The AI impact: a triager's perspective

BY ELEANOR BARLOW · MAY 5, 2026

As part of our recent AI blog series, and in addition to content on 'How AI is leveraged to enhance the Intigriti platform', we have provided multiple insights from the Intigriti team on the development and future of AI, how it impacts programs, and the Bug Bounty community.

So far, we have explored:

- 'How AI is changing vulnerability discovery', with COO, Ed Parsons.
- 'Common AI misconceptions debugged' with Head of Product, Greg Jenkins.
- 'A(I) future of Bug Bounty', with Program Leader, Chris Holt.

In today's blog, we talk with Intigriti's **Head of Triage, Lennaert Oudshoorn,** to discuss the challenges he observes, how the industry is adapting, and the solutions going forward.

As an accomplished hacker, Lennaert has found vulnerabilities in many large organizations, including the Dutch government. As Head of Triage at Intigriti, Lennaert not only handles diverse vulnerabilities and security issues daily but also has a frontline seat to the newest attack methods, approaches, and emerging vulnerability classes. In addition to his professional exploits, he still reports vulnerabilities in his role as a volunteer with the Dutch Institute for Vulnerability Disclosure (DIVD). At DIVD, he has worked several big cases, including some that made international headlines, such as the big July 2021 ransomware incident involving Kaseya.

How the AI conversation is lagging behind reality

The term 'slop', selected as 'Word of the Year 2025' by the Merriam-Webster dictionary, was coined to describe 'digital content of low quality that is produced usually in quantity by means of artificial intelligence'.

In the early 2020s, this low-quality AI content emerged, and as AI has evolved, so has its use.

A lot of the conversation seen in various circles around Bug Bounty is still focused on AI slop. But it is no longer the most interesting or impactful development that AI is causing in security research and Bug Bounty.

> **"One of the hardest parts of talking about AI in Bug Bounty is that every observation has a short shelf life. Something that felt like the main issue just a few months ago already feels outdated today. AI was often used to write or embellish reports. Now it is increasingly being used during actual research."**
>
> **Oudshoorn**

The bigger challenge is that the situation keeps changing. As Oudshoorn states,

> **“Triage teams are not adapting to one AI shift. They are constantly seeing new behaviour, new tooling, new report patterns, and new expectations.”**

What is AI’s current biggest impact on Bug Bounty?

For a while, the most visible AI-related problem in Bug Bounty was noise. But AI is no longer mainly being used at the end of the process, when a report is written. Instead, it is increasingly being used during the research itself.

- Existing and experienced researchers can move through recon, code review, payload iteration, and report writing more efficiently.
- Newer researchers can use AI to understand unfamiliar technologies, interpret errors, and explore attack paths that they would have previously gotten stuck on.

> **“The problem has shifted from “too many bad reports” to “more people can now produce good-enough research at a higher speed.”**
>
> **Oudshoorn**

New ways of working?

The main challenge is no longer only about spotting AI-generated slop. It is about handling an increased pace of legitimate research activity. More researchers can now reach a reproducible vulnerability. More duplicates arrive because multiple people are accelerated toward the same findings. While AI may no longer be flooding programs with only bad submissions, it is increasing the amount of real security work entering the system. Valid volume that still needs to be handled.

These changes have pushed teams towards new ways of working. Prioritizing the most impactful reports and focusing on the issues that are most likely to be valid and relevant. Aiding this is Intigriti’s AI-powered Triage Assist feature, which helps to quickly identify duplicates and look at past reports and decisions made, to ensure consistency.

Previously, writing quality often gave some indication of report quality. Not always, of course, but a clear, technically precise report usually suggested that the researcher understood what they had found. That signal is weaker now. And while AI usage in security research is evolving and showing more value, we do still see some undesirable usage of it, mainly from newer hunters who lack the experience to interpret and validate the AI’s findings themselves.

> **“In the past, a bogus report was quickly identified and easily dismissed; these AI-generated reports look serious and seem like they might contain valuable information and address a real issue at first glance. From a triage perspective, they require further research and take a much longer time before they can be dismissed.”**
>
> **Oudshoorn**

This can be attributed to the usage of AI by hackers who do not have a deep understanding of the actions they are taking.

> **“Reports and comments get pasted straight from an LLM into a platform, sometimes even including the prompt they gave the AI. We often get messages that include a header such as ‘Here’s how you can word your reply so it’s professional, clear, and addresses their request directly.’ Or ‘Copy and paste the text below into your reply.’ This can be inaccurate and time-consuming to the triager.”**
>
> **Oudshoorn**

Another time-consuming issue is the fact that an LLM will often write extremely long messages that the researchers will likely never read fully.

> **“A researcher can copy-paste their response into the LLM and let the LLM reply. It’s the triager that then must read and understand the entire reply, verify its contents, possibly reproduce and test various steps, to determine if it is bogus or not.”**
>
> **Oudshoorn**

Validation tools to speed up decision-making

Many prospects reach out asking Intigriti for advice regarding how to run programs and handle vulnerability reports in this new reality.

> **“Our customers trust our approach, sharing the same desire to work with humans, receive complete transparency when it comes to AI policies, and praise our triage team for filtering out any slop and verifying reports before they reach them. We're protecting our customers from bad reports while helping our community use AI responsibly as a research assistant, not a replacement for skill and verification.”**
>
> **Oudshoorn**

AI is a tool, not a replacement. Intigriti remains hacker-centric and requires human verification of all findings, working proof of concepts, and genuine security research. To do this, we include out-of-scope detection, triage assist features, and continued evolution of tooling.

> **“Our AI Triage Assist (validation tool) can automatically scan through submissions to support triage and, therefore, customers. Triagers still review submissions, but instead of starting from scratch, the AI is suggesting “this looks invalid”, and our expert human-in-the-loop makes the decision and performs the final check.”**
>
> **Greg Jenkins, Head of Product, Intigriti**

The advanced submission search allows Intigriti to quickly identify similar or duplicate reports within submission content, helping speed up triage decisions.

> **“We’ve already seen a significant increase in what triagers can do, just from Triage Assist. But the key point is that human experience and expertise remain central, while technology reduces the cognitive load and helps our teams spend more time on judgment and less time on repetitive scanning.”**
>
> **Jenkins**

Next steps for enhanced triage

Intigriti’s disclosure of AI usage requirement is in our Community Code of Conduct, and as a part of our strategy to combat slop, Intigriti ensures that educational material for hunters on how to use an AI to hack with or write reports without creating AI slop is provided.

> **“We, at Intigriti, believe AI will play a significant part in the future. Hackers, after all, use this technology to elevate their research workflows. It’s an evolution that hackers have always been a part of, exploring and hacking new technologies. But we don’t believe it will ever replace our hackers. We are committed to staying hacker-centric and securing our customers together with our community of talented hackers. AI can be a powerful assistant and a tool in this mission, but it needs to be used with a human in the loop. The last line of defense is, and will always be, our triage team.”**
>
> **Oudshoorn**

Invest in a single AI tool, or work with Intigriti and access hundreds of researchers who each bring their own AI tools to the table. For more information on our AI policies, read our AI Model Card or our blog on How AI is leveraged to enhance the Intigriti platform.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years’ experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.