Malanta

From detection to disruption

The New Playbook for Threat Intelligence Teams

A Malanta E-Book
June 2026

Table of content

Executive Summary

TI programs are operationally mature

Most teams have built structured collection programs, automated ingestion, and defined workflows that connect intelligence to detection and response.

Attack timelines have outpaced detection

Timelines have compressed so far that even the fastest detection and response can no longer limit the damage. The indicators TI teams depend on simply don't exist until the attack is already underway.

The setup window is where defenders have the most leverage

Attacker infrastructure is staged and visible before any payload moves, and intervening during that window carries the lowest cost and the greatest impact.

TI maturity comes down to where on the attack timeline your program can act

Four stages define that progression, from manual IOC review through to policy-driven pre-attack disruption.

Dark web monitoring has hit its structural limits

The data it surfaces has already been stolen or abandoned, and the forums that once made it viable have largely been seized or shut down.

Feed investment is producing volume, not outcomes

71% of organizations report significant overlap across their feeds, and 84% still rely on manual workflows to process what comes in.

Pre-attack signals are already visible to mature programs

Domain registrations, certificate issuance, and scanning behavior tied to attacker staging can all be detected and evaluated before the attack starts.

Pre-attack disruption runs on infrastructure you already have

Your feeds, SIEM, enforcement controls, and team workflows stay in place. Pre-attack prevention extends them into the setup phase with a new class of signal and a new set of decisions.

The Control Point Has Moved

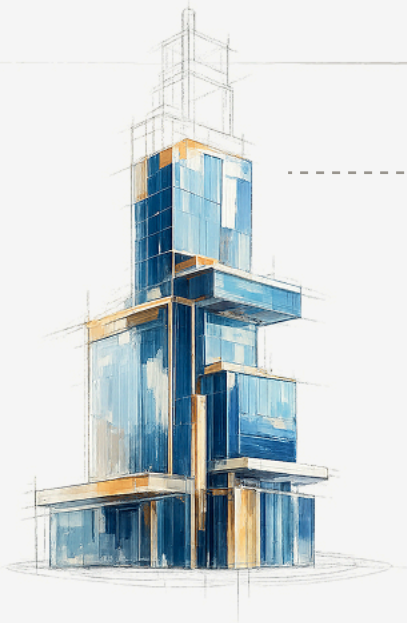
Threat intelligence teams do their jobs well, and then some. They live up to industry expectations - building collection programs, operationalizing feeds, automating IOC ingestion, and routing intelligence into their detection and response systems.

But ‘industry expectations’ have fallen behind attack timelines. Today, attack timelines have compressed so dramatically that even the fastest detection and response cannot limit the damage. And it’s not a team performance issue. The indicators TI teams depend on simply don't exist until the attack is already underway.

And by the time an IOC surfaces, the infrastructure behind it has already delivered the payload or the credential has already been used. The damage is done.

The signals that can change that equation appear earlier - during attacker setup, when domains are registered, certificates are issued, and delivery paths are tested. The setup window gives defenders the most leverage and the lowest cost of intervention.

Yet most TI programs have no operational path to act on it.



91% of organizations plan to increase their TI investment in 2026.

The question is whether that investment will move the control point upstream or add more volume to a model that already produces more data than teams can use. The answer depends on where your program sits today.

In this e-book, we’ll lay out four stages of TI maturity - each one tied to where on the attack timeline your program can act.

The goal is to help you identify your current position, understand the transition ahead, and map the path from detection-led intelligence to pre-attack disruption.

The TI Maturity Model

TI maturity comes down to one thing: where on the attack timeline your program can act. The four stages below define that progression:

Stage 1

IOC Reviews and Dark Web Monitoring

Manual review of indicators of compromise and monitoring of criminal marketplaces for exposed credentials, leaked data, and brand mentions.

Stage 2

IOC Ingestion and Feed Management

Structured intake of threat feeds into detection systems, with defined triage workflows and escalation criteria.

Stage 3

Early Warning and Pre-Attack Signal Detection

Active monitoring of attacker setup activity - domain registrations, certificate issuance, scanning behavior - and defined workflows to assess those signals and decide what to do with them before the attack starts.

Stage 4

Pre-Attack Disruption

Policy-driven enforcement that removes attacker infrastructure during the staging phase, measured by Mean Time to Preempt (MTTP).

