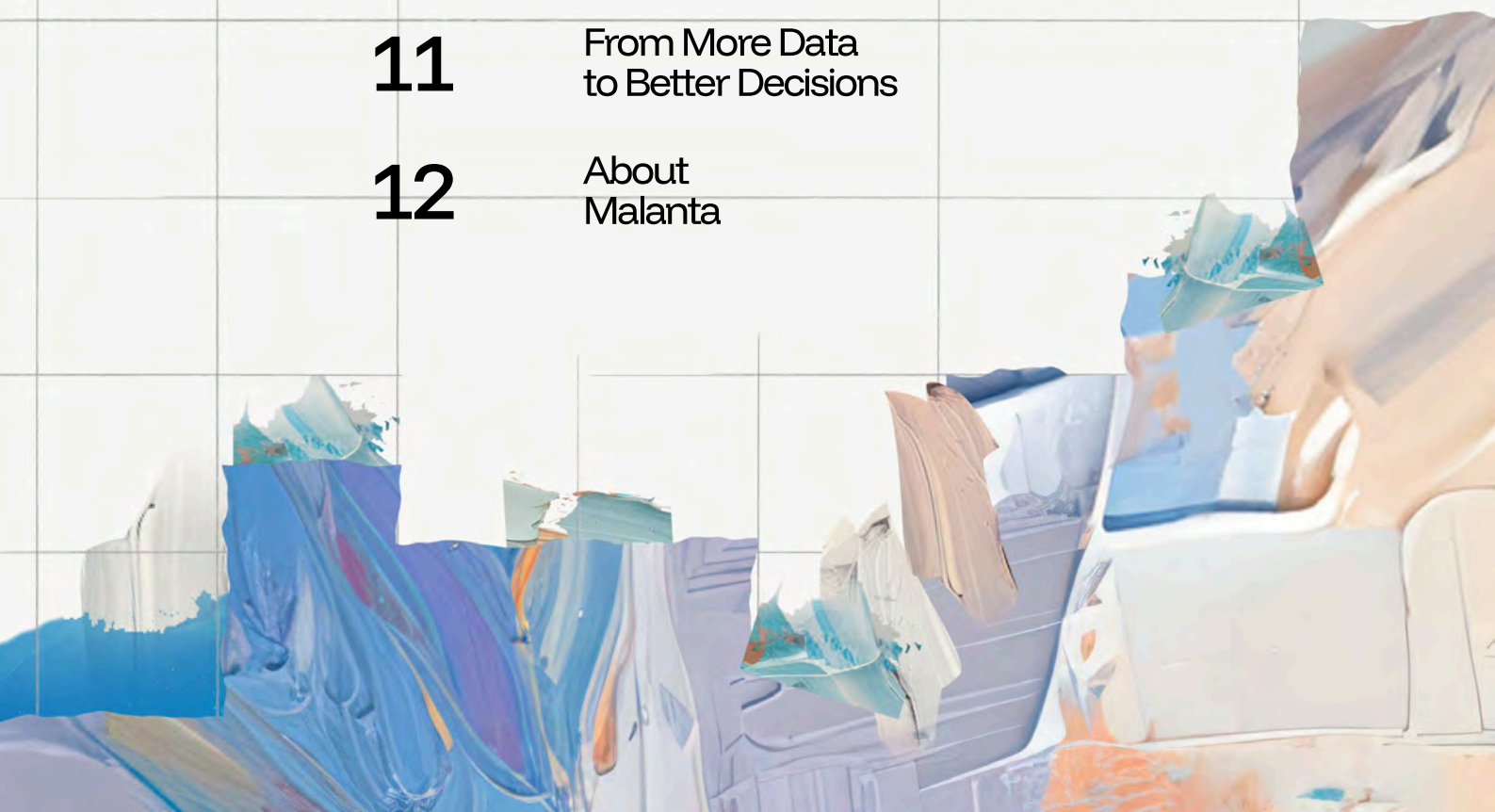
Malanta:

Contextual Risk

Prioritizing Pre-Attack Signals That Matter

A Malanta E-Book
May 2026



Executive Summary

Signals aren't the problem. Context is

Security teams are drowning in volume, not starved for data - the missing piece is the context that connects signals to real threats.

