ANOMALI

CASE STUDY

From Legacy SIEM to Modern Resilience

From Legacy SIEM to Modern Resilience

Our customer is a major American company providing financial information and market intelligence. They are a frequent target of sophisticated attacks due to their work with highly sensitive financial data that can impact the U.S. and global economies.

The cyber fusion and security operations department is tasked with detecting and responding to those attacks across the organization. “We’re the first line of defense,” said the department head, who has been with the company for more than a decade. “Anomali is one of our strategic products, which our teams use today to detect, respond to, and contain threat actors in our environment.”

The Problem

Like many organizations, the company was feeling the pain of data overload. Logs and observable data had become more than their SIEM — and budget — could handle. “One of the challenges our industry faces is the sheer growth of log data and its associated cost,” said the department head. “At some point, due to pressure — primarily cost — organizations begin trimming down logs. But when you do that, you risk losing telemetry that could help detect threat actors.”

Additionally, the company’s adversaries were using AI in phishing campaigns, lateral movement, breach attempts, and more. Attacks were coming more frequently and with more complexity, ratcheting up pressure on timely response. And the competition for skilled engineers to build resilient systems was at an all-time high.

They needed something different. They needed Anomali.

Overview

INDUSTRY

Financial Services

SIZE OF COMPANY

40,000+ Employees

LOCATION

New York, NY

Solution

Addressing the data management challenge was the first order of business. Their legacy SIEM had been designed as a long-term storage platform which drove up costs. "You're paying to store everything," said the department head. "But SIEM should be your most expensive storage tier. That means only data that needs frequent correlation or threat detection should stay in the hot tier."

Anomali Security Analytics enabled the company to create a tiered data architecture, decoupling storage and compute. Compliance and forensic data could be stored in a lower-cost tier, while data that needs frequent correlation or is used in threat collection stays in a hot tier.

> **"We're moving away from monolithic SIEMs into intelligent, use case-driven architectures with lower costs."**
>
> **– Head of Cyber Fusion and Security Operations**

Switching to Anomali also helped break down silos between security and IT observability, combining them in an open, unified security data lake. It's this security data lake that fuels Anomali's AI threat detection and analysis.

With Anomali's ultra-modern SIEM, the company could use cost-effective microservices and compute-on-demand to run complex, AI-powered searches and correlations at scale. "This is compute when you need it, at acceptable costs," said the department head. "That simply isn't possible with legacy or on-prem environments."

Anomali also fit well with the department head's philosophy on the purpose of logging in a world inundated with cyber threats. "Just retaining logs statically won't help you win against today's smart, AI-powered threat actors," he said. Logs must be "interactive," correlated and analyzed against actionable threat intelligence to identify risks.

> **"When you correlate logs with actionable threat intel, it surfaces investigations your teams can pursue to eliminate threats.** That's how you proactively defend your organization and get ROI on the cost of log retention."
>
> **– Head of Cyber Fusion and Security Operations**

Anomali Products

SECURITY ANALYTICS

Anomali Security Analytics fuses threat intelligence, AI, and a high-speed data lake into a single platform for ultra-modern detection, investigation, and response, at unmatched speed and scale.

THREATSTREAM

Anomali ThreatStream is the only AI-powered threat intelligence platform that correlates IoCs with threat actor TTPs, and natively links them to your security telemetry.

COPILOT

Anomali Copilot AI uses natural language and advanced threat intelligence to supercharge detection, investigation, and response.

Bringing the Solution to Life

"When we transitioned to Anomali, one concern was whether the system would scale," said the department head. "But with a strong underlying architecture and an engineering team that works closely with customers, that concern quickly went away." Anomali worked lock step with the customer team and partners, bringing in strong engineering talent to build resilient, AI-driven systems.

With strong change management and the needed technical abilities, risks were kept low during implementation. Anomali supports backward and forward compatibility through its many integrations and API connections.

"You can move data through extraction, transformation, and loading on the fly," said the department head. "Fleet management, from legacy to modern systems, is highly modernized."

The Anomali Impact

Before Anomali, the customer faced a no-win situation with their legacy SIEM: keep paying spiralling costs or lose visibility to the data needed for effective defense.

With Anomali, they rearchitected their data to keep costs low without sacrificing visibility. They dramatically improved their detection and analysis capabilities by running AI searches and correlations on their unified data lake. And with Anomali and partners, the company was able to build sustainable talent paths and manage the transition process seamlessly.

"This is compute when you need it, at acceptable costs," said the department head. "That simply isn't possible with legacy or on-prem environments."

Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. **Request a demo** to learn more.

ANOMALI