



# The Ethical Hacker Insights Report 2021

HIGHLIGHTING ETHICAL HACKER DEMOGRAPHICS & STATISTICS IN 2021







# Table of contents

Illustrations by [www.zwoltopia.be](https://www.zwoltopia.be)

5	Introduction	13	What are they?	24	What is the coolest thing they've done with their bounty money?	35	Hacker highlights from @Pieter
6	Unveiling ethical hackers	17	Evolving our community	26	Hacker highlights from @Pudsec	36	Collaborations
7	What can you take away from this report?	18	Closing the gender gap	27	What attracts our hackers to a bounty?	37	Hacker highlights from @Kuromatae666
8	Intigriti in numbers	19	How Intigriti is bringing more women into cybersecurity	29	How they work	38	Annual hacking events
9	Our hackers: Who are they?	20	Hacker highlights from @mstramgram	30	What does triage do?	39	Conclusion
10	3 types of ethical hackers	21	Why they work	33	Reaching organisations through other disclosure methods	40	Glossary
11	History of bug bounty & incentivised vulnerability disclosure	23	How they spend their earnings			41	About Intigriti
12	Where are they?					44	Contact us







# Introduction

In a world of rapid digitalisation, malicious hackers can attack from any angle. Keeping software, hardware, and data secure has never been more important. Yet, cybercriminal activity gets more sophisticated by the minute, which leaves companies scrambling to keep up with the relevant skills to defend themselves.

Luckily, they do not have to fight this battle alone. Worldwide, tens of thousands of ethical hackers are using their skills for the greater good. They're helping to build a safer digital environment by researching, identifying, and alerting companies to weak links in their security systems before they're taken advantage of.

Due to the widely reported reputation of cybercriminals, ethical hackers still have some work to do to convince businesses that they're here

for the right reasons. It's not unusual for companies to feel nervous about inviting a person who identifies themselves as a hacker into their 'home'.

However, perceptions are shifting, and today, ethical hackers are seen by many to be the backbone of IT security testing.

By being on the ground 24/7, businesses can protect their digital assets continuously and at scale. To date, Intigriti works with more than

100 businesses and aligns them with its network of over 35,000 security researchers.

But, who are these people? And what drives them to use their expertise for good?

❗ To date, Intigriti works with more than **100 businesses** and aligns them with its network of over **35,000 security researchers**.

RESEARCHER  
**Oxkasper**







# Unveiling ethical hackers

Starting on a journey with ethical hackers often begins with questions. In this report, we'll attempt to cover them all. From who our community of 35,000 hackers is, to what motivates them to hack for good. We'll highlight where they're from, when they work, and how they operate.

Too often, we hear of businesses talking about faceless security specialists hunting for bugs on their browsers. This report aims to demystify our community and reveal the faces of the people making your assets better protected.

However, it's not just about being seen that hackers have trouble with — they also have trouble being heard. Speak to any member of our community, and they'll tell you about a time they tried to inform a business about a critical vulnerability to no avail.

Often, this is due to companies mistaking or distrusting their good intentions for something more malicious.

As a result, 32% of reports go missing in the process and the weak link remains open. This is particularly apparent when there is no official

route for ethical hackers to disclose the issue, such as a vulnerability disclosure policy (VDP). By raising the profile of ethical hackers, and encouraging businesses to put effective processes in place for accepting external reports, we hope to bring about safer security for all.

**i** Too often, we hear of businesses talking about faceless security specialists hunting for bugs on their browsers.





# What can you take away from this report?

📌 **32% of reported risks remain undetected** by the company, and open to exploitation.

## Ethical hacking is evolving

### Perceptions of ethical hackers are changing

If you were to ask your average person 10 years ago to define a hacker, their answer would likely associate with something criminal, such as fraud, identity theft, and in extreme cases, terrorism. However, the world is waking up to the fact that not all hacking activity is malicious. In fact, many actively fight against it. Today, the industry of ethical hackers is thriving with millions of professionals operating in this field.

