



A GUIDE TO

Securing SaaS applications with continuous crowdsourced testing

Continuous security testing powered by crowd knowledge





Table of contents

4	Introduction	12	VDP vs bug bounty programs: What's the difference?	24	Hybrid pentesting: Combining the best of bug bounty with pentesting
5	A look at SaaS now	14	Ethical hacker communities	26	Glossary
6	Why SaaS organizations hire ethical hackers	17	How bug bounty programs work with Intigriti	27	About Intigriti
7	Clear vulnerability reporting structures	18	How Visma uses Intigriti to protect an ever-expanding attack surface		
8	VDP best practices: What to include	22	Penetration testing vs bug bounty programs		
10	Moving beyond “see something, say something” and incentivizing action				



Introduction

In recent years, there has been an exponential adoption of Software-as-a-Service (SaaS) solutions by businesses and individuals alike. So much so that the industry **has increased in size by around 500% over the past seven years¹. It's also thought that SaaS applications now make up 70% of total company software use².**

SaaS is known to deliver many advantages beyond simply making data available to users everywhere. Security, networks, hardware provisioning, software updates, etc. are all handled by the SaaS subscription provider, saving time and money, and allowing IT teams to focus on more strategic roles. Thanks to agile methodologies, SaaS tools are evolving so quickly that users can leverage their data and assets in innovative and highly productive new ways.

However, the widespread availability of valuable and sensitive data online also presents a lucrative target for malicious actors. Reports indicate that **45% of security incidents now are cloud-based³**, and so the need for robust cybersecurity measures has never been more pressing.

If you're reading this eBook, it's fair to assume that you are already facilitating the process for better security testing. Read on to discover:

- **Who** ethical hackers (security researchers) are
- **Why** SaaS Providers work with ethical hackers to strengthen their cybersecurity defenses
- **What** the difference is between responsible disclosure and incentivized disclosure methods
- **How** bug bounty programs differ from traditional security testing methods.

Plus, we'll cover best practices for creating a strong vulnerability reporting process.

¹go.intigriti.com/saas-statistics-and-trends

²go.intigriti.com/saas-statistics-and-trends

³go.intigriti.com/50-cloud-security-stats



A look at SaaS now

SaaS grew up fast

The growth of SaaS has been nothing short of spectacular. According to Statista, revenue in the SaaS market **is projected to reach US\$282.20bn in 2024⁴**. Clearly, the benefits of SaaS have been grasped by the business community.

Cloud-busting is making it rain

The rapid adoption of SaaS has also sparked some unwelcome trends. **According to a recent survey⁵**, 80% of companies have experienced at least one cloud security incident in the last year. With so much private and valuable data now online, it is inevitable that malicious hackers are seeking to breach cybersecurity defenses.

SaaS and the future of work

SaaS has emerged as a pivotal asset for businesses in recent years, particularly in catalyzing the shift towards remote work as the new norm. SaaS provides businesses with flexibility and connectivity, and today **99% of businesses use at least one SaaS solution⁶**.

SaaS Security at scale remains a concern

If SaaS promised—and delivered—a brave new world for users, it also delivered a new wild west for IT and Security departments. With the threat of security management being taken out of their hands, many enterprise players have hesitated over adopting SaaS for mission-critical services.

⁴go.intigriti.com/saas-worldwide

⁵go.intigriti.com/state-of-cloud-security-report

⁶go.intigriti.com/saas-statistics





Hiring ethical hackers enables businesses to:

- ✓ Reduce the risk of losses from a cyberattack
- ✓ Show a commitment to continuous security testing
- ✓ Increase their reputation and trustworthiness as data protectors
- ✓ Keep up with ever-evolving cyber threats
- ✓ Develop their internal teams based on key learnings and insights



Why SaaS organizations hire ethical hackers

Ethical hackers, or security researchers, are highly skilled individuals that can safely simulate the behaviors of malicious hackers to highlight weak links and blind spots in a company's digital environment. By working with ethical hackers, SaaS organizations can be alerted to their security vulnerabilities before they're potentially exploited.

