INTIGRITI

An Introduction To Bug Bounty Programs For Businesses

Agile security testing powered by the crowd

EBOOK

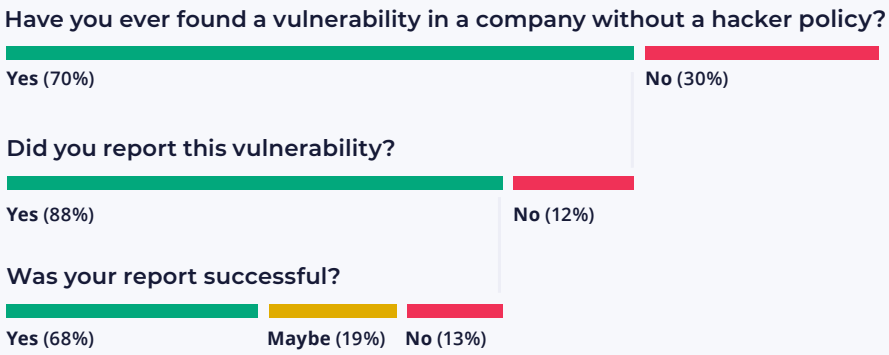
Table of contents

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

The challenge of digitalisation within businesses is that malicious hackers suddenly have a much larger attack surface to work with. For many businesses, IT departments are already stretched thin. Keeping up with new demands creates a situation whereby security is performed in firefight mode rather than proactively addressing vulnerabilities before they can be exploited by cybercriminals.

The need for modern, proactive security has never been more important. A simple yet proven method to protecting against cyber threats is to invite ethical hackers in. 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 2021, 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 the security risk concerns — but only around two thirds (68%) of reports are submitted successfully.



Source: The Ethical Hacker Insights Report 2021 | Intigriti

How do businesses address this issue?

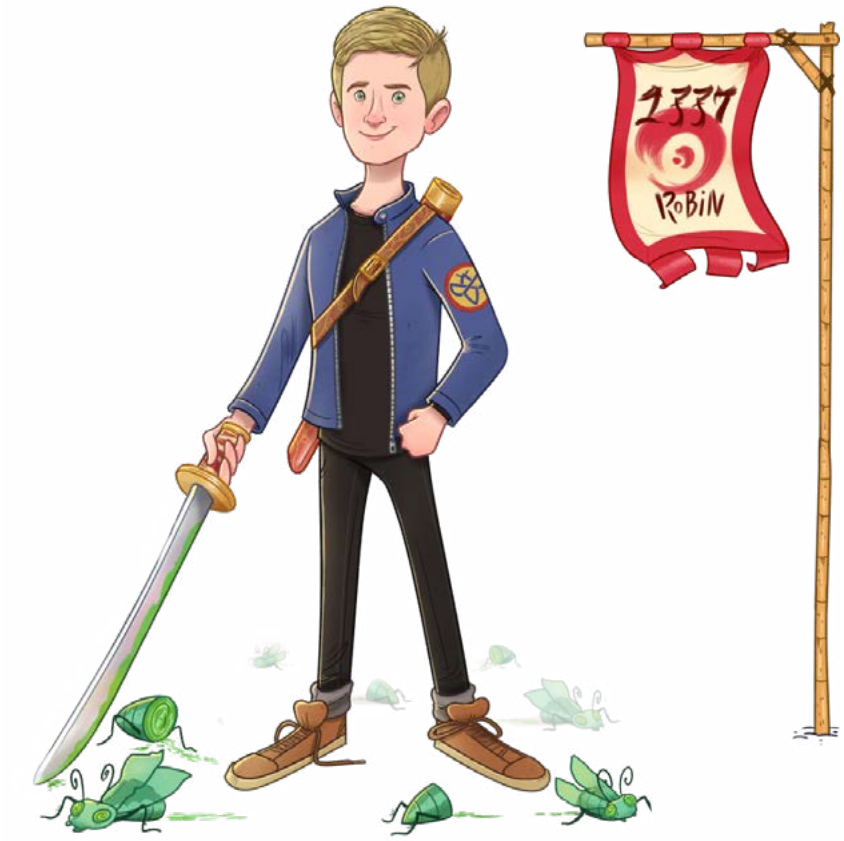
Bug bounty programs present businesses with an opportunity to work with independent security researchers (also known as ethical or white hat hackers) to report bugs. Most security researchers choose to report vulnerabilities through a crowdsourced security/bug bounty platform, like Intigriti. This is because a crowdsourced security platform provides the best infrastructure for security researchers to engage and communicate with companies in a structured, safe, and reliable way.

By continuously working with ethical hackers through a bug bounty program, organisations become aware of and fix their vulnerabilities. Not only does this improve the strength of their cybersecurity posture, but it empowers them to outmanoeuvre cybercriminals.

However, starting with a bug bounty program often begins with questions. In this eBook, we'll attempt to provide greater clarity on bug bounty programs, ethical hackers, where to host a program, 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.

