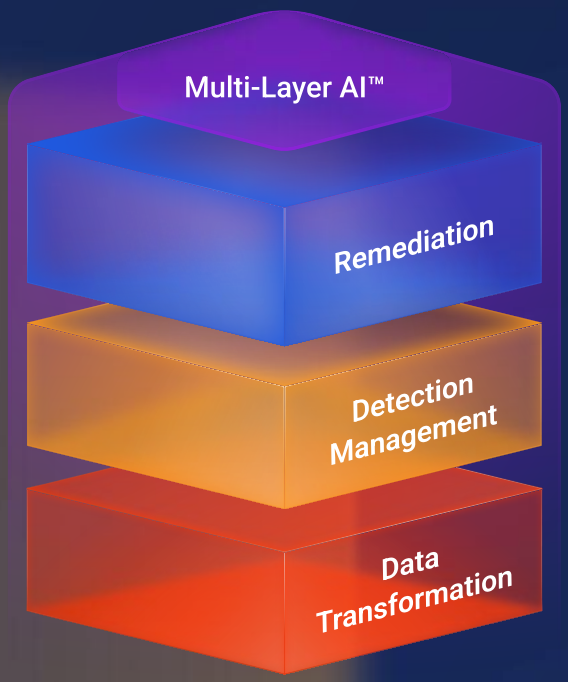
STELLAR CYBER®



Case Study

Public Agency Centralizes Security Operations with Stellar Cyber

Delivering Unified Visibility and Faster Response for a Distributed Government Organization

A regional public agency with multiple departments needed to modernize its security operations. With disparate systems and tools across divisions, the agency lacked unified visibility into threats and relied on manual processes that slowed investigations and increased risk. To bring efficiency and clarity to its security operations, the agency chose **Stellar Cyber's open and unifying SecOps platform.**

The agency's goals were to unify disparate security tools, reduce manual correlation, improve detection confidence, and accelerate response times. After deployment, the agency centralized visibility from all sources, reduced noise, and empowered its team to act with confidence.

Before

Fragmented Visibility

Security tools operated in silos with no centralized view of activity.

Manual Correlation

Analysts manually correlated alerts across systems, slowing response.

Slow Response

Investigations took too long due to disconnected tools and manual workflows.

Inconsistent Outcomes

Disparate systems produced inconsistent insights and coverage.

Underutilized Tools

Existing investments delivered limited value without integration.

With Stellar Cyber

Unified Security Operations

Centralized visibility across all telemetry sources provides a single operational view.

Automatic Triage & Prioritization

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

Faster Threat Response

Analysts now work from a unified incident queue with full context, reducing response times.

Consistent Security Outcomes

Shared context and automation ensure reliable detection and response across departments.

Maximized ROI from Existing Tools

Stellar Cyber works with existing tools, preserving investments while enhancing effectiveness.

Recognizing the MSP Security Visibility Gap

Before Stellar Cyber, the agency's security team depended on multiple point tools that operated independently. Analysts spent significant time manually collecting logs and piecing together activity from different systems, making it difficult to identify real threats in a timely way. This created inefficiencies, slowed incident response, and left security gaps that increased organizational risk.

Without a centralized platform, the team lacked the context needed to connect events across systems, often initiating investigations only after incidents had already escalated.

Why the Agency Chose Stellar Cyber

The agency evaluated several options, but it needed a solution that:

- **Centralized telemetry across tools**
- **Reduced manual effort required for investigation**
- **Preserved investments in existing security products**
- **Accelerated detection and response**

Stellar Cyber's **open and unifying SecOps platform** met those criteria. It integrates with the agency's existing security tools, automatically ingests and enriches telemetry, and uses **Multi-Layer AI™** to correlate related signals into meaningful, actionable incidents. Instead of forcing a rip-and-replace approach, Stellar Cyber met the agency where it was—preserving existing investments while improving outcomes.

By implementing the platform, the agency eliminated fragmented workflows and reduced the overhead required to manage and interpret disparate logs and alerts.

Security Operations After Stellar Cyber

Once deployed, the platform unified visibility into a central operational console, enabling analysts to see the full attack picture and understand threat progression. **Automatic triage** reduced alert noise, freeing analysts to focus on real threats instead of manual correlation. Analysts now work from a prioritized incident queue with contextual insights that accelerate investigation and response.

Stellar Cyber's **Multi-Layer AI™** groups related activity into high-confidence incidents and displays them in a single timeline, eliminating the need to pivot between tools. This shift supports a **human-augmented autonomous SOC** model—where automation handles routine triage and prioritization, and human expertise drives strategic response.

Outcome

The public agency achieved significant improvements in how it detects and responds to threats:

- Gained centralized, consistent visibility across all divisions
- Reduced manual effort in incident correlation
- Increased analyst productivity and confidence
- Improved consistency and quality of security outcomes
- Preserved ROI from existing security tools by unifying them into one operational platform

The agency now operates efficiently with clearer security insights and accelerated response capabilities, empowering its team to prioritize critical threats without being overwhelmed by noise.

> **Stellar Cyber's platform brought clarity and speed to our operations. We can now see threats across the entire organization, respond quickly, and trust the insights we receive.**
>
> **— Security Operations Lead, Public Agency**

By choosing Stellar Cyber, the agency centralized its security operations, improved decision-making, and aligned its SOC goals with broader organizational risk management—all while preserving existing tools and investments.

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®