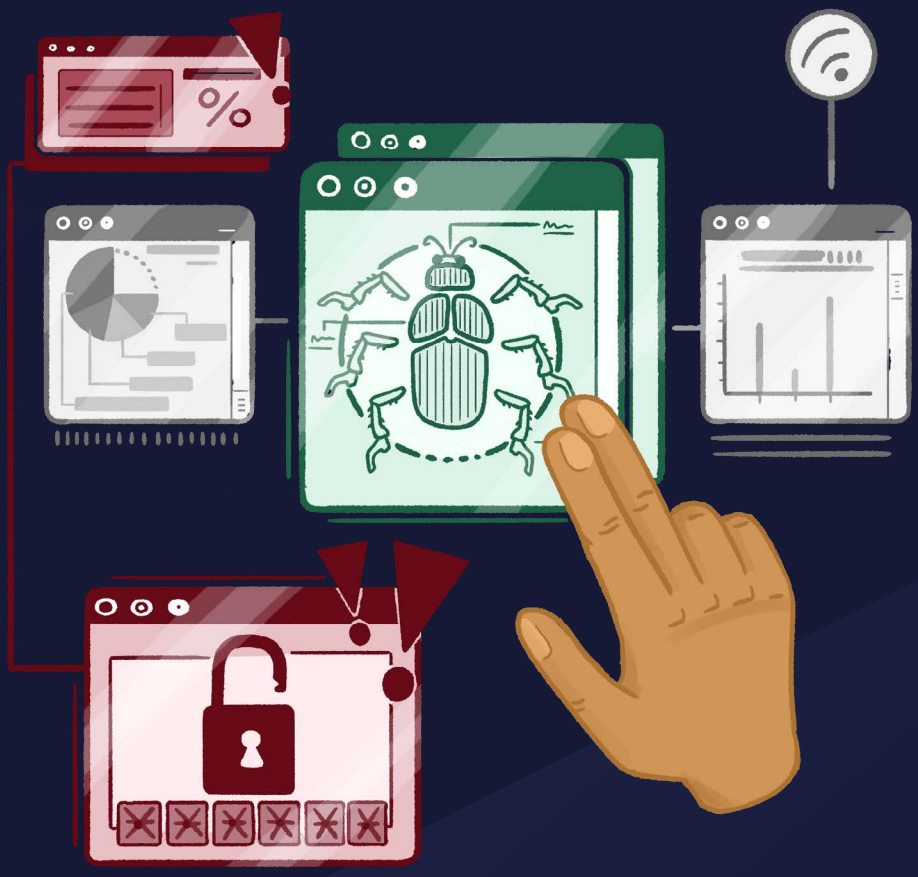
INTIGRITI

Information sheet

An overview of Bug Bounty Programs for businesses



intigriti.com

Agile security testing, powered by the crowd

Bug Bounty concepts explained

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 in a legally compliant matter.

Bugs

'Bugs' are security exploits and vulnerabilities. If deemed new and valuable, which depends on the scope provided with the program, the security researcher will report these quickly, reliably, and clearly via a submission describing the vulnerability.

Bug Bounty platform

Most security researchers choose to report vulnerabilities through a bug bounty platform, like Intigriti. This is because a bug bounty platform provides the best infrastructure for security researchers to engage and communicate with companies in a structured, safe, and reliable way, offering live updates and communication.

Bounty

If the submission is accepted by the organisation it relates to, the researcher is paid a reward or compensation which is better known as a 'bounty'. The reward or compensation can be monetary or reputation points, but also gifts like goodies and swag.

Security researchers

Security researchers are cybersecurity experts who use their skills and expertise to hack for good. They're also known as bug bounty hunters, white hat hackers and ethical hackers. Some of Intigriti's researchers are dedicated to bug bounty hunting full-time, whilst others are employed in full-time jobs.

How crowdsourced security helps organisations overcome cybersecurity challenges

The challenge	Bug Bounty as a solution
Cybersecurity skills gap 90% of security professionals say the cybersecurity skills shortage is an increasing challenge[1].	**Tap into a network of security experts** Leverage the skills, experience, expertise, and creativity of **thousands of security experts**.
Staying on top of cyber threats 59% of cybersecurity teams are understaffed, making it difficult to find time for training[2] - yet cyber threats continue to evolve.	**Invest in your team's development** Like a malicious hacker, bug bounty hunters are wired to spot what your team might miss. Organizations **invest in internal talen**t by allowing them to learn from incoming submissions and interactions from researchers.
Growing attack surfaces Digital transformation, cloud adoption, IoT and the increasing use of AI have led to dramatically growing attack surfaces. This has led to a **massive increase in cyber threats** globally year-over-year.	**Test security continuously** Businesses can **amplify and scale security testing** by running an ongoing bug bounty program. Security teams gain awareness of vulnerabilities faster, and in turn, can introduce a patch faster.
The cost & limitations of pentesting The average cost of a high quality pentest is between $10,000-$30,000 USD[3]. To run them continuously would be highly costly & unsustainable as you pay for testing time, not for results.	**Pay for results** Bug bounty hunters are rewarded if they expose a new, realistic, and actionable in-scope bug. By paying for results, the **cost-efficiency ratio** is giving companies much more impact for the same test budget.
Security awareness Keeping security awareness high is an ongoing challenge for internal cybersecurity teams. Configuration errors and insecure coding can easily lead to **significant costs and data breaches**.	**Gain the support & input of ethical hackers** Through the continuous flow of qualitative and **impact-driven submissions**, IT & development teams experience a boost in inspiration, to hacker mindset way of thinking and awareness throughout the year.
Lack of resources With higher expenses and new processes for enabling **continuous growth**, acquiring adequate cybersecurity resources can be a challenge.	**Centralize security testing** Bug bounty programs allow organizations to continuously test cybersecurity defences **within one platform**, and through the power of a crowd.

1 • isc2.org/Insights/2024/09/ISC2-Publishes-2024-Cybersecurity-Workforce-Study-First-Look

2 • businesswire.com/news/home/20231003937146/en/New-ISACA-Research-59-Percent-of-Cybersecurity-Teams-are-Understaffed

3 • blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/#:~:text=Penetration%20testing%20can%20cost%20anywhere,that%20of%20a%20large%20company

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

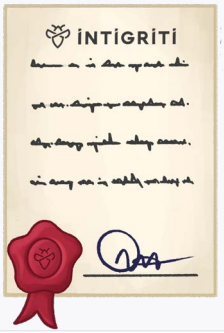
More than 125.000 security researchers use Intigriti to hunt for bugs — and we're growing!

400+ live bug bounty programs

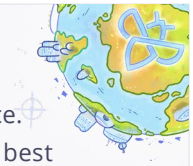
Companies of all sizes, and across multiple industries, trust Intigriti to launch their bug bounty program.

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