



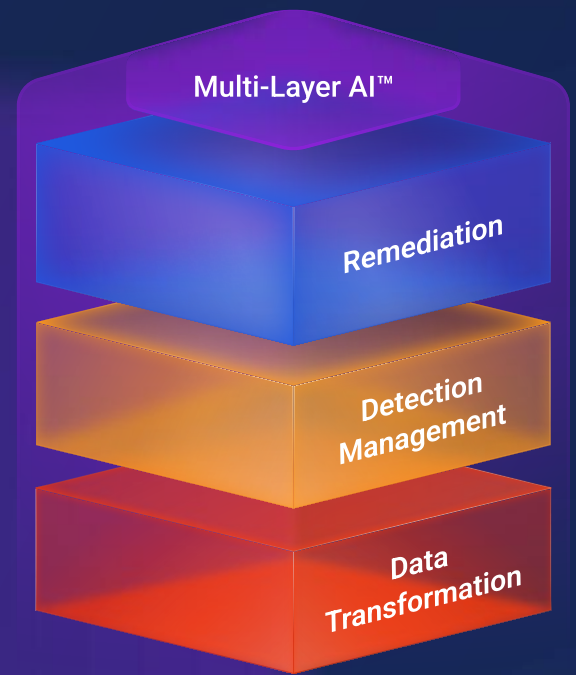
Case Study



# NTT DATA Improves Security Operations Productivity Through Unified Visibility

NTT DATA, a global technology services provider supporting mission-critical SAP environments, needed to improve the efficiency and effectiveness of its security operations. The organization operated across complex, highly connected infrastructure and relied on multiple security tools that produced large volumes of alerts but limited operational clarity.

The security team sought a way to centralize visibility, understand threats in real time, and respond faster, without replacing existing tools or increasing headcount.



## Life Before Centralization

Before modernizing its security operations, NTT DATA relied on manual processes to interpret alerts across multiple tools. Analysts needed deep expertise to correlate activity, making it difficult to understand detection volumes or identify meaningful patterns in real time.

The lack of unified context slowed investigations and increased dependence on a small number of experienced analysts, limiting scalability and increasing operational risk.

### Before



#### Limited Visibility

Analysts struggled to understand where threats were occurring across systems and networks.



#### Manual Correlation

Threat identification depended on expert knowledge and manual log analysis.



#### Slow Detection & Response

Threats often escalated before analysts could fully understand them.



#### Disconnected Tool Outputs

Existing tools generated alerts without shared context.



#### High Operational Overhead

Manual workflows limited productivity and scalability.

### With Stellar Cyber



#### Unified Operational Visibility

Security telemetry from network, endpoint, and log sources is consolidated into a single operational view.



#### Automatic Triage & Prioritization

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



#### Faster, Actionable Insight

Analysts now see daily detection trends and threat activity at a glance, accelerating response.



#### Maximized ROI from Existing Tools

Existing investments feed into a unified platform instead of being replaced.



#### Efficient, Scalable Operations

Automation supports a human-augmented autonomous SOC model.

## Why NTT DATA Centralized Security Operations

NTT DATA needed an approach that would:

- Work with existing security tools and telemetry
- Provide unified visibility across network, endpoint, and log data
- Automatically triage and prioritize alerts
- Support real-time monitoring and continuous operations

By centralizing telemetry and applying Multi-Layer AI, the organization moved away from manual correlation toward automated, contextualized incident analysis—meeting the team where it was while significantly improving operational efficiency.

## Security Operations After Centralization

With a unified security operations platform in place, analysts now work from a centralized incident queue that presents correlated activity with full context. Automatic triage and prioritization reduce noise and allow teams to focus on real threats instead of individual alerts.

Visual dashboards provide immediate insight into detection volumes and trends, enabling faster, more confident decisions. Analysts can clearly see where activity originates, how it progresses, and what requires action—without pivoting between tools.

This operating model supports a human-augmented autonomous SOC, where automation accelerates routine investigation and humans guide strategy and response.

NTT DATA achieved measurable improvements in security operations performance:

- Unified visibility across mission-critical systems
- Reduced reliance on manual correlation and expert-only workflows
- Faster detection and response through prioritized incidents
- Improved analyst productivity with minimal training
- Preserved value from existing security tools and data



**We can easily see how many detections occur in a day and understand the overall security picture**



**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