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

Proactive security testing

Security researchers are incentivised to find weaknesses and report them to your development team or engineers to fix.

Continuous coverage

With thousands of cybersecurity experts at your disposal, you can scale and continuously test your digital assets without increasing headcount or putting pressure on your team.

Quality assurance

All reports are validated and approved by our triage department first, meaning your internal teams can work smarter and faster.

Cost efficient

Bug bounty programs follow a pay only for results model, meaning keeping systems consistently secure is more affordable than infrequent but more costly alternatives.

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?

71%

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

53

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

37

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

<24-hours

Is how long it takes on average for Intigriti's triage team to review, and accept or reject a report.

About Intigriti

Intigriti 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. Intigriti goes beyond traditional pentesting or bug bounty programs; our customers publicly acknowledge our advanced guidance and unmatched agility.

400+ live bug bounty programs: Companies of all sizes, and across multiple industries, trust Intigriti to launch their bug bounty program. On average, 71% get a high to critical submissions within 48 hours of their program going live.

Strong European presence: In terms of hacker payouts, 8 out of 10 of the best performing countries were European. However, Intigriti is very much a global business. In 2020, vulnerabilities were submitted from more than 140 countries.

50,000+ researchers: Today, we have more than 50,000 researchers using Intigriti to hunt for bugs — and we're growing!

GDPR Complient: Compliance with the highest security standards.

Bug bounty programs vs penetration testing

Companies hire third-party agencies to complete a penetration test. Typically, it's performed for regulatory or compliance reasons, to honour a contractual agreement, or to meet customer expectations.

While penetration tests can be valuable, they are very different from working with ethical hackers on a bug bounty program.

	PENTESTING	BUG BOUNTY
Team size	SMALLER TEAMS OR INDIVIDUALS	THOUSANDS OF SECURITY RESEARCHERS
Brief	METHODOLOGY DRIVEN	CREATIVE APPROACH
Deadline	TIME-BOUND	CONTINUOUS
Invoicing	PAY FOR TESTING TIME	PAY FOR RESULTS
Scope	NARROW SCOPE	BROAD SCOPE
Resources	EXPERTISE & SKILLSETS OF SPECIFIC INDIVIDUALS	EXPERTISE & SKILLSET OF A CROWD

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.

Visit the website www.intigriti.com Get in touch hello@intigriti.com

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