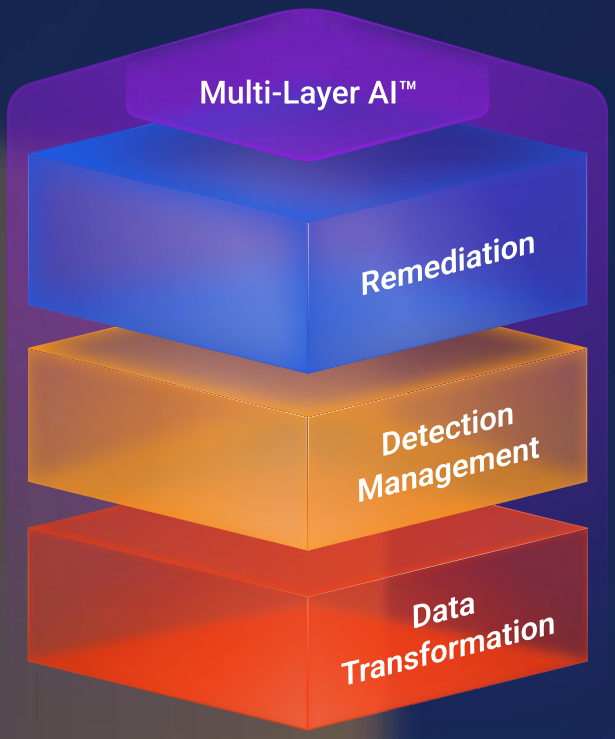
STELLAR CYBER®



Case Study

University of Zurich Strengthens Security Visibility and Incident Response with Stellar Cyber

The University of Zurich serves multiple campuses of students, faculty, and researchers. With a diverse IT environment, including research systems, administrative networks, and cloud services, the university's security team needed to centralize visibility, improve detection, and accelerate response across disciplines and technologies.

Traditional toolsets left gaps in visibility and produced high volumes of low-value alerts, forcing analysts into manual work. To address these challenges, the university selected **Stellar Cyber's open and unifying SecOps platform** to unify telemetry, automate triage, and elevate the effectiveness of its lean security team.

Life Before Stellar Cyber

Before deployment, the university's security team needed to manually correlate alerts across multiple consoles. A lack of a centralized view of activity across endpoints, cloud systems, and research networks lead to delayed detection and inconsistent response.

This compromised the team's ability to support dynamic research environments that face increasingly sophisticated threats. Manual investigation workflows slowed the identification of critical incidents, forcing staff to spend time on repetitive triage rather than strategic defense.

Before

Fragmented Security Tools

Teams used multiple tools that lacked interoperability and centralized context.

Manual Alert Overload

High volumes of alerts required analysts to manually review and correlate findings.

Slow Incident Response

Investigations dragged on due to disconnected systems and manual workflows.

Visibility Gaps

Tools lacked the ability to connect behaviors across cloud, endpoint, and network.

Resource Strain

Lean team struggled to keep pace with risks and alerts.

With Stellar Cyber

Unified Operational View

Stellar Cyber synthesizes telemetry into one console, eliminating silos and clarifying threat visibility.

Automatic Triage & Prioritization

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

Accelerated Investigations

Analysts now work from a single incident queue with full context and prioritized actions.

Full-Stack Visibility

Stellar Cyber reveals cross-domain activity, enabling earlier detection and response.

Empowered SOC Team

Automation increases capacity and supports a human-augmented autonomous SOC.

Why the University Chose Stellar Cyber

The university required a solution that would unify data from existing tools and deliver actionable insights without forcing wholesale replacement of established investments.

Stellar Cyber's open and unifying SecOps platform met that need by:

- Automatically ingesting and normalizing telemetry from firewalls, endpoints, identity systems, and cloud sources
- Using **Multi-Layer AI™** to automatically triage alerts into contextual incidents
- Prioritizing threats to focus analysts on what matters most sooner
- Preserving existing investments while delivering unified operations

By choosing a platform that met them where they were, the university avoided tooling disruption and accelerated time to value.

With Stellar Cyber fully deployed, the university now operates from a centralized incident queue where correlated activity appears in an integrated timeline. Analysts no longer juggle disparate alerts but instead view unified incidents with full context.

Automatic triage and incident prioritization reduce noise and let the team focus on real threats. Analysts of all levels can participate in enriched investigations, which supports a more modern, efficient security posture rooted in true visibility and automation.

With automation and human expertise, the university now sees the strategic benefits of a human-augmented autonomous SOC, where human insight directs strategic decisions and Multi-Layer AI™ accelerates routine triage and response.

Outcome

The university's analysts now detect threats earlier by linking activity across endpoints, network, and cloud data, and manual effort in investigation and correlation dropped significantly. Incident investigations now proceed with confidence because correlated incidents reveal real risk context.

By unifying diversified telemetry into one operational platform and applying Multi-Layer AI™, the university now sees more, knows more, and acts faster—without adding tools or additional personnel.

> **Stellar Cyber finally lets us see the connections between events that used to be invisible to us. We now respond earlier and with greater confidence.**

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®