Vulnpocalypse Now? How AI is changing vulnerability discovery

BY ED PARSONS · APRIL 23, 2026 · LAST UPDATED ON APRIL 24, 2026

What you will learn

- How vulnerability research and security testing may evolve in the future, based on expert insights and reflections from Intigriti COO Ed Parsons.
- How AI is reshaping vulnerability discovery, including the major trends and developments security teams should understand today.
- The ‘vulnpocalypse’, and what it signals about the future of AI-assisted hacking.
- The risks, opportunities, and practical impact of AI-supported hackers.

Contextualizing AI’s impact

Intigriti is one of several crowdsourced security companies experiencing a surge in AI-attributed vulnerability submissions. The impact is also being felt by organizations running their own bug bounty programs.

In a recent article discussing common AI misconceptions, we explained how Intigriti has seen volume increases not only due to AI productivity gains, but also from growth in researcher numbers and our customer base.

This article reflects on changes in the industry and where things might go from here.

A leader's perspective on AI in vulnerability research

For insights, we’ve turned to Ed Parsons, Chief Operating Officer at Intigriti, who brings perspective from a career spent in cybersecurity. From hands-on investigations to leading some of the industry's most respected organizations, Ed spent several years helping organizations defend against threats from nation-state actors and organized criminal groups, work that gave him a grounded view of how adversaries think and operate.

Before joining Intigriti, Ed served as Vice President of the world's largest member association for cyber professionals and led an international cybersecurity consultancy recognized for its research capability and technical depth. Now, as COO, Ed oversees Intigriti's triage, product, and engineering functions, and serves as the company's CISO.

His position sits at the heart of the questions this article explores. When AI changes the economics of vulnerability discovery, the pressure lands squarely on his teams to maintain signal quality at scale. Ed's view is shaped not by theory, but by hacker activity on our platform: how AI-assisted submissions are

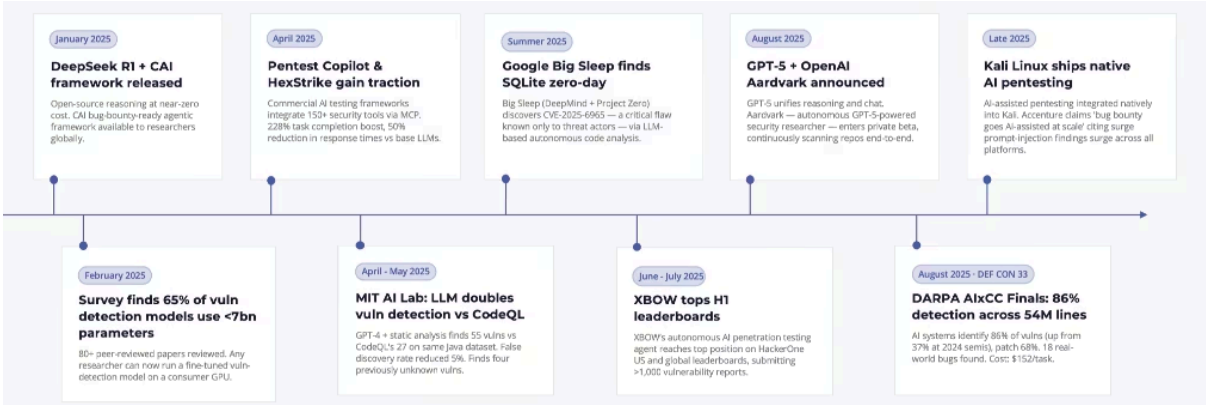
already shifting the demands on customer programs, what that means for the humans and systems processing them, and how platform-driven security services need to evolve.

Key developments in AI-powered vulnerability discovery

Changes in the technology landscape typically affect cybersecurity by creating opportunities for both attackers and defenders. Earlier examples include the shift toward cloud infrastructure and cloud native technologies, and the impact of penetration testing frameworks and scanners on offensive security.

In 2025, we saw advances in the use of AI for vulnerability discovery. Improvements in the performance and efficiency of Large Language Models (LLMs) for vulnerability discovery led to the democratisation of hacking LLMs. Autonomous security research moved from proof-of-concept to production infrastructure, culminating in the integration of AI-assisted penetration testing natively into Kali Linux, the popular hacking distribution.

For context, this timeline tracks major advances in AI for vulnerability discovery.



Major advances timeline in AI for vulnerability discovery.

The same capabilities have allowed hackers to [discover and exploit vulnerabilities] at an accelerated pace. [FIRST Vulnerability Forecast Feb 2026], predicts a (median) 60,000 CVEs this year, up from almost 50,000 in 2025 and 40,000 in 2024, [according to data gathered by Jerry Gamblin].

2026, Mythos and the ‘Vulnpocalypse’

The febrile environment around the phased release of Claude Mythos, together with [Project Glasswing], from Anthropic, has led to speculation that we have entered a ‘vulnpocalypse’, where vulnerabilities can be discovered and exploited faster and cheaper than they can be patched.

