ANOMALI

Customer Story

FROM THREE HOURS TO THREE MINUTES:

HOW A GLOBAL AIRLINE'S CTI TEAM HELD COVERAGE AFTER LOSING ITS BENCH

THE SITUATION

A global airline's cyber threat intelligence team dropped from five specialists to three. Two of the most seasoned practitioners left, including the team's primary intelligence lead, and their departure took years of accumulated context with them. It happened while attacks against the airline sector were increasing, not slowing.

The pressure did not shrink to match the smaller team. Executives still needed answers, often within the hour. A breaking advisory, a law enforcement notification, or a threat actor trending in the news would prompt the same question from the CISO, sometimes from the CEO: are we affected?

The team had to answer on a Friday night or while a leader was boarding a flight, and answer with enough confidence to stand behind it.

WHAT THE WORK LOOKED LIKE BEFORE

The hard part was never collecting data. It was interpretation. Analysts worked through thousands of indicators, shifting adversary names, changing infrastructure, and fragmented reporting, then turned all of it into a clear answer: are we impacted, and what do we do next. That correlation took deep expertise and hours of manual effort per question.

Assembling the indicators of compromise for a single inquiry ran about three hours. Repeat that across a week of advisories and active campaigns, and a three-person team spends most of its capacity building context instead of acting on it.

BASELINE VERSUS AFTER

MEASURE	BEFORE	AFTER
IOC collection, single inquiry	~3 hours	~3 minutes
Correlation and investigation	Hours of manual analysis	Minutes
Analyst focus during incidents	Report assembly under pressure	Confident decision-making

> "We went from three hours of IOC collection to three minutes…[it was] like having another mature analyst."
>
> Director of cyber threat intelligence

WHAT CHANGED

The airline already ran the Anomali Agentic SOC platform. When its most experienced analyst left, the team put Anomali Agentic AI to work on the gap.

There was a direct change to daily practice. Analysts ask questions in plain language and get back concise, structured answers: a summary of the threat actor's behavior, the relevant indicators of compromise, how the threat maps to the airline's own environment, and the recommended next steps.

> This is what "know what matters, act with confidence" looks like. The signal arrives already sorted and mapped to the business, so the analyst spends their time on the decision.

THE ANALYST EXPERIENCE

Speed mattered most when it was scarcest, during live incidents. Instead of scrambling to assemble a report while an incident was still unfolding, the team could spend that time deciding what to do. Stress dropped, confidence rose, and communication with leadership got clearer because the answer arrived before the pressure peaked.

> "You're not running around trying to figure out what's important," the director said. "The noise falls away."
>
> "It's like having a senior analyst on demand. You get the context, the prioritization, and an action plan without needing 25 years of experience."
>
> — a former CTI leader for the airline

WHY THIS MATTERS FOR SOC OPERATIONS

The improvements started in the threat intelligence team, but they carry across the operation. When a staffing shortfall hits CTI, the rest of the SOC feels it: advisories go unanswered longer, and the context that detection and response rely on arrives late. Holding that function steady with three people instead of five kept that dependency intact, and it reached the floor in two ways. Analysts got hours of manual context-building back as minutes, capacity that stayed available when the team was smallest. During live incidents, the intelligence behind a containment call arrived before the pressure peaked, so the team spent its time deciding rather than assembling reports. Because the capability ran on a platform the airline already used, none of it required standing up a new system mid-crisis.

The payoff is the kind that does not make news. Despite tracking prominent threat actors and active campaigns, the airline never appeared in a breach headline through the transition, with no public disclosure **and no visible customer impact. As a former leader put it: "When you respond fast enough, the story never becomes public. That's the real success."**

SEE ANOMALI IN ACTION

Request a Demo