



Agile testing powered by the crowd

Modern security requires staying one step ahead

The pandemic may have surged businesses forward in terms of digital transformation, but the proliferation of technology was already steadily on the rise. The challenge of digitalisation within businesses is that malicious hackers suddenly have a much larger attack surface to work with. For many businesses, IT departments are already stretched thin. Keeping up with new demands creates a situation whereby security is performed in firefight mode rather than proactively addressing vulnerabilities before they can be exploited by cybercriminals.

The need for modern, proactive security has never been more important. A simple yet proven method to protecting against cyber threats is to invite ethical hackers in. Bug bounty programs follow this concept at scale by applying a crowdsourced mentality to cybersecurity testing.

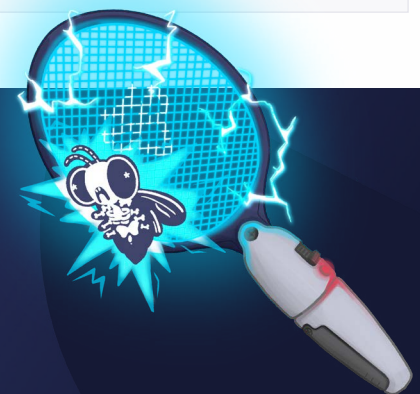
What is a Bug Bounty Program?

A Bug Bounty Program allows independent security researchers (also known as ethical or white hat hackers) to report bugs to an organisation. 'Bugs' are security exploits and vulnerabilities. If deemed relevant, which depends on the scope provided with the program, the researcher is paid a reward or compensation which is better known as a 'bounty'. Most researchers choose to report vulnerabilities through a Bug Bounty Platform, like Intigriti.

This is because they provide the best infrastructure for organisations to set up programs successfully while providing researchers with a clear and managed way to submit vulnerabilities and get rewarded.

Bug Bounty benefits

- 1 **Proactive security testing**
Security researchers are incentivised to find weaknesses and report them to your development team or engineers to fix.
- 2 **Continuous coverage**
With thousands of cybersecurity experts at your disposal, you can scale and continuously test your digital assets in real-world scenarios without increasing headcount or putting pressure on your team.
- 3 **Quality assurance**
All reports are validated and approved by our triage department first, meaning your internal teams can work smarter and faster.
- 4 **Cost efficient**
Bug bounty programs follow a pay-for-impact model, meaning you only pay for valid vulnerabilities reported and in scope, making your security budget go farther.
- 5 **Public vs private programs**
You're in control of whether your bug bounty program is private or public. With a private program, you can invite your preferred researchers to view and contribute to your program. With public programs, the entire researcher community is at your disposal.



What happens after you launch a Bug Bounty Program?

63%

of companies get a high to critical submission within the first 48 hours of their program launching on Intigriti.

5

is the average number of vulnerabilities submitted, within the first week after a program launches.

22

is the typical amount of submissions that are accepted, on average, within the first week of a program's launch.



About Intigriti

Global crowdsourced security provider trusted by the world's largest organizations

Intigriti's bug bounty platform provides continuous, real-world security testing to help companies protect their assets and their brand. Our community of ethical hackers challenge our customers' security against realistic threats: we test in precisely the same way malicious hackers do.



How vulnerability management works with Intigriti

- 1 Researcher tests and **searches** for a **vulnerability**
- 2 Researcher **submits** a **report** via Intigriti
- 3 Intigriti's **triage** begins **communication** with researcher
- 4 Intigriti's **triage** team applies **quality assurance** steps
- 5 In-scope, unique and well-written **reports** are **submitted** to client
- 6 **Client accepts** report, and **payment** is automatically processed

125.000+ researchers

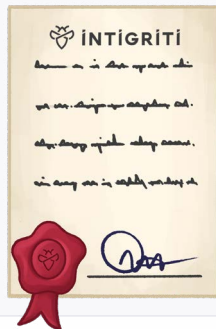
More than 125.000 security researchers use Intigriti to hunt for bugs — and we're growing!

400+ live bug bounty programs

Companies of all sizes, and across multiple industries, trust Intigriti to launch their bug bounty program.

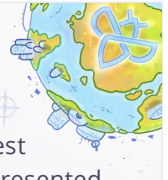
GDPR compliant

We ensure compliance with the highest security and data security standards.



Strong global presence

Intigriti has a strong global presence. In terms of hacker pay-outs, the 10 best performing countries are globally represented in North America, Europe and Asia. In 2025, vulnerabilities were submitted from more than 180 countries.



A vulnerability reported and fixed is one less opportunity for a cybercriminal to exploit. Ready to talk about launching your first bug bounty program? We're here to help you launch successfully.

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com

YOU'RE IN GOOD COMPANY

