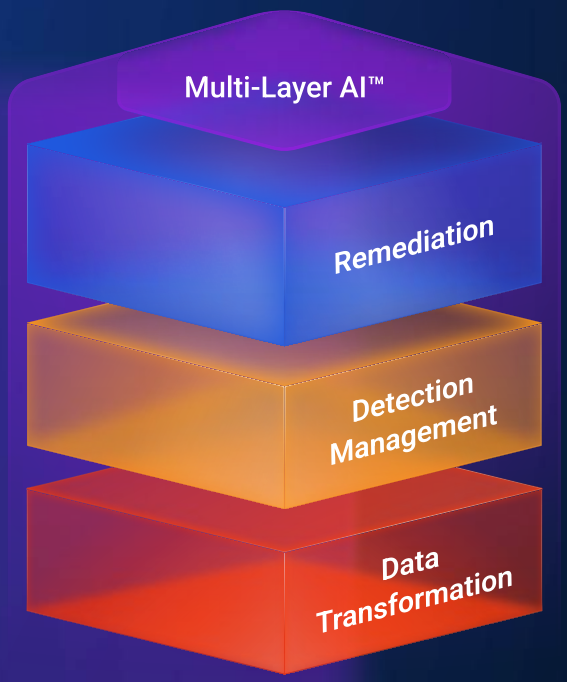
STELLAR CYBER®



Case Study

Large American City Government Strengthens Security with Stellar Cyber

Empowering a Lean Security Team with Unified Visibility and Automation

A major U.S. city with a population of over 650,000 needed to advance its cybersecurity posture while maintaining a lean IT team and tight budget. Relying on firewalls and a SIEM left the city exposed to complex, multi-vector attacks. The city's security leaders sought a more effective way to monitor, detect, and respond to threats while empowering a small team to operate at enterprise scale. After evaluating options, the city selected **Stellar Cyber's open and unifying SecOps platform** to unify telemetry and strengthen its security operations.

Before

Vulnerable Threat Posture

Relied on firewalls and siloed tools that left exposure to sophisticated attacks.

Fragmented Toolset

Analysts used separate tools, so no one had a full picture.

Manual, Slow Investigation

Analysts manually correlated alerts and investigated in isolation.

Understaffed Team

The team needed more analysts just to keep up.

Time-Consuming Response

Similar incidents took days or weeks to investigate.

With Stellar Cyber

Comprehensive Visibility

Unified telemetry from all security sources across the environment enables clear, complete visibility.

Single Operational View

Integrated, correlated incidents show full attack context in one place.

Automatic Triage & Prioritization

Multi-Layer AI™ automatically groups related activity into prioritized incidents.

Human-Augmented Autonomous SOC

Automation accelerates investigation and response, reducing analyst load.

Faster, Confident Response

Analysts can resolve incidents in minutes, not days, with full context.

Life Before Stellar Cyber

When the city's Director of Security first joined, he inherited a SIEM and firewall-centric security stack that offered only surface-level protection. Analysts specialized in individual tools, resulting in skill silos and no comprehensive view of the environment. Threat detection and blocking processes remained complicated and slow. The team faced pressures to hire more analysts or find automation that would reduce manual work, especially as threats grew more sophisticated.

Why the City Chose Stellar Cyber

During evaluation, the city needed a platform that worked with the tools already in place—not one that required ripping and replacing. Stellar Cyber's **open and unifying SecOps platform** met that need by integrating data from the city's existing security tools and sensors.

With **Multi-Layer AI™**, the platform automatically ingests, enriches, and correlates diverse telemetry into contextual incidents, then prioritizes what matters most. This reduced alert noise and gave analysts actionable insights without requiring deep expertise in multiple separate tools.

Stellar Cyber's approach met the city where it was, preserving existing investments and accelerating time to value.

Security Operations After Stellar Cyber

Once deployed, the platform delivered unified visibility across east-west and north-south traffic and presented incidents in a single timeline. Analysts could easily see where an attack started, how it evolved, and where to respond—without manually stitching together logs or pivoting between consoles.

Automatic triage and prioritization freed analysts from repetitive chores, allowing the team to focus on real threats with confidence. What previously took hours or days now took minutes. The intuitive interface empowered analysts of all skill levels to investigate effectively, reducing the dependency on highly specialized personnel.

Multi-Layer AI™ grouped related activity automatically, turning disparate alerts into **high-confidence incidents** that analysts could act on immediately, supporting a practical **human-augmented autonomous SOC** strategy.

Outcome

The city significantly improved its security posture while staying under budget and retaining a lean security team. Analysts now resolve incidents efficiently and proactively, supported by unified visibility and automatic triage. The platform continues to help the city:

- ☑ See the full attack picture across all telemetry sources
- ☑ Know where threats originate and how they progress
- ☑ Act faster with confidence, reducing mean time to investigate and respond

> **“The visibility we get into our environment is outstanding. We can triage from a generated incident to the source of what caused it, and automation saves us a lot of time.”**
>
> – Deputy CIO, Large American City Government

> **“One analyst can now get to the bottom of an incident within five to ten minutes versus days or weeks before. It’s been a game-changer, letting us keep our budget under control.”**
>
> – Deputy CIO, Large American City Government

By adopting Stellar Cyber’s open and unifying SecOps platform, the city achieved powerful, consistent security outcomes while preserving existing tool investments and empowering analysts to see more, know more, and act faster.

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®