The Feed Economy

Why more threat intelligence hasn't delivered more prevention

A Malanta Survey Report
March 2026

Malanta

Executive Summary

Organizations have optimized volume over quality

Threat intelligence has become a volume game, with 71% of organizations reporting multiple overlapping feeds and 100% struggling to connect signals to real threats.

71%

MULTIPLE OVERLAPPING FEEDS

100%

STRUGGLING TO CONNECT SIGNALS TO REAL THREATS

Manual processes consume time without improving outcomes

84% of organizations rely on manual or reactive threat intelligence processes, with only 31% having fully automated ingestion and blocking, leaving analysts tied up validating signals instead of preventing attacks.

Success metrics reinforce reactivity

Organizations measure success by MTTR and MTTD, yet only 12% track prevention-oriented metrics and 0% measure pre-attack disruption – showing a clear tendency towards reaction over prevention.

Visibility exists but confidence to act does not

Malanta completes manual triage and static feeds with automated, closed-loop prevention that enriches SOC, TIP, SIEM, and SOAR systems in real time.

The market is demanding a different approach

Security organizations consistently demand actionable context, earlier visibility, reduced noise, automated prioritization, and prevention-oriented metrics.

Prevention requires fundamental shifts in how threat intelligence operates

The industry must shift from feed aggregation to signal correlation, from enrichment to enforcement, from response metrics to prevention of metrics, and from detection speed to Attack disruption.

The Survey: Behind the Scenes

The data that follows in this e-book comes from a survey of 100 security professionals conducted by Malanta between September and November 2025. The respondents represent a cross-section of security leadership across enterprise organizations - 22% at the executive level (CISO, VP, or CXO), 28% as directors, 35% as managers or senior managers, and 15% as team leads or senior individual contributors.

The survey captures perspectives from security teams in organizations where threat intelligence infrastructure is mature, budgets are substantial, and operational complexity is high.

The majority of respondents work in large organizations. 58% come from enterprises with 10,000 or more employees. 27% work in organizations with 1,001 to 10,000 employees.

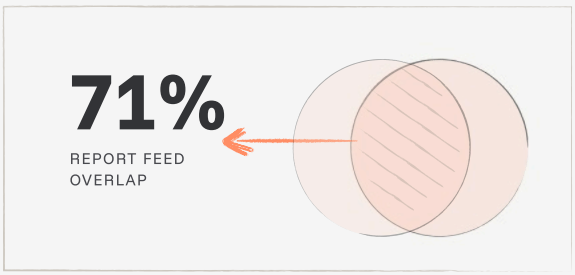
The respondents span 35+ industries across 6 countries. Geographic representation includes the United States (72%), United Kingdom (11%), Canada (5%), and Europe and other regions (12%). The industry mix reflects critical sectors: Healthcare, Financial Services, Technology, Government, Manufacturing, Insurance, and dozens of additional verticals.

Introduction: The Feed Economy

At some point in the past decade, threat intelligence became a volume game. More feeds and broader coverage became accepted indicators of operational maturity. Organizations bought into this, stacking platforms and assigning teams to manage the endless stream of external threat data. Indeed, our survey found that most enterprises now operate 5 to 8 feeds, with some managing as many as 53!

The logic seemed sound: comprehensive visibility requires comprehensive data.

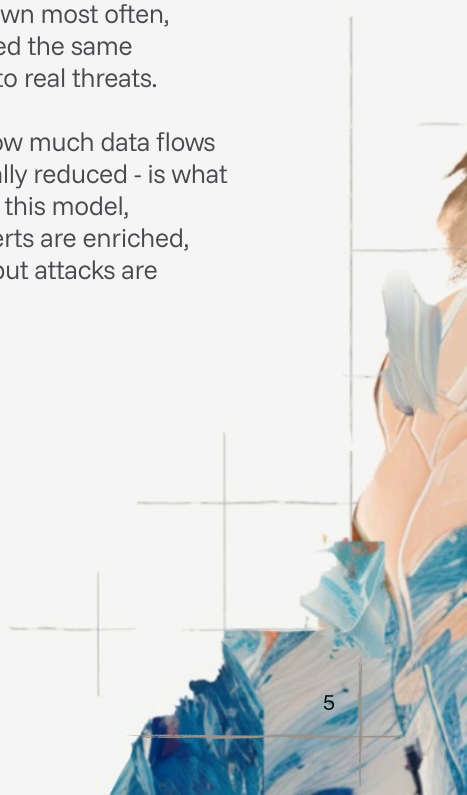
our survey found that 71% of organizations now report massive overlap across their feeds.



