INTIGRITI

A GUIDE TO

Crowdsourced security testing for financial services

Securing the bottom line

EBOOK

Table of contents

Introduction

Cybercriminals frequently target the financial services sector due to the abundance of confidential client information it carries. These attacks can be highly damaging, leading to monetary losses, harm to reputation, and damage to customer confidence. It is imperative for financial organizations to prioritize cybersecurity and take proactive steps to defend against constantly evolving threats.

The sector faces a significant financial burden due to cybercrime. According to **recent estimates**, global cybercrime costs the financial services industry billions of dollars annually. These losses stem from various factors, including stolen funds, business disruption, regulatory fines, and the cost of implementing cybersecurity measures. Cyberattacks can also lead to a loss of customer trust, which can further damage an organization's reputation and profitability.

Luckily, the financial services industry does not need to fight this cybersecurity battle alone. Worldwide, thousands of security researchers are using their ethical hacking skills for good through crowdsourced security testing platforms, such as Intigriti.

RESEARCHER
Sklon

[1]go.intigriti.com/blackfog

If you're reading this eBook, it's fair to assume that you are already facilitating the process for better security testing within your organization. Read on to discover how ethical hacking communities can help security teams to:

- → Ensure sufficient testing coverage for all assets
- → Access real-world threat simulations
- → Identify and address vulnerabilities before malicious hackers do
- → Mitigate vulnerabilities through continuous security testing
- → Bolster cybersecurity posture while complying with industry regulations

Keep reading as we also put a leading banking app in the spotlight to showcase how they're already tackling these challenges.

RESEARCHER
Foodbar7

Where penetration testing falls short

A crucial method for enhancing cybersecurity readiness is through the implementation of penetration testing (pentesting). Pentesting is a critical tool for financial institutions to protect themselves from cyberattacks. By simulating real-world attacks, pentesting helps financial institutions identify and fix vulnerabilities before they can be exploited by malicious actors.

However, despite its benefits, there are some common pain points we hear today from security professionals in the industry that penetration tests fail to address.

Limited scope

Penetration tests may focus on specific systems or applications, leaving gaps in coverage across the entire IT infrastructure.

Lack of context

Penetration test reports may lack context or actionable insights, making it challenging for organizations to prioritize and remediate identified vulnerabilities effectively.

Limited coverage of emerging threats

Traditional penetration tests may overlook emerging threats or attack vectors, such as zero-day vulnerabilities.

False sense of security

Penetration tests provide a snapshot of security posture at a particular point in time, potentially leading to a false sense of security as threats evolve.

Inability to mimic real-world attacks

Penetration tests may not accurately simulate real-world attack scenarios, failing to uncover vulnerabilities that adversaries could exploit.

Resource intensive

Penetration tests can be resource-intensive and time-consuming, especially for large, complex financial institutions with extensive IT infrastructure.

Scalability challenges

Traditional penetration testing approaches may struggle to scale to meet the evolving needs of dynamic financial services organizations.

A proven solution to these challenges is to invite ethical hacker (security researcher) communities to help. Businesses can rely on the power of these crowds to assist them in their security testing. Further still, they can utilize bug bounty platforms to manage the remediation of new and unknown vulnerabilities.

RESEARCHER
FarahHawa

Bringing security testing into the 21st century

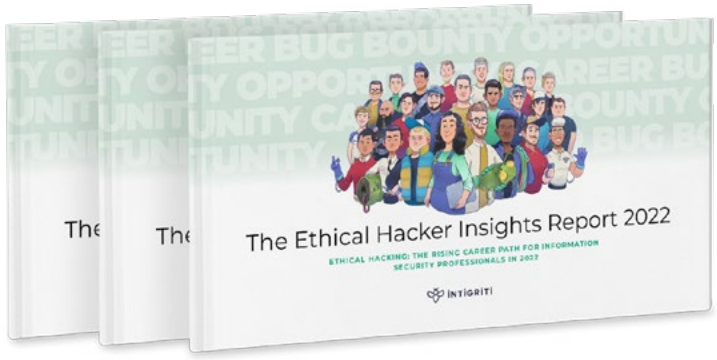
Ethical hackers are highly skilled individuals who can safely simulate malicious hackers' behaviors to highlight weak links and blind spots in a company's attack surface. Security teams, developers, and engineers at a financial company can quickly be made aware of vulnerabilities and fix them by working with ethical hackers. Not only does this improve the strength of their organization's overall cybersecurity posture, but it empowers them to stay one step ahead of cybercriminals.

