The between-reports problem: why security teams miss what attackers see

BY GREG JENKINS · JULY 20, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/blog/business-insights/why-security-teams-miss-what-attackers-see

What you will learn

- Why faster discovery and higher volume can still leave teams blind between vulnerability reports.
- Why scanners and inventories are necessary, but not enough to explain attacker focus and intent.
- What "between-reports visibility" actually means (without the product pitch).
- What we believe security teams will need next: earlier signals that support action before the next report lands

Over the last few weeks, we've explored what AI is changing in security: discovery is faster, volume is higher, and the human layer, triage, judgment, and prioritization has become more important, not less.

There's a deeper implication hiding underneath all of that. Most security teams still only learn from successful outcomes. A vulnerability report lands, a scanner flags something, an incident forces attention, and only then do we feel like we "know" what's going on. Everything in between is where the blind spot grows.

The between-reports problem

Most security programs are designed around what can be proven and counted:

- Assets we already know
- Findings that are already confirmed
- Reports that are already submitted

Those are essential. They're also often the end of the story. Attackers don't start with "reportable vulnerabilities." They start with intent:

- What looks interesting
- What feels misconfigured
- What seems forgotten
- What can be chained
- What is reachable from the internet *right now*

That intent rarely shows up as a clean alert. But it shapes what happens next.

So the question isn't just "What did we confirm?" It's also: "What is being explored before anyone can prove it?"

Scanners don't see intent; they see surfaces

Let's be clear: asset inventories, Attack Surface Management and External Attack Surface Management (ASM/EASM), and scanners are foundational. They answer an important question of what we can detect and scan. The gap is that security teams also need a different question answered between vulnerability reports. And that question is **'What are threat actors paying attention to right now, and what is drifting out of our control?'**

Because threat actors don't behave like scanners. They don't enumerate for completeness. They explore for advantage. When your visibility is built around scan coverage and confirmed outcomes, you can miss earlier signals such as:

- Where researchers concentrate effort
- Which paths keep getting explored (even when no vulnerability is submitted yet)
- Which assets keep resurfacing because they "feel exploitable"
- Which parts of the surface are effectively untouched (no attention, no meaningful signal)

That's the between-reports problem. The "work in progress" on your external exposure is largely invisible, right up until it isn't.

The reality gap: documented scope vs. what is actually exposed

Even in well-governed programs, "what's documented" and "what's reachable" drift apart quickly:

- M&A leftovers and forgotten domains
- Shadow environments and orphaned subdomains
- Exposed admin panels or internal tools
- Misconfigurations and third-party glue (SSO redirects, OAuth boundaries)

Most of these don't show up as a clean red flag. They show up as soft signals, often noticed first by humans doing real exploration. And here's the uncomfortable part. When nothing is reported for a while, teams conclude they are safer. But "no reports" can mean two very different realities:

1. you're safer, or
2. you're blind in the wrong places

Between reports, most teams can't confidently tell which is true.

Why does this get harder in the AI era?

AI compresses timelines:

- More assets can be discovered faster
- More paths can be tested sooner
- More partial signals appear before anyone has time to interpret them

So the window between “discoverable” and “exploitable” shrinks, and relying only on confirmed outcomes becomes riskier.

The more useful question is no longer “How fast can we find vulnerabilities?” It is “**How quickly can we detect what matters before the next successful outcome exists?**”

What’s missing is an earlier signal layer (before the next report)?

This isn’t a discussion against scanners or ASM/EASM. It’s a discussion that those tools weren’t built to provide one missing layer:

Credible, proof-safe signals between reports that help teams:

- Surface unknown exposure earlier.
- Understand attention and coverage (what was explored vs. ignored).
- Prioritize investigation before the next report lands.

In other words: teams need to see more of the story; not just the ending.

Where we’re going next

The between-reports blind spot isn’t going away, and AI is making it harder to ignore.

If we only learn from confirmed outcomes, we keep reacting late: after the report lands, after the alert fires, after the incident forces attention.

In our previous article on reconnaissance and context, we showed that the work before the report is often the part that determines what comes after. That same concept applies here: between reports, what matters is the context being created through real attacker exploration.

Next, we’ll pull back the curtain on what we’re launching, so security teams can finally make the “between-reports” context visible, actionable, and impossible to ignore. Stay tuned.

AUTHOR

Greg Jenkins

Greg Jenkins is Head of Product at Intigriti, with a diverse leadership background and two decades of experience scaling product teams across the tech space. Having worked across telecommunication, e-commerce, fraud and music, Greg brings deep customer empathy to how B2B SaaS products are built and improved. He oversees the entire product lifecycle and data, modernising delivery for the AI era without losing focus on outcomes, and is known for building high-performing product cultures.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com