CASE STUDY

Healthcare Organization Builds a SOC for Centralized Security, Visibility and Control

Starlight connects the dots to show all real threats while cutting down false positive noise

A multi-facility healthcare organization based in the Southeast wanted to ensure the tightest security posture in light of recent well-publicized breaches of patient billing information. Between HIPAA requirements and a need to protect its patients' financial information, the organization found security to be an increasingly complex and expensive proposition until it found Starlight from Stellar Cyber.

ALERT FATIGUE

Over the years, the firm had layered on firewalling, identity management, log aggregation, IDS, IPS, SIEM and other security tools, but the growing collection of discrete tools continually increased burden on its analytical staff. There were multiple security consoles to monitor, and there were so many alerts on false positives that the team spent too much time chasing false threats – it took days or weeks to respond to the real ones.

"My analyst teams were overworked," says the CISO at the company, "and we were spending a fortune on more than a dozen discrete tools, from SIEM and IDS/IPS to log aggregation and identity management. We had to pull information from multiple consoles in order to chase down threats and produce management reports, and we wanted something simpler and more consolidated."

CHOOSING STARLIGHT

As she considered possible solutions, the CISO realized that the organization needed a security operations center (SOC) that would consolidate information from multiple threat vectors – cloud, physical and virtual assets, network and endpoints – into a single pane of glass to enable the analyst team to run with maximum efficiency. Stellar Cyber's Starlight stood out from the competition.

> "When we looked at Starlight, we saw a very clear and efficient dashboard that identified threats throughout the kill chain."

"When we looked at Starlight, we saw a very clear and efficient dashboard that identified threats throughout the kill chain," says the CISO. "We also liked the overall platform and its ability to provide dozens of tightly-integrated security applications under one umbrella at one price."

> "Typically, our teams spent a lot of time writing response procedures to counter the various threats they were seeing with the old systems, but Starlight eliminates that burden. The product learns what's important to us and presents that information within the kill chain to show our analysts exactly how to respond."

PROOF OF CONCEPT

Of course, the proof was how well it actually worked. During a proof of concept trial, the organization's security team noticed that there were far fewer alerts coming through the Starlight 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.

"Machine learning is a new frontier, but it enables the security solution to get better and better at spotting real threats," says the CISO. "Once you learn to trust the software and allow it to make decisions for you, you increase productivity dramatically."

BOOSTING ANALYST PRODUCTIVITY

Event correlation was another key attribute. Starlight's Interflow™ technology correlates multiple events to catch security attacks that other solutions miss. For example, a login from a hospital administrator 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.

"Typically, our teams spent a lot of time writing response procedures to counter the various threats they were seeing with the old systems,

but Starlight eliminates that burden," says the CISO. "The product learns what's important to us and presents that information within the kill chain to show our analysts exactly how to respond."

Starlight is also a complete solution. "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," says the CISO.

Multi-tenancy was another advantage. "We have over two dozen clinics and hospitals, and it's very important to be able to separate them into discrete units so we can capture the overall security posture and compare one site with another," the CISO added.

For this healthcare organization, Starlight has replaced more than a dozen discrete security tools while presenting threat information in a clear, easy-to-use interface. Analysts are more productive, the organization spends far less time training its team, and analysts can respond to real threats far more quickly. 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.