A **vulnerability disclosure policy (VDP)**, **penetration test**, or a **bug bounty program** is the most common way to work with ethical hacker communities.

About 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 Report**[3] found that 70% of our hackers operate on our platform to learn and develop their skills, while 'the challenge' drives 40%. For a fifth of our community, making the internet a safer and more secure environment is their primary goal.

The unique occupation of bug bounty hunting offers a heightened level of freedom and lifestyle that traditional jobs cannot provide but that today's security professionals desire.



Intigriti's Report[4] explored this trend further and found that 96% of ethical hackers would like to dedicate more time to bug bounty hunting in the future, and 66% are considering it as a full-time career.

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%).

[3]https://go.intigriti.com/ethical-hacker-insights-report-2021
[4]https://go.intigriti.com/ethical-hacker-insights-report-2022

The QR code goes to this link
[4]https://go.intigriti.com/ethical-hacker-insights-report-2022

Working with ethical hacker communities

Before we explore how to maximize the success of working with ethical hackers through VDPs and bug bounty programs, let's take a quick look at the similarities and differences between them on Intigriti's platform.

	VDP	BUG BOUNTY
Compliance	**Meets industry standards** | Supports ISO/IEC 29147:2018 and ISO 27001:2013.	
Legal considerations	**Provides a legal framework** | Companies provide ethical hackers with the 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 always to obtain an accurate view of their security posture.	
Communication	**Centralized within the platform** | No need for sharing encrypted mails: the platform will allow secure and reliable communication.	
Search culture	**See something, say something** Allows ethical hackers to report security issues when they notice them without being afraid of legal repercussions.	**Actively search & find something** Security researchers are continuously motivated through bounties without being afraid of legal repercussions.
Reward system	**No promises** There is no promise of 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 the impact.
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.	

A step-by-step guide to building a vulnerability disclosure policy

What is a vulnerability disclosure policy?

Having a vulnerability disclosure policy (VDP) for your company's website is important because it allows ethical hackers (and good-willed citizens) to assist your business if they encounter 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 chance of losing revenue due to an expensive cyberattack
- Minimizes time-to-remediation
- Streamlines your vulnerability reporting process

Some companies choose to keep this process in-house, while others opt to publish a VDP on a bug bounty platform, such as Intigriti. Either way, many in the security industry describe vulnerability disclosure policies as following a "see something, say something" approach.

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 business concerned.

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

Considering that global **cybercrime costs the financial services industry billions of dollars annually**; 44% of undetected risks is a concerning statistic.

RESEARCHER
Alicanact60

[5] go.intigriti.com/cybercrime-in-the-financial-sector

VDP best practices: What to include

A good VDP should detail what information the security researcher should report and what they can expect from the disclosure process. We suggest including the below six components:

01

Company background

Ensure you provide a brief background on your business within this opening section. For example:

- Who you are
- Business sector & purpose
- Unique selling points
- Customers - B2B and/or B2C
- 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.

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 area is an excellent opportunity to introduce 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 also helpful to other stakeholders such as partners, regulators, and the media. 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 clearly explain what the company perceives to be within the scope and what they perceive to be outside. Doing this helps put everyone on the same page from the offset.

SCAN[6]
To see more VDP tips on our blog

[6]https://go.intigriti.com/vdp

04

Legal safe harbor

You want ethical hackers to disclose bugs in your system responsibly without fear of legal consequences. Therefore, it's essential 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 encouraging ethical hackers to report issues to your business. The language you use should be clear and 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 a third-party initiates legal action 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 establishes 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