According to a 2021 survey by [Intel](#)<sup>1</sup>, 73% of IT security professionals say they prefer to buy technology and services from vendors who are proactive about security, including leveraging ethical hacking and having transparent communications about vulnerabilities.

### Bug bounty hunters help fill the cybersecurity skills gap

Through their sheer determination, and natural curiosity, ethical hackers are propelling cybersecurity forward and helping to fill organisational skills gaps. They're empowering security teams everywhere to scale up without the additional headcount.

According to a 2020 study by [Robert Walters and Vacancysoft](#)<sup>2</sup>, 70% of European companies say they do not have the appropriate cybersecurity talent available. A network of security experts, such as a community of bug bounty hunters, means organisations can tap into a larger network of skills, experiences, and expertise.

## Areas for improvement

### Penetration testing isn't enough to keep organisations secure year-round

Penetration testing is a common service offering in information security. However, its budget and time constraints can affect the strength of a company's overall security posture. The rapid evolution of agile practices has further complicated matters as to when to perform a security test and what budget to allocate for testing.

This is where bug bounty hunters are making waves in helping companies protect their digital assets. Through ongoing, scalable security testing, companies stay on top of exploitable vulnerabilities and weak points in their security posture.

### 1 in 3 vulnerability reports go missing for companies without a clear VDP

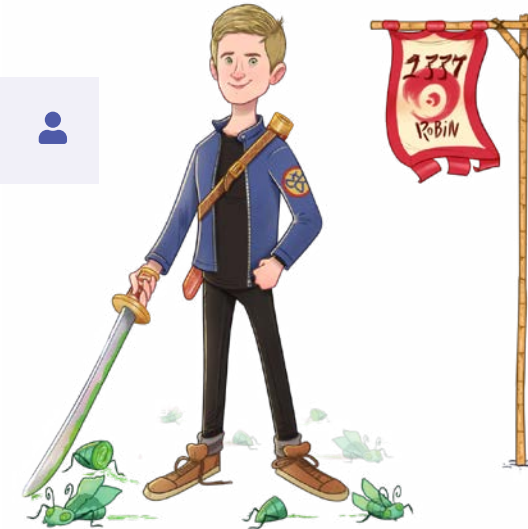
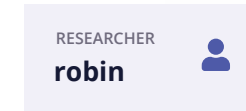
Moving off bug bounty platforms, 70% of our community say they've discovered a vulnerability before but found no clear route to report it. After further analysis, the data revealed that 32% of reported risks remain undetected by the company, and open to exploitation. How companies make themselves available to the assistance of hackers needs attention.

<sup>1</sup> <https://threatpost.com/cybersecurity-bug-hunting-enterprise-confidence/164782/>

<sup>2</sup> <https://www.fenews.co.uk/press-releases/54318-expert-commentary-says-only-10-of-tech-talent-has-cyber-skills-to-fill-skills-gap>



# 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.





# Our hackers: Who are they?

## Redefining what 'hacker' means

Defining a hacker is almost guaranteed to spark a debate. At some point, it's likely we've all imagined a hacker to look and behave how we see in films.

In 2021, becoming an ethical hacker is a popular ambition amongst information security professionals around the world. Like malicious hackers, they're driven by an overriding goal: to break through a target's system defences. However,

as the name suggests, an ethical hacker operates within the law and will disclose vulnerabilities to the companies they work with.

Despite having the same skill sets, education, and creative way of thinking, malicious hackers have taken claim over the title. But at Intigriti, we're looking to change that. By shifting how the world perceives security researchers, we can take back ownership of

the term and redefine what 'hacker' means.

### Ethical Hacker definition

A security expert that specialises in the testing of computer and software systems or processes to evaluate, strengthen and improve security.

📌 An ethical hacker **operates within the law** and will disclose vulnerabilities to the companies they work with.



