An introduction to crowdsourced security for businesses

Agile security testing powered by the crowd

EBOOK

Table of contents

3 Organizations without vulnerability disclosure policies are failing to address researchers' security warnings

4 How do businesses address this issue?

5 Ethical hacking explained

6 Why do companies hire ethical hackers?

7 Deciphering bug bounty terminology

8 Can investing in crowdsourced security help mitigate costly security breaches?

9 Who should pay for bug bounty rewards? Allocating budget for your crowdsourced security program

10 How companies handle vulnerability management on Intigriti

11 Penetration testing vs bug bounty programs

13 Classic vs Pentest as a Service (PTaaS)

15 How Kinepolis uses its bug bounty program to keep its systems safe

17 How crowdsourced security helps organizations overcome cybersecurity challenges

19 How Brussels Airlines uses a bug bounty program to improve IT security posture

21 The pros and cons of a DIY bug bounty program

23 How the European Commission helps secure open-source software

27 About bug bounty communities

29 Handling hesitations & misconceptions around crowdsourced security

33 What happens at a live hacking event?

34 About Intigriti

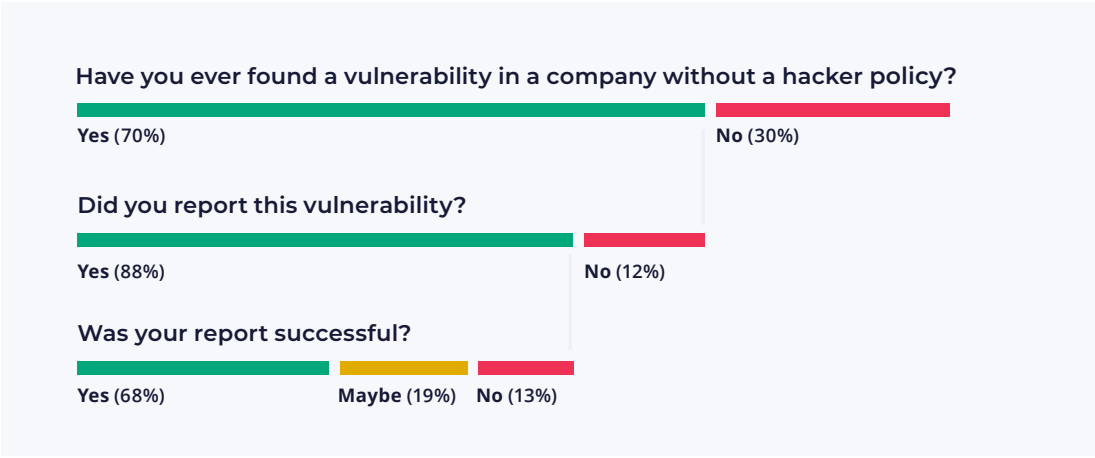
Organizations without vulnerability disclosure policies are failing to address researchers' security warnings

The challenge of digitalization 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.

Added to this, the EU Cyber Resilience Act[1] mandates that any software or hardware sold within the European Union must have adequate security vulnerability management embedded throughout the product lifecycle, from design to end product. In short, the act seeks to:

- → **Make products and services safer**
- → **Ensure consumers are more aware of cybersecurity**
- → **Guarantee that manufacturers take responsibility for the cybersecurity of their products before and after-sale**
- → **Drive better product cybersecurity throughout the EU into the future.**

Therefore, the need for modern, proactive security has never been more important. A simple yet proven method to protect against cyber threats is to invite ethical hackers in. But who are these people? And where might you find them? Well, chances are, they've already been trying to communicate with you. According to The Ethical Hacker Insights Report[2], 70% of ethical hackers have found a vulnerability within a company's website but found no clear route to report it (such as a Vulnerability Disclosure Policy.) Fortunately, 88% of those people still take steps to reach out to the company about security risk concerns—but only around two-thirds (68%) of reports are submitted successfully.



Source: The Ethical Hacker Insights Report | Intigriti[3]

[1] https://go.intigriti.com/eu-cyber-resilience-act
[2,3] https://go.intigriti.com/ethical-hacker-insights-report

How do businesses address this issue?

Bug bounty programs, PTaaS and other crowdsourced security services such as live hacking events, allow businesses to work with independent security researchers (also known as ethical or white hat hackers) to report bugs. Most security researchers choose to report vulnerabilities through a platform like Intigriti. This is because a crowdsourced security platform provides the legal framework for security researchers to engage and communicate with companies in a structured, safe, and reliable way.

By continuously working with ethical hackers, organizations become aware of and fix their vulnerabilities. Not only does this improve the strength of their cybersecurity posture, but it empowers them to outmaneuver cybercriminals.

However, getting started with crowdsourced security often begins with questions. In this ebook, we'll attempt to provide greater clarity on bug bounty programs, PTaaS, ethical hackers, and more.

Ethical hacking explained

‘Hacking’ refers to the action of using computer programming or technical skills to break through a cybersecurity barrier. Mainstream media coverage of hacking tends to associate this with something criminal. However, ethical hacking is quite the opposite.

What is an ethical hacker?

Like malicious hackers, ethical hackers have extensive knowledge of systems, codes, and programming. They’re also driven by a shared overriding goal: to break through a target’s defence systems. However, as the name suggests, an ethical hacker operates within the law and will disclose vulnerabilities to the companies they work with.

Today, many companies (including Google, Facebook and Microsoft) hire ethical hackers to work with them to find cybersecurity vulnerabilities in their digital assets.

RESEARCHER
tamaytandiran

At Intigriti, we often refer to ethical hackers as **‘security researchers’**. We find that this term does more justice to the long hours of research, study and perseverance it takes to find vulnerabilities while avoiding any of the negative connotations that are sometimes associated with the term hacker.

