Malanta:

Operational Pre-Attack Playbooks

Turning Early Signals into Fast, Defensible Action

A Malanta Operational Briefing
February 2026

Executive Summary

Attack timelines have collapsed

Adversaries now register infrastructure, provision tooling, test access paths, and launch campaigns at machine speed. AI-assisted operations compress what used to take weeks into minutes. In this environment, reacting after execution is no longer a sufficient control model.

Security teams already see early indicators of this activity. Domains, certificates, scans, and access probes appear well before an attack is launched. The problem is not visibility. The problem is that these signals lack a defined operational path.

Early signals arrive fragmented across tools. No shared thresholds determine what matters; No ownership exists for deciding when to act.

As a result, attacker infrastructure often remains live until it is actively used.

This ebook introduces Operational Pre-Attack Playbooks: a practical, SOC-native model for turning early attacker signals into enforceable action during the setup phase. It defines workflows, analyst decision points, response paths, and KPIs that allow teams to disrupt adversary infrastructure before first contact.

Malanta provides the platform layer that enables these playbooks to run at scale, integrated into existing SOC workflows and controls.

The Operational Shift:
From IOC Response to IoPA Prevention

Traditional SOC operations are built around Indicators of Compromise (IOCs). These are forensic artifacts of attacks that have already occurred: malware hashes, confirmed phishing domains, exploited credentials, command-and-control traffic.

Pre-attack prevention focuses on Indicators of Pre-Attack (IoPAs). These are observable artifacts of attacker setup activity that appear before execution.

IOC-Driven Model	IoPA-Driven Model
Evidence after compromise	Evidence during setup
Control point: detection & response	Control point: infrastructure staging
Metrics: MTTD / MTTR	Metric: MTTP
Scope: single indicator or actor associated	Scope: Infrastructure-level disruption

This model aligns directly with the Resource Development (TA0042) phase of the MITRE ATT&CK framework, where adversaries assemble domains, certificates, infrastructure, and tooling.

By shifting the SOC's control point to this phase, defenders regain initiative. Instead of containing damage, they disrupt capability.

What Qualifies as a Pre-Attack Signal

Not all early signals are actionable. Most internet activity is noisy and benign. IoPAs are signals that meet three criteria:

They represent attacker setup activity that has preceded real attacks.

They align with known attacker tradecraft or reuse patterns.

They show relevance to the organization or its exposed surface.

Core IoPA Signal Families

Brand and impersonation setup

- Lookalike domain registrations.
- Early MX, DNS, or TLS configuration.
- Certificate issuance prior to campaign activation.

Staged social engineering infrastructure

- Hosted phishing kits and landing pages.
- Credential harvesting frameworks not yet used.
- Template and infrastructure reuse across campaigns.

C2 and tooling staging

- Provisioned servers associated with known malware frameworks
- Reuse of certificates, ASNs, or hosting providers
- Infrastructure patterns observed before prior attacks

On their own, these signals are ambiguous. They only become operational when evaluated through a structured workflow that establishes relevance, readiness, and actionability.

SOC Pre-Attack Workflow

Pre-attack prevention operates as a dedicated SOC lane. It mirrors how analysts already work and introduces explicit decision points that drive action.

Objective and Scope

Objective

Detect, validate, and disrupt adversary setup activity before it becomes operational.

Scope

- Defensive actions only
- Internal control changes, blocking, and lawful external coordination
- Fully auditable and governed

This workflow runs alongside detection and response. It does not replace them.

Workflow Overview

The pre-attack lane follows four SOC-native stages. Each stage represents a concrete analyst decision point and feeds directly into existing security operations.

S0: Ingest and Normalize

Signals are ingested from threat intelligence feeds, DNS telemetry, certificate transparency logs, scanning data, and external infrastructure monitoring.

Actions

- Deduplicate by entity (domain, IP address, certificate)
- Normalize attributes across sources
- Enrich with ownership data, timing, and infrastructure characteristics

Outcome

A clean, structured intake of candidate Indicators of Pre-Attack (IoPAs) ready for evaluation.
Malanta supports this stage by consolidating and enriching disparate pre-attack telemetry into a single operational intake, reducing manual aggregation and noise.

