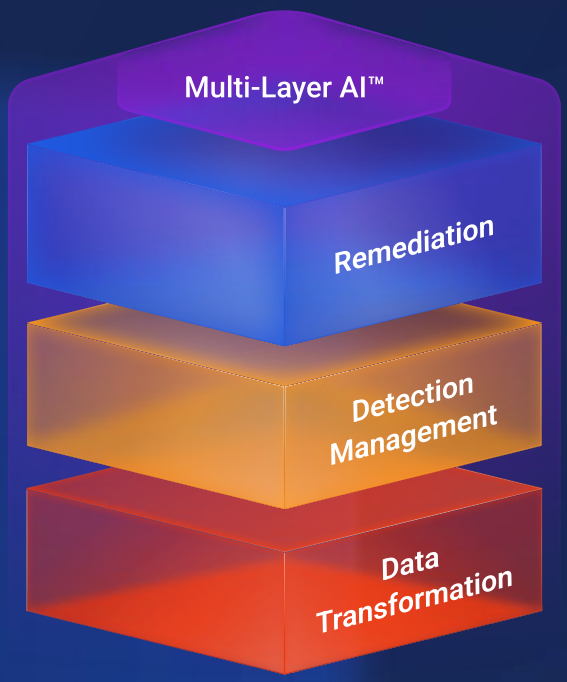
STELLAR CYBER®



Case Study

SECURICENTRIX

SecuriCentrix Selects an Open and Unifying SecOps Platform to Power Their Security Offerings

SecuriCentrix provides independent information security and compliance services worldwide. With a team experienced in information security and compliance, SecuriCentrix helps organizations mitigate risk and maintain compliance with major industry regulations.

They selected the open and unifying SecOps platform to evolve their offerings based on its flexibility, breadth of integrations, and ease of use.

> The open and unifying SecOps platform's multi-mode approach to detecting threats means we get fewer false positives while identifying more potential threats without spending time configuring rules. When I saw the open and unifying SecOps platform, I knew this was the solution we need to meet our customers' demands today and in the future.

– David Steele, Managing Director, SecuriCentrix

Before

Wasted Time

Analysts spent significant time on tasks that made the existing security platforms work as required.

Manual

Threat identification relied on expert personnel skills and experience.

Learning Curve

Bringing new analysts aboard took a long time, as learning how to use and manage the prior SIEM products required a lot of work.

With the Open and Unifying SecOps Platform

Efficiency Gains

The unified platform provides comprehensive capabilities required to identify threats as part of the solution, eliminating wasted analyst time.

Automation

The platform's automation of repetitive, time-consuming tasks lets analysts focus on what they do best — investigate threats.

Intuitive

The solution's ease of use means you do not need to be a security expert to work with the platform effectively.

Security Operations After Stellar Cyber

SecuriCentrix was founded in 2010 to provide pragmatic "value add" compliance and cybersecurity services. They are the trusted security partner for organizations across Africa, Australia, Europe, India, and the UK. In its early years, SecuriCentrix focused on PCI DSS compliance. Today, however, they have evolved their portfolio of cybersecurity offerings based on client needs.

To continue the evolution of their business, SecuriCentrix knew they wanted to upgrade their security operations platform and began a broad investigation into available options. Frustrated with what they were using, SecuriCentrix sought a platform that:

- **Delivered comprehensive threat coverage out of the box**
- **Eliminated many manual processes and tasks**
- **Was simple enough for anyone in the SOC to participate in**

> Before the open and unifying SecOps platform, my team spent too much time on manual tasks such as correlation and rule management. So I knew we needed a new solution, which turned out to be the open and unifying SecOps platform.

First, the unified platform automatically normalizes and enriches data from every sensor and security tool used by SecuriCentrix upon ingestion. Then, **Multi-Layer AI™** engines automatically evaluate and group related alerts and identify new threats based on abnormal user and asset behaviors, producing a **prioritized list of contextual incidents** on the platform's intuitive dashboard.

Based on discussions and live demonstrations, SecuriCentrix selected the platform as the new hub of its security operation activities. Going forward, the **open and unifying SecOps platform** is the central hub, saving analysts significant time and effort. Now, after deploying the platform, SecuriCentrix is realizing benefits every day. The automated approach embedded in the platform enables SecuriCentrix to bring on new customers confidently, knowing that integrating the customer's security products into the platform is fast and easy.

How the Platform Works

The **open and unifying SecOps platform automatically normalizes and enriches data** from every sensor and security tool upon ingestion. Then, **Multi-Layer AI™** engines **automatically evaluate and group related alerts and identify new threats** based on abnormal user and asset behaviors, producing a **prioritized list of contextual incidents** on the platform's intuitive dashboard. Navigating incident context and timelines helps analysts efficiently detect, investigate, and respond.

The Results

The platform's practicality and adaptability enabled SecuriCentrix to react quickly during crises. For example, when a government agency notified a SecuriCentrix client that file signatures related to ransomware were detected in their environment, SecuriCentrix took decisive action. The team rapidly deployed platform sensors in the client's environment to begin data ingestion and signature review. This response allowed the client and SecuriCentrix's SOC to see the environment within a matter of hours.

SecuriCentrix plans to continue growing its security service offerings, taking advantage of the hundreds of pre-built integrations now available. This approach empowers the SOC to provide effective and timely 24×7 monitored detection and response services.

> **"After integration with the client's major data sources, we narrowed down the infected servers and endpoints to have them remediated and identify the root cause of the infection. The open and unifying SecOps platform made this swift response possible."**
>
> – Mike Saylor, CEO, Blackswan Cybersecurity

The platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill level to secure their environments successfully. With the platform, organizations reduce risk through early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity — delivering an 8× improvement in mean time to detect (MTTD) and a 20× improvement in mean time to remediate (MTTR).

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 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.

stellarcyber.ai sales@stellarcyber.ai

STELLAR CYBER®