The model above is a reflection of operational posture, not team or program quality.

Your program may operate across multiple stages at once. The goal is to identify where your primary capabilities sit today and what the next transition requires.

Stage 1

IOC Reviews and Dark Web Monitoring

Most TI programs start here. Analysts review IOCs from past incidents, cross-reference them against known threat actor activity, and monitor dark web sources for exposed credentials, brand mentions, and leaked data.

The work relies heavily on manual effort, and the intelligence it produces – while useful for attribution, context, and tuning detection rules - still describes activity that has already taken place.

Dark web monitoring, long considered the gold standard for external threat intelligence, works by scanning criminal marketplaces, stealer log channels, and underground forums. As a source of credential hygiene and breach detection, it can deliver value. Yet it suffers from a serious structural constraint: the data that surfaces on the dark web has already been stolen, sold, or abandoned by the time it reaches your team. What's more, the forums that once made dark web monitoring valuable have largely been seized or shut down. This has pushed the more sophisticated threat actors off the dark web entirely and into encrypted channels and private communities that no monitoring tool can reach.

Taken together, IOC reviews and dark web monitoring give you a program that can tell you what was compromised and when – but not what infrastructure is being built to reach your environment.

What You Should Have in Place

1. Define what you're monitoring - which credentials, brands, and data types are in scope.
2. Know who sees findings, how fast, and what qualifies an alert for escalation.
3. Make sure compromised credential alerts reach identity teams with enough context and speed to act before the attacker does

How to Move to the Next Level

1. Start managing your feeds more deliberately - know which sources you trust, why, and how current they are.
2. Connect feed output to your SIEM so IOCs generate alerts automatically rather than landing in a spreadsheet.
3. Build a structured analyst workflow with defined triage ownership and escalation criteria.
4. Establish documentation standards so every alert is traceable from source to decision.

Stage 2

IOC Ingestion and Feed Management

At this stage, your IOCs move from spreadsheets into systems. Feeds are connected to your SIEM or TIP, alerts are generated automatically, and analysts work from structured queues with defined triage criteria. The program has moved past manual review and into operational workflow.

This is where most TI programs concentrate their investments. Teams subscribe to multiple commercial and open-source feeds, fine-tune the ingestion rules, and build escalation paths.

The question is what that investment actually produces. Malanta's State of Threat Intelligence survey found that 71% of organizations report significant overlap across their feeds, and 84% still rely on manual workflows to process what comes in. Programs at this stage are spending more time managing feed volume than acting on what the feeds surface.

Your program processes IOCs faster and with better traceability at this stage. Yet as substantial as the operational improvements are, they still don't change where on the attack timeline you can intervene.

What You Should Have in Place

1. Know which feeds you trust and why - and have a process for dropping the ones that generate noise and nothing else.Have your SIEM set up to route IOCs differently based on type and confidence, not flag everything the same way.
2. Know who owns triage, what threshold moves an alert to incident response, and how that handoff works.
3. Make sure every IOC that drives an action can be traced back to its source and the decision that was made on it.

How to Move to the Next Level

1. Expand your intake beyond feeds - DNS telemetry, certificate logs, and domain registration data that can show you what is being prepared before it is used.
2. Get the mandate and the tooling to act on signals that appear before execution, not just the ones that confirm it happened.
3. Track setup-phase activity as its own operational input, separate from your IOC workflows.

Stage 3

Early Warning and Pre-Attack Signal Detection

This is where your program starts looking forward. Your analysts can see attacker setup activity as it unfolds - domain registrations that follow known staging patterns, certificates issued to support phishing or command-and-control infrastructure, scanning behavior aimed at your exposed services. You have operational paths to evaluate these signals, assess their relevance to your environment, and determine which ones qualify for escalation.

That said, the window after an attack begins remains too narrow to control. Average eCrime breakout time fell to 29 minutes in 2025 - down from 48 minutes the year before.

Once an attacker is inside, the timeline from initial access to lateral movement leaves almost no room for intervention. The setup phase - when infrastructure is staged and visible and no damage has been done - is the only window with real defensive leverage.

At this stage, your team is already working with what Malanta calls Indicators of Pre-Attack (IoPAs) - the domains, certificates, servers, and tooling that adversaries prepare in advance. The next step is building the operational structure to move from seeing those signals to acting on them before the infrastructure is used.