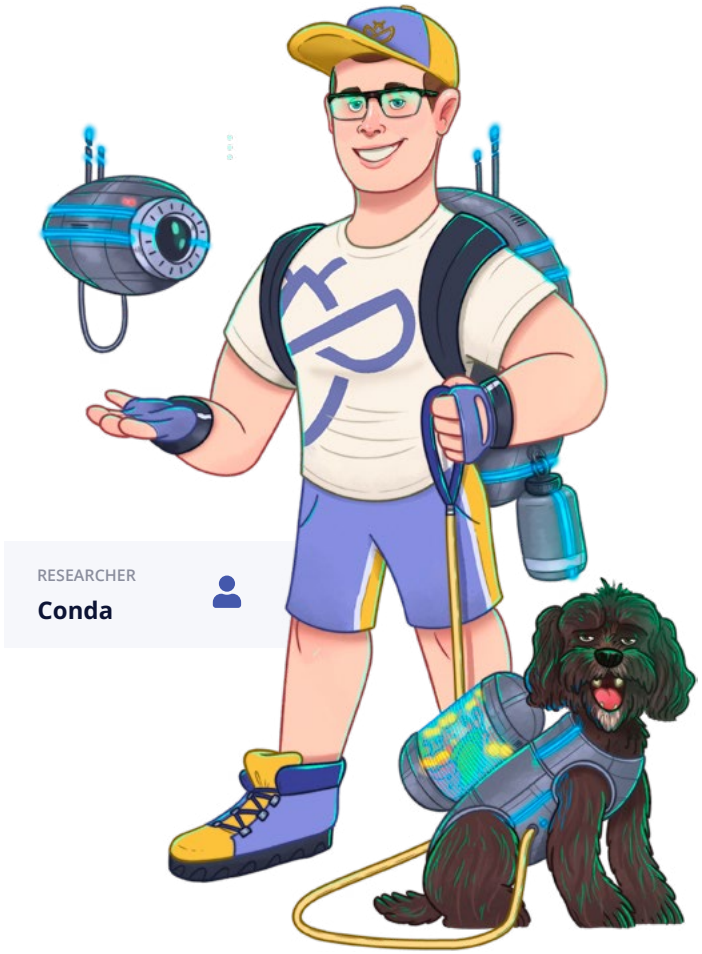
Remember that the researchers have already invested significant time and effort in testing your systems, so it's crucial to only ask for information you'll genuinely need. Ask for too much, and you may put contributors off entirely.

06

What to expect after a submission

This policy area is a good place to outline how your company (and bug bounty platform, if relevant) will evaluate reports 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 regarding what kind of acknowledgments, 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.

Financial services 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.

The impact of bug bounty programs on cybersecurity

By launching a bug bounty program, **organizations** experience:

More robust protection

Company data, assets, brand, and reputation have additional protection through continuous security testing.

Enabled business goals

An improved security posture leads to a more secure platform for innovation and growth.

Improved productivity

Increased workflow with fewer disruptions to the availability of services. More strategic IT projects that executives have prioritized, with fewer security "fires" to put out.

Increased skills availability

Internal security team's time is freed by using a community for security testing and triage.

Clearer budget justification

Ability to provide more significant insights into the organization's security posture to justify and motivate for an adequate security budget.

For **CISOs, CIOs, and security leaders**, the personal benefits of a successfully run bug bounty program are also impactful:

Peace of mind

Knowing that the organization's infrastructure, applications, and assets have an additional layer of security testing.

High morale

Team spirit improves by reducing manual tasks, resulting in other departments increasingly seeing the CIO or CISO as a good leader.

Confidence

The organization's security policy is progressive and more mature. The team and security leaders can hit personal and company cybersecurity KPIs.

Improved relationships

Project delays significantly decrease without the reliance on traditional pentests. The CIO or CISO comes to be seen as a project enabler rather than a roadblock by project managers, engineers, and other teams, resulting in a better reputation.

SUCCESS STORIES: cake

How Cake uses bug bounty programs as a tool for security transparency

About Cake

The free and independent banking app, Cake, allows its users to connect all their bank accounts into one central place, get a clear overview of their transactions and auto insights into their spending habits. It al makes bank accounts profitable again b giving the opportunity to earn cashbacks on purchases.

Cake's commercial model openly uses its user data to create reports and statistics about what consumers are spending on, which they then sell to companies. Privacy is a big selling point for the app: "Privacy and security are the basis of everything we do." User data is anonymised and aggregated