Not only does this improve the strength of their IT security posture, but it empowers them to stay one step ahead of cybercriminals. Another reason companies employ ethical hackers is because it helps limit their liability. In the case of a real cyberattack, for example, businesses can demonstrate the steps they've taken to avoid it.



Our Security Director has a simple rule of thumb. He says \$1 spent in bug bounty is between \$10 and \$100 later — and I completely agree with him.

IOANA PIROSKA

SECURITY ENGINEER & BUG BOUNTY PROGRAM MANAGER, VISMA

Many in the security industry describe vulnerability disclosure policies as following a

“
see something,
say something
approach.”



Clear vulnerability reporting structures

What is a vulnerability disclosure policy?

Having a vulnerability disclosure policy (VDP) for your website is important because it allows ethical hackers (and good-willed citizens) to assist your business if they come across a security vulnerability.

By having a policy, your business:

- Shows a public commitment to cybersecurity
- Builds trust with customers and other stakeholders
- Reduces the risk of potential exploitations going undetected
- Decreases the risk of losing revenue due to an expensive cyberattack
- Minimizes time-to-remediation
- Streamlines your vulnerability reporting process

Without a VDP, 44% of vulnerability submissions aren't successfully reported

When an ethical hacker identifies a vulnerability, the majority will look for a way to report it to the concerning business.

Worryingly, 70% of Intigriti's ethical hacker community have identified vulnerabilities for websites without a VDP. Of that group, 12% didn't escalate the report. For those that did, 32% of them said the report got lost in the process or they weren't sure whether it was successfully reported. That's 44% of the risks that remain potentially undetected.



VDP best practices: What to include

01

Company background

Make sure to provide a brief background on your business within this opening section. For example:

- Who you are
- Business purpose
- Unique selling points
- Customers
- Other relevant stakeholder groups

The reason for providing context around your business is because it helps the researcher know what is important to you from a security standpoint.



SCAN

TO SEE MORE VDP
TIPS ON OUR BLOG

TIP

02

Commitments

In this section, you can declare your commitments to customers and stakeholders, and explain how you intend to keep their data safe. This is a good opportunity to introduce the reasons why you have the policy, and how it helps your business honor its promises.

03

Scope

The scope is mostly directed at security researchers but is helpful for other stakeholders (such as partners, regulators and the media) to be aware of too. The essence of this section is to guide researchers on what is acceptable to test for vulnerabilities. However, the scope also defines:

- Types of vulnerabilities that should be reported
- Products, features or assets that your company would especially like researchers to test
- Behavior that is not allowed, such as disruption testing or privacy violations

A good scope will not only clearly explain what the company perceives to be within the scope but also what they perceive to be on the outside. Doing this helps put everyone on the same page from the offset.

go.intigriti.com/vdp

A good VDP should detail what information the security researcher should report, as well as what they can expect from the disclosure process.

04

Legal safe harbor

You want ethical hackers to disclose bugs in your system responsibly without fear of legal consequences. Therefore, it's important to provide permission to act and to assure that no legal action will be taken against them, provided they remain in scope.

You're actively trying to encourage ethical hackers to report issues to your business. The language you use should be clear, concise but also inviting.

Here is an example of what you could write as part of your safe harbor policy:

"[Your company name] considers ethical hacking research conducted consistent with this policy to constitute as "authorized" under criminal and civil law. [Your company name] will not pursue civil action or initiate a complaint about accidental, good faith violations.

If legal action is initiated by a third party against you and you have complied with the Terms, [Your company name] will take steps to make it known that your actions were conducted in compliance and with our approval."

05

Reporting methods

This section outlines the process for how ethical hackers should submit vulnerabilities to your business. Be as clear as possible and never assume contributors will know what information you need to process a report. Cover aspects such as:

- Preferred communication channels
- What information they should include
- Whether you require submissions to be written in a specific language

Bear in mind that the researchers have already invested significant time and effort to test your systems so it's important to only ask for information you'll genuinely need. Ask for too much and you may put contributors off entirely.