What You Should Have in Place

1. Know which domain registration patterns, certificate behaviors, and scanning activity look like attacker staging - and have a clear line for what crosses the threshold for action.
2. Assign a role or team that owns pre-execution signals before they become confirmed threats.
3. Define at what confidence level a signal moves from monitoring into active evaluation, and make sure someone is accountable for that call.
4. Build a routing path so qualified signals move forward into disruption workflows instead of piling up in a backlog.

How to Move to the Next Level

1. Build a repeatable pipeline - collect, correlate, validate, disrupt, enrich - and make sure every step has a clear owner.
2. Swap out MTTD and MTTR for Mean Time to Preempt (MTTP) as your operating metric - the clock should start when the pre-attack signal appears, not when the incident is confirmed.
3. Get enforcement capability in place that can act on pre-attack signals before execution begins

Stage 4

Pre-Attack Disruption

This is where your program moves from seeing attacker infrastructure to actively neutralizing it. Validated IoPAs trigger enforcement - takedowns, blocking, hardening - through policy-driven workflows that run across your existing controls. The setup window is no longer something you observe. It is something you close.

The operational model here runs as a five-stage pipeline: collect pre-attack signals, correlate them to your assets and brands, validate their exploitability, disrupt the underlying infrastructure, and enrich your detection systems with the results to prepare for the next time.

The metric that matters here is Mean Time to Preempt (MTTP) - the time between spotting adversary setup activity and eliminating the infrastructure behind it.

This is what the Malanta platform does. It monitors setup-phase activity at internet scale, maps it to your environment, validates which exposures are exploitable, and applies policy-based enforcement - automatically or through controlled review. Every action is logged, traceable, and tied to a specific risk removed.

What You Should Have in Place

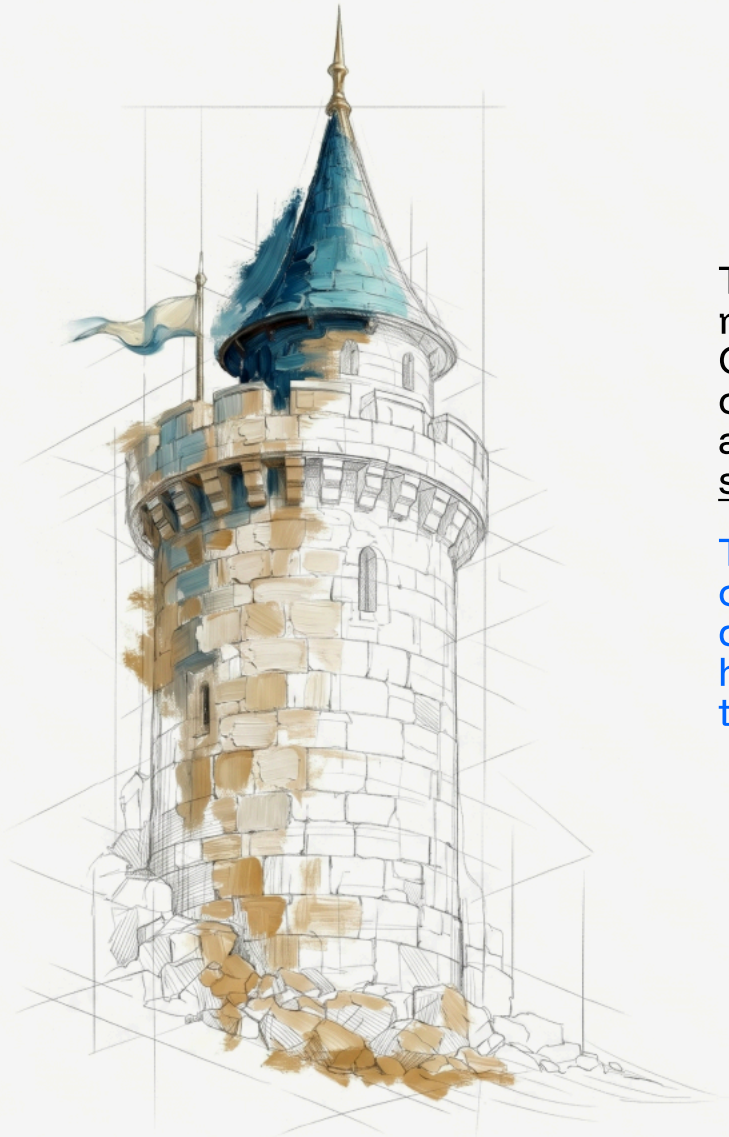
1. Define what action looks like for each infrastructure type - which signals trigger automatic takedown, which go to an analyst, and who has final sign-off.
2. Wire validated IoPAs into your existing enforcement controls - secure web gateway, email security, DNS filters, identity provider - so blocking happens without a manual step in between.
3. Know who is authorized to submit external takedown requests, what evidence they need, and when legal and communications need to be in the loop.
4. Feed takedown outcomes back into your qualification process so the team gets better at recognizing the same staging patterns earlier next time.

