



# An Overview Of Bug Bounty Programs For Businesses





# An Overview Of Bug Bounty Programs For Businesses

## Agile security testing, powered by the crowd

### Bug bounty concepts explained

#### ③ 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.

#### ③ 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.

#### ③ Security researchers

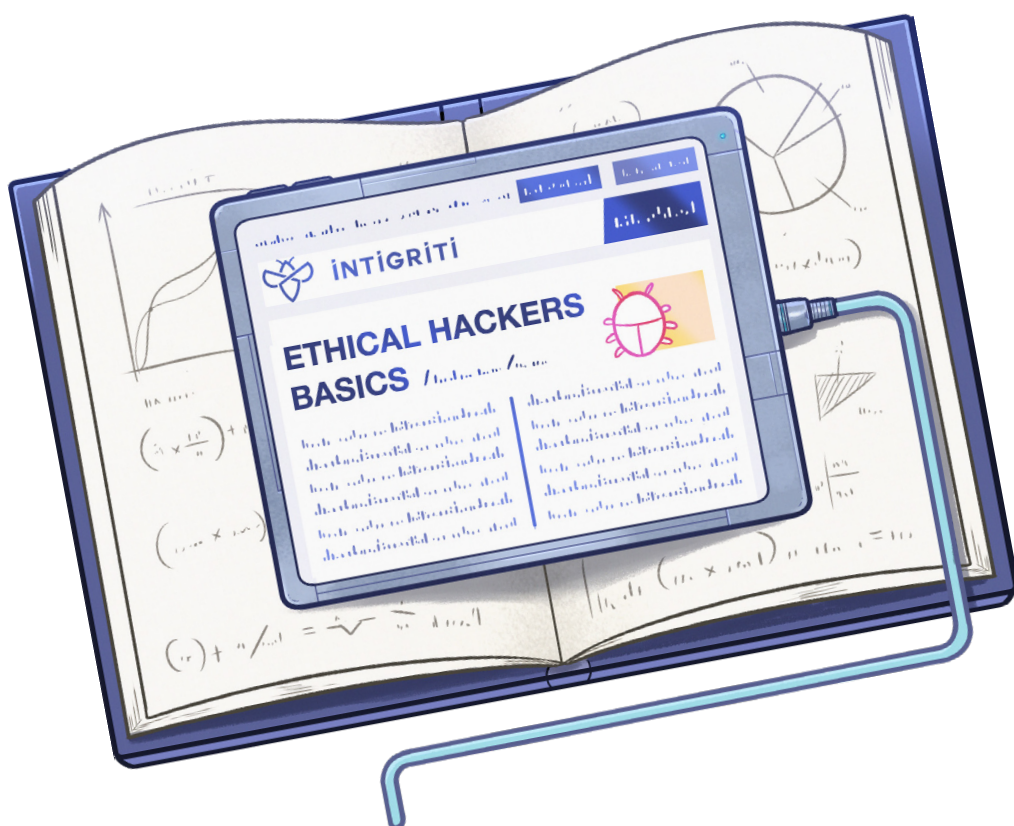
Security researchers are cybersecurity experts who use their skills and expertise to hack for good. They're also known as bug bounty hunters, white hat hackers and ethical hackers. Some of Intigriti's researchers are dedicated to bug bounty hunting full-time, whilst others are employed in full-time jobs.

#### ③ 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.

#### ③ 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.





# How crowdsourced security helps organisations overcome cybersecurity challenges



## The challenge

### ⊗ Cybersecurity skills gap

95% of security professionals say the cybersecurity skills shortage is an **increasing challenge** ([↗ SearchSecurity<sup>1</sup>](#)).

### ⊗ Staying on top of cyber threats

59% of security professionals say the demands of their job makes it **difficult to find time for training** ([↗ SearchCompliance<sup>2</sup>](#)) – yet cyber threats continue to evolve.

### ⊗ Growing attack surfaces

Digital transformation, moving to the cloud and scaling fast in continuous development cycles has resulted in ever-expanding attack surfaces. This has led to a massive **increase in cyber threats** globally year-over-year ([↗ Help Net Security<sup>3</sup>](#)).

### ⊗ The cost & limitations of pentesting

The average cost of a high quality pentest is between \$10,000-\$30,000 USD ([↗ RSI Security<sup>4</sup>](#)). To run them continuously would be highly **costly & unsustainable** as you pay for testing time, not for results.

### ⊗ 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**.

### ⊗ Lack of resources

With higher expenses and new processes for enabling **continuous growth**, acquiring adequate cybersecurity resources can be a challenge.

## Bug bounty as a solution

### ✓ Tap into a network of security experts

Leverage the skills, experiences, expertise, and creativity of **thousands of security experts**.

### ✓ Invest in your team's development

Like a malicious hacker, bug bounty hunters are wired to spot what your team might miss. Organisations **invest in internal talent** by allowing them to learn from incoming submissions and interactions from researchers.

### ✓ 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.

### ✓ 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.

### ✓ 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, hacker-way of thinking and awareness throughout the year.

### ✓ Centralise security testing

Bug bounty programs allow organisations to continuously test cybersecurity defences **within one platform**, and through the power of a crowd.

<sup>1</sup>[searchsecurity.techtarget.com/feature/4-ways-to-handle-the-cybersecurity-skills-shortage](https://searchsecurity.techtarget.com/feature/4-ways-to-handle-the-cybersecurity-skills-shortage)

<sup>2</sup>[techtarget.com/searchsecurity/feature/Cybersecurity-professionals-Lack-of-training-leaves-skills-behind](https://techtarget.com/searchsecurity/feature/Cybersecurity-professionals-Lack-of-training-leaves-skills-behind)

<sup>3</sup>[helpnetsecurity.com/2021/02/26/expanding-attack-surfaces/](https://helpnetsecurity.com/2021/02/26/expanding-attack-surfaces/)

<sup>4</sup>[blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing](https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing)



## About Intigriti

### Agile security 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.



#### 90,000+ researchers

More than 90,000 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 European presence

Intigriti has a strong global presence. In terms of hacker pay-outs, the 10 best performing countries are globally represented in America, Europe and Asia. In 2021, vulnerabilities were submitted from more than 170 countries.

#### TAKE YOUR FIRST STEPS

-  Request a demo [www.intigriti.com/demo](https://www.intigriti.com/demo)
-  Visit the website [www.intigriti.com](https://www.intigriti.com)
-  Get in touch [hello@intigriti.com](mailto:hello@intigriti.com)

### How vulnerability management works on Intigriti



### You're in good company

Revolut



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.**