RESEARCHER
Rekter

The challenge

Ensure user data is continuously safe

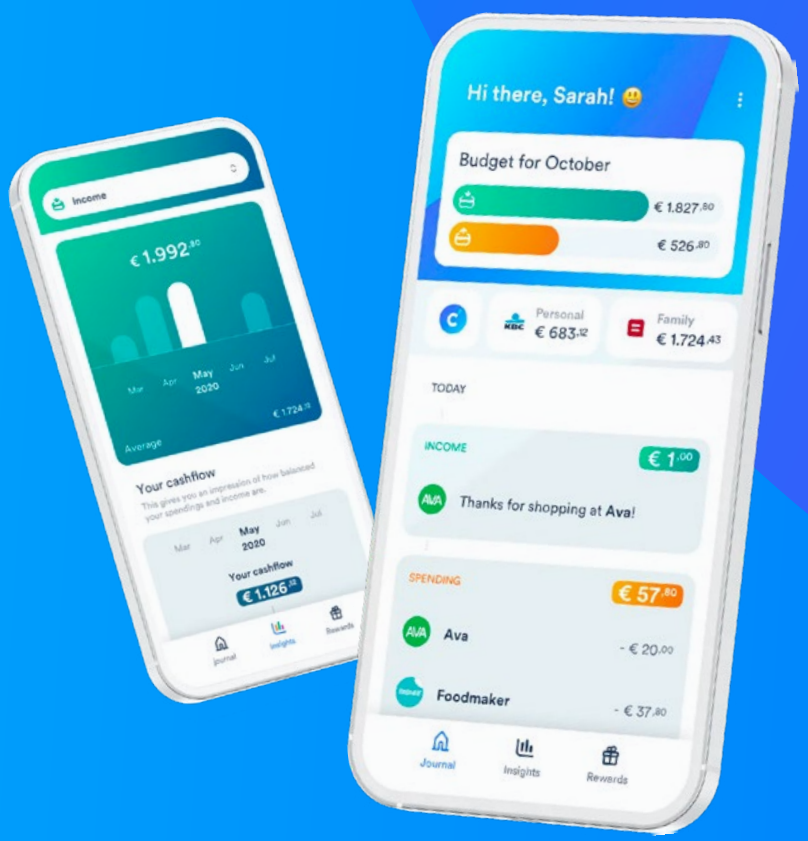
Building a financial service or product comes with operational and security risks — and Cake is no exception. The financial banking app has access to around 140,000 bank accounts in which they've processed more than 150 million transactions for a total monetary value of €36 billion.

Cake's Co-founder and Head of Engineering, Pieter Schelfhout, explains the importance of security within a banking app:

> "We have access to very sensitive information, so the security and privacy of our user's data are important to us. When you build something in the financial sector, you want to make sure that what you build is built securely."

For these reasons, Pieter was keen to encourage researchers to continuously try and hack Cake's systems to expose the vulnerabilities that his team might miss.

After some research, he decided to launch a set of bug bounty programs on the Intigriti platform. Like Cake, Intigriti is a Belgian startup with big ambitions — and Pieter was also keen to work with a company that offered flexibility in terms of their security testing setup needs.



SUCCES STORIES: cake

The solution

Launch a private and public bug bounty program

Cake's first program on Intigriti is public and focuses on its consumer-facing app. Security researchers (ethical hackers) on the platform can report issues continuously, meaning Pieter's team always have the latest insights into the app's security posture.

Cake also runs a private program through Intigriti, which focuses on the app's back-end applications. A select few security researchers contribute to the program, which began with them being shared login credentials so that they can safely test for security vulnerabilities.

The result

Faster fixing of potential security issues

The programs have successfully given Pieter's team greater visibility over the app's attack surface:

> "One of the biggest advantages of using a bug bounty program and relying on a community of ethical hackers is the many different perspectives you get on your application. Our bug bounty programs have been a real success and we've been able to find several issues that we were able to fix quickly, thanks to Intigriti."

Pieter also explains why he is satisfied with the interaction his team gets on the platform and from the community testing their applications:

> "You can tell that you're working with a series of passionate ethical hackers. They will write very detailed reports about their findings. Our team then works with the hacker to mend the issue on our end, and the hacker will test the issue again once we've resolved it."

Bug bounty closely aligns with transparency & openness values

Cake's vision is to develop more tools for its users to improve their financial savviness. As part of the roadmap to achieve this goal, transparency and openness towards its users is vital. Cake's bug bounty program is a key part of this journey.

> “Having a bug bounty program closely aligns to our values. It shows we don’t just want to do security; we want to be open about security and try to use the wisdom of the crowd to get as much feedback as possible."

