Malanta

Redefining Readiness: The CISO Guide to Preventing AI Attacks

A Malanta E-Book
October 2025

Table of content

Executive Summary

Readiness can no longer wait for an alert. It needs to begin where attacks are born.

The new CISO mandate: act before execution

Defenders must shift their focus from detection to disruption—identifying attacker intent early and stopping threats before they turn into active attacks.

The readiness gap now defines risk

Exposure grows in the time between attacker setup and defender action. Closing that gap ensures fewer attacks succeed or reach operational systems.

Traditional tools see only fragments

Threat intelligence teams often rely on multiple threat feeds and industry alerts, analyzing them manually. The lack of automation and integration across sources leaves blind spots where AI-driven attacks can take shape.

Integrated prevention sustains readiness

Integrating validated Indicators of Pre-Attack (IoPAs) into SOC, SIEM, and SOAR workflows embeds prevention into daily defense and keeps it continuous.

AI has redrawn the boundaries of defense

AI compresses reconnaissance, setup, and launch into minutes, forcing defenders to act earlier and faster than traditional detection allows.

Setup is now the optimal point of control

Detecting attack infrastructure as it forms allows defenders to dismantle threats before execution and completely eliminate impact.

Pre-attack prevention redefines readiness

Pre-attack prevention detects and dismantles attacker infrastructure while it is still being built, giving defenders the ability to intervene before execution and eliminate risk at its source.

Making readiness measurable

Success is defined by Mean Time to Preempt (MTTP) – the time between adversary setup and defender action – showing how quickly threats are neutralized before activation. Readiness can no longer wait for an alert. It needs to begin where attacks are born.

Introduction: The New Battleground

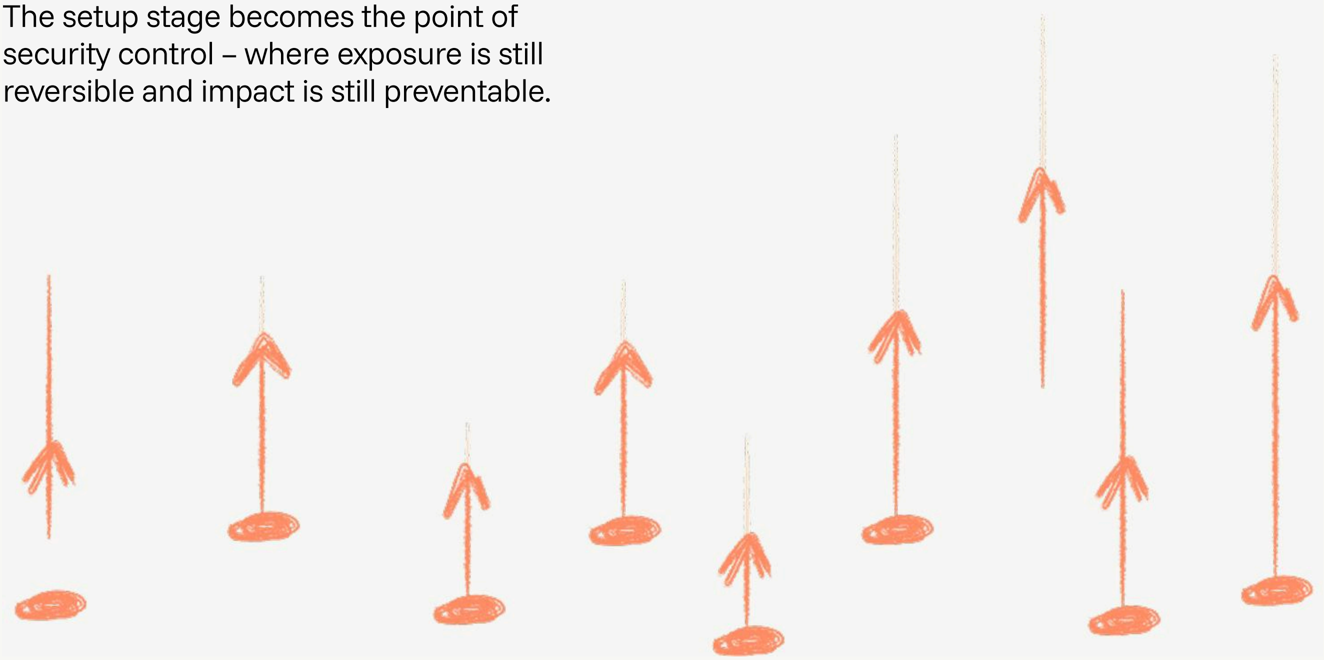
AI has changed the speed of attack. What once took days of setup now happens in minutes. Automated systems can scan for weaknesses, register domains, and spin up entire command infrastructures before most defenders notice a thing. Yet many security programs still begin at detection. By the time the first alert fires, the attack is already in motion.

