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** Working with a provider like Intigriti means submissions are triaged, allowing your security team to focus on fixing vulnerabilities, not sifting through noise.
Validating submissions	**Handled internally** Without sufficient internal resource, 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

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

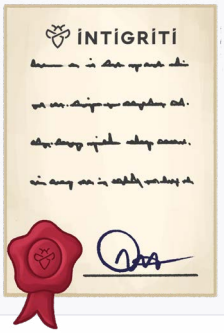
More than 125.000 security researchers use Intigriti to hunt for bugs — and we're growing!

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

Dropbox · Coca-Cola · Nestlé · Personio · NVIDIA · intel · Red Bull · Microsoft · UBISOFT