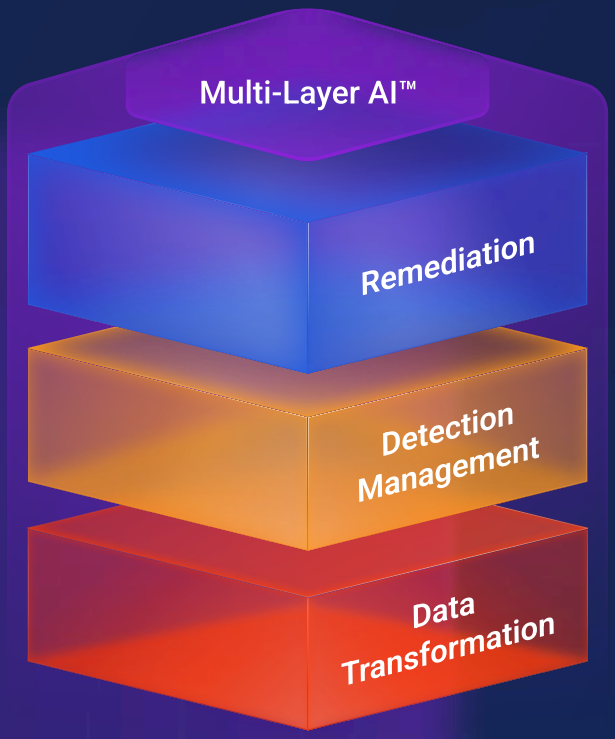
STELLAR CYBER®



Case Study

K-12 School District **Strengthens Security Visibility and Response** with Stellar Cyber

A public school district in the western United States, serving over **20 schools, 2,000 staff, and 20,000 students daily,** needed better ability to detect and respond to threats across its diverse technology environment.

With a lean security team, the district recognized that existing tools and open-source technologies left **gaps in visibility and response capability.**

After a comprehensive evaluation, the district selected **Stellar Cyber's open and unifying SecOps platform** to reduce manual processes, eliminate security gaps, and improve threat detection and response._

Life Before Stellar Cyber

Before deployment, the district's security team handled logs and alerts largely through manual processes, making it difficult to identify patterns or respond quickly.

Analysts searched open-source systems such as ELK stack for anomalies, but the approach lacked context, consumed valuable time, and left gaps in visibility.

Before

Manual Effort

Daily operations depended on analysts searching for anomalies with open-source tools.

Visibility Gaps

Deployed security products left blind spots across users, devices, and assets.

Fragmented Detection

Analysts manually correlated alerts that lacked context.

Response Delays

Threat identification relied on manual effort and expert knowledge.

Tool Silos

Security data lived in disparate systems without unified investigation capabilities.

With Stellar Cyber

Automation & Automatic Triage

Multi-Layer AI™ automatically ingests, normalizes, and analyzes data, eliminating manual processes and prioritizing incidents.

Unified Insights

Stellar Cyber provides clear visibility across the full environment, eliminating critical gaps.

Contextual Incident Correlation

Multi-Layer AI™ correlates related signals into meaningful incidents, enabling faster, confident response.

Accelerated Threat Response

Prioritized incidents allow analysts to act promptly and reduce mean time to respond.

Connected Ecosystem

Stellar Cyber integrates visibility from all sources and works with existing tools at no added cost.

Why the School District Chose Stellar Cyber

The district needed a solution that would integrate with existing security tooling—without forcing expensive replacements—and simplify security operations.

Stellar Cyber's open and unifying SecOps platform met these requirements by:

Automatically ingesting and analyzing data

Using Multi-Layer AI™ to normalize and enrich telemetry

Providing prioritized, contextual incidents

Delivering intuitive workflows

During the proof of concept, the district immediately recognized how much more quickly they could identify and remediate threats with automated visibility and correlation.

With Stellar Cyber, the district now automatically ingests and analyzes security data across users and devices, eliminating the need for manual log parsing. Multi-Layer AI™ correlates independent alerts into prioritized, contextual incidents, allowing analysts to respond faster and with more confidence than before.

Analysts now work from a centralized incident workflow that guides investigation and action. This lets the team deliver consistent security outcomes across all campuses and systems.

Outcome

Today, the school district has a clear line of sight into its security environment, with automation that saves time and increases accuracy. Analysts use integrated contextual incidents to respond faster, reducing risk and improving overall security posture—without adding staff or replacing existing tools.

The district now operates a practical human-augmented autonomous SOC where automation and expert judgment work together to defend against threats.

By transitioning to Stellar Cyber's open and unifying SecOps platform, the school district eliminated manual security overhead, closed visibility gaps, and now detects and responds to threats with speed and context. This real-world application of Multi-Layer AI™ and automation demonstrates how even lean security teams can achieve powerful, consistent security outcomes.

> **Using Stellar Cyber and its automated detection, we can efficiently monitor activity from all our users. The threat intelligence has helped us fix gaps in our security posture that we weren't even aware of.**

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®