How to Operationalize Pre-Attack Disruption at Scale

If your team already runs threat intel feeds into a SIEM, triages alerts through defined workflows, and enforces policy through existing controls - you already have most of the operational infrastructure pre-attack disruption needs. Pre-Attack Prevention simply extends that infrastructure into the setup phase by adding a new class of signal - IoPAs - and a new set of decisions about when and how to act on them. Your tools, your teams, and your enforcement paths remain largely the same.

What changes is scope and timing. Your program takes in signals that appear before any alert fires, evaluates them against your assets and risk thresholds, and routes qualified findings into disruption or escalation paths. Each step needs an owner, a defined threshold, and a traceable decision.

That operational clarity is what turns pre-attack intelligence into pre-attack disruption at scale.

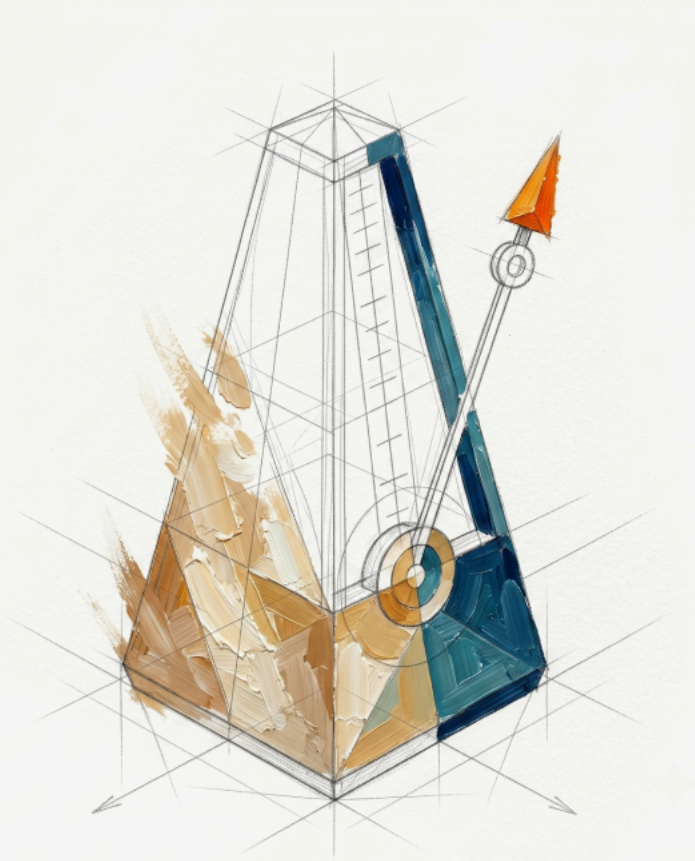


The market is already moving in this direction. Gartner projects that preemptive cybersecurity solutions will account for nearly 50% of IT security spending by 2030.

The teams that operationalize pre-attack disruption now will define how that investment translates into outcomes.

Own the Timeline

Your TI program already has the foundations - operational feeds, defined workflows, and teams that know their craft. The question is whether those capabilities are aimed at the right point on the attack timeline.



Every stage in the maturity model above describes a necessary function. What separates them is where on the timeline your program has the authority and the operational structure to intervene.

Moving upstream - from detection to disruption - means your team spends less time containing damage and more time eliminating the conditions that cause it.