Three layers determine what actually warrants action

Not every signal is a priority. Organizational context is what separates signal from noise.

Not all signals are equal

The difference between noise and priority is whether a signal maps to something that actually matters.

Prioritization needs a process

Without a structured pipeline, high-volume signal stays inventory - it never becomes a decision.

Every attack has a setup phase

Infrastructure preparation is measurable and finite - and that window is where defenders have the most leverage.

A ranked list isn't a defense

Priority without ownership is just a sorted version of the same problem.

Breakout times are now 29 minutes

Waiting for initial access to occur means the window for effective defense has already closed.

MTTP shifts the metric from response to preemption

The clock starts when the signal appears - not when the attack does.

Indicators of Pre-Attack make attacker intent visible

The evidence exists before the attack begins - the question is whether your team is positioned to see it.

The goal is relevance, not volume

Teams that act on what matters to their organization stop financial exposure before it materializes.

Signal Overload Is Actually a Context Problem

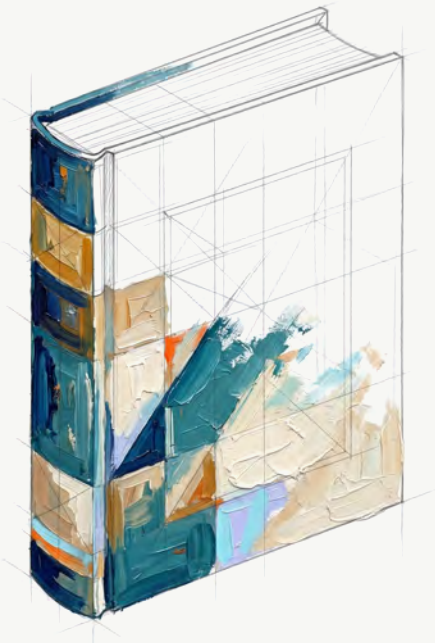
Security teams struggle with many challenges. A shortage of signals is not one of them. At some point in the past decade, the threat intelligence domain became a volume game - more feeds, broader coverage, more indicators.

A recent survey by Malanta found that most enterprises now operate five to eight feeds, with some managing as many as 53. Yet 100% of respondents identified the same breakdown point: connecting signals to real threats.

Meaning - the problem is not volume. **It is context.**

For example, a newly registered domain is a data point. A newly registered domain that shares certificate attributes with infrastructure previously used against financial services firms, and that resolves to an IP range scanning your customer portal - that is a priority data point. The difference between the two is not the data point itself. It is what the data point maps to.

We call this **contextual risk**. It's the difference between knowing a signal exists and knowing what it means for your organization. Without that distinction, teams sort through volume instead of acting on relevance. The signals that deserve immediate action often sit alongside hundreds that do not, and there is no reliable way to tell them apart.



This e-book provides a structured approach to making that distinction operational.

It covers the setup window where attackers are most exposed, how to correlate pre-attack signals to what your organization stands to lose, and how to move from prioritization to action before the window closes.

The Setup Window: Where Context Matters Most

Every attack begins with a preparation phase. MITRE PRE-ATT&CK defines this as reconnaissance and resource development - the stages where attackers register domains, provision servers, issue certificates, and configure delivery paths before any payload is deployed. We call this the setup window. **It's a finite period where attacker infrastructure is observable, and where defenders still have the leverage to act.**

Signals in the setup window surface days or weeks before execution begins. Teams can even see them. What most organizations lack is a structured way to evaluate what they are looking at. Signals land across different tools and teams without a shared framework that helps decide what is worth acting on - and without context, that framework cannot exist.

The setup window is measurable and shrinking - construct.

The CrowdStrike 2026 Global Threat Report found that the time between initial access and lateral movement dropped to just 29 minutes in 2025, a 65% increase in speed from 2024. Once an attack moves from setup to execution, that window closes fast.

What Signals Are Already Telling You

Most security teams already have access to the signals that precede an attack. We call them Indicators of Pre-Attack (IoPAs), and they fall into four primary categories:

Domain registration patterns

Naming conventions reused across campaigns, tied to specific brands, lures, or operational themes.

