Look Left.

Where Pre-Attack Intelligence Fit in Today's Security Stack

A Practical Comparison for Security Leaders

The Stack You Inherited

Most enterprise security stacks have grown to the right over the years. Driven by vendor release cycles and incident-driven procurement – stacks have threat intel feeds, dark web monitoring, DRP and SIEM/SOC tooling well covered.

Still, vendors keep selling layers that look different but operate in the same after-the-fact, post-execution window. And still, threats from the left of the kill chain - where attackers register their domains, provision their servers, issue their certificates, and stage their delivery paths - go unchallenged for days or weeks before execution begins.

Like new visitors to London, security leaders are learning to look to the left of the traditional kill chain. But questions remain. Where does pre-attack intelligence actually sit relative to the tools already in place? What does it replace? What does it complement?

This guide compares four established categories - traditional threat intelligence feeds, dark web monitoring, digital risk protection, and SIEM/SOC tooling - against pre-attack intelligence across a shared set of criteria: what each category sees, when it sees it, what action it enables, and where it falls short.

The Comparison Matrix

	Traditional TI Feeds	Dark Web Monitoring	Digital Risk Protection	SIEM / SOC Tooling	Pre-Attack Intelligence
WHAT IT SEES	IOCs from past incidents	Stolen credentials, breach data, actor chatter, leaked documents	Lookalike domains, brand impersonation, executive spoofing, leaked content	Internal logs, endpoint telemetry, network traffic, correlated events	Attacker infrastructure during staging: domain registrations, certificates, hosting patterns, scanning, C2 setup
WHEN IT SEES IT	Post-campaign - after activity has played out	Post-breach - after data exfiltration or compromise.	Mid-to-late stage - after fraudulent assets are live and reachable	Post-execution – after attacker reaches internal systems	Pre-execution - Days or weeks before the attack begins
WHAT ACTION IT ENABLES	IOC matching, blocklist updates, alert enrichment, attribution	Credential resets, exposure assessment, incident scoping	Takedown requests, brand alerts, spoofed identity flags	Alert triage, investigation, incident response, automated playbooks	Infrastructure takedowns, preemptive blocking, IoPAs routed into SIEM/SOAR/TIP
NIST CSF MAPPING	Detect, Respond	Detect, Respond	Detect, Respond	Detect, Respond, Recover	Identify, Protect
PRIMARY LIMITATION	Retrospective by design - feeds describe what already happened	Forensic by nature - monitors the aftermath of breaches	Calibrated for harm that is already visible - sees impersonation after it goes live	Operates inside the perimeter - no visibility into external attacker infrastructure	Covers the setup phase only - detection and response tools still necessary for threats that reach execution

Traditional Threat Intelligence Feeds

Feeds are the backbone of most threat intelligence programs. They deliver a steady stream of IOCs pulled from incidents across the industry. Teams match these to internal telemetry, tune detection rules, build blocklists, and tie activity to known actors.

The catch is that every IOC in a feed exists because a compromise already happened. A malicious campaign ran, researchers catalogued the artifacts, and the feed distributed them. That timeline makes feeds indispensable for recognizing threats that are already in circulation… yet blind to threats that are clearly taking shape.

AI-Powered Pre-Attack activity

In June, 2026, Anthropic dropped a study that will shape how security leaders talk about AI-powered threats for the next year. 832 banned accounts. 13,873 attack technique observations. 12 months of data. Mapped onto MITRE ATT&CK v18. They released an interactive navigator with per-technique risk scores and actor counts.

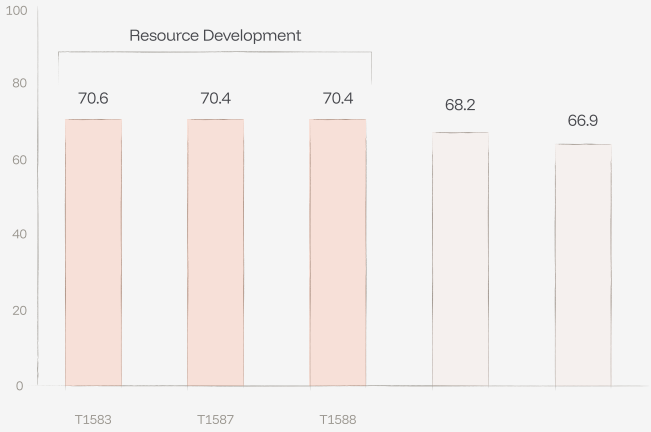
Pre-attack intelligence works with some of the same data types as TI feeds – notably domains and IPs. But it reads them at the opposite end of the timeline. It flags malicious assets while they are being assembled, parsing signals that TI feeds were never designed to track: certificate issuance, hosting patterns, and staging behavior.

Threat intelligence feeds tell you what already happened. Pre-attack intelligence tells you what's being built to happen next.

Observation 1 - Risk

Of the top 5 highest-risk techniques are Pre-Attack T1583 (70.6), T1587 (70.4), T1588 (70.4). Resource Development dominates the risk leaderboard.

Source :
https://www.anthropic.com/research/attack-navigator
https://www.anthropic.com/news/AI-enabled-cyber-threats-mitre-attack



Dark Web Monitoring

Dark web monitoring made sense when the major criminal forums were still active. But government seizures have driven the most sophisticated actors into encrypted channels and invitation-only communities that no security vendor can reliably crawl. The forums that remain are dominated by recycled breach dumps and low-level resellers.

And even when dark web coverage did surface something relevant, it could only ever show intent - what someone claimed to be planning, somewhere, at some point.

Pre-attack signals are concrete - domain registrations, certificate issuance, hosting configurations, DNS activity - evidence that an attacker is actively building, not just talking.

