DAYS TO SECONDS: HOW ONE AIRLINE REWIRED ITS THREAT INTELLIGENCE OPERATION

Anomali Customer Success Story

Aviation security is high stakes. The European Aviation Safety Agency (EASA) estimated a monthly average of 1,000 airport cyberattacks in 2020, with a 600% increase in aviation cyberattacks reported between 2024 and 2025. Any gaps in threat intelligence aren't just operational inconveniences they're open doors.

For one of the world's prominent private and business charter airlines, a growing mismatch between its security ambitions and its technology stack had quietly become a liability.

The airline had invested significantly in a known threat intelligence platform (TIP) to anchor its cyber defense program. The tool was well-regarded in the industry. But as the airline's security team began expanding its intelligence requirements, including pulling from dark web monitoring services, specialized data feeds, and sector-specific sources, a fundamental limitation emerged: the incumbent platform wasn't built to aggregate.

A Fragmented Picture

Security oOperations analysts found themselves toggling between their primary TIP and a growing number of external feed sources, manually stitching together a coherent picture of the threat landscape. The process was slow, labor-intensive, and prone to blind spots.

"When your analysts are spending hours correlating data between systems instead of acting on intelligence, you're not running a security operation. Instead, what you're really running is a data management problem," said a threat intelligence director, familiar with the deployment. “Every hour of delay is an hour of exposure."

For an airline catering to corporate executives, government officials, and high-net-worth individuals, the stakes of that exposure are particularly acute. The attack surface spans flight operations, client data, maintenance systems, and procurement, which is an incredibly complex environment that demands a unified, real-time view of risk.

> **"Instead of days of work to investigate a specific threat, they could do it in seconds."**

The Case for a New Approach

After a rigorous evaluation process that attracted competitive bids from multiple vendors, the airline selected Anomali ThreatStream Next-Gen, deployed on-premises to meet its data sovereignty and operational requirements. The deal also included Anomali Agentic AI, an AI-powered investigation layer, a sandboxing capability for malware analysis, and a threat feed covering dark web intelligence.

The decision wasn't made lightly. Switching TIPs mid-operation carries real risk: workflow disruption, data migration complexity, and the ever-present concern of capability gaps during transition. To address this, Anomali's team worked alongside channel and technology alliance partners to ensure continuity and to close any gaps between the incumbent solution and the new stack.

The value proposition that ultimately won the deal centered on aggregation. Anomali ThreatStream Next-Gen is architected to ingest, normalize, and enrich intelligence from hundreds of disparate intel feed sources into a single operational view, which is exactly what the airline's multi-feed strategy required. Rather than replacing intelligence sources, it unified them.

AI as a Force Multiplier

Perhaps one of the most striking elements of this engagement was the impact of Anomali Agentic AI, the platform's AI-driven analysis layer. During a pre-project workshop, the airline's security team was walked through a live threat investigation scenario.

Tasks that would traditionally require a seasoned analyst a full day or more (pivoting across indicators, enriching context, mapping to threat actor profiles) were completed in seconds. The demonstration wasn't a curated sales exercise; it was a working proof of capability that reset the airline's expectations of what a modern agentic platform could deliver.

Dark web monitoring, previously a gap in the airline's coverage, was addressed through one of Anomali's tech alliance's feed integration, giving analysts visibility into credential leaks, threat actor chatter, and targeted campaigns that might otherwise go undetected until it was too late.

Lessons for Security Leaders

The airline's experience carries broader implications for any organization evaluating its threat intelligence and agentic AI infrastructure. A platform that cannot aggregate and operationalize intelligence from multiple sources A platform that can't aggregate and operationalize intelligence from multiple sources isn't a true threat intelligence platform that can drive decision-making in the SOC.

As threat actors grow more sophisticated using AI and attack surfaces expand, the ability to consolidate intelligence, automate enrichment, and act in near-real time is becoming a baseline requirement.

For the airline, the shift to Anomali represents a structural upgrade in how threat intelligence flows through the organization — from collection and enrichment, through analysis and investigation, to operational response. With AI accelerating each stage of that workflow, the gap between detection and action has narrowed dramatically.

In an industry where a single security incident can ground operations, damage client trust, and trigger regulatory scrutiny, that speed advantage may prove to be the most valuable asset on the balance sheet.

Set up a confidential one-on-one meeting with Anomali to discuss your pressing needs and concerns.

SCHEDULE A MEETING