs easier. “We wanted to spend our cybersecurity budget on the right things,” says Rockwell. “A lot of companies are spending a fortune on manpower and having elite security pros going through a bunch of mundane tasks and proving false positives. It doesn’t make sense. Why spend more money on more false positives?”

“If we need to pay a lot of money for a bunch of different tools, we can only compete in the enterprise space,” says Rockwell. “Our mission goes well beyond that – we’re trying to bring this down to everyone – we don’t want anyone to say no because of money. Stellar Cyber makes that possible.”

MEDIA CONTACT:
Kristian Wright | Kristian.Wright@in-soc.com

SALES CONTACT:
Hannah Lloyd | Hannah.Lloyd@in-soc.com

Stellar Cyber Open XDR platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering an 8X improvement in MTTD and a 20X improvement in MTTR. The company is based in Silicon Valley. For more information, visit https://stellarcyber.ai.