Reconnaissance unleashed: Meet CrowdRecon

BY RADU VOLOAGA · SEPTEMBER 1, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/blog/news/reconnaissance-unleashed-meet-crowdrecon

At Intigriti, we have been exploring a simple but important shift in security: the work that happens before a vulnerability report is often where the real signal begins. As vulnerability discovery accelerates, organizations need practical ways to identify and reduce risk before vulnerabilities are used in attacks.

In *Reconnaissance for exposure management*, I discussed how context turns scanning and generic testing into targeted discovery. Reconnaissance is not just a prelude to the report; it is the foundation that explains why certain paths matter, why some assets attract attention, and why human curiosity still creates advantage in the AI era.

The between-reports problem explores the blind spot that exists when security teams only learn from confirmed outcomes. If nothing is reported, teams can be left assuming they are safer or are left anxious that they may be missing a significant piece of the puzzle. The missing layer is the work-in-progress signal: what researchers are exploring, what they are noticing, and what they believe is worth attention before a vulnerability is discovered.

It's time to bring that trusted hacker context into view. Today, we're excited to introduce CrowdRecon, a new Intigriti product that makes high-quality reconnaissance, shared by our researcher community, visible, useful, and rewardable. CrowdRecon adds a human-led context layer before and between vulnerability reports, helping organizations identify exposure, refine scopes, demonstrate coverage, and pre-empt risk, while creating new ways for researchers to collaborate, contribute, and be recognized for valuable recon work.

The value in understanding signals earlier

Researchers spend countless hours mapping organizations attack surfaces, identifying hidden systems, following unusual paths, and building an external view of how an environment really behaves. Much of that work never becomes visible to the company if it does not end in a vulnerability report.

What's more, when a vulnerability is not found, the discovered assets are rarely reported. Attack paths and lessons learnt are not shared or collaborated on, researcher effort is not recognized or rewarded, and customers miss insight into what the community actually saw.

A researcher may discover:

- A domain that appears forgotten.
- A staging environment that mirrors production.
- A marketing site launched without wider security awareness.
- A developer test environment that exposes unexpected attack surface.

- An internal-facing asset that should not be reachable externally.
- A path that looks promising but needs more collaboration before it becomes actionable.

None of these are guaranteed to be vulnerabilities on their own. But they are signals that can uncover real risks. They help customers understand what exists, what the community sees that tools often miss, what is changing, what has drifted, and where real adversarial attention may go next. In sum, hacker activity creates insights.

The result is a missed opportunity on both sides. Companies lose trusted hacker context that can help them validate and refine where attention may be needed earlier. Researchers lose the opportunity to turn high-quality reconnaissance into shared progress, collaboration, and reward.

That is the opportunity CrowdRecon is designed to unlock!

Making shared recon possible. Early beta results

CrowdRecon is a new Intigriti product being built to turn trusted hacker reconnaissance into a shared context layer for earlier human-led exposure validation.

- **For researchers,** it creates an approach to be recognized and rewarded for high-quality research effort that brings value to the industry, even when that work does not immediately result in a vulnerability submission.
- **For customers**, CrowdRecon adds hacker context before and between vulnerability reports, helping teams decide what to review, test, investigate, prioritize, follow up, or pre-emptively mitigate, next across exposure, scope, coverage, and security program decisions.

We have been working with a selection of our hacker community and customers to understand the value that can be derived from community reconnaissance. The early beta has already provided insights that demonstrate just how much valuable context can exist outside the vulnerability report itself, and we are amazed by the findings!

Community reconnaissance highlighted:

- Domains that were intended to be deprecated.
- Vibe-coded marketing sites released without broader security knowledge.
- Developer testing sites that contained unexpected attack surface.
- Assets intended for internal usage that were externally discoverable.
- Hidden surfaces that scanners and internal inventories had missed or forgotten.

That is exactly the type of between-reports visibility customers need to help their security teams see parts of their environment through the eyes of the community and understand where attention, curiosity, and potential risk are forming.

How CrowdRecon works for continuous security

We've built CrowdRecon around a framework that supports the full loop, from researcher discovery through customer validation to community reward. In essence, reconnaissance improves visibility and

generates more intelligence, which leads to better outcomes. CrowdRecon has always been continuous, but we are increasing visibility of researcher activity. These outcomes create more opportunities, ultimately attracting more researchers to a program. As the number of researchers grows, so does reconnaissance, and the cycle continues.