Why do companies hire ethical hackers?

There are a few reasons why companies hire ethical hackers. Primarily, employing the help of ethical hackers enables businesses to execute a defensive strategy with an offensive approach.

Ethical hackers are highly skilled individuals and can safely replicate the behaviours of malicious hackers to highlight weak links and blind spots in a company's attack surface. By working with ethical hackers, companies become aware of and fix their vulnerabilities. Not only does this improve the strength of their cybersecurity 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 case of a real cyberattack, businesses can demonstrate the steps they've taken to avoid it.

Hiring ethical hackers also enables businesses to:

- → **Show a commitment to continuous security testing**
- → **Reduce the risk of losses from a cyberattack**
- → **Increase their reputation and trustworthiness as data protectors**
- → **Better keep up with ever-evolving cyberthreats**
- → **Develop their internal team based on key learnings and insights.**

There are a few types of ethical hackers that businesses can employ, including security researchers and penetration testers.

> Bug bounty programs and responsible disclosure (RD) are an essential part of Visma's Security Program, and it's the final layer of security verification we can do for our applications.

IOANA PIROSKA
SECURITY ENGINEER AND BUG BOUNTY PROGRAM MANAGER AT VISMA

Deciphering bug bounty terminology

Bug bounty programs often come with a set of terminologies and jargon specific to the field of cybersecurity and ethical hacking. Here are some common terms used in bug bounty programs at Intigriti:

What is Intigriti

Intigriti is a global crowdsourced security provider, with a variety of security testing offerings. Our platform connects ethical hackers with businesses seeking to identify and rectify vulnerabilities within their digital systems, applications, and networks. Our clients find us to be the most reliable method to leverage crowdsourced security due to our unrivaled customer service, community, and triage services

Security researchers

Also known as ethical hackers or bug bounty hunters, security researchers are cybersecurity experts who use their skills and expertise to hack for good.

Bug bounty program

A Bug bounty program allows independent security researchers to report bugs to an organization in exchange for recognition and compensation. Programs can be private or public.

Private vs public programs

A Private program is invitation-only and visible to a defined set of security researchers. Companies that opt for private programs usually have specific reasons for keeping their vulnerability assessment efforts discreet. A Public program is visible to the wider internet and publicly listed on the Intigriti website. This means a public program is indexable by major search engines and can be found by searching the company's brand name online.

Bounty

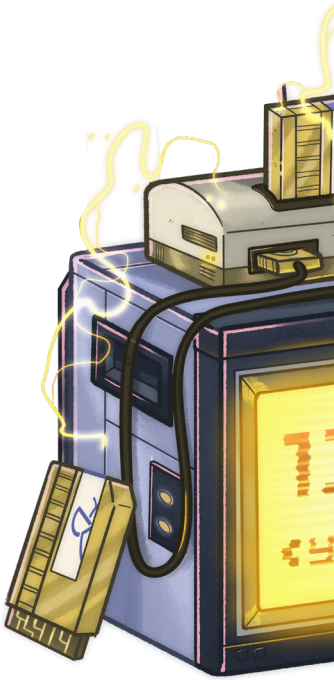
If a vulnerability report is accepted by the organization it relates to, they'll pay the security researcher a reward or compensation which is better known as a 'bounty'. This incentivizes individuals to disclose potential threats, enhancing the overall security posture of the organization. Eligibility criteria and reward amounts are outlined in the program's policies and guidelines.

Triage

Triage is a process in which Intigriti validates submissions based on defined criteria from the customer and Intigriti. This is completed by a highly experienced team of security analysts. They will filter out duplicate reports and 'out of scope' submissions, as well as reproduce the vulnerability, based on the information presented by the researcher.

Crowdsourced security testing

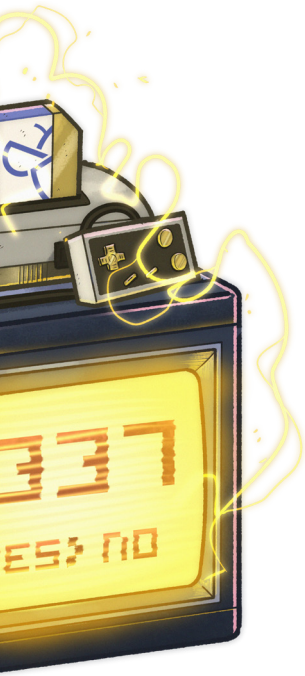
Crowdsourced security testing is a method employed in the field of cybersecurity and software testing. It is characterized by the engagement of a diverse and geographically dispersed group of security researchers to assess and evaluate the security posture of a digital system, application, or software product



Can investing in crowdsourced security help mitigate costly security breaches?

The average cost of a bug bounty program varies, but in general, it can cost up to $250,000 for large organizations looking for a bells-and-whistles model to suit their needs, while smaller businesses with fewer targets can create a robust program with less than $35,000. Regardless of the size of the company, one thing is for sure—a bug bounty program is an investment. However, falling victim to a breach carries a significantly higher price.

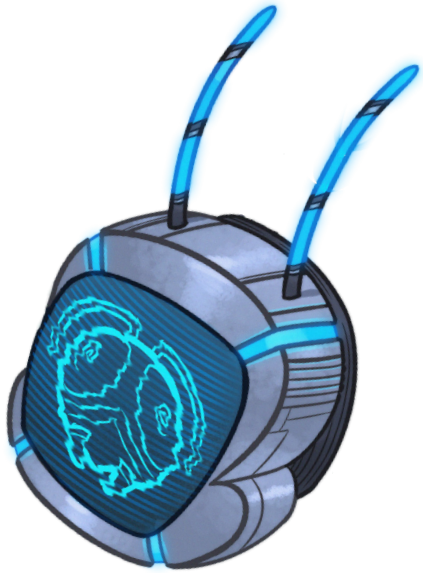
In 2024, the average data breach cost was $4.88 million, according to IBM[4]—a 10% increase over last year. Risk mitigation experts at Aon[5] also estimate that companies that are ineffective in post-event crisis management have on average suffered 29% more damage compared to the better-prepared ones by day 100, with the average loss of shareholder value after 100 days at around $3 billion.