06

What to expect after a submission

This area of the policy is a good place to outline how reports will be evaluated and what happens when they're accepted or rejected. You should also define a timeline for when they can expect to hear from you.

Including this information helps to manage expectations with regards to what kind of acknowledgements, recognitions and remuneration researchers can expect to receive. You should also indicate when researchers will know (if at all) whether they can publicly disclose a vulnerability they reported to you.



Moving beyond “see something, say something” and incentivizing action

Unlike a VDP, which takes a more passive approach to vulnerability reporting, bug bounty platforms allow businesses to work with independent security researchers to report bugs proactively.

SaaS companies will often launch and manage a bug bounty program through a platform, like Intigriti. Organizations with high-security maturity may open their bug bounty program to all ethical hackers in the platform’s community—known as a public program. However, most businesses begin by working with a smaller pool of security talent through a private program.

How bug bounty platforms work

Intigriti defines crowdsourced security through bug bounty platforms as “agile security testing powered by the crowd.” Below, we outline how a bug bounty platform is the connecting agent between thousands of ethical hackers and security-driven organizations.



Crowd

A global community of ethical hackers test your systems, software, digital assets, and devices against realistic threats. Ethical hackers look for weaknesses in your security in precisely the same way malicious hackers do, then report their findings.



Bug bounty platform

An interactive platform, usually a cloud service, that facilitates secure communications between ethical hackers and IT security teams, featuring real-time reports of identified vulnerabilities.



Expertise









Tap into the skills, knowledge, and experiences of an entire ethical hacker community. Plus, benefit from client support, continuous hacker engagement, technical expertise, program management, and more.



VDP vs bug bounty programs: What's the difference?

The key difference between a VDP and a bug bounty program is that a VDP follows a passive approach whereas a bug bounty program incentivizes action. Go to the next page to understand the similarities and differences between them on Intigriti's platform.



	VDP	BUG BOUNTY
 Compliance	Meets industry standards Supports ISO/IEC 29147:2018	
 Legal considerations	Provides a legal framework Companies provide contributors with assurance that no legal action will be taken against them provided reports are made in good faith.	
 Vulnerability management	Track submissions in real-time Companies can streamline the vulnerability disclosure process and keep track of submission security statuses in real-time, allowing them to obtain an accurate view of their security posture at all times.	
 Communication	Centralized within the platform No need for sharing encrypted mails, the platform will allow communication in a safe and reliable way.	
 Search culture	Say something, see something Allows people to report security issues when they notice them, without being afraid of legal repercussions.	Actively search & find something Security researchers are continuously activated through bounties, without being afraid of legal repercussions.
	No promises There is no promise for a reward, but a thank you is appreciated.	Rewarded for results Enables continuous security testing by incentivizing the community through bounties. The size of the reward depends on impact (severity).
 Reward system		
 Researcher quality	A diverse community of security enthusiasts In our experience, beginner to intermediate security researchers tend to focus on VDPs, whereas bug bounties attract more experienced hacking talent.	
 Quality assurance	Handled by Intigriti Intigriti's triage team provides a layer of quality assurance before escalating vulnerabilities to businesses. This means your security team only receives reports that are valid, unique, and in scope.	



Ethical hacker communities

Ethical hackers are highly inquisitive, curious, and investigative people. They're eager to develop their knowledge of the fast-moving and ever-changing security landscape.



▲ **The Ethical Hacker Insights Report⁸** found that 70% of our hackers operate on our platform to learn and develop their skills, and 40% are driven by the challenge.

For a fifth of our community, making the internet a safer and more secure environment is their primary goal.