Certificate issuance activity

TLS certificates issued at scale to support phishing and malicious command-and-control infrastructure before any

Infrastructure placement signals

Repeated use of specific hosting providers and autonomous system numbers across operations.

Reconnaissance and identity probing

External scanning of exposed services, followed by account discovery and credential testing.

Each of these IoPAs reflects a decision the attacker made during setup - and each one carries information about what they are building and where it is aimed.

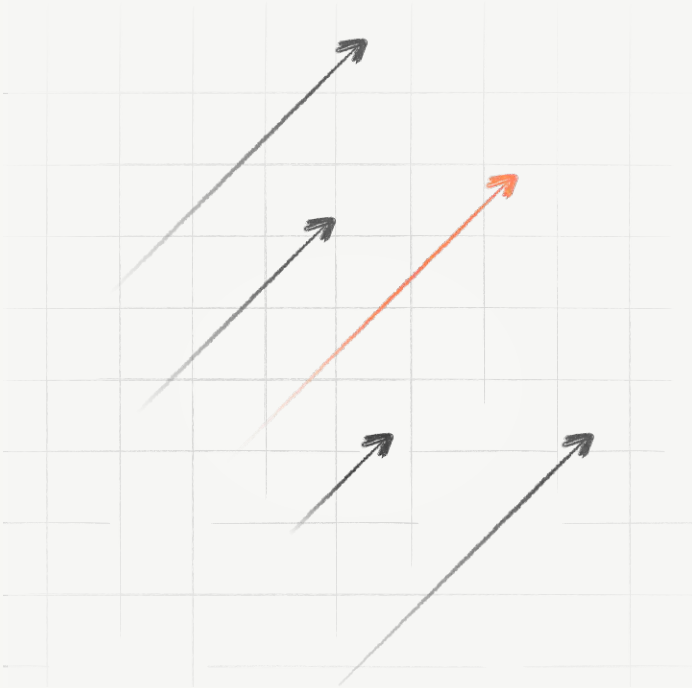
But there's a lot to sort through. For example, the Infoblox 2025 DNS Threat Landscape Report identified over 100 million newly observed domains in a single year, with more than 25 percent classified as malicious or suspicious. That is a lot of observable attacker preparation - and a lot of noise surrounding it.

Yet the takeaway is that the raw signals exist. What most teams are missing is a structured way to read them - to connect a domain registration, a certificate cluster, or a scanning pattern to attacker intent, target selection, and timing.

Correlating Signals to What Attackers are Targeting

What turns an IoPA into a priority is correlation - figuring out what the attacker is building and connecting it to what your organization actually stands to lose. **We recommend mapping correlation across three layers:**

Enterprise assets	The domains, cloud environments, exposed APIs, and internal systems that form your operational infrastructure.
Customer-facing exposure	The data flows, portals, and service paths that connect your organization to the people who depend on it.
Brand and revenue risk	The products, identities, and transaction channels that attackers impersonate or disrupt to cause financial and reputational damage.



