ANOMALI

Brief

HOW A CTI LEAD PROVES THE VALUE OF A THREAT INTELLIGENCE PROGRAM

A decision-stage brief for defending the program upward: how to measure operationalized intelligence, govern it, and report it to a CISO or board.

In most quarterly business reviews, the threat intelligence program gets described in activity terms: feeds ingested, advisories published, indicators added. The CISO is asking a different question. She wants to know which decisions the program improved and what it caught before it ran. When the gap between initial access and lateral movement is counted in minutes, intelligence that waits in a report for someone to look it up has arrived too late to matter. A CTI program earns its budget on how much of what it knows has already become action by the time a decision has to be made.

WHAT MAKES A THREAT INTELLIGENCE PROGRAM WORTH ITS BUDGET?

Operationalized intelligence. A program is worth what its intelligence changes, not what it collects. Measure it four ways: operationalization rate (the share of high-confidence intelligence that becomes an enforced control or detection, and how fast), incidents preempted before execution, triage time returned to the SOC, and the risk decisions the program directly informed.

Curated, scored intelligence that becomes a live detection the same day is worth far more than the same intelligence sitting in a portal for an analyst to find later. Track how much of your high-confidence intelligence reaches enforcement and how long it takes, then pair it with named preemption: a campaign blocked before it reached you, a vulnerability moved up the patch queue because intelligence showed it under active exploitation in your sector. One named, preempted event carries a budget meeting further than a quarter of indicator totals. The other two measures, triage time returned and decisions informed, are what tie the program to the SOC's output and to the business's own risk calls, so log both.

HOW DO YOU REPORT INTELLIGENCE VALUE TO A CISO OR BOARD?

Report in the language of risk and decisions, on a cadence matched to the audience. Open every board update with outcomes, what was preempted and what a decision avoided, then support each with the intelligence that produced it. Keep indicator counts and coverage detail for a separate operational review.

Anchor the value in numbers the finance side already understands. IBM's 2025 Cost of a Data Breach Report put the average breach lifecycle at 241 days and found that organizations using AI and automation extensively across their security programs contained breaches roughly 80 days faster and about $1.9 million cheaper than those that did not.

A program that shortens the distance between detection and containment is working that same measure, so frame a preempted or faster-contained incident against it. Match the report to the reader: a board briefing is quarterly, short, and built around the actors targeting your sector; the operational review is monthly and carries coverage, source performance, false-positive trends, and RFI turnaround.

HOW MANAGED INTELLIGENCE AS A SERVICE OPERATIONALIZES YOUR PROGRAM

Managed Intelligence as a Service (MIaaS), powered by Anomali ThreatStream, is how a CTI program makes operationalized intelligence its normal state. It's built for security operations, not just threat research. The curation standards, confidence thresholds, and source grading the team already maintains become the operating logic applied to every event, correlated against your telemetry and turned into action, without the CTI team hand-maintaining.

Provenance and confidence scoring stay on every indicator, so the traceability and auditability a defensible program needs come from the platform rather than a spreadsheet the CTI lead keeps on the side. ThreatStream correlates indicators of compromise and predictive indicators of attack against your environment, so high-confidence matches surface where they matter and can drive enforced controls under analyst supervision, with each action carrying its justification into the audit record.

> For a CTI lead defending the program upward, that reframes the case: the intelligence function becomes the managed control layer the security operation relies on to act correctly at speed, which is a stronger argument than the cost of producing reports.

Find out how to make intelligence the foundation of every security decision and close the gap between knowing and acting. Schedule a demo now.

FAQ

WHAT METRICS PROVE THE VALUE OF A THREAT INTELLIGENCE PROGRAM?

Operationalization rate (how much high-confidence intelligence becomes an enforced control or detection, and how fast), incidents preempted before execution, triage time returned to the SOC, and the risk decisions the program informed.

WHAT IS OPERATIONALIZED INTELLIGENCE?

Operationalized intelligence is about embedding intelligence directly into the decisions, workflows, and actions that define modern security operations. A vetted, scored indicator becomes an enforced control, a detection, or attribution attached to an alert, instead of sitting in a report for an analyst to look up after the fact.

WHAT IS MANAGED INTELLIGENCE AS A SERVICE?

Managed Intelligence as a Service (MIaaS), powered by Anomali ThreatStream, correlates a curated intelligence repository against an organization's telemetry and turns it into action, with provenance and confidence preserved. It makes a CTI team's curation standards the operating logic the security operation runs on, under analyst supervision.