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 bug bounty hunters and penetration testers.

> Working with ethical hackers shows that we are really trying, and not just sitting around waiting for something to happen.

JEAN-FRANÇOIS SIMONS
CISO AND DATA PRIVACY OFFICER, BRUSSELS AIRLINES

Bug bounty concepts explained

Bug bounty program

Security-driven organisations can publish a bug bounty program, incentivising independent security researchers to search for and submit bugs to them. Programs can be published publicly (where anyone can contribute) or privately (where specific researchers are invited to participate.) They can also be time-bound or have no end date. However, most companies opt for the latter to ensure they have continuous security testing in place.

Bugs

'Bugs' are security exploits and vulnerabilities. If deemed new and valuable, which depends on the scope provided with the program, the security researcher will report these quickly, reliably, and clearly via a submission describing the vulnerability.

Bounty

If the submission is accepted by the organisation it relates to, the researcher is paid a reward or compensation which is better known as a 'bounty'. The size of the bounty is determined by the security maturity of the asset and potential impact of the security issue. Researchers can earn anything between €50 to a few thousand euros for reporting a single bug.

Bug bounty platform

Most security researchers choose to report vulnerabilities through a crowdsourced security/bug bounty platform, like Intigriti. This is because a crowdsourced security platform provides the best infrastructure for security researchers to engage and communicate with companies in a structured, safe and reliable way, offering live updates and communication.

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 dedicated to bug bounty hunting full-time, whilst others are employed in full-time jobs. For example, around 50% of Intigriti's community are Penetration Testers.

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 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.

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

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 bug bounty programs help organisations overcome cybersecurity challenges

The challenge

Cybersecurity skills gap

95% of security professionals say the cybersecurity skills shortage is an **increasing challenge** (SearchSecurity).

Staying on top of cyber threats

59% of security professionals say the demands of their job makes it **difficult to find time for training** (SearchCompliance) – yet cyber threats continue to evolve.

Growing attack surfaces

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

Bug bounty as a solution

Tap into a network of security experts

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

Invest in your team's development

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

Test security continuously

Businesses can **amplify and scale security testing** by running an ongoing bug bounty program. Security teams gain awareness of vulnerabilities faster, and in turn, can introduce a patch faster.

The challenge

The cost & limitations of pentesting

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

Security awareness

Keeping security awareness high is an ongoing challenge for internal cybersecurity teams. Configuration errors and insecure coding can easily lead to **significant costs and data breaches**.

Lack of resources

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

Bug bounty as a solution

Pay for results

Bug bounty hunters are rewarded if they expose a new, realistic, and actionable in-scope bug. By paying for results, the **cost-efficiency ratio** is giving companies much more impact for the same test budget.

Gain the support & input of ethical hackers

Through the continuous flow of qualitative and **impact-driven submissions**, IT & development teams experience a boost in inspiration, hacker-way of thinking and awareness throughout the year.

Centralise security testing

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

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

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

Self-hosting bug bounty programs or publishing via a platform. Which is best?

Ethical hackers dedicate significant amounts of time to discover and report security flaws to businesses. Creating a stress-free and sensical way for them to disclose security vulnerabilities to you is critical. Not only does it encourage responsible disclosure, but it maximises the success of their contribution.

Read on to discover the key differences between self-hosted programs and bug bounty platforms.

	SELF-HOSTED PROGRAMS	BUG BOUNTY PLATFORMS
Program engagement	**Reactive and passive engagement** Good-willed customers, citizens and ethical hackers will inform businesses of a potential security issue.	**Active engagement** Security researchers are continuously engaged through bounty opportunities, points and reward systems, leader boards, hacking events, education, and more.
Vulnerability disclosure policy requirements	**Required** Having a VDP ensures that people outside your organisation understand how to inform you of vulnerabilities they have discovered.	**Advised** It is advisable for businesses to have a VDP on their website too to direct people that wish to inform them of a security issue to their program.
Validating submissions	**Handled internally** Without enough resources, the handling of non-valid submissions can be a time-consuming exercise.	**Handled by triage** Triage teams provide a layer of quality assurance before escalating vulnerabilities to businesses.
Handling comms	**Handled internally** Owned by the team tasked with fixing incoming submissions.	**Handled by triage** Communication carried out within the platform. A triage department works as the go-between for client & researchers.
Budget allocation & payment processing	**Manual** Responsibility of a finance department. Worldwide payments can be tricky to manage and come with high fees if not managed properly. To maintain good working relationships with researchers, it's important to provide payment promptly.	**Handled by the platform** Processes automatically after a submission is accepted by the organisation. Payment and administration are taken care of by the platform.
Responsible disclosure	**Encouraged** Researchers encouraged to perform responsible disclosure.	**Platform agreement** Researchers must agree to responsible disclosure.

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, 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 (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.

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.

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 2021 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.