This gap – between attacker speed and defender readiness – is where the next generation o cybersecurity must focus. The earliest phases of an attack (defined by MITRE PRE-ATT&CK as 'reconnaissance and resource development') have long been considered untouchable. Most teams assume that nothing can be done until the first compromise occurs.

That assumption no longer holds.

Pre-attack prevention fundamentally changes howdefense works. It identifies and removes attacker infrastructure while it is still being built. Teams can act before execution begins and contain threats at their source. Visibility shifts to what is forming instead of what has already happened. The setup stage becomes the point of security control – where exposure is still reversible and impact is still preventable.

This e-book explores how AI is reshaping the threat landscape, how pre-attack prevention redefines readiness, and how CISOs can turn prevention into a measurable, repeatable discipline. The takeaway is simple: you can prevent what you once thought was unpreventable.



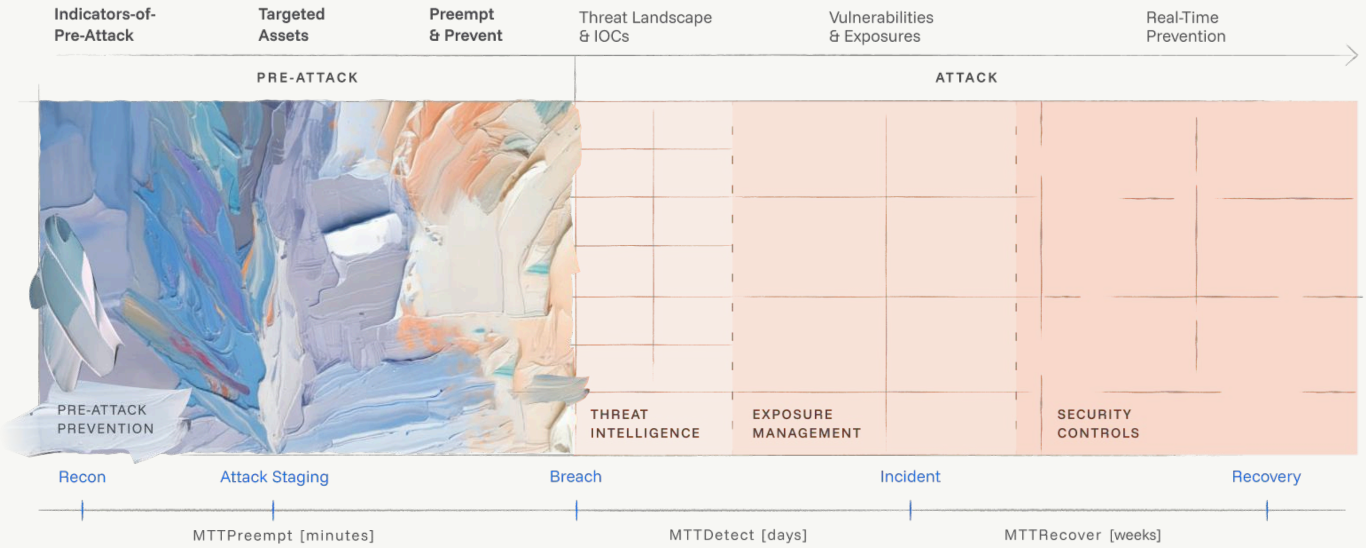
The AI-Accelerated Threat Landscape

AI has redefined how attacks are built. Machine-learning models now handle reconnaissance, mapping, and setup automatically. Algorithms scan DNS records, domain registrations, and internet-wide telemetry to identify exploitable assets in real time. Generative tools create fake portals, cloned brands, and adaptive phishing kits that evolve with every interaction.

What once required coordinated teams now runs on autopilot. A single AI agent can register, test, and deploy thousands of domains within minutes.
These systems learn as they go, adjusting payloads, updating infrastructure, and scaling attacks continuously.

Despite this, most defense paradigms still treat attacks as linear events that begin with detection. In reality, AI merges setup, launch, and execution into one process. This compression widens the readiness gap – the time between adversary setup and defender awareness.

To close it, organizations must act at the same stage where AI operates best: the setup phase. This is the only point where prevention can move as fast as the threat itself.



