CASE STUDY

Financial Firm Builds a SOC for Centralized Security, Visibility and Control

In-house SOC Delivers Automated Anomaly Detection and Response Supercharging Analyst Productivity While Slashing Attack Response Times

A financial services firm based in Central United States was increasingly concerned about its ability to detect and respond to network security threats. Over the years, the firm had layered on firewalling, identity management, log aggregation, IDS, IPS, SIEM and other security tools, but as its collection of tools grew, so did the burden on its analytical staff. There were multiple security consoles to monitor, and the volume of alerts was such that the staff had difficulty differentiating between real and false threats, not to mention responding quickly to the real ones.

"My analyst teams were drowning in alerts," noted the CISO at the company. "There was simply too much information to manage and too many false positives to enable us to respond quickly. I had heard about exploits at Experian, Target and other places where it took months to detect a breach, and I didn't want to be in that position."

SELECTING STARLIGHT

As he considered possible solutions, the team realized that the firm needed a security operations center (SOC) that would consolidate information into a single pane of glass and automate data collection, threat investigation and responses to enable the analyst team to run with maximum efficiency. Stellar Cyber's Starlight stood out from the competition.

"What we saw with other solutions was the same deluge of data, the same requirement that analysts track down every alert," noted the CISO. "We didn't need another layer of complexity; we needed a new way to think regarding how our SOC would collect the right information at the right time, distill it into manageable form, separate the false alerts from the real ones, and then automatically respond to threats. Starlight looked like it could provide those features."

> "We didn't need another layer of complexity; we needed a SOC that would collect the right information at the right time, distill it into manageable form, separate the false alerts from the real ones, and then automatically respond to threats."

During a proof of concept trial, the team noticed that there were far fewer alerts coming through the dashboard. Concerned that Starlight was missing threats, the team tracked down some perceived threats that Starlight had not alerted on, and found that they were not real threats at all. Starlight's machine learning technology and its ability to correlate multiple security events helped it weed out false threats from real threats.

> "Starlight's ability to distill information from all available sources, curate it, and help us make decisions on the important data really sets it apart from other solutions."

"It's a leap of faith," noted the CISO. "You have to learn to trust the software and allow it to make decisions for you."

Starlight's InterFlow™ technology actually correlates multiple events to catch security attacks that other solutions miss. For example, a login from a trusted user in the middle of the night may not cause an alert, but that event, correlated with the user's request to exfiltrate data to a Russian domain, would cause an alert.

Starlight's global dashboard revealed the entire threat kill chain, and its automated data collection, detection, investigation and response technology made it much easier to train the analyst team because they didn't have to spend a lot of time chasing down false positives and false negatives.

"Typically, the teams had to spend a lot of time writing response procedures to counter the threats they were seeing with the old systems, but Starlight eliminates that burden," noted the CISO. "The software responds by itself, using machine learning to improve its ability to spot threats as it goes along. As a result, our security capabilities grow stronger and stronger over time."

Another advantage to Starlight is its built-in application platform, which offers more than

40 tightly-integrated security tools in a single workspace. While other products force users to consult separate consoles for each tool in use, Starlight delivers a full-featured security workbench that's available under a single pane of glass.

Starlight is also a complete solution. "It collects data from all potential threat locations, including physical and virtual assets, containers, end users and cloud platforms, so we can be sure that we have the whole picture," the CISO noted. "Starlight's ability to distill information from all available sources, curate it, and make decisions on the important data really sets it apart from other solutions."

For this financial services firm, Starlight has formed a solid foundation for the company's SOC while slashing false positives and negatives to make the security teams more productive. Starlight enables the firm's analyst team to spot and respond to threats in seconds rather than days or weeks, putting it at the forefront of security awareness and protection.