## Ethical Hacking Origins

While ethical hacking, often dubbed white-hat hacking, may have only evolved into a common cybersecurity profession in the last decade, it actually predates black-hat hacking activities. Throughout the sixties, hacking simply meant optimising systems and machines to make them run more efficiently. Most of these activities used to take place in Western Europe and the United States, but this has changed significantly.



# 3 types of ethical hackers



## 1 Bug bounty hunter

Crowdsourced cybersecurity enthusiasts and professionals that perform security testing. Rather than being remunerated for their time, an organisation will reward them with a bounty if they successfully report a new, unique vulnerability.



## 2 Red team/blue team

A specialist cybersecurity assessment team that gauges the strength of an organisation's security posture to identify weaknesses using offensive techniques (Red Team) and improve defences (Blue team.) The model comes from the navy where a Red Team attacks and a Blue Team defends. These highly trained cybersecurity professionals often collaborate closely to improve security through continuous feedback and bi-directional knowledge transfer. The goal is to strengthen the organisation's preventative, detection, and response controls.

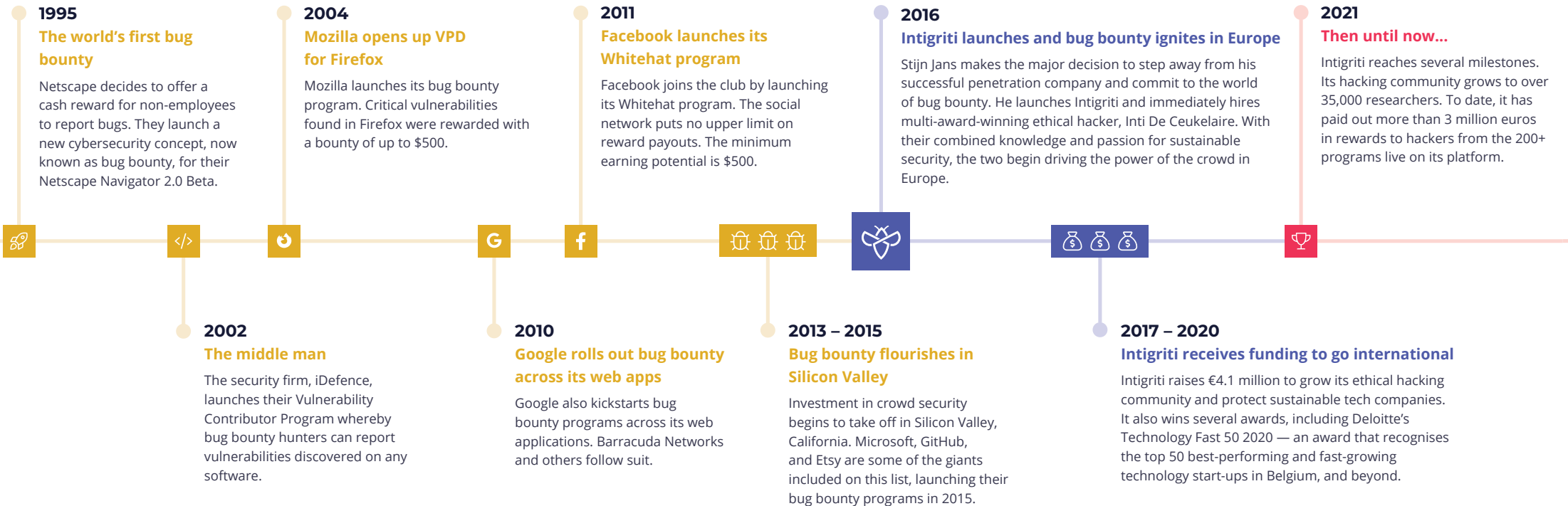


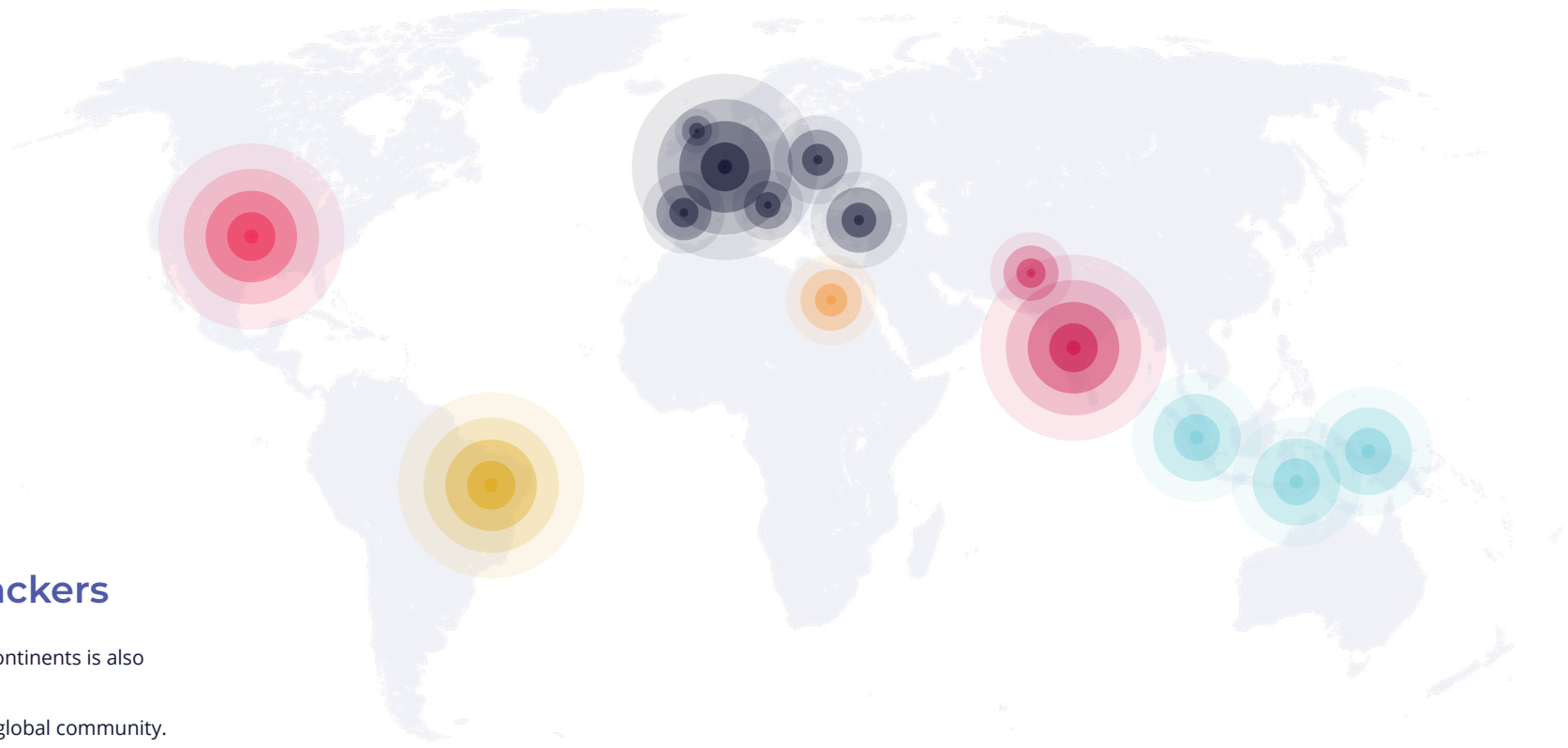
## 3 Penetration tester

A penetration tester evaluates the security of a computer system or network by simulating an attack from malicious outsiders, typically within a given timeframe and/or target scope as set out by the client. Their purpose is to identify attack vectors and vulnerabilities, and control weaknesses. It involves the use of a variety of manual techniques supported by automated tools and looks to exploit known vulnerabilities.