⁸go.intigriti.com/ethical-hacker-insights-report

Earning potential is also an attractive aspect for security researchers. **Just over three-quarters (76%) of our community hack with a financial motive.** For example, 20% search for low-hanging fruit by choosing what they describe as 'easy targets.' 23% seek out bounties that offer fast payments, and a third (33%) look for vulnerability programs that offer a large maximum or minimum payment.

Reasons for picking a bug bounty target according to [The Ethical Hacker Insights Report](#)⁸

68%

says lots of scope

42%

says responsive team



80%

of our community **work within the IT industry** and use Intigriti as a secondary source of income.

Where do the rest come from?

- Engineering or manufacturing
- Business, consultancy, or management
- Healthcare
- Teacher training or education
- Accountancy, banking or finance
- Energy and utilities
- Media
- Retail
- Law
- Public services or administration



Most of Intigriti's researchers are young adults — but don't let that dupe you into thinking they're lacking experience. **More than half (55%) of our community have completed a bachelor's degree and a further 15% have a master's degree.** The majority are working within cybersecurity-related jobs and 40% hold an official information security certificate.

The majority (80%) of our community work within the IT industry and use Intigriti as a secondary source of income. However, 79% still devote up to 20 hours a week to bug bounty hunting. **For their day-job, popular professions include Penetration Tester (43%), Security Analyst (27%), and Software Developer (6%).**



How bug bounty programs work with Intigriti



The security researcher **searches** for a **vulnerability**



The researcher **submits** a **report** via Intigriti



Intigriti's **triage** team begins **communication** with researcher



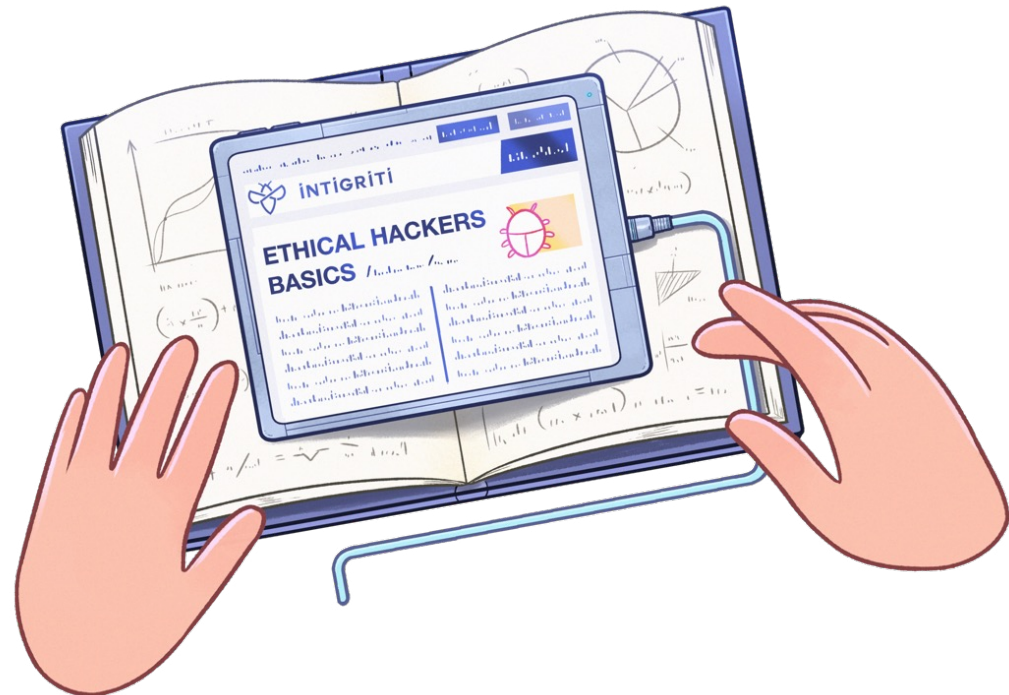
Intigriti's **triage** team applies **quality assurance** steps



In-scope, unique and well-written **reports** are **submitted** to the client



The **client** **accepts** the report, and **payment** is **automatically** processed



[REQUEST A DEMO](#)



How Visma uses Intigriti to protect an ever-expanding attack surface

About Visma

Visma is a leading provider of cloud software solutions in Europe and Latin America, with over 1 million active customers. They provide solutions that simplify and digitize core business processes. Their vision is to shape the future of society through technology by building and delivering software solutions in the private and public sectors.