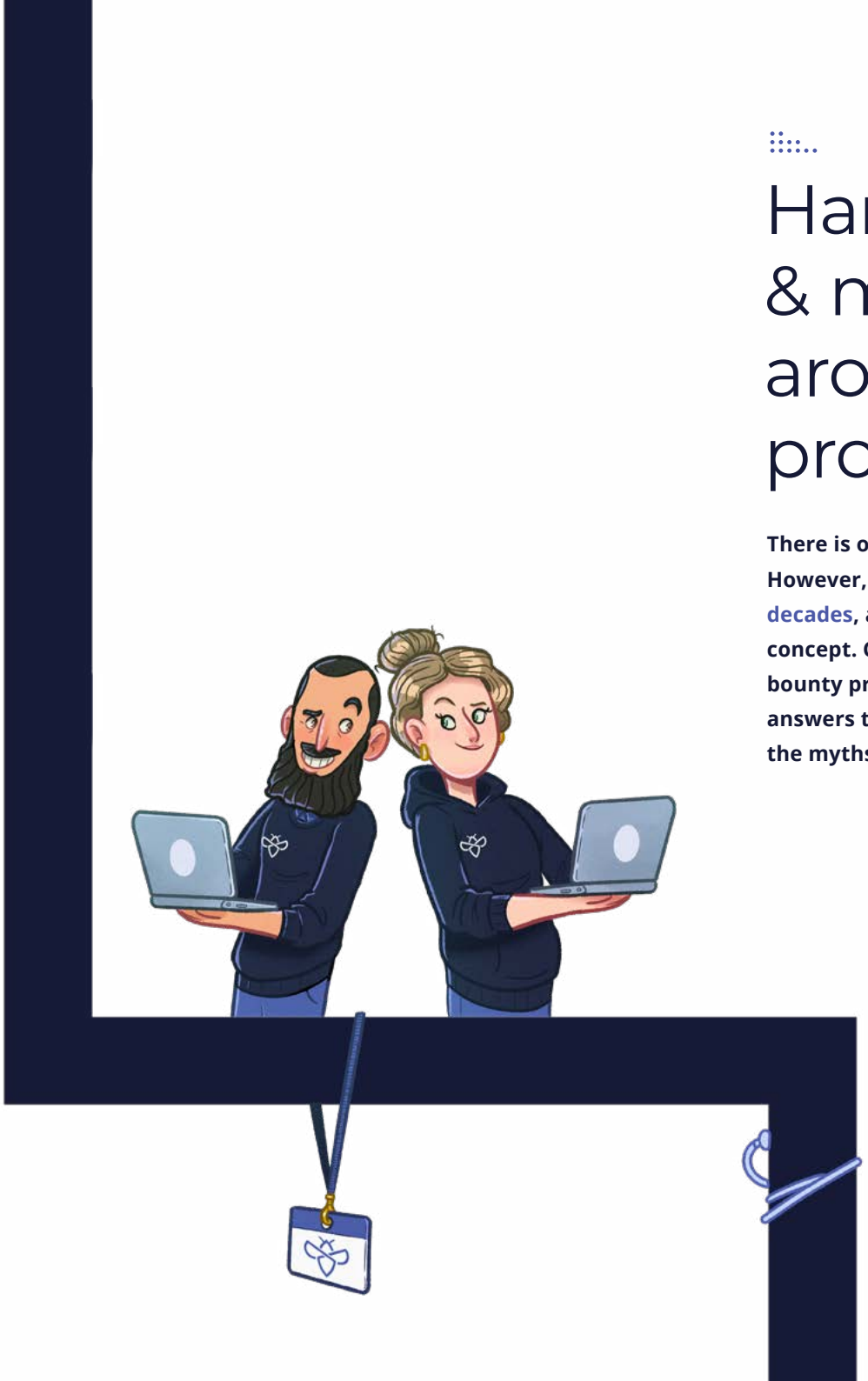
There are obvious benefits to taking the legal route to disclose vulnerabilities: The money, the recognition and the free swag. But ultimately, ethical hacking is about being part of a community of people with a strong desire to help.

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

Why do ethical hackers use Intigriti?

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

Source: The Ethical Hacker Insights Report 2021 | Intigriti



Handling hesitations & misconceptions around bug bounty programs

There is only one truth to what a bug bounty program does. However, despite bug bounty programs being around for decades, a few stubborn misconceptions linger on around the concept. Consequently, people can feel hesitant to buy into bug bounty programs. Here's six commonly asked questions and answers that will help organisations separate the truths from the myths.

#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 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?

There are many reasons why this is unlikely. When signing up to Intigriti, for example, 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.

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

#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.

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.

www.intigriti.com

40,000+ researchers

More than 40,000 security researchers use Intigriti to hunt for bugs — and we're growing!

300+ 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 European 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. In 2020, vulnerabilities were submitted from more than 140 countries.

Triaging & customer support

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

Intigriti hackwithintigriti @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