# History of bug bounty & incentivised vulnerability disclosure





## Where are they?

### A truly global community of hackers

The majority of Intigriti's programs come from European companies, which consequently has drawn in a strong European crowd of cybersecurity enthusiasts. When looking at where our researchers are based, Belgium, The United Kingdom, France, Germany, Turkey, and The Netherlands are among the top 10 locations. Additionally, 8 out of 10 of the best performing countries (in terms of hacker payouts) were European. However, Intigriti's

presence in other continents is also steadily increasing — making it a truly global community.

As the work-from-anywhere culture grows in businesses, so too has the world of bug bounty. Remote working has made it possible for companies and researchers to collaborate from all corners of the world. In 2020, Intigriti's security researchers submitted vulnerability reports from more than 140 countries.



#### Researcher residency location

- |                     |                |
|---------------------|----------------|
| 01. India           | 09. Pakistan   |
| 02. Belgium         | 10. Brazil     |
| 03. United States   | 11. Egypt      |
| 04. United Kingdom  | 12. Bangladesh |
| 05. France          | 13. Indonesia  |
| 06. Germany         | 14. Italy      |
| 07. Turkey          | 15. Spain      |
| 08. The Netherlands |                |



#### Best performing researchers

- |                     |               |
|---------------------|---------------|
| 01. Belgium         | 09. Romania   |
| 02. The Netherlands | 10. Sweden    |
| 03. France          | 11. Morocco   |
| 04. India           | 12. Russia    |
| 05. Germany         | 13. Poland    |
| 06. Turkey          | 14. Indonesia |
| 07. United States   | 15. Spain     |
| 08. Italy           |               |





## What are they?

### Smart, young, do-gooders

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

This crowd of IT experts takes cybersecurity seriously. But in most cases, they're on the Intigriti platform because they're curious, seeking a challenge, and wanting to have fun. For a fifth of our community, making the internet a safer and more secure environment is their primary goal.

📌 More than **half (55%)** of our community have completed a **Bachelor's degree** and a further **15%** have a **master's degree**.

RESEARCHER  
iqimpz





13 to 17-year-olds

3%

18 to 24-year-olds

51%

25 to 34-year-olds

33%

35 to 49-year-olds

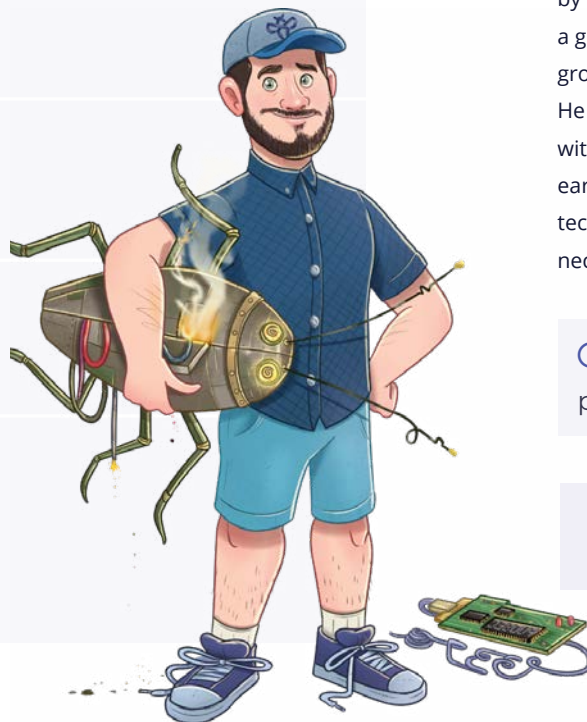
12%

50 to 64-year-olds

1%

More than 65-years old

0%



## Demographics

### Digital natives with a hunger to learn

The majority of our community are digital natives. The term was coined by Marc Prensky in 2001 to describe a generation of people who have grown up in the era of technology. He describes them as 'comfortable with technology and computers at an early age' and people who consider technology to be an integral and necessary part of their lives.'

This is reflected in our data.

Unsurprisingly, the dominating age group for hackers on the platform is 18-24-year-olds (51%).

