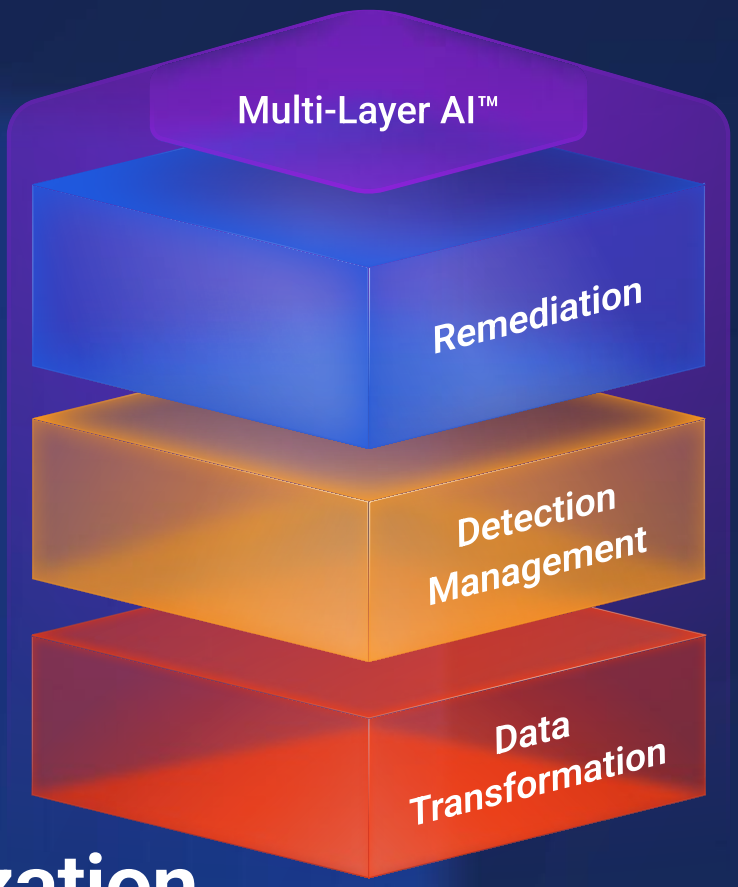
STELLAR CYBER®



Case Study

Healthcare Organization Enhances Security Operations with Stellar Cyber

A mid-sized healthcare organization faced growing risk from ransomware, impersonation, and credential abuse, but lacked unified visibility across endpoints, network, cloud, and identity systems. Limited staffing further constrained the security team's ability to scale detection and response as threats grew more sophisticated.

To strengthen its security operations without replacing existing tools, the organization selected Stellar Cyber's open and unifying SecOps platform to consolidate telemetry, automate investigation, improve prioritization, and elevate analyst efficiency.

Life Before Stellar Cyber

Before Stellar Cyber, the healthcare organization depended on multiple point products that generated noisy alerts with little context. Manually reviewing and correlating events across consoles wasted time and slowed incident investigation and response.

The team lacked consolidated visibility into critical attack vectors, including cloud activities and identity-based threats, making it difficult to detect lateral movement or credential compromise before they escalated.

Without an integrated platform, manual processes consumed precious hours, and lean staff struggled to keep up with daily security demands.

Before

Fragmented Toolset

Security tools produced isolated alerts, requiring manual correlation across consoles.

Alert Overload

High alert volume overwhelmed analysts, slowing response.

Manual Investigations

Analysts manually pieced together events from different tools.

Limited Visibility

The team lacked insight into cloud and identity behavior.

Resource Constraints

Lean security operations struggled to scale.

With Stellar Cyber

Unified Operational View

Stellar Cyber integrates telemetry from all tools, giving analysts coherent, contextual insight.

Automatic Triage & Prioritization

Multi-Layer AI™ automatically groups related signals into actionable incidents.

Faster, Confidence-Driven Response

Automated correlation and context reduce time from detection to resolution.

Full Stack Visibility

Stellar Cyber reveals cross-domain activity with correlated incidents and timelines.

Human-Augmented Autonomous SOC

Automation supports elevated productivity across the team.

Why the Organization Chose Stellar Cyber

The IT team needed a solution that would:

- **Integrate with existing tools** without forcing replacement
- **Provide unified visibility** across endpoint, network, cloud, and identity sources
- **Prioritize correlated activity** so analysts focus on real threats
- **Accelerate detection and response** with automation

Stellar Cyber's open and unifying SecOps platform met those requirements by ingesting diverse telemetry sources, normalizing them into a common context, and applying Multi-Layer AI™ to automatically triage alerts into high-confidence incidents. This approach preserved the value of existing security investments while giving the team the visibility and efficiency required to improve outcomes.

> Stellar Cyber brought clarity and speed to our security operations. Having one platform that ties everything together has been transformational

Security Operations After Stellar Cyber

Once deployed, the platform delivered consolidated incident views and prioritized workflows. Analysts now work from a unified incident queue that presents correlated events with clear context and a defined investigation path.

Automatic triage reduces noise and surfaces meaningful threats early in the attack lifecycle. Instead of manually pivoting between systems, analysts now inspect full incident timelines that cross endpoint, network, cloud, and identity behavior.

This shift supports a human-augmented autonomous SOC, where automation handles repetitive triage and enrichment, and human expertise focuses on strategic investigation and response.

Outcome

The healthcare organization saw measurable improvements in detection, response, and operational efficiency:

Reduced alert noise
allowing analysts to focus on actionable incidents

Faster investigation and response
reducing time spent on each incident

Enhanced visibility across the full attack surface,
including cloud and identity

Improved cross-team collaboration
with shared, contextual incident views

By unifying telemetry and correlating events automatically, the organization gained confidence in its security operations and strengthened its ability to stay ahead of threats, even with limited staff.

With Stellar Cyber's open and unifying SecOps platform, the healthcare organization now sees more, knows more, acts faster—and does so while maximizing the value of existing tools and optimizing team productivity.

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®