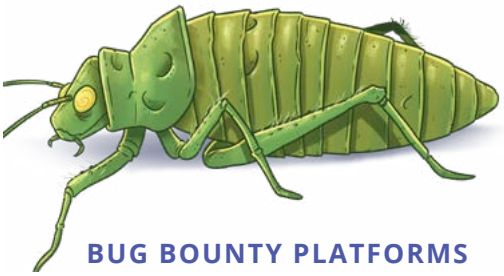
Self-hosting a bug bounty program vs publishing via a bug bounty platform

Businesses can choose to receive and manage vulnerability disclosure reports themselves or publish and host through a bug bounty platform, such as Intigriti.



	SELF-HOSTED PROGRAMS	BUG BOUNTY PLATFORMS
Program engagement	**Reactive and passive engagement** Good-willed customers, citizens and ethical hackers will inform businesses of a potential security issue.	**Active engagement** Security researchers are continuously engaged through bounty opportunities, points and reward systems, leader boards, hacking events, education, and more.
Vulnerability disclosure policy requirements	**Required** Having a VDP ensures that people outside your organisation understand how to inform you of vulnerabilities they have discovered.	**Advised** It is advisable for businesses to have a VDP on their website too to direct people that wish to inform them of a security issue to their program.
Validating submissions	**Handled internally** Without enough manpower, the handling of non-valid submissions can be a time-consuming exercise.	**Handled by triage** Triage teams provide a layer of quality assurance before escalating vulnerabilities to businesses.
Handling comms	**Handled internally** Owned by the team tasked with fixing incoming submissions.	**Handled by triage** Communication carried out within the platform. A triage department works as the go-between for client & researchers.
Budget allocation & payment processing	**Manual** Responsibility of a finance department. To maintain good working relationships with researchers, it's important to provide payment promptly.	**Handled by the platform** Processes automatically after a submission is accepted by the organisation. Payment and administration are taken care of by the platform.
Disclosure agreement	**Responsible disclosure** Researchers encouraged to perform responsible disclosure via a VDP.	**Platform agreement** Researchers must agree not to disclose reports publicly unless given permission.

About Intigriti

Agile testing powered by the crowd

Intigriti's bug bounty platform provides continuous, realistic 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.

50,000+ researchers

More than 50,000 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 standards.

Strong European presence

In terms of hacker pay-outs, 8 out of 10 of the best performing countries are European. However, Intigriti is very much a global business. In 2020, vulnerabilities were submitted from more than 140 countries.

How vulnerability management works on Intigriti

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

You're in good company

Kahoot! · European Commission · Showpad · Fortnox · SHOP APOTHEKE EUROPE · VISMA · randstad

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.

Speak to our team today.

TAKE YOUR FIRST STEPS

- Request a demo www.intigriti.com/demo
- Visit the website www.intigriti.com
- Get in touch hello@intigriti.com

INTIGRITI

Information from Q2/2022. We are constantly growing, so please contact our sales department or see our website for an accurate number.