CEO insights: holding the human layer sacred in the AI era

BY STIJN JANS · MAY 11, 2026

As founder and CEO of Intigriti, I've spent a long time around hackers, and one thing is clear. The best ones don't fear AI. They use it.

What they do fear, however, and what I take seriously as a founder, is a world where platforms quietly replace them under the banner of efficiency. Where their work trains models they don't benefit from, and where the economics of the craft erode while everyone smiles and calls it progress.

The beating heart of the Bug Bounty industry

In the ten+ years of building Intigriti, we've seen a lot. We watched COVID-19 rewrite how the world works, and with it, how security teams operate, hire, and trust people they've never met in person. We watched the rise of the side hustle economy, where talented people wanted a way to earn a meaningful income next to a day job. Bug Bounty has become one of the most legitimate, skill-based approaches to that. We've seen regulation arrive, customer expectations shift, the threat landscape mature, and the researcher community grow into a global workforce of its own.

Through it all, and amidst every change, one thing held. The hackers were the heart of it.

AI is the next shift, and it's arguably bigger than the others. But the principle doesn't change. At the end of the day, it does not matter if you have AI tools trying to find vulnerabilities, if you have a nation-state actor, or a black hat trying to break into your system. Intigriti exists because human creativity finds the vulnerabilities that matter, and bug bounty exists as a legal way to do this. AI makes that work faster, sharper, and less painful. But it does not replace the hacker. It serves them.

Acknowledging strengths and weaknesses

AI is going to commoditize the bottom of the offensive security stack. Surface mapping, known vulnerability classes, dependency scanning, and configuration drift. All of it becomes continuous and automated. That's a good thing, and it's not where great hackers should be spending their valuable time.

It's worth being precise about where AI is strong today. Current LLMs are quite good at reasoning over source code, spotting known patterns, and flagging insecure constructs.

They are far less effective at interacting with a running system, building state across requests, understanding application behaviour, and adapting when something unexpected happens. And, while they will improve, that gap is still significant.

Human researchers are, and will always be, essential.

Where human hackers fit in

This isn't the first time the industry has been here. When automated scanners first appeared, people predicted the end of manual testing. The opposite happened. Scanners raised the floor, which made the ceiling matter more. Good hackers got sharper because they could skip the boring work. New hackers gained entry in because the tooling lowered the barrier to start finding real issues. AI is the same pattern, just bigger.

What's left for humans is what actually matters. Business logic. Chained attacks across systems. Novel attack classes in emerging tech, including AI agents themselves. The adversarial creativity that comes from understanding what a product does, not just what it has. AI doesn't replace any of this. It enhances the hacker doing it.

What businesses will face in the next 3 to 5 years

That's where the customer choice gets interesting. A company can buy a single AI security product. Or they can work with thousands of hackers on Intigriti, each running their own AI stack, their own models, their own prompts, their own creative angle. One vendor's AI versus thousands of hackers amplified by AI. The second approach finds things that the first structurally cannot. Diversity of tooling combined with diversity of thinking is the moat.

In 3 to 5 years, programs might tier explicitly: Continuous AI scanning for breadth. Time-bound human research for depth. A creative researcher layer for the work that neither AI nor scanners will ever touch. Customers who understand this will spend less and find more. The ones who don't will buy AI-only solutions and learn the hard way that real attackers are still human.

The platforms that win are the ones that hold the human layer sacred. Every product decision is built around amplifying the hacker, not replacing them. That's what "human-shaped" means. It's not marketing. It's an architectural choice. And that’s what we're building Intigriti to be: that platform.

Thought leadership, insights, and next steps

Our team is at the forefront of AI insights, trends, and discussions.

As part of our recent AI blog series, and in addition to content on ‘How AI is leveraged to enhance the Intigriti platform’, our senior leadership has provided multiple insights on the development and future of AI, its impact on programs, and the Bug Bounty community.

- If you are interested in the “Vulnpocalypse” and how AI is changing vulnerability discovery, then check out the content from our COO, Ed Parsons.
- If you want to know more about common AI misconceptions and how they impact your team, then head over to this article from our Head of Product, Greg Jenkins.
- For an insight into the future of AI within Bug Bounty, our Program Leader, Chris Holt, provides his opinions on how AI helps and hinders programs.

- And for insights from a triager's perspective, our Head of Triage, Lennaert Oudshoorn, shares his insights into behaviour, tooling, patterns, and expectations triage teams are seeing.

And there is plenty more to come.

I will be sharing my viewpoints on your most pressing AI questions regarding our AI Model Card, efficiency, speed, and empowerment. So, watch this space!

In the meantime, sign up to our newsletter and connect with us on socials to stay in the loop.

AUTHOR

Stijn Jans

Stijn Jans is the Founder and CEO of Intigriti, the leading Bug Bounty and ethical hacking platform that connects organizations with a global community of security researchers. Under his leadership, Intigriti has grown into a trusted cybersecurity partner for enterprises worldwide, championing transparency and continuous vulnerability disclosure to help companies stay ahead of emerging threats.