The challenge

Providing complete cybersecurity for a vast and rapidly evolving attack surface

Visma has a roster of over 6,000 talented developers pushing out software on agile timeframes from multiple entities. Visma is also growing fast. On average, they acquire a new company at the staggering rate of nearly one per week. These factors make a well-organized and scalable cybersecurity strategy for their attack surface essential. However, they also make it very challenging.

As Visma's Security Engineer & Bug Bounty Program Manager, Ioana Pirooska has a key role in ensuring onboarding and continuous security assurance for the internal teams at Visma.

- “
- “Our job in the security department is
 - to help all these internal teams improve
 - the security of their products. We do this
 - through a security program called the
 - Visma Security Program (VSP). VSP includes
 - training and awareness, code scanning SAST
 - and DAST (static and dynamic application
 - security testing, internal pentesting, threat
 - intelligence, log management, incident
 - response), and more.”

Although this thorough approach achieved good results, it wasn't sufficient in protecting against specific security threats that Visma faced. As Ioana explains:

- “
- “There are bugs that automated tools for
 - scanning cannot pick up. For these, you need
 - to understand the application flow. Only the
 - human mind is capable of doing this. So, while
 - our automated tools are vital, they can't cover
 - all the required bases.”

Visma, therefore, knew they needed a human component that would complement and complete their security testing.

The solution

Using the Intigriti bug bounty platform to leverage human skills

Scanners and other automated cybersecurity testing tools are renowned for finding common vulnerabilities in systems and software. However, they have their limits, so Visma turned to the Intigriti bug bounty platform to supplement their automated testing.

Rapid scalability was a must for such a large and diverse company, as was high-quality support as they quickly grew their presence on the Intigriti

platform. Ioana explains why the partnership with Intigriti immediately worked so well:

- “
- “Intigriti is very close to its customers. We
 - have personal and direct contact with our
 - success manager, who answers our questions
 - almost instantly via Slack. At the same time,
 - the product team listens, and we've seen
 - several features implemented
 - on our request.”



The result

Hitting security goals

When Ioana and her team set up their Intigriti bug bounty programs at Visma, they had some clear goals in mind. These included continuously onboarding new product teams; onboarding their marketing websites; launching a Responsible Disclosure program on the platform; and making sure they had a fast process in place to triage reports, pay bounties, and resolve bugs.

They hit every goal and saw a significant improvement in cybersecurity as a result.

Beyond scans and pentests

Pentests and other automated scans remain a critical part of VSP at Visma. However, Ioana is clear that bug bounty programs need to complement these processes to provide additional cybersecurity testing:

“With bug bounty programs, your tests are performed continuously, compared to a normal pentest which takes place once or twice a year. Add to this the advantage of the number of testers you have through crowdsourcing. In a bug bounty program, hundreds of testers can look at your digital assets simultaneously.”

Ioana also worked with her Intigriti Success Manager to tailor private bug bounty programs to Visma's specific needs for the initial onboarding of products:

“With Intigriti, we were able to run private programs where we could choose which specialized hackers to invite to cover all programming languages, web apps, and mobile apps. As a result, the quality of the reports is outstanding.”