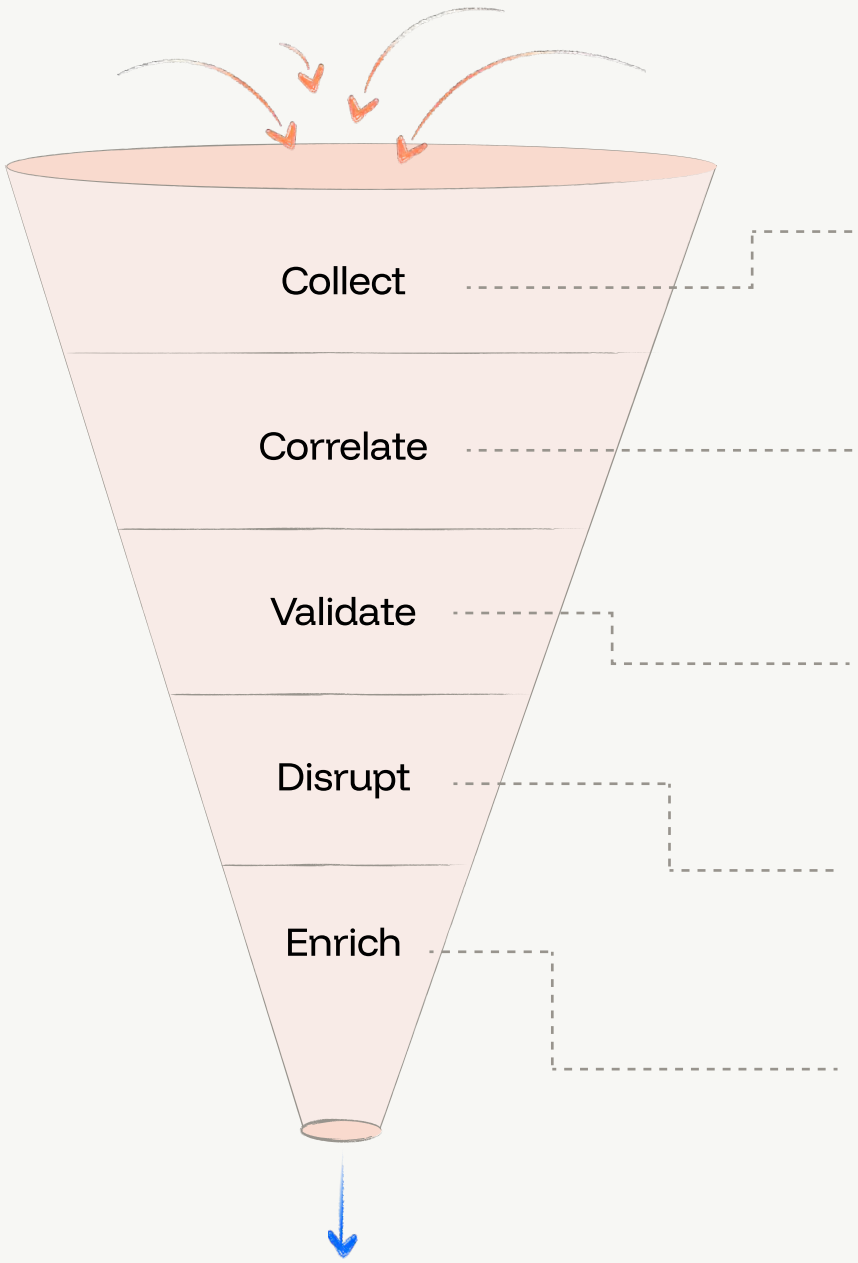
When an IoPA maps cleanly to one of those layers, its priority becomes clearer. A lookalike domain with no connection to your environment sits low on the list.

That same domain pointed at a customer login portal handling high transaction volumes demands immediate action.

A Prioritization Framework

Correlation tells you a signal is relevant to your environment. Prioritization tells you where it sits in the queue - and how fast you need to move.

To further distill prioritization, we break it down according to a five-stage model. Each stage narrows the stream of incoming signals into a focused set of validated priorities:



Signals come in from across the internet, get normalized, and are filtered against baseline criteria. Volume goes in. Qualified signals come out.

Signals get mapped to your assets, customer exposure, and revenue paths. No meaningful overlap means no further action.

Correlated signals are tested for exploitability and scored for confidence. Strong alignment with known attacker behavior moves a signal forward.

Validated signals drive action, prioritized by how close the infrastructure is to activation and what it is aimed at.

Validated intelligence feeds back into SIEM, SOAR, and TIP systems, sharpening future correlation.

By the time a signal reaches the bottom of this funnel, what remains is a small, high-confidence set of priorities - each tied to a real target. The question at that point is no longer what to act on. It is who acts, and when.

From Prioritization to Action: Closing the Ownership Gap

A prioritized signal still needs someone to act on it. This is where many teams drop the ball. Signals get evaluated, ranked...and routed into a queue that nobody owns.

The SANS 2025 SOC Survey found that 66% of teams cannot keep pace with incoming alert volumes, as things are. Add pre-attack signals to that backlog without clear ownership and defined response paths, and the attacker's infrastructure stays live.

Closing the ownership gap requires three things:

1	Defined thresholds	Clear criteria that tell your team when a signal demands immediate action and when it can be monitored.
2	Routing logic	A validated signal gets to the right person or system without manual handoffs.
3	Documented accountability	Someone who owns the decision, approves the response path, and records the outcome.