PIETER SCHELFHOUT
CO-FOUNDER AND HEAD OF ENGINEERING

How bug bounty programs work with Intigriti

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

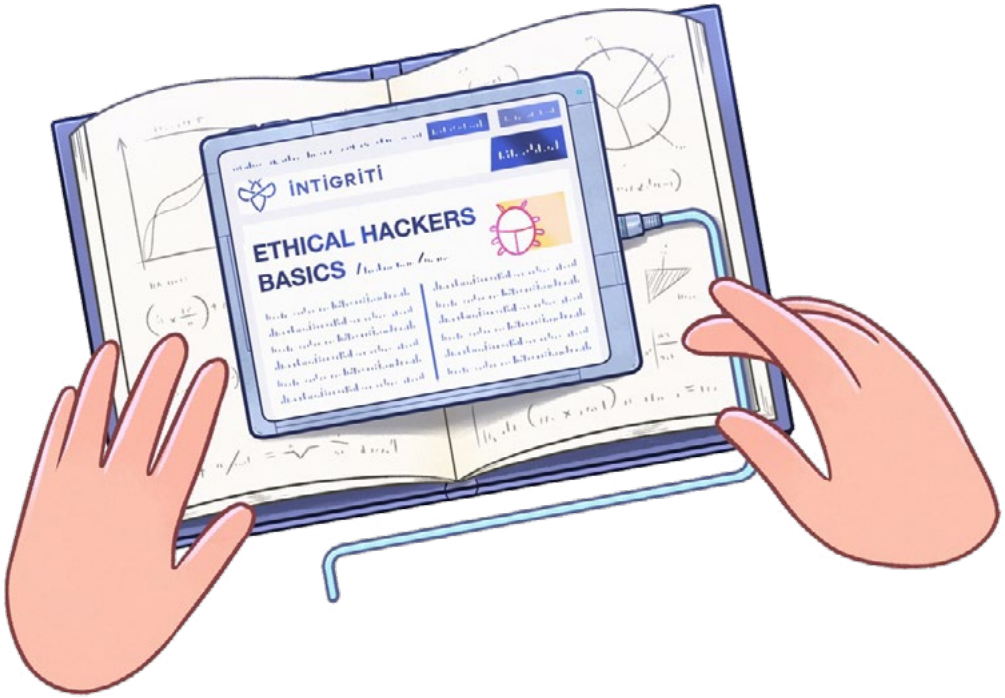
The researcher **submits** a **report** via Intigriti

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



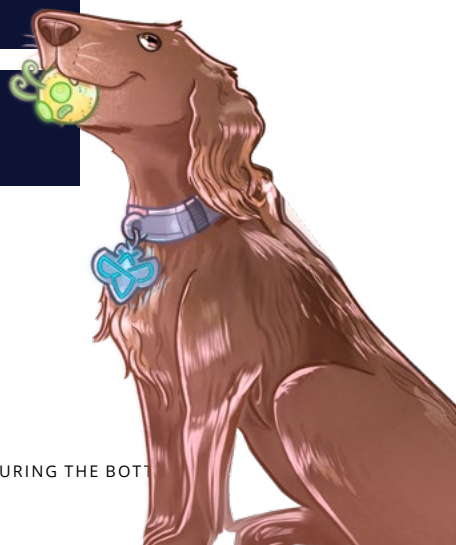
REQUEST A DEMO

Penetration testing vs. bug bounty programs

There are some alternatives to bug bounty programs, such as penetration tests (pentests.) Bug bounty programs and pentests both aim to identify vulnerabilities that hackers could exploit. However, there are some key differences:

While your company will receive a certificate to say it's 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 where bug bounty programs work well as a follow-up to pentests.

	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.

SCAN[13]
To learn more about Hybrid Pentesting

[13]https://go.intigriti.com/hybrid-pentesting

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.

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 companies to better calculate the bounty budget on their new scope item.

BUSINESS NEED

New to bug bounty programs

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 companies can share with customers to prove the security maturity of their products.

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

Bug bounty program

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

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.

Security researchers

Also known as bug bounty hunters, white hat hackers, and ethical hackers. Security researchers are cybersecurity experts who use their skills and expertise to hack for good. Some of Intigriti's researchers are full-time bug bounty hunters, while others are employed in full-time jobs and hack during their leisure time.

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.

Bounty

If the organization accepts the submission, the researcher receives a reward or compensation, better known as a 'bounty.'

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.

Hybrid pentesting

The hybrid pentest enables our clients to request dedicated security testing time from a selected researcher within a fixed time window. However, it comes with the reward model, motivation, reporting, and triage of bug bounty programs.

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

Information from Q2/2024. We are constantly growing, so please contact our sales department or see our website for an accurate number.

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—all submissions are rigorously assessed by our dedicated triage team before we transmit them to the client. This enables your team to stay focused on business-critical tasks. Our offering includes triage, account management, customer success, knowledge base, technical support, and more.

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 organizations to identify and remediate risks quickly.

04 Customized pricing

We provide a scalable model that aligns with customer aspirations and program expansion. Clients of all sizes and from various business sectors, use our services.

Intigriti hackwithintigriti @intigriti Intigriti Intigriti

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

HELLO@INTIGRITI.COM

Illustrations by Zwoltopia