Considering the financial costs involved, it's important for organizations to know what the ROI (return on investment) is for crowdsourcing their security. It's hard to definitively put a cost on a security breach due to the fluctuating nature of one—the financial impacts depend on variables such as the size of the company, the value of the data it holds, the length of downtime caused by the breach, and the loss of trust by the consumer.

Richard Hollis, Director at Risk Crew, a risk and compliance consulting consultancy, estimates that a small to medium-sized enterprise (SME) might face financial impacts of up to $1.2 million in a single incident, depending on various factors, as well as costs associated with loss of public trust and compensating consumers. This can mean that falling victim to a breach can be almost five times more expensive than the average launch of a bug bounty program alone.

Ultimately, companies with mature security postures often adopt a strategy that assumes they will be targeted by hackers and then work backward to mitigate that risk. With an increasing media focus on cybersecurity incidents, numerous high-profile cases have made headlines worldwide in recent years, prompting an important question: "How much would a company be willing to invest to avoid becoming the next headline news story about a major security breach?"



[4]https://go.intigriti.com/ibm
[5]https://go.intigriti.com/aon

Who should pay for bug bounty rewards? Allocating budget for your crowdsourced security program

When launching a new bug bounty program, there's usually a discussion around which department should 'foot the bill' for the costs of the rewards, however, there is no universally agreed-upon standard regarding which department should take charge.

Departmental budget responsibility for budget bounty spend varies greatly depending on the size and scale of the organization running the program. For example, in many cases, it comes directly from the security team's budgets. In other cases, organizations believe it should be funded by the product and engineering teams that own the affected asset. Legal, risk and compliance teams can also pick up the tab in less common cases.

Intigriti's Customer Success Manager, Harry Prestwich, remarked: "There is no definitive answer regarding the source of the budget. However, in my experience, the most effective approach is when the security team takes ownership of the investment while the budget for bounty rewards is allocated among the product teams responsible for each affected asset. This arrangement proves successful as it establishes the groundwork for a product development life cycle that prioritizes security."

Speaking to Intigriti, Javvad Malik, Lead Security Awareness Advocate at the Security Training organization KnowBe4, views the issue differently, arguing that while security teams usually have a budget for pentesting (which is traditionally done pre-launch without risk exposure), bug bounties can have a long tail, and therefore "aren't really feasible for a security team to budget for them".

Regardless, having the security team involved in the process is beneficial because it:

- → **Leads to security-minded product developers: when product and engineering teams are responsible for funding approved vulnerability rewards, it incentivizes the business to prioritize educating development teams on mitigating vulnerabilities and risks.**
- → **Increases awareness around the ever-evolving cyber threat landscape: engaging the product and engineering teams directly through their financial backing, is a proven way of achieving greater awareness in this area.**
- → **Drives change through financial obligation: when product and engineering teams witness the costs associated with mitigating vulnerabilities within their budgets, it often serves as a catalyst for positive change.**

How companies handle vulnerability management on Intigriti

Triaging & customer support

Customers have access to an industry-leading triage department, as well as a dedicated customer success manager and program manager.

- Researcher **searches** for a **vulnerability**
- 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 client
- **Client accepts** report, and **payment** is **automatically** processed

Penetration testing vs bug bounty programs

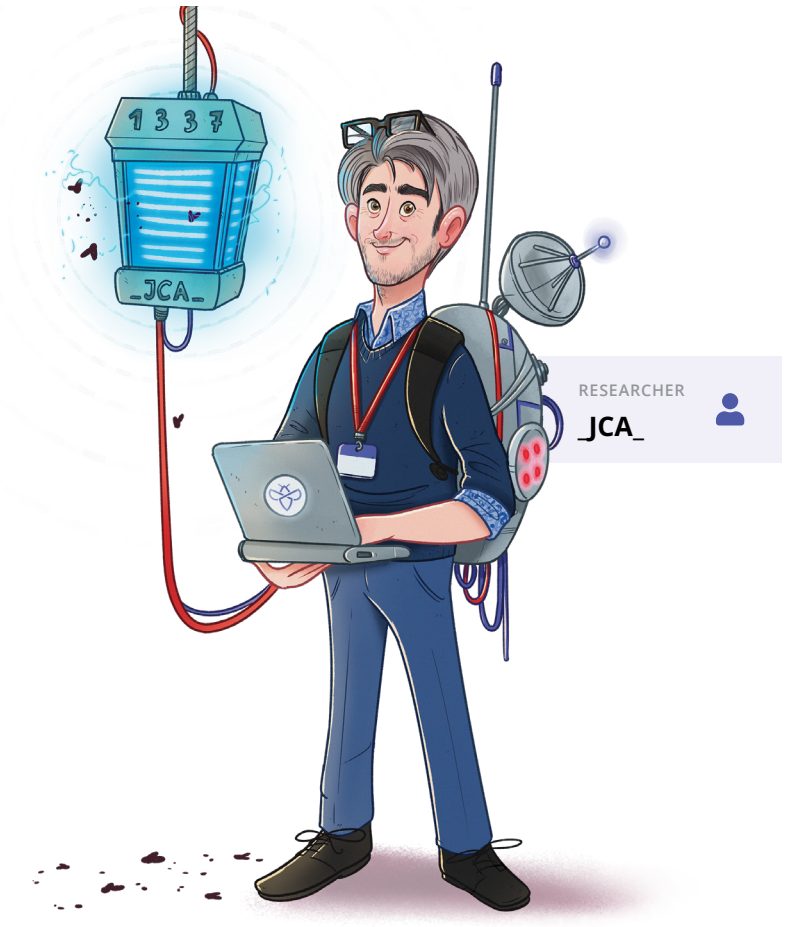
Bug bounty programs and penetration tests (pentests) both aim to identify vulnerabilities that could be exploited by hackers. However, there are some key differences. Pentests focus on one moment in time, whereas bug bounty programs are continuous.

