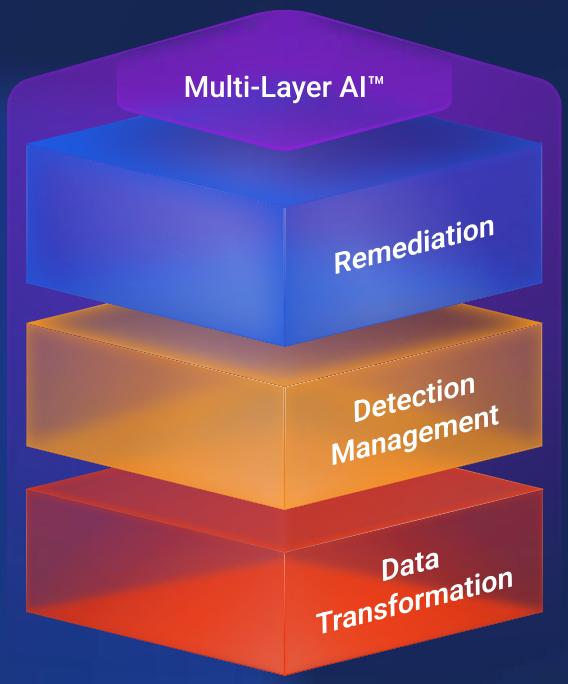
STELLAR CYBER®



Case Study

Financial Firm Builds Open and Unifying AI-Native SecOps Platform Powered SOC for Correlating Alerts Across the Entire Attack Surface

Stellar Cyber's AI-Native SecOps Platform Delivers Automated Anomaly Detection and Response, Supercharging Analyst Productivity While Slashing Attack Response Times

Overview

A financial services firm based in the 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, endpoint detection, 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 other partner organizations like Experian, Target and other places where it took months to detect a breach, and I didn't want to be in that position."

Before

Alert Fatigue

Time wasted chasing false threats

Time Wasted

Teams spent time writing response procedures

Multi-Interface

Forced users to consult separate consoles for each tool in use

With Stellar Cyber

Comprehensive Dashboard

Alert correlation from a single console

Efficient

Save time training analysts

Multi-Layer AI™

Improve detection, response and triage capabilities through machine learning, LLMs and Agentic AI

Integrated

NDR / OT, ITDR / UEBA, NG SIEM, automatic triage and Open XDR – accessible through a single platform.

Selecting Stellar Cyber's AI-native SecOps platform

As he considered possible solutions, the team realized that the firm needed a solution that would consolidate information into a single pane of glass and automate data collection, threat-hunting and responses to enable the analyst team to run with maximum efficiency. Stellar Cyber's next-generation security operations platform stood out from the competition.

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

> …we needed a new way to think regarding how our system would collect the right information at the right time, distill it into manageable form, separate the alerts from the real incidents telling us a bigger breach is underway, and then automatically respond to them. The Stellar Cyber open and unifying SecOps platform looked like it could provide those features.

Leveraging Multi-Layer™

Stellar Cyber's integrated AI technology correlates multiple types of alerts and data automatically. Logs, endpoint data, network traffic are all integrated into a case management framework, catching 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 incident, correlated with the user's request to exfiltrate data to a Russian domain, would cause an alert.

The unifying capability's case-management 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 Stellar Cyber eliminates that burden," noted the CISO. "The software responds by itself, using Multi-Layer AI 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 the Stellar Cyber platform is that it integrates core security capabilities – NDR and NG SIEM, for example – in a single platform and the ability to use any endpoint vendor. While other products force users to consult separate consoles for each tool in use, Stellar Cyber delivers a full-featured security workbench that's available under an actionable dashboard.

Building on Success

Stellar Cyber also integrates and interprets data from popular third-party security tools (i.e., EDR, firewalls, etc.) so it is 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. “The platform’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, Stellar Cyber has formed a solid foundation for the company’s next-generation security infrastructure while slashing false positives and negatives to make the security teams more productive. The teams’ mean time to detect (MTTD) threats has dropped by a factor of 8, while its mean time to respond to attacks has decreased by a factor of 20.

Stellar Cyber 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.

About Stellar Cyber

Stellar Cyber's open and unifying SecOps platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments.

With Stellar Cyber, organizations move from manual, alert-driven operations to a human-augmented autonomous SOC that identifies, validates, and responds to risk with speed and precision. Customers reduce false positives by more than 80%, improve analyst productivity, and lower operational costs—while retaining existing security investments and gaining measurable improvements in risk reduction and response consistency. The company is based in Silicon Valley.

stellarcyber.ai
sales@stellarcyber.ai

STELLAR CYBER®