Feed growth outpaced operational integration – and most organizations kept adding more feeds instead of getting better at using the ones they had.

The result was a system optimized for signal accumulation, but not for stopping attacks. Organizations spent money and effort consuming threat intelligence that rarely translated into reduced risk. When asked where their threat intelligence process broke down most often, 100% of respondents identified the same problem: connecting signals to real threats.

That disconnect - between how much data flows in and how much risk is actually reduced - is what we call **the Feed Economy**. In this model, intelligence is aggregated, alerts are enriched, analysts reconcile overlap… but attacks are rarely prevented.



> We mainly automate the ingestion of standard threat lists and IOCs from our primary vendor directly into our SIEM.
> It's a purely reactive process focused on known malicious resources.

Security Architect, Logistics and Supply Chain

The Manual Reality

The Feed Economy still relies largely on manual processes.

Our survey found that 84% of organizations rely on manual or reactive approaches to threat intelligence.

Threat data lands in systems, yet teams wait until incidents occur to validate the findings. Threat intelligence is accessed during incident response rather than embedded into preventive controls. Analysts scramble to find context manually during active attacks rather than having validated intelligence ready beforehand. This model supports attack containment. It does not support attack disruption.

Only 31% of respondent organizations have fully automated ingestion and blocking. The other 69% rely on manual work somewhere in the process. 52% have some automation paired with manual oversight. And 66% still rely on ad-hoc or manual evaluation even when assessing new feeds.

Organizations are also investing significant time on validation. Our survey found that 68% of respondents spend 1 to 2 hours each week on indicator validation alone. 17% spend several hours daily on this task. Analysts are tied up validating signals, while threats continue to move faster than manual processes can handle, in any case.

When validation happens after the fact - long after attack infrastructure is already operational - the window for early action closes before anyone realizes it was open.

> We heavily rely on manual processes such as communicating with our threat intelligence team to retrieve additional insights as cyber incidents are being worked on. This is leading to an extremely inefficient triage and response process.

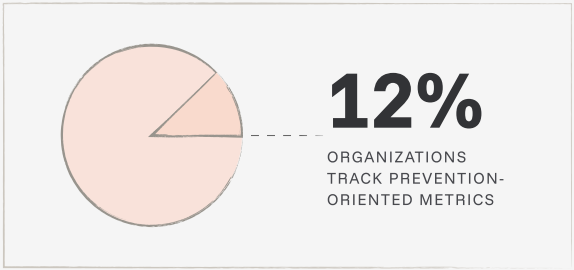
Global Head of Threat Detection, Insurance

The Measurement Bias

Currently, most organizations optimize for reactivity. They quantify how fast teams respond once something goes wrong. Our survey found that 91% track Mean Time to Respond (MTTR). 89% measure Mean Time to Detect (MTTD).
54% monitor false positive rates.

48% track incident volume. This measurement bias is inherent in the Feed Economy - a system designed around signal accumulation and response, not prevention.
Interestingly, what organizations do not measure reveals the gap between their stated priorities and actual practice.

Only 12% of organizations track prevention-oriented metrics.



Zero percent measure pre-attack disruption. Despite this, when evaluating threat feeds, organizations value accuracy and false positive rates (89%), relevance to their industry (82%), timeliness and freshness (78%), integration capability (71%), and actionable context (65%).

There's a fundamental mismatch here: organizations say they want actionable context and timeliness, but they measure success by how fast they respond to incidents.

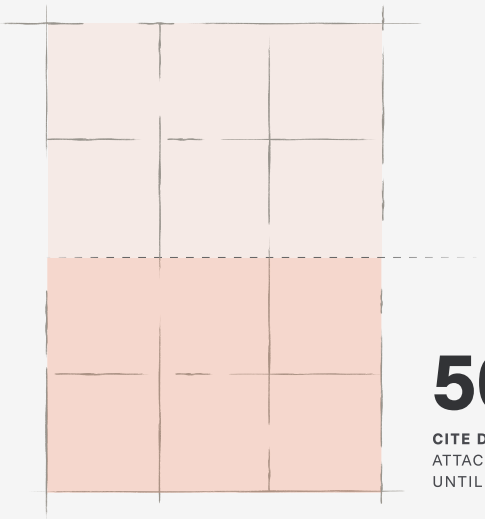
This measurement bias locks them into a reactive posture where prevention never gets funded or prioritized.