Whilst you'll receive proof of attestation and an overview of some vulnerabilities found within that specific time-frame of the penetration test, your security posture will change as you release new features or updates. This is where bug bounty programs work well as a follow-up.

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.

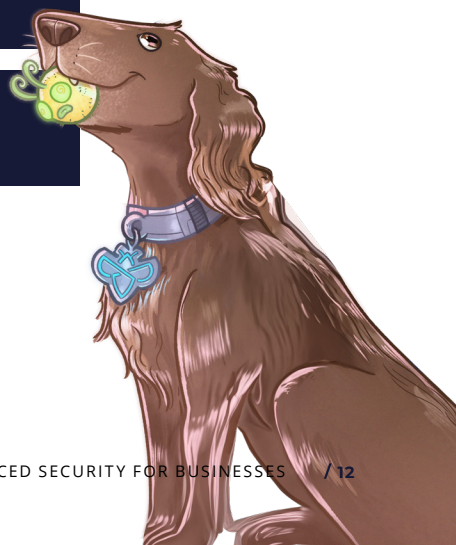
Unlike pentesting, a bug bounty program doesn't follow a specific methodology. Businesses that opt into Intigriti's ethical hacking platform, for example, will pay a subscription fee to list their program[6] in a controlled environment. This allows a community of ethical hackers to assess the security 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.



[6]https://go.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



Classic vs Pentest as a Service (PTaaS)

Intigriti offers an alternative pentesting solution that combines the pay-for-impact approach of bug bounty programs with the dedicated resourcing strategy found with classic penetration testing.

As well as providing a new format for seasoned security researchers to earn a sustainable living, organizations can achieve:

- **Pentesting performed by the world's most respected security researchers**
- **Results within two weeks, which is significantly faster than traditional pentesting**
- **ISO 27001 and SOC2 for compliance-focused security testing.**

	CLASSIC PENTESTING	PENTEST AS A SERVICE (PTAAS)
REPORTING	The business receives a formal report at the end of the testing period with recommendations on what needs fixing.	**The business is able to see live reports as they come in through the platform. All reports are validated by an in-house triage team.**
EXPERTISE	The business chooses a pentesting company. The company selects which of their pentesters will do the job.	**The business chooses security researchers from Intigriti's top-ranked ethical hackers. They are able to view applications and select the researchers best suited for the job.**
PLANNING	The business defines its own parameters and plans the pentest, which the pentesters then carry out.	**Intigriti helps the business to define the project based on a few simple questions.**

CUSTOMER SPOTLIGHT

How Kinepolis uses its bug bounty program to keep its systems safe

The Challenge
Increase the overall IT security across websites and systems

Being a leading international cinema company, Kinepolis' main interaction point with its customers is its web platform. Keeping its systems secure is of utmost importance, and so the cinema company was already working with a penetration testing partner to help with their IT security challenges.

The Solution
Continuous security testing

Kinepolis decided to run a bug bounty program as a follow up to their penetration test on the Intigriti platform. They invited crowdsourced security researchers to look for vulnerabilities in their systems in a safe and controlled way. The decision to work with ethical hackers was not taken lightly.

> "The biggest challenge of starting with Intigriti was fear of the unknown. Yet, once you publish your website, it is out there in the world anyway. It's accessible — not only to people with good intentions but also to malicious hackers."

Adding a layer of quality assurance to the process

The Intigriti platform is the central hub of communication between external researchers and Kinepolis. When a researcher finds a vulnerability, they submit their findings to the platform so that Intigriti's triage department can check the vulnerability.

The Results
Keeping systems safe in a joint effort

Intigriti's security researchers and Kinepolis shared a common goal: To keep their systems safe for end-users. As a result of using Intigriti's bug bounty platform, Kinepolis' internal IT security teams felt they had sufficient support to perform high-quality security testing.

"Intigriti's triage process makes sure that only genuine issues are submitted to our IT security team, who can immediately work on a solution.

BJORN VAN REET
CIO – KINEPOLIS GROUP

KINEPOLIS

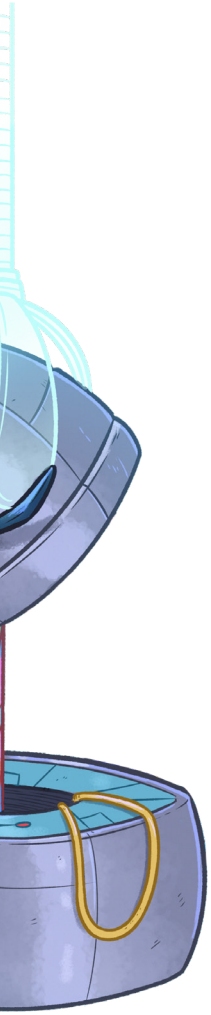
INDUSTRY
Entertainment, cinema

NUMBER OF CINEMAS
111 worldwide

EMPLOYEES
4,600

How crowdsourced security helps organizations overcome cybersecurity challenges

THE CHALLENGE	THE SOLUTION
Cybersecurity skills gap 95% of security professionals say the cybersecurity skills shortage is an increasing challenge.	**Tap into a network of security experts** Leverage thousands of security experts' skills, experiences, expertise, and creativity.
Staying on top of cyber threats 59% of security professionals say the demands of their job make it difficult to find time for training—yet cyber threats continue to evolve.	**Invest in your team's development** Ethical hackers are wired to spot what your team might miss. Organizations invest in internal talent by allowing them to learn from incoming submissions and interactions with researchers.
Growing attack surfaces Digital transformation, moving to the cloud and scaling fast in continuous development cycles have resulted in ever-expanding 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 or conducting PTaaS. Security teams gain awareness of vulnerabilities faster, and in turn, can introduce a patch faster.