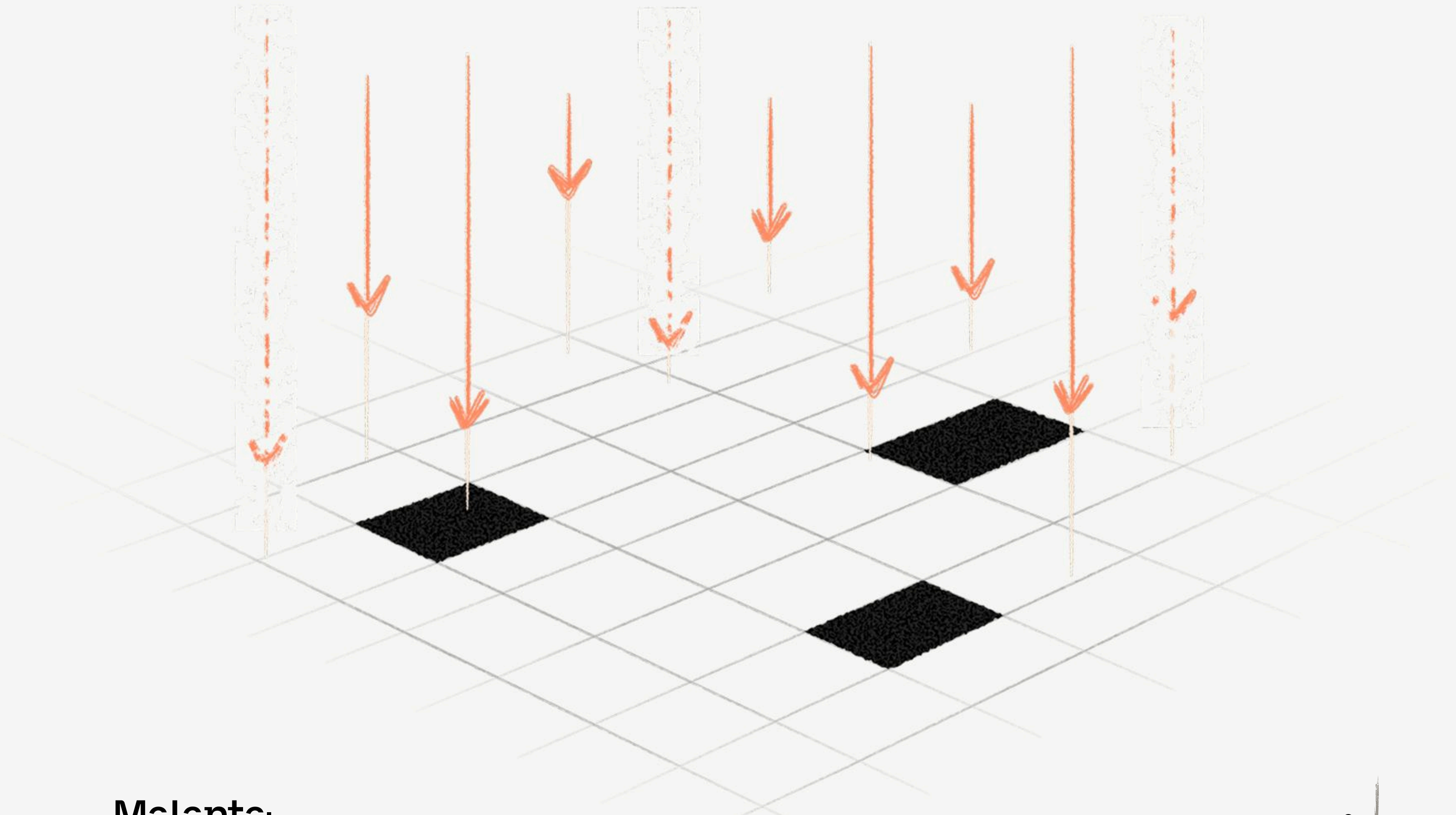
The Limits of Detection and Visibility

The readiness gap exists because today's security systems activate too late. Most workflows depend on Indicators of Compromise (IoCs) that appear after an attack begins. SIEM and SOAR tools organize that data efficiently, yet they only describe what has already happened.

Threat intelligence and external attack surface management each contribute partial visibility. One tracks adversary behavior across the internet. The other maps exposed enterprise assets.
Yet these systems rarely align their insights. Analysts must reconcile them manually, filtering false positives while attackers continue building unseen.
The result is a reactive cycle –
a disconnect between external threat data and internal asset visibility.

AI-driven operations exploit this. Automated reconnaissance and resource development unfold before any alert exists, leaving traditional defenses with no entry point.

Pre-attack prevention bridges this gap. It correlates external reconnaissance with internal exposure data to reveal where attacker setup intersects with enterprise assets, brands, and customers. This connection turns fragmented data into actionable insight and moves defense to the only stage where prevention is still possible.



The Pre-Attack Prevention Framework

The pre-attack prevention framework is a focused process that detects, validates, and removes adversary infrastructure before it ever turns hostile. The five-stage process includes:

Collect

Gather reconnaissance and staging data from across the internet. This includes new domain registrations, DNS artifacts, and early command-and-control activity that signals attacker setup in progress.

Correlate

Connect those Indicators of Pre-Attack (IoPAs) to your own environment. Mapping them to corporate domains, brands, and customer assets reveals where attacker intent meets business risk.

Validate

Confirm which signals matter. Automated analysis tests exploitability and filters out false positives so teams focus only on credible threats.

Prevent

Dismantle attacker infrastructure before launch. Registrar actions, provider takedowns, and automated interdictions remove the threat at its source.

Enrich

Feed verified intelligence into existing systems - SOC, SIEM, and SOAR - to strengthen daily operations with live prevention data.

> When these steps run as a loop, defense becomes proactive by definition. The result is readiness defined by prevention, not reaction.