The second most popular age group within the community is 25-34-year-olds (33%).

❗ The **dominating age group** for hackers on the platform is **18 to 24-year-olds** (51%).

RESEARCHER  
pudsec







## Bringing many angles of security to a single environment

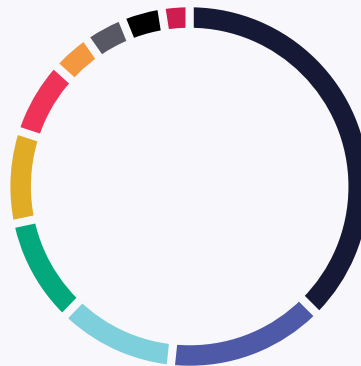
The majority (80%) of our community work within the IT industry and use Intigriti as a secondary source of income. However, 79% still devote up to 20 hours a week to bug bounty hunting.

For their day-job, popular professions include Penetration Tester (43%), Security Analyst (27%), and Software Developer (6%).

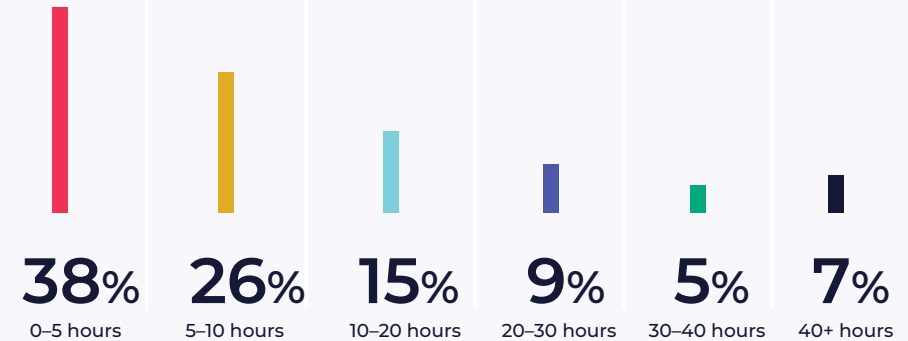
📌 80% of our community works in IT and use Intigriti as a secondary source of income.

### Where do the rest come from?

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



### Number of hours spent on bug bounty hunting per week



RESEARCHER  
sumgr0





## Self-educated security enthusiasts, eager to break the mould

Bug bounty is still a relatively new and exciting landscape for security enthusiasts. It's also a less traditional security career path. Around half (56%) of our community only arrived on the bug bounty scene in the last year. For the hacking community, age is just another number, and the proof is evident

in [our leaderboard](#)<sup>1</sup>. The average age of the hackers occupying our leaderboard is 25 years old. To be a successful vulnerability researcher, you need to be able to approach the problem with a fresh perspective, apply unharnessed creativity, and be unafraid to go against the grain.

① The **average age** of the ethical hackers occupying our leader-board is **25 years old**.



How much experience do our researchers have in bug bounty?

**56%**

have less than a years  
experience

**25%**

have 1 - 2 years  
experience

**14%**

have 2 - 4 years  
experience

**5%**

have more than 4 years  
experience




## Evolving our community

To prosper as a hacker, education is key — but not necessarily in the traditional sense. Most hackers use a combination of self-teaching, online blogs & articles, and online courses to learn how to hack.

Many of our researchers, however, have taken the steps to build upon their highest level of education which demonstrates their inherent need to keep developing. Around a fifth (19%)

have CEH (Certified Ethical Hacker) Certification, OSCP (Offensive Security Certified Professional) certification, and/or Offensive Security Web Expert (OSWE) certification.

However, certification isn't always accessible to everyone, and learning outside of the traditional classroom can offer a truer reflection of cybercrime activity and techniques.

 We're **proud to empower the next generation of cybersecurity talent** with unlimited learning resources.