THE CHALLENGE

The cost & limitations of pentesting

A high-quality pentest costs between $10,000-$30,000 USD(RSI Security[7]). Running them continuously would be highly costly & unsustainable as you pay for testing time; not 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 continuous growth, acquiring adequate cybersecurity resources can be challenging.

THE SOLUTION

Pay for results

Security researchers 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 and 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.

Centralize security testing

PTaaS and bug bounty programs allow organizations to continuously test cybersecurity defenses within one platform, and through the power of a crowd.

[7]https://go.intigriti.com/rsi-security

How Brussels Airlines uses a bug bounty program to improve IT security posture

The challenge
Obtain internal buy-in for bug bounty programs

Ethical hacking through bug bounty concepts caught the attention of Jean-François Simons, CISO of Brussels Airlines, years ago. For the management team, however, the prospect of letting crowdsourced security experts find undetected issues was not an easy decision to take.

Mr Simons' was able to explain why the Airlines needed to work with ethical hackers, not against them:

> "We need the support of ethical hackers to reinforce our IT Security before non-ethical hackers find a possible vulnerability which they will, of course, not report to us."

The solution

Penetration testing as a clean-up before bug bounty

Jean-François Simons' team saw penetration testing as a step to take before launching a bug bounty program:

> "I consider pentesting to be a sequential review to improve the general security of your systems. Afterwards, you give it to the specialists on a bug bounty platform."

Explaining further, Simons said: "Ethical hackers are specialists in their domain — some do cross-site scripting, some specialise in SQL injection, and so on. Pentesting does SQL injection too but on a higher level. The vulnerabilities found through our program could only be discovered by very specialised and highly-skilled people."

The result

PR value, collaboration opportunities & greater security awareness

It is not just finding the bugs and vulnerabilities that makes Intigriti valuable for Brussels Airlines. Mr Simons points out the PR value:

> "The fact that we are using a bug bounty program shows we really try to go one step further. Should we face a major issue, we will be able to use this. Working with ethical hackers shows that we are really trying, and not just sitting around waiting for something to happen."

Bug bounty provides the DevOps and digital teams at Brussels Airlines with a new collaboration opportunity. People learn from what has been discovered. As a result of working with ethical hackers, more IT people at Brussels Airlines are aware of ongoing cybersecurity threats, and actively contribute to improve the information security.

> "We wanted to come as close as possible to a bulletproof IT security situation. We called upon Intigriti's ethical hackers, who found a critical vulnerability which we then mitigated."

brussels airlines

INDUSTRY

Aviation

REVENUE

1.6 billion EUR

PASSENGERS

10.2 million

The pros and cons of a DIY bug bounty program

Choosing to launch a bug bounty or vulnerability disclosure program can be an exciting time, however, the options can also become confusing and overwhelming. You might even ask yourself: can I just do it myself?

In-house bug bounty programs aren't unheard of, with the likes of Apple, Facebook, and other big players in the tech industry choosing to employ a dedicated team to manage their own vulnerability disclosure environment. Other businesses or organizations choose to engage the services of a bug bounty platform, which can offer tailored support and management for their programs, allowing them to offer a bug bounty program without the need for an in-house team.

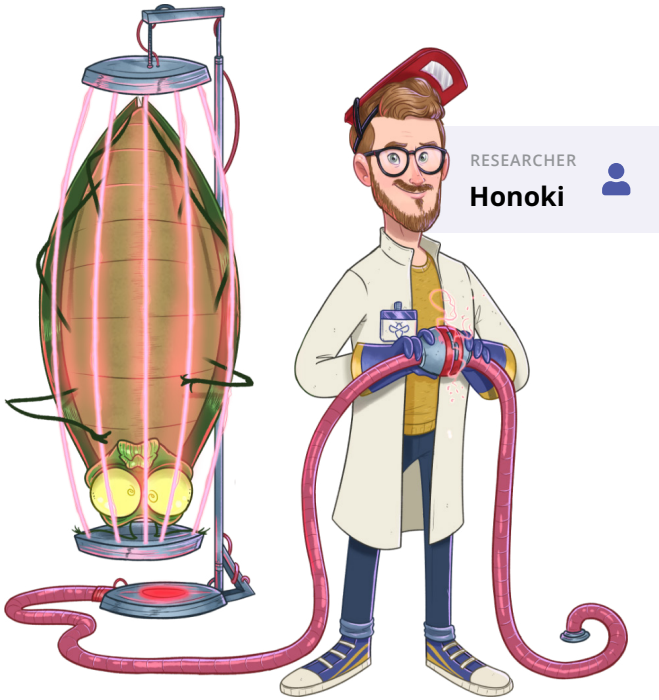
In-house bug bounty program

Customize to your exact requirements

The benefit of managing your own bug bounty program is that you can customize it to your exact requirements and have full control over each stage of the process, from bug submission to triage, to making the payment to the researcher. You can also change and adapt your program to suit you, circumventing any restrictions or timescales you might face by using a third-party provider.

Potential cost-saving with an in-house model

Hiring a team to run your bug bounty program doesn't come for free, so you might be looking for ways you can run your own program without the additional budget. This is possible; for example, your business might choose to ask existing colleagues to absorb it into their work. However, it's worth noting that running the program would be on top of all of their existing responsibilities, which isn't an option for some organizations.