Greater visibility and security awareness internally

Using bug bounty programs as a core component of VSP has paid dividends for security at Visma. Since launch, the program has already received over 3,000 submissions, 98% of which are valid. As Ioana explains:

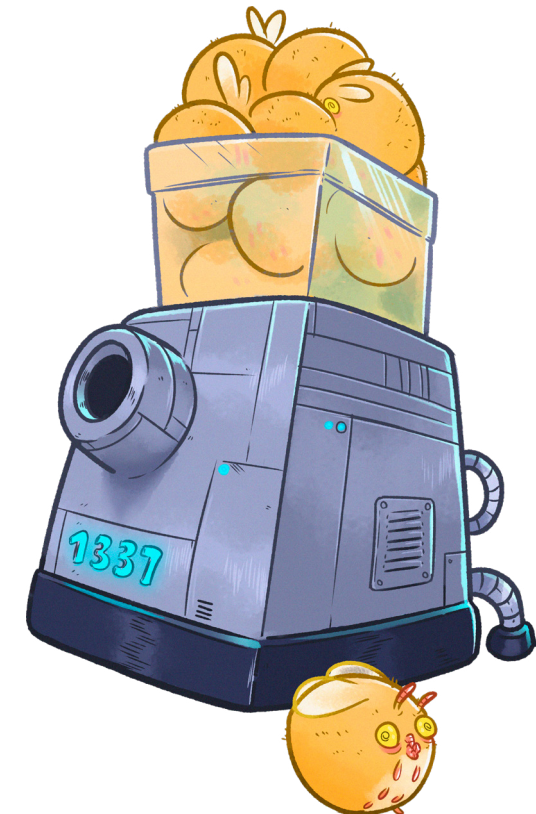
“More than 50% of the vulnerabilities discovered are IDOR or access control problems, which are bugs that automated scanning tools cannot find. In my view, this is one of the highest values of bug bounty programs in general. Some of these findings could have had huge consequences if they were not surfaced and fixed as a result of the

bug bounty program.”

Beyond these timely findings, Ioana has seen other significant benefits to running a bug bounty program through the Intigriti platform:

“The reports we receive are great learning materials for our internal teams. They see their mistakes and learn how to avoid them in the future. They also learn how hackers think, and this helps them create products that are “secure by design.” There’s no doubt that security awareness has elevated because of the program. Today our teams feel more confident about security.”

The team’s time to fix vulnerabilities also decreased as a result of these factors.





Penetration testing vs bug bounty programs

Bug bounty programs and penetration tests (pentests) both aim to identify vulnerabilities that could be exploited by hackers. However, there are some key differences. Pentests focus on one moment in time, whereas bug bounty programs are continuous.

Whilst you'll receive a certificate to say you're secure at the end of a penetration test, it won't necessarily mean that's still the case the next time you make an update. This is why continuous testing is important.

Another big difference between pentests and bug bounty programs is the pricing model. With a bug bounty platform, the security researcher gets a fee if they discover and report a previously undetected bug. What you pay also depends

on how critical the vulnerability is — you pay according to impact. Pentesting, on the other hand, pays for the service delivered by the ethical hacker.

Unlike pentesting, a bug bounty program doesn't follow a specific methodology. Businesses that opt into Intigriti's ethical hacking platform, for example, will pay a subscription fee to [list their program](#)¹⁰ in a controlled environment. This allows a community of ethical hackers to assess the security of their digital assets by taking a more creative approach.

Programs can be open to the entire community or they can be set to private. A private program means security researchers may only contribute to a company's program if they're invited.





¹⁰go.intigriti.com/bug-bounty-programs





PENTESTING

BUG BOUNTY

 TEAM SIZE	Smaller teams or individuals	Thousands of security reseachers
 BRIEF	Methodology-driven	Creative approach
 DEADLINE	Time-bound	Continuous
 INVOICING	Pay for testing time	Pay for results
 SCOPE	Narrow scope	Broad scope
 RESOURCE	Expertise & skillsets of specific individuals	Expertise & skillset of a crowd



Hybrid pentesting: Combining the best of bug bounty with pentesting

As an alternative to bug bounty programs and pentests, Intigriti defined a new approach. Hybrid pentests utilize aspects of both testing solutions to create a new and additional solution to what's currently available on the security testing market.

What is hybrid pentesting?

Intigriti's hybrid pentest is a program type specifically developed to support clients who need more control over their bug bounty security testing.

