ANOMALI

Guide

FROM THREAT INTELLIGENCE PLATFORM TO MANAGED INTELLIGENCE: WHAT CHANGES AND WHY

A CTI analyst identifies a new command-and-control domain tied to an actor already active in their sector. They tag it, apply a confidence rating, write it into a bulletin, and push it to the threat intelligence platform. Then it sits until a detection engineer runs a search that happens to touch it, or until someone reads the bulletin before the next standup, or until the domain surfaces in a log and an analyst thinks to check the TIP. The intelligence was accurate and current the moment it landed. Whether it drove a decision depended on who queried what, and when.

That gap between knowing and acting is the one a threat intelligence platform was never built to close. Understanding why is the difference between buying a better repository and changing how intelligence reaches your security operations.

WHAT A TIP WAS BUILT TO DO

The threat intelligence platform solved a real problem well. Before the TIP, intelligence lived in spreadsheets, email threads, vendor portals, and analysts' heads. The TIP gave CTI teams one place to aggregate feeds, store indicators, deduplicate overlapping data, and run manual analysis against a common repository. It became the system of record for the intelligence program.

A TIP is a place where intelligence is collected and held. Aggregation, storage, deduplication, and analysis are all operations a human performs against a repository. The analyst pulls the feeds, resolves the overlap, scores the indicators, writes the finished intelligence, and disseminates it by hand. The platform holds the data, and the analyst does the work of turning that data into something a detection or an investigation can use.

For a research-driven program, that model fit. Analysts had time to query, correlate, and produce. The consumers of intelligence, mostly other analysts and the occasional executive brief, operated on a timeline measured in days.

WHAT MANAGED INTELLIGENCE AS A SERVICE IS

Managed Intelligence as a Service, or MIaaS, describes intelligence delivered as a continuously curated service rather than a repository queried on demand. The curation, scoring, enrichment, and maintenance run as an ongoing function. The output is applied to your security data at the point of ingestion, so context is already present when an alert fires or an investigation opens.

Anomali delivers MIaaS through ThreatStream Next-Gen. The mechanics matter for a CTI evaluation: indicators are sourced, confidence-scored, and maintained on a continuous basis rather than shipped as static feeds; enrichment is applied to logs, alerts, and events in real time; and the resulting context follows the alert and the investigation instead of waiting in a separate tool for an analyst to go retrieve it.

The distinction is easy to state and consequential in practice. A TIP is where intelligence is stored; MIaaS is intelligence delivered to the decision.

THE CORE DIFFERENCE: A REPOSITORY YOU WORK BY HAND VERSUS CONTEXT THAT ARRIVES

Picture the same C2 domain in each model.

In the TIP model, the analyst does the connecting. The domain is in the repository. When an alert involving that domain reaches the SOC, someone has to know to check the TIP, run the query, find the record, read the attribution, and carry that context back to the investigation. Every step is a manual handoff, and every handoff is a place the context can fail to arrive. The intelligence exists, but reaching it is the analyst's job.

In the MIaaS model, the context is already attached. When the alert fires, the enrichment, the actor attribution, the campaign association, the confidence score, all of it travels with the alert into the investigation. The analyst is not reconstructing what the intelligence program already knew, but starting from it.

The TIP asks the analyst to bring the alert to the intelligence. MIaaS brings the intelligence to the alert. Same underlying data, curated by the same discipline, but what changes is whether it reaches the moment of decision on its own or waits to be queried.

WHAT "MANAGED" CHANGES FOR PROGRAM ECONOMICS

Feed hygiene is continuous, not a recurring analyst project. Feed overlap, indicator decay, and deduplication are not one-time cleanups. They are permanent conditions of running an intelligence program. Feeds duplicate each other. Indicators age out and go stale. New sources introduce new overlap. **In a TIP program, keeping the repository clean is standing analyst labor, and it competes directly with the analysis that actually produces value. Under a managed model, that maintenance runs as a service function rather than a line on your team's weekly capacity**.