Using a crowdsourced security platform

Access a triage team that works on your behalf

Bug bounty platforms offer an established triage team whose job it is to prioritize reports on behalf of organizations, responding to its community of hackers and keeping them engaged. This team will also manage communications with the researcher, so if any further information is needed, this is taken care of, freeing the IT department to focus on the important task of fixing the issue at hand.

Without a dedicated team focused on maintaining a program, the signal-to-noise ratio can quickly become overwhelming. There are often a fair number of low-quality or false-positive reports that can take time to sift through, and in the absence of a triage team, these kinds of submissions cannot be differentiated from others, meaning every report is potentially taken as a serious threat until it is proven otherwise.

Avoid possible legal issues stemming from international payments

One of the positives of running a public bug bounty program is that you can gain access to some of the best security researchers in the industry. It does, however, also come with some added due diligence to ensure that you're not falling foul of international laws.

Businesses and organizations must be compliant and avoid making payments to sanctioned countries, a list of which can be found on the OFAC website[8]. This can be tricky to do for a company not specialized in this area, not to mention time-consuming. Bug bounty platforms such as Intigriti conduct daily OFAC screenings on behalf of their customers, ensuring that payments are not sent to unauthorized bank accounts. It also requires all bug bounty participants to undergo identity checks and conducts regular watchlist screening to ensure the people behind the username are exactly who they say they are.

Access a tried-and trusted model for crowdsourced security

Bug bounty platforms specialize in helping businesses and organizations to crowdsource vulnerability testing, and so have solid knowledge of how to maximize a company's security posture no matter the industry, location or budget.

For example, check out Intigriti's Bug Bounty Calculator[9], which can help an organization see whether the bounties they are offering are below the industry average, and can also advise on what skill level of hacker its bounty levels are estimated to attract.

[8] https://go.intigriti.com/ofac
[9] https://go.intigriti.com/bountycalculator-blog

How the European Commission helps secure open-source software

The challenge
Help open-source communities secure their software

The European Commission became aware of the criticality of open-source software in 2014 when the Heartbleed vulnerability caused substantial losses and impact worldwide. It was at this moment that the European Commission made a commitment to help open-source communities in securing their software.

In January 2016, the European Commission launched the ISA2 Programme[10], which supports the development of digital solutions that enable public administrations, businesses and citizens in Europe to benefit from interoperable cross-border and cross-sector public services. The Programme supports a set of different actions to develop interoperability solutions.

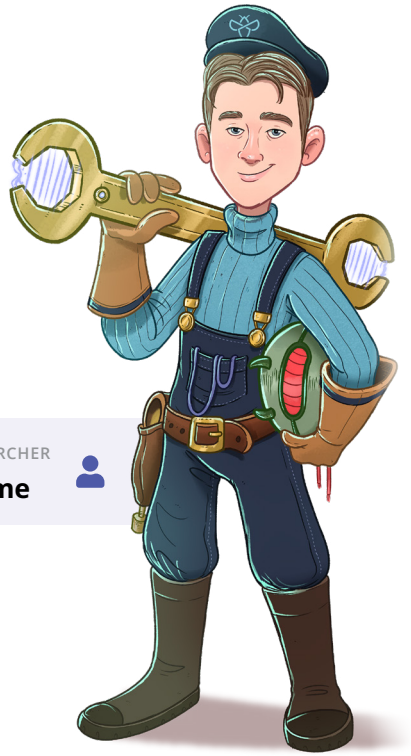
One of these actions, called Sharing and Re-Use action[11] (2016.13), was assigned to the Open Source Programme Office (OSPO). Under this action, the OSPO decided to use bug bounties as a means to secure open-source software that it is widely used by public services. The effort continues in 2021 under the current action.

[10] https://go.intigriti.com/european-commission-1
[11] https://go.intigriti.com/european-commission-2

The solution

Secure three open-source software using bug bounty services

As part of the Sharing and Re-use action (2016.31.), the Commission decided to use bug bounties, a form of crowdsourced security testing. Three bug bounty programs were launched on 11 January 2021 using the Intigriti bug bounty platform.



RESEARCHER
Holme

The selected software for the bug bounty program:

1. **MOODLE**
   An eLearning platform widely used by public administrations and universities worldwide.

2. **ZIMBRA**
   A popular email server solution that includes group calendars and document collaboration.

3. **ELEMENT (MATRIX)**
   An instant messaging platform used by public services in France and Germany.

The bounties were funded by the Commission's ISA2 programme but focused entirely on open-source software widely used by European Public Services.

European Commission

INDUSTRY
Government administration

FOUNDED
1958

NUMBER EMPLOYEES
10,000+

The results

Modernised security testing with immediate impact

In a matter of weeks, vulnerability reports were being submitted. In one software, three “critical” vulnerabilities were discovered. Additionally, at least one “high” vulnerability was found and disclosed for all three software projects.

Knowing these vulnerabilities meant the open-source communities could quickly fix them via a patch, leading to more secure software.

> Bug bounty platforms align very well with open source software because what you have is a community of ethical hackers helping another community. It is collaboration at the highest level.

MIGUEL DÍEZ BLANCO
PROJECT LEAD OPEN SOURCE PROGRAMME OFFICE, AT DIGIT – EUROPEAN COMMISSION.

When asked about their experience, **Zimbra** said:

> “Let’s do this again! Participating in the European Commission’s Bug Bounty Program was a worthy and valuable project for Zimbra. It was a great exercise for us, with mostly low to medium-security issues related to scripting and forgery that our vulnerability scanner had failed to catch, keeping us alert 24/7.”