Prioritization without ownership is just a ranked list.
Context is what makes the two work together - it tells your team what a signal is aimed at, how serious that target is, and what the right response looks like.

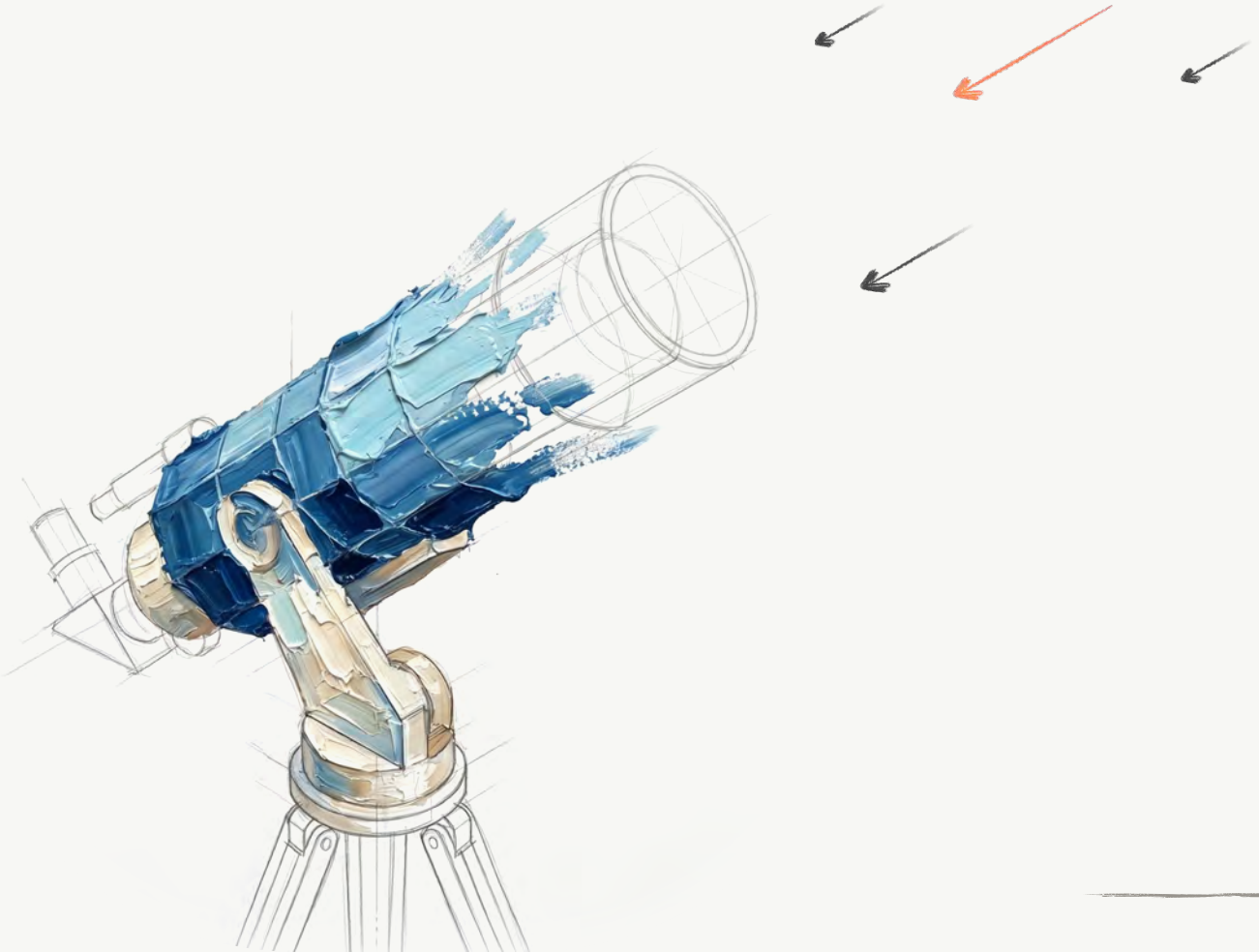
Making Contextual Risk Measurable

Prioritization and ownership solve the operational problem. The executive problem is different - how do you prove that early action is working, and what does that proof look like to a board that thinks in financial terms?

