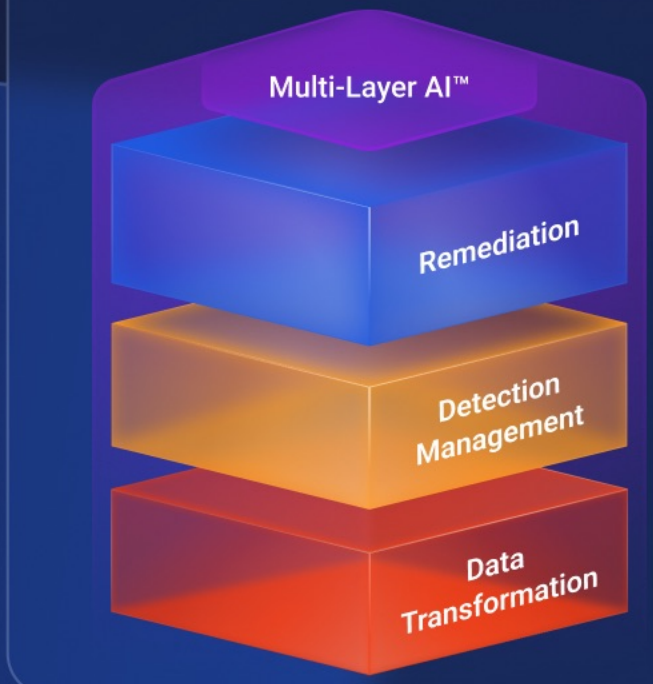
STELLAR CYBER®



Case Study

Large Midwestern University Boosts Threat Visibility and Security Posture with Stellar Cyber

Empowering a Lean Higher-Ed Security Team to See More, Act Faster

Overview

A prominent university recognized that its IT and security team needed stronger visibility across all faculty, staff, and student activity to better detect and mitigate threats. With existing tools providing logs but not actionable context, the team needed a modern solution that could integrate with their environment, reduce manual effort, and speed response times.

After evaluating options, the university selected **Stellar Cyber's open and unifying SecOps platform** because it met key requirements: simplicity of use, integration with existing tools, intuitive dashboards, and the visibility they were missing. Within minutes of starting a proof of concept, they saw how the platform would transform their operations.

Before

Limited Visibility

Threat visibility was near impossible; logs lacked context, leaving blind spots across critical assets and user activity.

Manual Investigation

Analysts manually reviewed logs without automation, slowing investigation and increasing risk.

Resource Boundaries

Expert personnel bore the burden of threat hunting, limiting team capacity.

Reactive Posture

Without proactive insight, security teams continuously reacted to threats.

Disconnected Tools

Existing sensor data sat in silos with little interoperability.

With Stellar Cyber

Unified Visibility

Stellar Cyber provides holistic insight across the environment so the team can identify and mitigate critical threats fast.

Automatic Triage & Actionable Incidents

Multi-Layer AI™ automatically triages alerts, correlates related activity, and presents prioritized incidents in a central queue.

Efficiency Gains for Teams of All Skill Levels

Teams now work directly from the incident queue, accelerating response and enabling less experienced personnel to contribute.

Proactive Security

Multi-Layer AI™ combines context and automation so analysts see the full story and act before escalation.

Connected Ecosystem

Stellar Cyber normalizes and enriches data from all tools, preserving existing investments and enhancing ROI.

Life Before Stellar Cyber

Before deployment, the university team could collect logs, but that data didn't provide the visibility needed to understand risk or stop threats effectively. Near impossible visibility forced the team to react rather than anticipate attacks. Analysts manually reviewed disparate logs and struggled to correlate activity across systems, limiting their ability to confidently secure the environment.

Why the University Chose Stellar Cyber

The team looked for a solution that could be integrated quickly, used without heavy customization, and produce results without overwhelming staff with data.

Stellar Cyber's open and unifying SecOps platform stood out because it:

- **Integrated with existing logs and sensors without ripping out tools**
- Used **Multi-Layer AI™** to automatically normalize, enrich, and correlate data
- Reduced analyst burden through automatic triage and prioritization
- Delivered an intuitive dashboard that anyone on the IT team could operate

From the moment the proof of concept began, the university saw results without management overhead common to other products.

> **The platform quickly became our central security management point because it delivered results without burying us in data.**
>
> — Anonymous University Information Security Architect

Security Operations After Stellar Cyber

With Stellar Cyber deployed, the university gained the visibility and operational efficiency it had been missing.

The platform now provides immediate, actionable insight across all telemetry by automatically evaluating and grouping related alerts into high-value incidents. Analysts no longer shift between consoles; instead, they view the entire attack lifecycle in one place and respond faster and more consistently.

Stellar Cyber's automatic triage and prioritization mean the team spends less time on noise and more time on action. Staff of all skill levels now participate in security operations confidently, supported by contextualized incident data.

Outcome

After completing the proof of concept, the university moved directly into full production. They now deliver consistent security outcomes across their entire environment—logging, threat detection, investigation, and prioritized response—without adding staff or replacing core tools.

The platform's ease of use enabled the university to drastically improve metrics such as **mean time to detect (MTTD)** and **mean time to respond (MTTR)**, turning previously siloed data into unified operational insight.

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®