Enrichment tuning becomes ongoing rather than periodic. Deciding which context matters for your environment, and adjusting scoring as your telemetry and priorities change, is work that never finishes. Treating it as a continuous service means it keeps pace with your environment instead of drifting between quarterly reviews.

The economic argument is not about headcount reduction. It's more about where a finite analyst team spends its hours. A managed model moves the repetitive maintenance load off the team so the same analysts spend more time on judgment and less on plumbing. For a CTI lead being asked to justify program value, that reallocation is the more defensible story than any raw cost figure.

WHERE THE ANALYST'S ROLE SHIFTS

MIaaS does not remove the analyst. It changes what the analyst does with their day, and the change favors the parts of the job that require a human.

AI-assisted correlation and scoring handle the volume. Indicator correlation, confidence scoring, enrichment, and prioritization across campaigns and actors are pattern-recognition problems that machine assistance handles well and at a pace no analyst can match by hand. Anomali scopes this assistance to the operational tiers that are generally available today, which for triage and correlation means machine-led support with the analyst in the loop rather than autonomous action on its own authority.

Analyst-led judgment and dissemination remain human. Deciding what a correlated cluster of activity means for your organization, which threats warrant a change in posture, and how to communicate that to the people who act on it, that is analyst work, and it does not automate. The role moves up the value chain. Less time resolving feed overlap, more time on the interpretation and dissemination that only a person can do.

The honest framing for an evaluating team: this is a change in the shape of the work, not the elimination of it. Analysts who spent a third of their week on repository maintenance get that third back for analysis.

DOES MIAAS REPLACE OR EXTEND A TIP?

This is a category evolution, not a replacement of one tool by a competing one. The threat intelligence platform did its job. What changed is the speed of operations around it. A repository that waits to be searched can't keep up with its own consumers. Adversaries now operate at machine speed, and those consumers are increasingly detection and response systems, not human analysts with time to query.

Anomali's path through that evolution is worth naming plainly, because it is a reason to take the framing seriously rather than as marketing.

> **ThreatStream began as a threat intelligence platform, and it built the curation discipline, the confidence scoring, the community sharing, and the integrations over more than a decade of production use. Managed Intelligence as a Service, powered by ThreatStream Next-Gen, is that heritage carried forward into a delivery model built for operational tempo. The curated intelligence you would recognize from a TIP is still the substrate. What changed is that it now travels to the decision instead of waiting to be retrieved.**

For a CTI team, that means the evaluation is not "rip out the TIP and start over." It is "does the same intelligence discipline, delivered continuously and applied at ingestion, close the gap my current program leaves open?"

A FIT CHECK: WHEN A CTI TEAM SHOULD LOOK AT MIAAS

Not every program needs to move now. A few conditions make the question worth asking sooner rather than later.

1. Feed hygiene is eating your analysts' week. If a meaningful share of your team's time goes to deduplication, decay management, and reconciling overlapping sources, that is maintenance labor a managed model is designed to absorb. Measure it before you evaluate. The number is usually higher than teams expect.
2. There is a lag between what your program knows and what your operation acts on. If intelligence you have already curated regularly fails to reach the alert or the investigation in time to matter, the problem is delivery, not data. That lag is the specific thing MIaaS is built to remove, and it is worth quantifying with a few recent cases where the intelligence existed but did not arrive.
3. You are being asked to prove the program's value. A CTI program judged by reports produced is on weak ground. A program judged by decisions influenced is on firm ground. If you are struggling to show operational impact rather than analytical output, a model that operationalizes intelligence by design gives you a clearer line from your team's work to outcomes the business recognizes.

If none of these describe your program, a TIP may still serve you well. If one or more do, the gap they describe is the one this category evolution exists to close, and it is worth a closer look at how Anomali's MIaaS delivers it.

Anomali can help you move from detecting alerts to driving better security decisions. See what Managed Intelligence as a Service looks like. Request a demo.

SEE ANOMALI IN ACTION

Request a Demo