About their involvement, **Moodle LMS** (Learning Management System) Product Manager Sander Bangma said:

> “Security is of paramount importance to Moodle as the world’s most customisable and trusted open-source learning management system (LMS). Moodle’s development practices include security by design and participation in the ISA bug bounty program has been a welcome addition to further enhance Moodle’s security.”

Regarding their experience on Intigriti’s bug bounty platform, **Matrix** commented:

> “Intigriti provided excellent service by pre-triaging reports and ensuring that we only had to address validated submissions. Though most accepted issues were of low severity, we did receive a few higher severity reports too.”

About bug bounty 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[11] found that 70% of Intigriti's hackers are on the platform to learn and develop their skills, and 40% are driven by the challenge.

To be a successful vulnerability researcher, you need to be able to approach the task of hacking with a fresh perspective, apply unharnessed creativity, and be unafraid to go against the grain.

There are obvious benefits to taking the legal route to disclose vulnerabilities: The money, the recognition and the free swag. But ultimately, ethical hacking is about being part of a community of people with a strong desire to help.

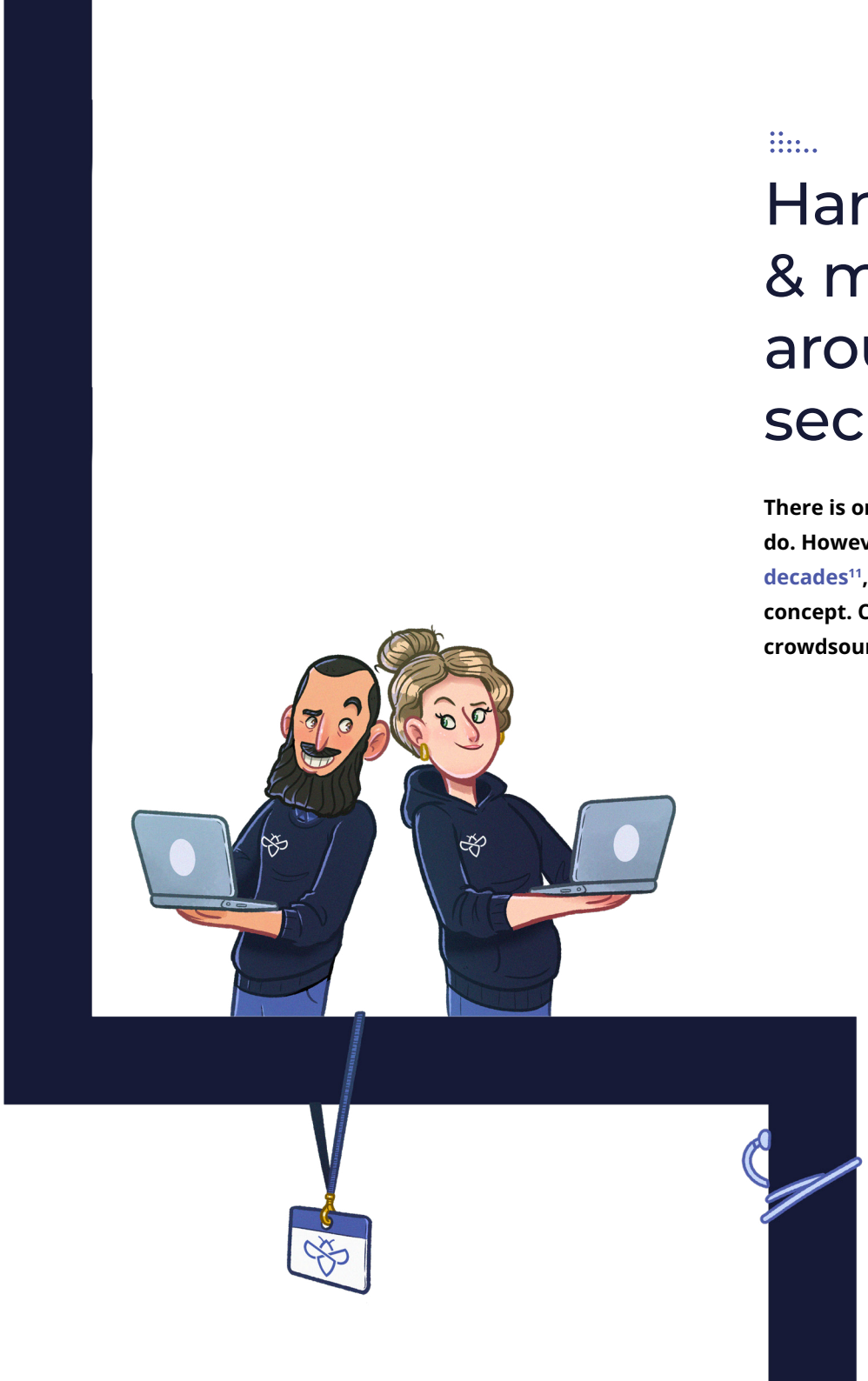
For 21% of our community, their primary goal on the platform is to do good and 21% want to help defend against cybercrime.

[10]https://go.intigriti.com/ethical-hacker-insights-report

Why do ethical hackers use Intigriti?

* Multiple-choice question: Participants could select more than one answer.

Source: The Ethical Hacker Insights Report | Intigriti



Handling hesitations & misconceptions around crowdsourced security

There is only one truth to what crowdsourced security can do. However, despite bug bounty programs being around for decades[11], a few stubborn misconceptions linger around the concept. Consequently, people can feel hesitant to buy into crowdsourced security.

[11] https://go.intigriti.com/bug-bounty-history

#Q1

By exposing our company to ethical hacking communities, aren't we exposing ourselves to more risk?