The answer starts with the right metric. Most security metrics - Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) - measure speed after the fact. They tell you how quickly your team cleaned up after an attack. These metrics accept reactivity as a given. Yet a proactive, preventative approach can be a game-changer.

At Malanta, we measure Mean Time to Preempt (MTTP) - the time between the first appearance of a pre-attack signal and the completion of a preventive action. The shorter the MTTP, the less opportunity attackers have to turn preparation into execution.

For CISOs, MTTP translates prevention into language that boards already understand. Fewer incidents, shorter disruption windows, and lower recovery costs are all downstream of a strong MTTP. Each pre-attack takedown represents financial exposure that never materialized - and that belongs in a board report alongside margin, uptime, and operational performance.

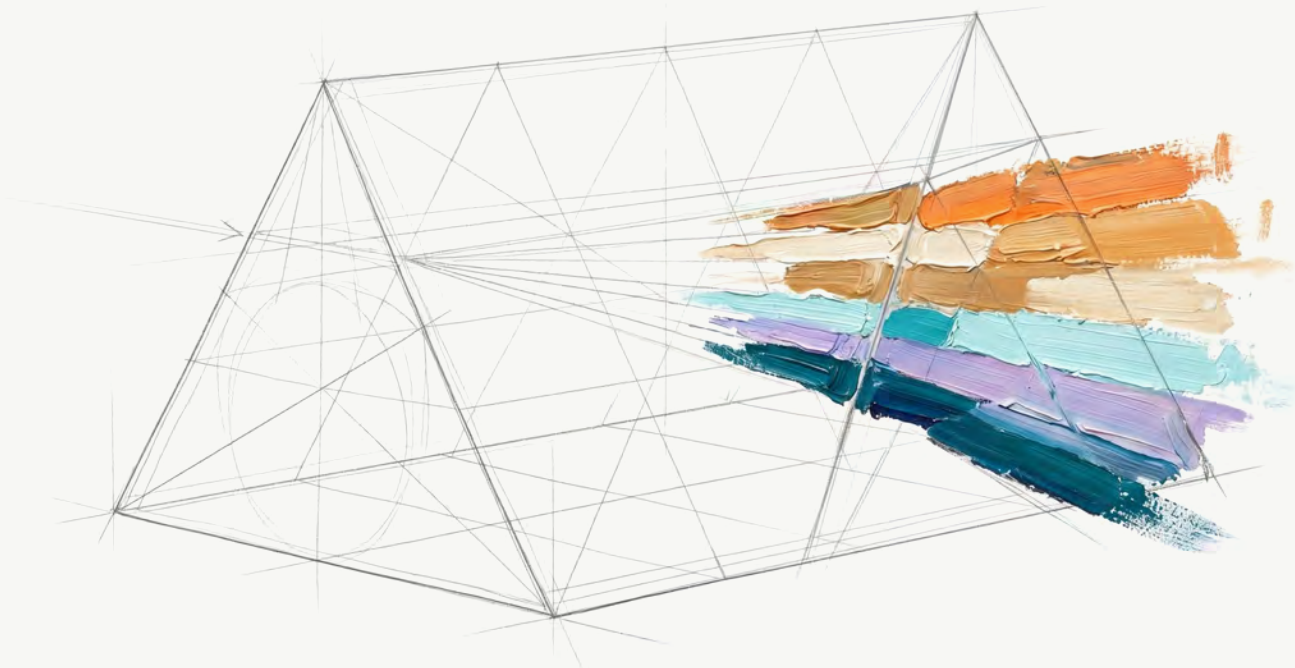


From More Data to Better Decisions

Security teams are not short on signals. What they are short on is contextual risk analysis - the ability to evaluate a pre-attack signal not just for what it is, but for what it is aimed at and what the cost would be if it reached its target.

Security teams are not short on signals. What they are short on is contextual risk analysis - the ability to evaluate a pre-attack signal not just for what it is, but for what it is aimed at and what the cost would be if it reached its target.

When pre-attack signals are correlated with high-value targets, customer data flows, and revenue streams, the flood becomes a focused stream. Teams act on relevance, not volume. The right signals reach the right people.
The setup window gets used.



More data was never the answer.

Better decisions are - and contextual risk analysis is what makes them possible.

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