At a high level, CrowdRecon enables:

- **Clear standards for high-quality reconnaissance**. This means that we are providing clear guidelines on the type of reconnaissance researchers can log on the platform and have their own technical validation that checks elements such as “Is it DNS resolved?” or “Is it HTTP reachable?” to ensure that we capture valuable data.

- **A structured submission process for researchers**. This means that we are adding a new “logging” flow on the platform, which can only be used to log reconnaissance data. This entails a 3-step flow while providing full transparency on the data that is being logged.

- **Streamlined review, validation, and insights for customers**. There will be different data visualisation types, starting with a table, which will have a multitude of filtering capabilities, including some default filters that customers can use to navigate the data easily. Other data visualisation types will follow, such as the constellation, which aims to create a full picture of the attack surface built from different data sources (ASM, scanners, and of course CrowdRecon data). Customers will also be able to validate the data in the platform and take several manual steps, such as adding a new sub-domain to their existing BBP, or running a PTaaS on a set of newly discovered domains.

- **Reward-based incentives for impactful logs**. We developed a selection of ways for researchers to get rewarded for valuable recon logs. Pay-per-log, leaderboard payouts,and a kickback model are three types that will be available for customers.

The result is intelligence that returns value to both customers and researchers, and better collaboration around attack paths, hidden surfaces, and emerging areas of interest.

The goal is not to flood customers with noise, but to capture meaningful reconnaissance context and turn it into usable insight for exposure, scope, coverage, investigation, and follow-up decisions/mitigation. That distinction matters. CrowdRecon is not just more data; it is a way to preserve and operationalize the value that researchers are already creating and reduce risk before vulnerabilities are discovered.

What the community sees that tools often miss

ASM and AI-driven testing help teams map what is externally visible and maintain a broader view of their attack surface. CrowdRecon is additive: it shows how trusted hackers engage with that surface, what they explore, ignore, revisit, or treat as worth attention. Researchers do not simply enumerate assets. They explore, infer, follow intuition, connect weak signals across systems, and highlight when something looks out of place. That human context helps teams validate and refine where review, investigation, scope changes, or follow-up may be needed.

Across our tests, we found that on average:

- 5% of total attack surface discovered was shown in scope of a program.

- 30% was discovered by scanners.

- 65% was further discovered by the community.

- Out of that 65% discovered by the hackers, 20-30% is valid from a technical perspective (or is live).

That split suggests that community reconnaissance can reveal a substantial layer of attack surface that would otherwise remain harder to see, interpret, or prioritize.

This is only the beginning

CrowdRecon brings an important new source of security intelligence into view, but what excites us just as much is what this makes possible next.

We're already working on bringing more layers of this vision to life, connecting security signals to build a richer understanding of where attention may be needed across an organization's exposure. CrowdRecon brings the perspective of the hacker community into that bigger picture, giving us a strong foundation for what comes next, and we could not be more excited to be building towards it.

Our ambition is to help security teams validate exposure earlier and with more confidence, without expecting them to piece together context from disconnected tools, reports, and individual findings. There is much more to come, and CrowdRecon is an important step in making that possible.

We're only getting started.

Join the public beta

CrowdRecon recognizes that the community not only finds vulnerabilities, but it also creates context, discovers hidden surfaces, shows where attention is forming, and helps customers understand how their external environment is interpreted by real researchers. This is an important step in how we think about the future of human-led exposure validation.

Reconnaissance deserves to be treated as a first-class asset, and that is why we built CrowdRecon.

We're incredibly proud to finally put CrowdRecon into the hands of our customers and community, and even more excited to see how their feedback and experience will help shape what comes next.

Interested in bringing CrowdRecon into your security program? Register for the public beta today.

AUTHOR

Radu Voloaga

Radu Voloaga is a Senior Product Manager at Intigriti, working at the intersection of bug bounty program operations and the hacker community. He collaborates closely with both customers and security researchers to understand what drives high-signal submissions and how recon and asset discovery translate into real, reportable vulnerabilities. Over the last couple of years, he has helped shape Intigriti's PTaaS offering and led a research initiative on hacker reconnaissance and the measurable value it creates for both hunters and program owners.