S1: Validate Target Alignment

“Is this about us?”

At this stage, analysts determine whether the signal meaningfully aligns with the organization.

Validation criteria

- Brand similarity or impersonation indicators
- Alignment with corporate domains, services, or identities
- DNS, MX, or TLS configuration consistent with targeting
- Infrastructure timing that suggests preparation rather than coincidence

Signals that fail alignment are retained for pattern analysis but do not advance.

Outcome

A reduced set of IoPAs that plausibly target the organization.

Malanta accelerates this step by correlating signals against brand assets, domains, and known exposure points, while leaving final judgment with the analyst.

SOC Pre-Attack Workflow

S2: Assess Imminence and Exploitability

“Is this ready to be used?”
Validated IoPAs are assessed for operational readiness and urgency.

Assessment factors

- Completeness of infrastructure setup
- Evidence of tooling or credential harvesting readiness
- Proximity to known execution patterns
- Potential impact if activated

For example, a fully configured phishing site with valid certificates and mail infrastructure carries higher urgency than a parked lookalike domain.

Outcome
Prioritized IoPAs with a clear understanding of likelihood and impact.

Malanta supports this stage by evaluating infrastructure maturity, reuse patterns, and behavioral alignment observed across campaigns.

S3: Decide Action Path

Based on confidence and priority, the SOC selects an action path:

- Immediate internal blocking and hardening
- Coordinated external disruption
- Continued monitoring with defined escalation criteria
-

Ownership, approval requirements, and evidence thresholds are predefined to avoid hesitation or inconsistency.

Outcome
A defensible, auditable decision that moves directly into execution.

Malanta routes validated IoPAs into the appropriate enforcement or investigation of workflows based on policy.

Response Runbooks

Execution follows standardized runbooks tied directly to S3 decisions.

Runbook A: Block and Harden Internally

- Block domains, IPs, and URLs across DNS, email security, and secure web gateways
- Increase authentication friction for targeted users
- Update brand protection and user-facing warnings

Used for high-confidence signals where internal controls are sufficient.

Runbook B: External Disruption

- Submit registrar, hosting, or CDN abuse requests
- Attach evidence bundles from validation stages
- Coordinate with legal and communications teams when brand impact is likely
- Track takedown outcomes and timelines
-

Used when attacker infrastructure must be dismantled outside the organization.

Runbook C: Campaign-Level Clustering

- Expand from a confirmed IoPA to related infrastructure
- Identify shared certificates, naming patterns, hosting ASNs, or configuration reuse
- Disrupt multiple assets associated with the same operation

Used to degrade attacker capability at the campaign level rather than treating individual indicators.

Measuring Success

Pre-attack prevention requires different metrics than traditional response.

Key KPIs

- Mean Time to Preempt (MTTP): time from IoPA observation to disruption
- Time to validate IoPA (S0 → S1)
- Time to disrupt (S2 → execution)
- Campaign-level disruption rate
- Reduction in downstream phishing and credential abuse incidents
-

These metrics quantify avoided risk and demonstrate the operational value of early action.

30-60-90 Day Adoption Plan

First 30 Days

- Define IoPA signal families relevant to the organization
- Assign ownership for validation and enforcement
- Establish governance and approval paths

Next 60 Days

- Operationalize the S0–S3 workflow
- Integrate enforcement controls
- Begin tracking MTTP and validation metrics

Within 90 Days

- Automate low-risk actions with human oversight
- Formalize audit trails and reporting
- Align workflows with governance frameworks such as NIST CSF 2.0

Closing

Pre-attack signals already exist in your environment. The difference between seeing them and acting on them is operational structure.

Operational Pre-Attack Playbooks provide that structure. Malanta enables teams to execute these workflows at scale, inside existing SOC operations, with speed, precision, and accountability.

The result is a SOC that disrupts attackers before they act.

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.