> We would love to have a prevention KPI as well - one that talks about what was prevented, not just how fast we cleaned up.

VP, Cloud Engineering, Financial Services

The Detection Ceiling

One key symptom of the Feed Economy is the detection ceiling. When asked what stands between them and preventing attacks,
50% of respondents cited detection gaps - they simply don't see attacks until damage occurs.
Only 33% cited resource constraints.



50%

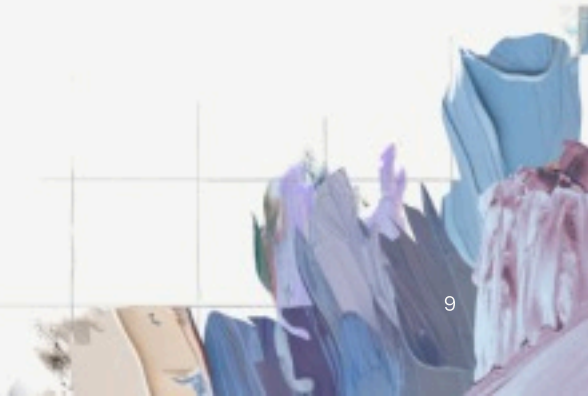
CITE DETECTION GAPS
ATTACKS GO UNSEEN
UNTIL DAMAGE

So, most organizations have resources to devote but lack the visibility into early-stage attack activity. They've got the threat data, but only 65% of organizations say their feeds actually provide actionable context. And even when they've got a semblance of context, their confidence to act on it before an attack unfolds remains low.

This is the detection ceiling. Organizations reach it when they have signals but lack the context or correlation to validate them. Threat intelligence lands in their systems, but it remains noise without a way to connect signals to real threats.
Breaking through the detection ceiling requires a fundamentally different approach - one that lets organizations act on signals before they become attacks.

> The challenge is that most feeds overlap heavily, adding volume without truly advancing our ability to predict or prevent attacks. We're prioritizing intelligence sources that can identify adversary intent and infrastructure earlier.

Director, IT Services



What Enterprises Actually Want

The survey revealed consistent demand across five areas - a clear signal that security organizations want out of the Feed Economy. They want intelligence that enables action upstream, not reaction downstream.

01

82%

Actionable context

Organizations want threat intelligence that arrives ready to use, not raw data requiring manual enrichment and validation.

02

78%

Earlier Visibility

They want to see threats taking shape, not confirmation after damage occurs.

03

74%

Reduced noise

With 71% experiencing feed overlap, organizations are drowning in duplicates. They want filtering, not more volume.

04

68%

Automated prioritization

Manual triage consumes massive amounts of analyst time. Organizations want systems that rank threats by relevance and urgency automatically.

05

65%

Prevention-oriented metrics

The market has been optimized for MTTR and MTTD. Organizations want to measure what they prevent, not how fast they respond.

> Success would look like proactive blocks and hunts that actually stop a potentially successful attack before it happens.

Deputy CISO, Financial Services

Beyond the Feed Economy

The Feed Economy has reached its limit. Organizations have built sprawling threat intelligence operations around feed aggregation, manual enrichment, and response metrics. Yet these foundations cannot support what enterprises actually need. A fundamental shift is required in how threat intelligence operates at its core.

Shift from feed aggregation to signal correlation.
Organizations need to stop collecting feeds endlessly and shift to connecting the signals they already have into a coherent picture of how attackers are building infrastructure.

Shift from response metrics to prevention of metrics
Organizations should stop measuring MTTR and MTTD and shift to tracking what they prevented from happening in the first place.

Shift from enrichment to enforcement.
Organizations need to stop enriching threat data in dashboards and shift to using intelligence that drives decisions and triggers automated responses in real time.

Shift from detection speed to Attack disruption
Organizations need to stop optimizing fast detection and shift to finding and dismantling attacker infrastructure before it ever becomes operational.

Following this shift, the maturity of threat intelligence will be defined not by how much data is collected, but by how many attacks are prevented.

About Malanta

Malanta is the Pre-Attack Prevention Platform. It detects, validates, and dismantles adversary infrastructure during the setup phase, enabling security teams to measure avoided risk through Mean Time to Preempt and campaign-level disruption metrics.