CASE STUDY

# Public Agency Centralizes Security with a New Security Operations Center

## Starlight-based SOC delivers visibility and control across the entire kill chain

A state government agency based in the Northeast wanted to ensure the tightest security posture in light of recent cyber-ransom attacks on cities, but it needed a security operations center (SOC) that would consolidate multiple applications and respond automatically to threats. Stellar Cyber's Starlight formed the basis of a new SOC that delivers comprehensive security while supercharging analyst productivity.

### COLLECTING THE WRONG INFORMATION

Over the years, the agency 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 most of its time chasing false threats – it took days or weeks to respond to the real ones.

"We couldn't respond quickly enough because we were getting inundated with useless information," says the agency's CISO. "We were spending a fortune on discrete security applications, from SIEM and IDS/IPS to log aggregation and identity management, yet we still weren't getting the information we needed to respond quickly to threats."

> "Starlight's dashboard shows us the right information at the right time," says the CISO. "The platform gives us access to dozens of tightly-integrated security applications under one interface at one price, so we can drill down on alerts in many different ways."

### THE STARLIGHT SOLUTION

As he considered possible solutions, the CISO realized that the agency 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. The SOC also needed to provide access to all of the security applications the agency needed. Stellar Cyber's Starlight stood out from the competition.

> "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."

"Starlight's dashboard shows us the right information at the right time," says the CISO. "The security platform gives us access to dozens of tightly-integrated security applications under one interface at one price, so we can drill down on alerts in many different ways."

Starlight is also comprehensive – it collects useful data from network, endpoint, cloud, container and virtualized attack vectors so analysts can see the whole picture throughout the kill chain, and it is smart enough to dismiss false positives so analysts can focus on the real threats.

Moreover, Starlight leverages machine learning technology to actually improve its detection and response capabilities over time. "The machine learning aspect of the product enables us to get better and better at responding to threats as we go along," says the CISO.

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 an 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."

Multi-tenancy was another advantage. "We have over two dozen departments, 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 department with another," the CISO added.

## REAL-WORLD RESULTS

Of course, the proof was how well it actually worked. During a proof of concept trial, the agency'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, seemly random security events helped it weed out false threats from real threats.

For this public agency, Starlight has built a SOC that replaces more than a dozen discrete security tools while identifying real threats in a clear, easy-to-use interface. Analysts are more productive, the agency spends far less time training its team, and analysts can respond to real threats far more quickly (in seconds rather than days or weeks), keeping the agency protected against cyber-ransom attacks.