If you operate online or own digital assets, the reality is that you're already exposed to hackers—and bad actors won't seek your permission to hack your business. A simple yet proven method to protect against cyber threats is to invite ethical hackers in. Bug bounty programs, hacking events, and PTaaS all follow this concept at scale by applying a crowdsourced approach to security testing.

#Q2

Is it possible for malicious hackers to join the platform in disguise as ethical hackers?

A crowdsourced security platform isn't what a cybercriminal would consider to be a good place to find targets. Malicious hackers typically seek out an easy win that they can exploit with minimal effort. When your business launches a bug bounty program or PTaaS, for example, it's publicly announcing that it takes security seriously, and so your profile immediately doesn't fit the profile of an ideal hacking victim.

Besides this, when signing up to Intigriti, ethical hackers are required to complete several legal steps before they are granted access to the platform. One of these steps includes an official identification check.

#Q3

We already have an annual penetration test. Do we need a bug bounty program too?

Penetration tests rely on one person or a small number of people, which restricts the number of perspectives, and relies on the same person's attack methods and approaches. They also cost by the hour or service performed. Because of their expense, pentests are typically time-bound and penetration testers are briefed to follow a narrow scope. For example, they might attempt a specific cyberattack method or test specific assets for the client.

It's possible that penetration testers will detect high-level vulnerabilities, but they won't have much time to dig deeper. They also cannot comment on the state of a business's security after the test is over. If your company makes a new update or brings out a new feature, for example, your digital landscape will change, meaning your security posture changes too.

The goals of penetration tests and bug bounty platforms are very different. Penetration tests aim to provide you with some assurance for the state of your information security, based on a one-time assessment. Bug bounty programs cover a very different goal, in that they provide constant attention to your digital assets through continuous testing.

#Q4

We use automated scanners. Doesn't this do the same job?

Automated scanners scratch the attack surface for businesses and identify high-level vulnerabilities. This makes them a good fit for finding low hanging fruit, but not for finding vulnerabilities that are aligned with complex attacks.

Scanners are programmed to find known patterns of weaknesses and vulnerabilities. Malicious hackers do the opposite, as do ethical hackers. They rely on creativity and out-of-the-box thinking. They're also actively incentivised to seek out undiscovered and elusive security vulnerabilities within a set scope through financial rewards (the bug bounty). Therefore, they're far more likely to pick up on complex but potentially damaging flaws in your system than an automated scanner.

#Q5

What's the difference between a public and private bug bounty program? And which is right for my business?

Publicly listed programs are available for anyone. They tap into the expertise of thousands of researchers and are meant for programs with a high security maturity.

Private programs enable companies to leverage communities and researchers of their choice based on the requirements and success goals of the program. Through this route, businesses can invite researchers to the program that they already have a relationship with or define the type of researcher who can gain access to the program. The program will only be visible to those that are invited to participate, and new researchers can be added at any point.

Most businesses choose to begin with a private bug bounty program before progressing to a public program. It's also a good option for companies that have more sensitive testing environments. Either way, every program can be set up with its own ruleset to specify a list of in-scope items, out-of-scope items, budget limitations, bounty schemes, and more.

#Q6

When is a good time to launch a bug bounty program? Are we ready?

You can start working with ethical hackers at any point. However, in our experience, running high-level security tests (such as automation scanning or pentesting) before you launch is a great preparatory step. Doing so gives your engineers the opportunity to fix high-level security vulnerabilities that will undoubtedly show up in the program, and in turn, allows you to get better use out of your bug bounty budget.

Most companies like to get a taste for bug bounty platforms without committing to a public program. In that case, it's worth starting with a private program. This involves working with a select few security researchers first, rather than the entire network. You can also choose to restrict testing areas, or ask researchers to look for specific breaches, such as vulnerabilities with potential financial impact. These are elements you'd include in the program's scope.

Once you're comfortable handling more reports, you can steadily open up the scope until the point where you're ready to launch publicly (if that is what you desire). Whichever program you choose, you'll receive award-winning support from our customer success team throughout every step of your journey.

What happens at a live hacking event?

A live hacking event brings ethical hackers from across the world together in one place to compete. The event's goal is almost always the same—discover as many vulnerabilities as possible in the allotted time to provide rapid and useful security feedback on the targeted assets.

> You get this creative outburst that you've never seen before. That is the true power of live hacking events.

INTI DE CEUKELAIRE
CHIEF HACKER OFFICER – INTIGRITI

Live hacking events usually share the following qualities:

1. **FIXED DURATION**
   Anything from 24 hours to two weeks is common.
2. **PHYSICAL EVENT**
   Hackers and security professionals gather in person; though the events shifted online during the pandemic.
3. **PREDEFINED SCOPE**
   A set of assets defined as the target for the testing.

Why should I host a live hacking event?

One of the benefits for businesses is that time constraints and competitive elements often result in multiple high-value bug submissions within a matter of days. As Visma Security Engineer and Bug Bounty Program Manager, Ioana Piroska, recalls from Visma's live hacking event: "In the two weeks of live hacking, Visma received 363 submissions and 251 were considered valid. The vulnerabilities reported included two exceptional, two critical, and two 0-days. The event gave us a fantastic opportunity to engage with our community, and the result was a set of impactful reports in a short amount of time."

Intigriti works with organizations to help them plan, scope, and execute their entire event.

This includes providing a triage team for the event (or enabling an organization to assemble its own) and assisting with services such as marketing the event beforehand.

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.

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 standards.

Strong global presence

In terms of hacker pay-outs, 8 out of 10 of the best performing countries were European. However, Intigriti is very much a global business.

Triaging & customer support

Customers have access to an industry-leading triage team, as well as a dedicated customer success manager and program manager.

Information from Q3/2025. We are constantly growing, so please contact our sales department or see our website for an accurate number.

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