For many in the industry, it feels like we’ve been in that situation for a while. Among the deluge of hot takes, beneath sophistic calls to accelerate patching, there is speculation about the demise of vulnerability research and bug bounties. Some imagine a world without human security researchers, seeming to ignore the demand for novel research created by mass adoption of AI, both to secure the technology itself and the proliferation of AI-generated code.

What does the age of AI-supported hackers mean? And what is the impact?

The age of AI-powered/supported hackers is upon us, and the impact is clear. As a crowdsourced security company receiving thousands of vulnerability submissions every year, Intigriti sees how AI technology is being used by security researchers.

1. Many hackers are leveraging AI in their workflows, contributing to a rise in the average number of submissions per researcher.
2. AI has lowered the barrier to entry for security research and accelerated vulnerability discovery.
3. AI has the potential to improve report language and overall quality, which could accelerate processing.

We are also seeing a higher volume of AI-generated out-of-scope submissions and abuse of technology, which creates work without adding value. This has impacts on the whole vulnerability lifecycle, from discovery through to validation and remediation.

Is the game up for human hackers? Or will AI replace security researchers?

The ability of LLMs to discover vulnerabilities has led to speculation over the future of vulnerability research and the role of human actors therein. Beyond the excitement about new model releases and the marketing campaigns, it's worth noting that:

- Researchers are *already* finding bugs in AI and discovering vulnerabilities by using the technology in novel ways.
- Organizations are finding incredible value through creative, meaningful engagement with the hacker community.
- The remarkable advances in vulnerability discovery in software aren't seen across all vulnerability classes and technologies.
- The results of AI testing tools don't always meet expectations.

Nevertheless, at Intigriti, we believe this is a paradigm shift, characterised by unprecedented scale and speed, and requires a rapid adaptation. While the situation is developing, in this 'new normal', our focus remains on the problems we understand well.

These include creating maximum impact for customers while operating at a significantly larger scale and supporting researchers working with AI while challenging behaviours that threaten the integrity of crowdsourced security.

What will the future hold?

At Intigriti, we acknowledge that AI is disrupting vulnerability research and security testing, largely through the automation of discovery across certain classes and technologies. It is changing the way

security researchers work, with many embracing AI in their workflows. Hybrid (human and AI) approaches will remain essential to discover novel vulnerabilities and drive new applications of AI to vulnerability research.

The pace of change and adoption of AI-driven products will also create demand for validation and reproduction, while shifting customer expectations further away from traditional (service) delivery methodologies.

AI will not only change the way security researchers work, but also how they create value. As we've stated, ethical hackers and threat actors already use AI in their workflows. Increasingly, they will operate at a higher level of abstraction: orchestrating AI, validating its output, and ensuring its safe use. The elite will build proprietary models and workflows based on their own expertise, scaling their impact.

Increased adoption of AI for vulnerability research and security testing will also generate demand for the processing of machine-generated output. This will result in more need for automation, and the application of deterministic and agentic AI, like Intigriti's AI Triage Assistant, into validation, reproduction, prioritisation, and remediation. This volume, combined with improvements in model accuracy, will lead to greater agency, challenging current expectations about 'humans in the loop', and precisely where human intelligence can provide most value. We also need reliable safeguards for AI testing tools.

The promise of AI-driven testing will accelerate the industry trend towards more continuous, scalable, and cost-effective forms of assurance that mirror the threats organisations face. Crowdsourced security already offers these properties and complements AI-driven approaches better than traditional penetration tests.

Summary and final reflections

At Intigriti, we have a unique perspective on how hackers are using AI, its impact on vulnerability discovery generally, and the associated operational challenges. We are experimenting, learning, and improving based on feedback from researchers and customers on how to deploy AI and reflecting those lessons in our approach.

As AI develops, applied security research advances, and products mature, but our principles remain the same.

- As we develop new AI features, we'll prioritize "giving back" to the community. After all, the world will always need security researchers!
- We believe in transparency about how we use AI: The model card has been updated to maintain consistency on data privacy principles.
- We do not allow third parties to train on the data.
- Humans remain responsible and accountable for the application of AI to our work.

Next steps

For more AI-related thought leadership, take a look at our latest series and read more about 'Common AI misconceptions debugged', 'The AI future of Bug Bounty', 'Vulnerability disclosure for AI safeguards',

which discusses how open programs should be and what incentives are necessary, and 'How AI is leveraged to enhance the Intigriti platform'.

If you have any questions regarding the content in this article, please reach out to your designated manager. Or, if you are new to Intigriti, follow us on socials, comment on our posts, check out our knowledge base, and contact the team for more information.

AUTHOR

Ed Parsons

Ed Parsons is Chief Operating Officer for Intigriti. Before joining Intigriti, Ed was Vice President of the world's largest member association for cyber professionals and led an international cybersecurity consultancy, renowned for research and technical expertise. As a cybersecurity professional, Ed spent several years helping organizations investigate and respond to cyber threats from nation-states and organized crime groups. He is a Certified Information Systems Security Professional (CISSP) and a UK Chartered Cyber Security Professional.