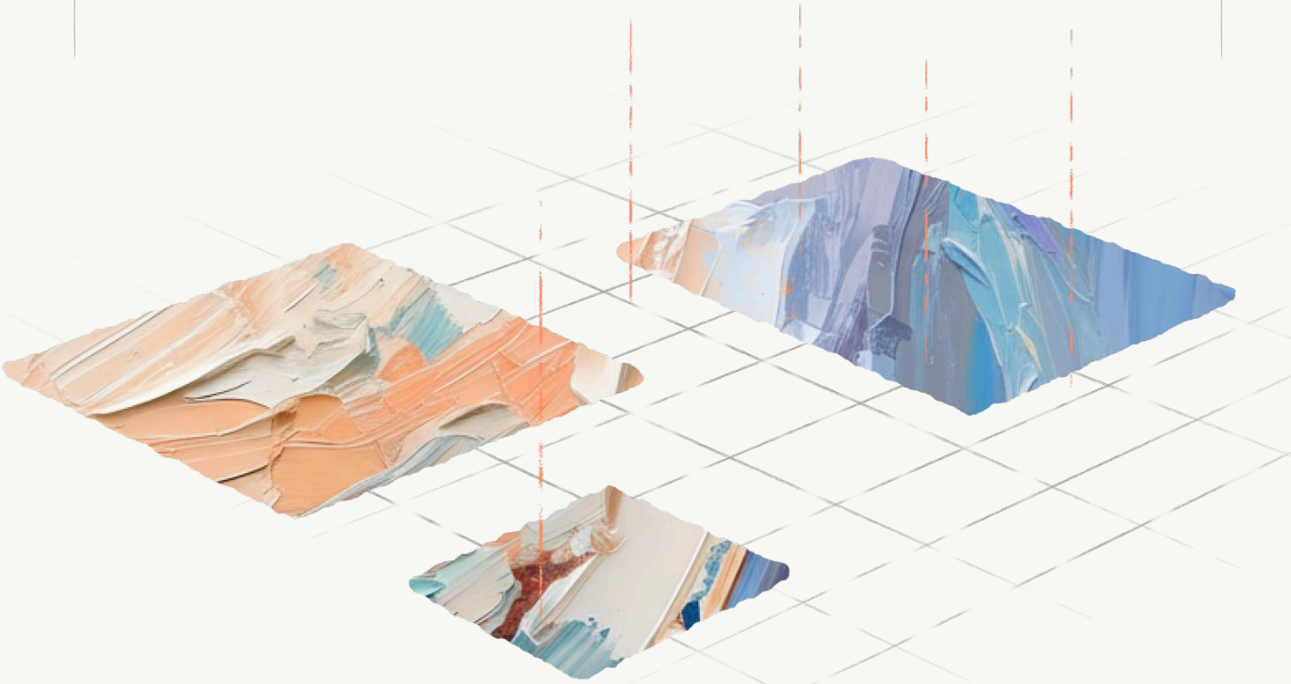
Introducing A New Metric: Mean Time to Preempt (MTTP)

Most security metrics tell the story after the fact. Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) measure how fast teams clean up, not how early they act. That focus made sense when every defense started at detection. It no longer fits a world where AI-driven attacks move faster than any response plan.

Mean Time to Preempt (MTTP) changes that focus. It measures the time between spotting adversary setup activity and shutting it down. The shorter the MTTP, the less opportunity attackers have to turn preparation into action.

MTTP gives leaders a way to prove that prevention works. It links early visibility to real outcomes – fewer incidents, shorter dwell times, and lower recovery costs. It also supports governance needs under frameworks like NIST AI RMF and the EU AI Act by showing clear evidence of control at the setup stage. Over time, MTTP becomes both a performance metric for security teams and a governance metric for the business as a whole.

Mean Time to Preempt (MTTP) changes that focus.



