ANOMALI

Customer Story

WHEN SPEED IS THE ONLY DEFENSE: HOW A GLOBAL AIRLINE CLOSED THE THREAT INTELLIGENCE GAP

In the airline industry, margins are razor thin, systems are sprawling, and downtime is not an option. Every minute an aircraft sits idle costs money. Every disruption ripples across customers, loyalty programs, partners, and regulators. And in the background, threat actors are constantly probing for weaknesses often faster than security teams can reasonably respond.

> "Airlines have historically prioritized getting butts in seats – anything that touched revenue directly," said Chris Staab, co-founder of the Loyalty Security Alliance (LSA), a travel industry loyalty program research and conference collective. "Mindsets are shifting because they are being forced to shift. The days of not prioritizing cybersecurity are over for airlines. Whether it's state actors seeking travelers' details for intelligence gathering purposes or organized fraud rings who find airline reservations and frequent flyer miles easy to steal and then re-sell, airlines face constant cyber threats."

Staab also shed light on the staffing shortages in cybersecurity, which he says is "playing out in real time" noting that a material number of his airline and travel industry customers have changed jobs. "Cyber analysts are in incredibly high demand," Staab said. "And as a result, talent is moving quickly, and that constant churn makes it even harder for airlines to build and maintain strong cybersecurity programs. This isn't theoretical anymore. It's happening right now across the airline sector."

For one global airline, that reality became painfully clear during a period of organizational transition. Veteran cyber threat intelligence leaders had moved on. Team size shrank. Tribal knowledge walked out the door. Meanwhile, cyber threats didn't slow down, they accelerated.

> "Talent is moving quickly. That constant churn makes it even harder for airlines to build and maintain strong cybersecurity programs."
>
> – Chris Staab, Loyalty Security Alliance

What followed offers a glimpse into how modern security teams are adapting to an uncomfortable truth: attackers are homing in on the airlines. Cybersecurity experience gaps are inevitable, but response gaps don't have to be.

A THREAT LANDSCAPE THAT NEVER SLEEPS

Airlines are uniquely exposed. Millions of loyalty program members. Always-on websites. Vast cloud environments. A mix of financial, personal, and operational data, which are all attractive to attackers looking for quick monetization.

Account takeovers, credential abuse, inventory hoarding by competitors, gen-AI enabled phishing campaigns, and exploitation of known vulnerabilities are routine. Opportunistic cybercrime often targets loyalty programs first not because they're the most complex, but because they're often unchaperoned accounts making them highly profitable for financially motivated cyber criminals. For example, compromised credentials can be bought cheaply on the dark web and reused across industries with minimal effort.

> "It's not always about hacking airplanes," one former senior threat hunting leader explains. "It's about finding the fastest way to make money."

The challenge isn't just detection, it's interpretation. Threat intelligence teams are flooded with data: thousands of indicators, evolving adversary names, shifting infrastructure, and fragmented reporting. Turning that raw information into a clear answer (Are we impacted? What do we do next?) traditionally requires deep expertise and hours of analysis.

Hours that most resource-constrained airline teams no longer have.

WHEN EXPERIENCE WALKS OUT THE DOOR

The airline's threat intelligence team once operated with a deep bench of experience. Over time, though, staffing dropped from five specialists to three. Two of the most seasoned practitioners, including the team's primary threat intelligence lead, departed.

Suddenly, they lost significant time and context.

> "You don't realize how much work is being done until it's gone," the former leader says. "Threat intelligence is storytelling. It's connecting thousands of data points into something actionable. That's hard to replace overnight."

At the same time, executives still expected answers and often urgently. A breaking advisory. A law enforcement notification. A threat actor suddenly trending in the news. Someone, typically the CEO to the CISO, would inevitably ask, 'Are we affected?'

And they would need that answer quickly sometimes on a Friday night, sometimes while an executive was boarding a flight.

COMPRESSING HOURS INTO MINUTES

While the airline had been using the Anomali Agentic SOC platform as part of their security operations already, they saw an opportunity to take advantage of Anomali Agentic AI to help fill the gaps once their most experienced analyst left.

They saw improvements in performance right away. Analysts were able to ask plain-language questions and receive concise, structured responses: summaries of threat actor behavior, indicators of compromise (IOCs), relevance to the airline's environment, and most critically recommended next steps.

What once took hours of manual correlation could now be completed in minutes. The global airline's Director of Cyber Threat Intelligence said, "Having the Anomali Agentic SOC platform is like having another mature analyst. We went from three hours of IOC collection to three minutes. Cyberthreats have increased dramatically, while the threat research team has gone from five people to three."

> "We went from three hours of IOC collection to three minutes."
>
> – Director of Cyber Threat Intelligence

> "It's like having a senior analyst on demand," a former threat intelligence leader for the airline added. "You get the context, the prioritization, and an action plan without needing 25 years of experience."

During live incidents, that speed mattered even more. Instead of scrambling to assemble reports under pressure, teams could focus on decision-making. Stress dropped. Confidence rose. Communication with leadership improved.

> "You're not running around trying to figure out what's important," the director of cyber threat intelligence commented. "The noise falls away."

FASTER RESPONSE, QUIETER OUTCOMES

In cybersecurity, successful outcomes can be measured by what's prevented.

> Staab said, "Airlines focus resources and budget to increase customer lifetime values, but one major security incident can make years of this work disappear."

Despite tracking highly visible threat actors and active campaigns, the airline never appeared in breach headlines. No public disclosures. No reputational fallout. No visible customer impacts.

That absence is the point.

> "When you respond fast enough, the story never becomes public," the former leader noted. "That's the real success."

For an industry where trust is everything — where passengers entrust personal data and physical safety — quiet containment is the ultimate metric.

THE NEW REALITY OF THREAT INTELLIGENCE

The airline's experience reflects a broader shift across security teams. Talent shortages are real. Budgets are tight. Threats are multiplying.

AI won't replace experienced threat intelligence analysts, but it can scale their thinking, codify their instincts, and increase their bandwidth.

> "This is a chess match," the former leader says. "Attackers get faster. So do we."

For this global airline, closing the threat intelligence gap was about collapsing time and ensuring that even in moments of transition, the business stayed airborne.

Have questions? Book a confidential 1:1 with an Anomali expert to talk through what you're facing and get the answers you need.

SEE ANOMALI IN ACTION

Request a Demo