Ideally suited to the fast pace of change in the SaaS industry, this new solution can assist and augment a continuous testing strategy, depending on the organization's business needs:

BUSINESS NEED

Expanding the scope of a bug bounty program

Security teams can get a first glimpse of the security posture of a new asset before adding it to the scope of an existing bug bounty program. The hybrid pentest allows saas companies to better calculate the bounty budget on their new scope item.

BUSINESS NEED

New to bug bounty programs

SaaS companies can run a hybrid pentest to kick off their community-powered testing journey. They'll start with a single security researcher to get comfortable with Intigriti's platform, while at the same time ruling out low-hanging fruit.

BUSINESS NEED

Compliance requirements call for a penetration test

Fulfill testing and compliance requirements that come with a dedicated deadline. Intigriti's hybrid pentests provide a letter of attestation that SaaS companies can share with customers to prove the security maturity of their products.



SCAN¹¹

To learn more
about Hybrid
Pentesting



¹¹go.intigriti.com/hybrid-pentesting



Intigriti in numbers

53

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

37

is the **average number of submissions** that are accepted within the first week **of a program's launch**.

24h

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

48h

is how long it takes on average for customers to **accept or reject the report (if escalated)**.

23%

of our registered ethical hackers submit **at least one report every month**.

71%

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



Glossary

Q 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 and hack at their leisure.

Q Bugs

'Bugs' are **security exploits and vulnerabilities**. If deemed new and valuable, which depends on the scope provided within the program, the security researcher will report these via a submission.

Q Bounty

If the submission is accepted by the organization it relates to, the researcher is paid a **reward or compensation** which is better known as a 'bounty'.

The reward or compensation is typically monetary, but it can also be in the form of gifts like goodies and swag.

Q VDP

A vulnerability disclosure policy (VDP) is also known as a responsible disclosure policy. It provides ethical hackers with an **outline for submitting vulnerabilities to an organization**.

It's also an opportunity for organizations to demonstrate their willingness to work with external actors working in good faith.

Q Bug bounty program

A bug bounty program allows independent security researchers **to report bugs** to an organization in a legally compliant matter.

Q Bug bounty platform

A bug bounty platform provides a trustworthy infrastructure for security researchers to **engage and communicate** with companies **in a structured, safe, and reliable way**.

Most security researchers choose to report vulnerabilities through a bug bounty platform, like Intigriti.



About Intigriti

Intigriti is a rapidly growing cybersecurity company that specializes in crowdsourced security services to help organizations protect themselves from cybercrime.

Founded in 2016, Intigriti now has a global team of 100+ employees spread across Belgium, the United Kingdom, the Netherlands, and South Africa. And with the backing of our recent Series B Funding, we're planning on taking our growth to the next level.

Agile security testing powered by the crowd



What to expect as an Intigriti customer

01

Conquer the limitations of traditional security testing

Continuously test your digital assets for vulnerabilities by leveraging the expertise of Intigriti's 90,000 registered security researchers.

02

Industry-leading support

Only receive unknown, unique, valid, and in-scope vulnerability reports to enable your team to focus on business-critical tasks. Our offering also includes Account Management, Customer Success, Knowledge Base and Technical Support as standard.

03

Reduced risk

On average, Intigriti clients receive 53 vulnerability reports within one week of launching a bug bounty program through our platform. Intigriti's support empowers organisations to identify and remediate risks quickly.

04

Customized pricing

We provide a scalable model that is aligned to customer aspiration and program expansion. Clients of all sizes and from a wide array of business sectors utilize our services.

 Intigrity  hackwithintigrity  @intigrity  Intigrity  Intigrity



Contact us

Need some help getting started with ethical hackers? Our experts can help you maximise the success of your bug bounty program. Get in touch today to connect with the brightest and most experienced researchers on the globe.

[WWW.INTIGRITI.COM](https://www.intigrity.com)

HELLO@INTIGRITI.COM

Illustrations by [Zwoltopia](#)