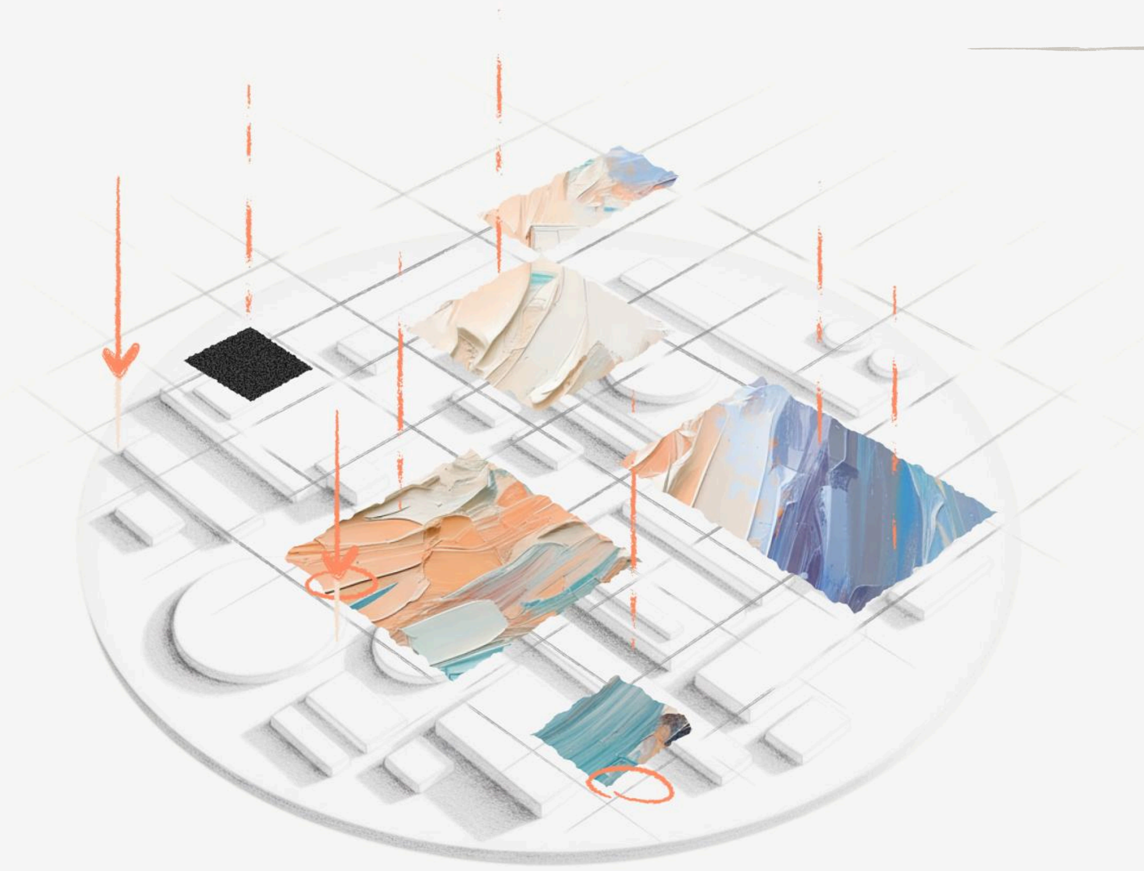
Embedding Prevention into Security Operations

Pre-attack prevention is most effective when it operates inside existing security workflows. Integrating validated pre-attack intelligence into SOC, SIEM, and SOAR workflows turns prevention into part of the normal cycle of defense.

Today, SecOps run in sequence. External threat intelligence identifies indicators. Analysts validate them manually, pass results to incident response teams, and rely on SIEM rules to trigger action. Each step depends on the previous one. The process moves slowly, and visibility fades between handoffs.

With pre-attack prevention in place, that sequence becomes a loop. External reconnaissance connects directly with internal telemetry. Pre-attack indicators flow through standard workflows, with automation both validating relevance and triggering intervention. Results from each action feed back into analysis, improving accuracy and response over time.

Readiness becomes easier to measure, too. Metrics such as Mean Time to Preempt (MTTP) show how quickly infrastructure is identified and removed before activation. Progress is visible and repeatable – evidence that prevention is operating as an effective part of daily defense.



Lessons from the field

Malanta is already having a significant real-world impact at the Israel National Cyber Directorate (INCD).

Leveraging Malanta's Indicators of Pre-Attack (IoPAs), INCD identified and dismantled real adversary infrastructure targeting hundreds of Israeli companies across multiple sectors.

By intervening at the setup stage, INCD was able to detect, validate, and dismantle attacker infrastructure before it became operational.