Dark web monitoring captures what actors say they plan to do (if they're even still there). Pre-attack intelligence captures what they are already building.

Digital Risk Protection and Brand Monitoring

DRP and brand monitoring share more ground with pre-attack intelligence than any other category in the stack. These tools catch lookalike domains, brand impersonation, spoofed executive profiles, leaked content and other brand violations. And for many organizations, they remain the closest thing to an outside-in view of risk.

The key difference between DRP, brand monitoring and pre-attack intelligence is timing. DRP picks up impersonation after the fraudulent asset is live and reachable a cloned login page, a spoofed social account, a fake app listing.

Brand monitoring detects unauthorized use of logos, trademarks, and brand assets after they appear in the wild. For both, detection is ex post facto - after the damage to customers or brand reputation is already happening.

Pre-attack intelligence works earlier in the timeline - when the domain is registered, the certificate is issued, the hosting is configured. It maps those signals to your assets, validates the threat, and enables takedown before any customer or employee is exposed.

DRP tells you someone is already impersonating your brand. Pre-attack intelligence tells you someone is getting ready to.

SIEM/SOC Tooling

Every other category in this guide - TI feeds, dark web monitoring, DRP - feeds into the SIEM. So, what changes when you add pre-attack intelligence to the stack? Aside from more effective alerts, faster triage, and fewer wasted analyst hours - not a lot.

Your SIEM works the same way it always has - it processes, correlates, and surfaces whatever arrives. Of course, since it does not generate the intelligence itself, it's only as good as the intelligence behind it. And today, almost everything behind it is oriented toward the same moment: after an attack is already in motion.

The detection and correlation work perfectly, but the signal arrives after the window for prevention has closed.

When validated Indicators of Pre-Attack (IoPAs) start flowing in, alerts show up earlier in the timeline, detection rules reflect what's actually active in the threat landscape, and analysts get cases with more context and less guesswork. The SIEM stays the same. What it processes gets better.

Your SIEM processes whatever it receives. Pre-attack intelligence changes what that is.

How These Layers Work Together

No category in this guide replaces another. Each is positioned at a different point on the attack timeline. Each does something the others cannot.

What changes when pre-attack intelligence enters the stack is that the timeline itself expands. TI feeds, dark web monitoring, DRP, and SIEM/SOC tooling have got the post-execution window covered. Pre-attack intelligence extends coverage to the left - into the days or weeks when attacker infrastructure is being assembled.

The result is that validated IoPAs flow downstream into the tools already in place: TI platforms get better indicators, SIEM detection rules reflect infrastructure that is active right now, and SOAR playbooks can initiate takedown or blocking before an analyst ever opens a case.

With pre-attack prevention, the rest of the stack gets a longer runway to work with. Because the coverage gap in most security programs is not between categories. It is the open window to the left of all of them.

Pre-attack intelligence does not replace your stack.
It extends the timeline your stack can see.

Observation 2 - Usage

Combining all TA0042 and TA0043 technique observations from the navigator dataset:

Source :
https://www.anthropic.com/research/attack-navigator
https://www.anthropic.com/news/AI-enabled-cyber-threats-mitre-attack

69%

OF ALL ACTORS USED AI FOR DEVELOP CAPABILITIES (T1587)
574 of 832 actors. The single most common parent technique in the entire dataset.

57.9%

OF ALL ACTORS USE AI TO ACQUIRE INFRASTRUCTURE
482 actors acquiring domains, VPS, web services, servers.
T1583 ranks #5 among parent techniques by actor count and #2 in adjusted risk (70.6).

Decision Framework: Where to Invest First

Not every stack has the same gaps. Answer these four questions to help you find yours:

How much of your TI feed output actually reaches an analyst's workflow?

If most indicators are ingested and never acted on, start by consolidating your feeds, improving your enrichment, and tightening your SIEM correlation rules. Once your feeds are delivering clean, actionable IOCs, pre-attack intelligence is the natural next step - extending visibility into the setup phase that feeds were never designed to cover.

When was the last time dark web monitoring led to a concrete defensive action?

If nothing comes to mind, consider redirecting your dark web coverage budget. The forums that once made dark web monitoring essential have largely been seized or abandoned. The signals that lead to concrete action now live elsewhere – often on the open internet. That is pre-attack prevention territory.

The enhancements your stack needs depend on which window you are trying to close.

Does your organization have an outside-in view of brand risk?

If impersonation and lookalike domains are reaching customers before your team sees them, get DRP in place to catch live abuse and initiate takedowns. Once that coverage is running, the next question is whether you can see fraudulent infrastructure before it goes live - during assembly, not after deployment. That is where DRP ends and pre-attack intelligence begins.

Where does your post-mortem trail end up?

If incident reviews consistently uncover attacker infrastructure that was visible days or weeks before the first alert, the gap is not in your response. The signals were there. The stack just had no way to reach them in time. Adding pre-attack intelligence to your stack means those signals get caught on the way in - and the infrastructure gets taken down before there is a post-mortem to write.

Look Left

Nothing in your stack is broken. TI feeds, dark web monitoring, DRP, and SIEM/SOC tooling - each does what it was designed to do. The problem is that what they were designed to do happens to the right of the timeline - after the attack is in motion.

It's time to start looking left to the pre-attack window. These are observable, actionable signals – and they're happening right now. Attacker infrastructure takes shape for days or weeks before attacks launch, yet the tools most organizations rely on have no way to see it, let alone shut it down.

This window is where Malanta operates. The platform detects attacker infrastructure during setup, validates it against your environment, and takes it down before execution begins. In London, looking left keeps you safe. In cybersecurity, it keeps you ahead.

Start preventing attacks before they launch.

GET ACCESS TO MALANTA TODAY