The setup window is open right now

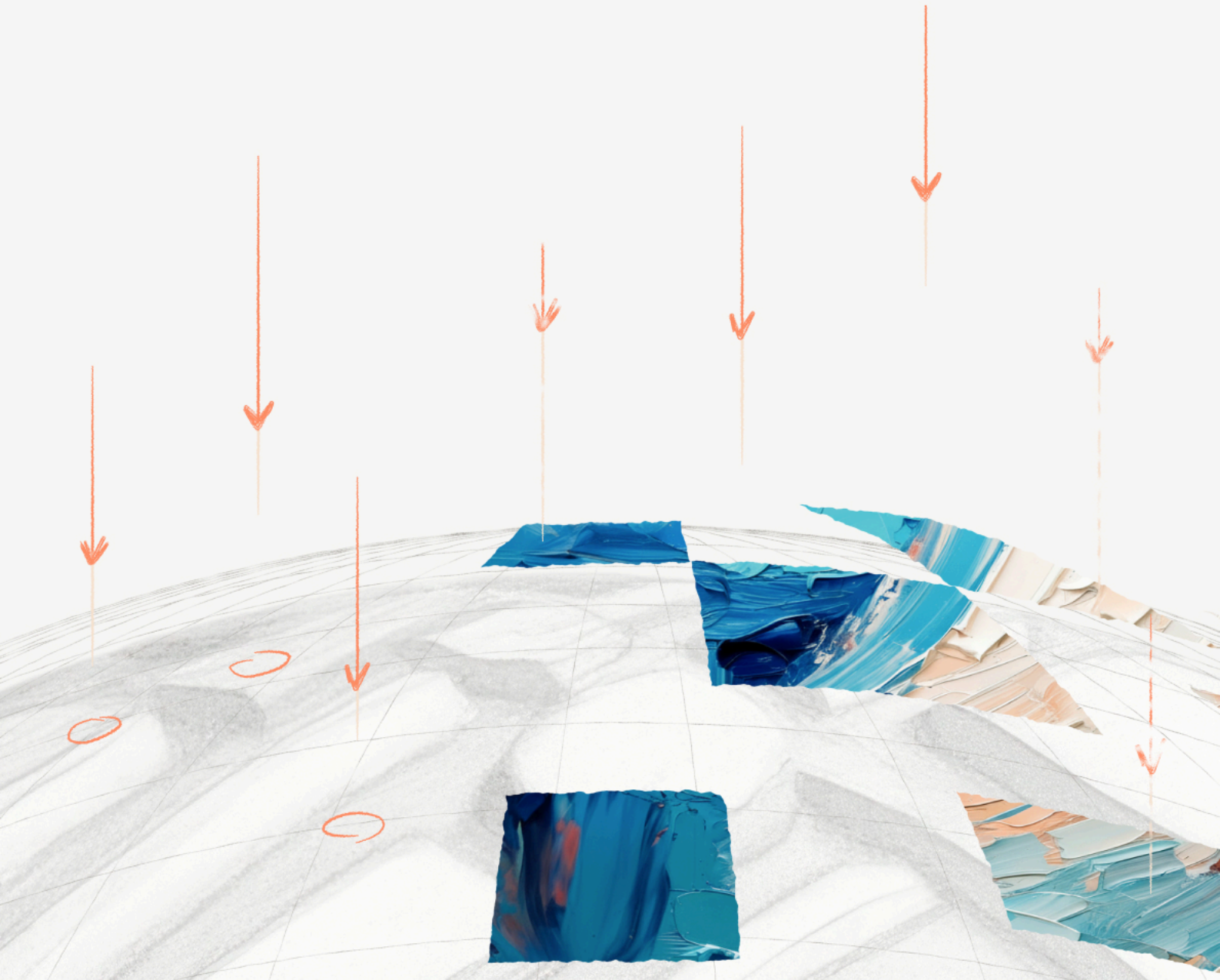
Attacker infrastructure is being staged and aimed at environments like yours.

The teams that close that window will set the standard for what threat intelligence looks like in 2026 and beyond. Start preventing attacks before they launch.

Get access to Malanta today

About Malanta

Malanta provides the first Pre-Attack Prevention Platform. It detects, validates, and dismantles adversary infrastructure before activation, enabling CISOs to quantify avoided risk through the Attack Prevention Index and Mean Time to Preempt (MTTP).



For more information, please visit:

malanta.ai