This proactive approach limited exposure, prevented potential disruption across critical sectors, and demonstrated how pre-attack prevention delivers measurable, repeatable results at scale.

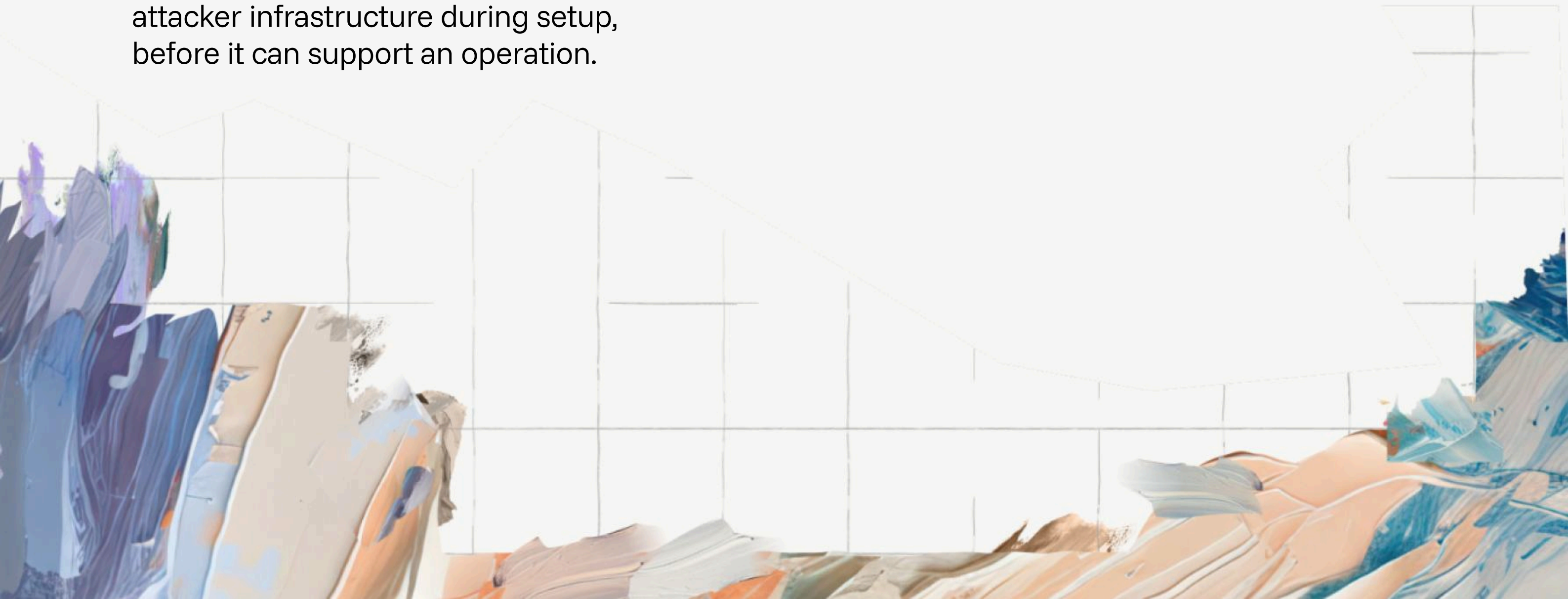
The Takeaways

AI has changed how attacks form and how defense must respond. Setup and execution now unfold in parallel, granting attackers the momentum and leaving defenders little time to react.

Traditional security tools were designed for a slower threat environment – one defined by detection and response.

Pre-attack prevention meets the new tempo by identifying and dismantling attacker infrastructure during setup, before it can support an operation.

This change reframes what readiness means. Instead of measuring speed after compromise, security teams measure how quickly they detect intent and defuse it. For CISOs, this is the moment to redefine control. The advantage belongs to organizations willing to act first and make prevention the core of their security practice.



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 contact us at Hello@malanta.ai