<sup>1</sup> <https://app.intigriti.com/leaderboard>

<sup>2</sup> <https://blog.intigriti.com/hackademy>

### Top 3 Highest Level of Education Amongst Intigriti's Community

**55%**

have a bachelor's degree

**22%**

completed upper secondary school

**15%**

have a master's degree



### How we keep our community's knowledge & skill sets relevant

We're proud to empower this and the next generation of cybersecurity talent with unlimited learning resources. The [Intigriti hackademy<sup>2</sup>](#) is a collection of free online, educational resources in the field of web security. For every vulnerability category, we provide our community with detailed

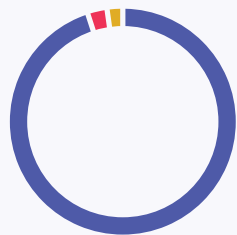
explanations of how they work, with real-life examples, write-ups, bug bounty tips, and explainer videos. We also update our hackers regularly with the latest infosec news so they can stay informed about what's happening in the world of security.



# Closing the gender gap

Currently, 95% of cybersecurity researchers are male

Cybersecurity is facing a gender diversity issue — and this is reflected in our data, with 95% of Intigriti hackers identifying themselves as male. Together with our industry peers, we need to do better.



Gender Breakdown Of Intigriti Hackers

95%

identify as male

3%

Identify as female

2%

Prefer not to say





## How Intigriti is bringing more women into cybersecurity:

Intigriti is actively working towards diversifying cybersecurity, with a strong focus on gender. Here are just a few examples of that:

### Influencing the next generation of female security talent

We're proud to work with some awesome female influencers to increase the profile of women in cybersecurity.

Currently, these include:

Katie Paxton-Fear [@InsiderPhD](https://twitter.com/InsiderPhD)<sup>1</sup>,

Mariem El Gharbi [@PentesterLand](https://twitter.com/PentesterLand)<sup>2</sup>,

Farah Hawa [@Farah\\_Hawaa](https://twitter.com/Farah_Hawaa)<sup>3</sup>,

Vickie Li [@vickieli](https://twitter.com/vickieli)<sup>4</sup>

### Supporting women in security

We're headlining as a Platinum Sponsor of [NahamCon](https://nahamcon2021.splashthat.com/)<sup>5</sup> 2021 for Women In Security.

### Fighting discrimination

In 2020, we introduced our zero-tolerance policy towards sexism (as well as other forms of discrimination) within our bug bounty platform, and beyond.



<sup>1</sup> <https://twitter.com/InsiderPhD>

<sup>2</sup> <https://twitter.com/PentesterLand>

<sup>3</sup> [https://twitter.com/Farah\\_Hawaa](https://twitter.com/Farah_Hawaa)

<sup>4</sup> <https://twitter.com/vickieli>

<sup>5</sup> <https://nahamcon2021.splashthat.com/>



## Hacker highlights from @mstramgram @PentesterLand

**Hi Pentesterland! Can you tell us a bit about yourself?**

**Pentesterland:** Hi, I'm Mariem, a 34-year-old hacker and entrepreneur living in Morocco. I initially wanted to specialise in Cryptology as I was doing a Masters degree in Cryptology and IT Security. However, the "IT Security" part was so fun and fascinating that I ended up doing an internship on DNS Rebinding attacks. I fell in love with web security and the idea of analysing web security mechanisms to understand how they work and subvert them. I got a job as a penetration tester and as I was rummaging through InfoSec news to stay updated, I discovered bug bounty programs and was instantly hooked.

**One huge hurdle hackers face is information overload. How do you keep up with the fast pace?**

**Pentesterland:** Information overload was an issue for me because I used to specialise in penetration testing. Pentesters have to be polyvalent and be able to cover more surface than bug hunters in a short time. So, when I started bug bounty hunting, I thought I had to learn about all vulnerability types, tools, and tips at the same time. But then I noticed that many bug bounty hunters are successful in doing a deep dive into a single bug class.

I've changed my learning strategy because of this. I note down any new research and information, and only come back to it when it's the subject of my focus.

**Do you have a favourite bug class or type of target that you focus on?**

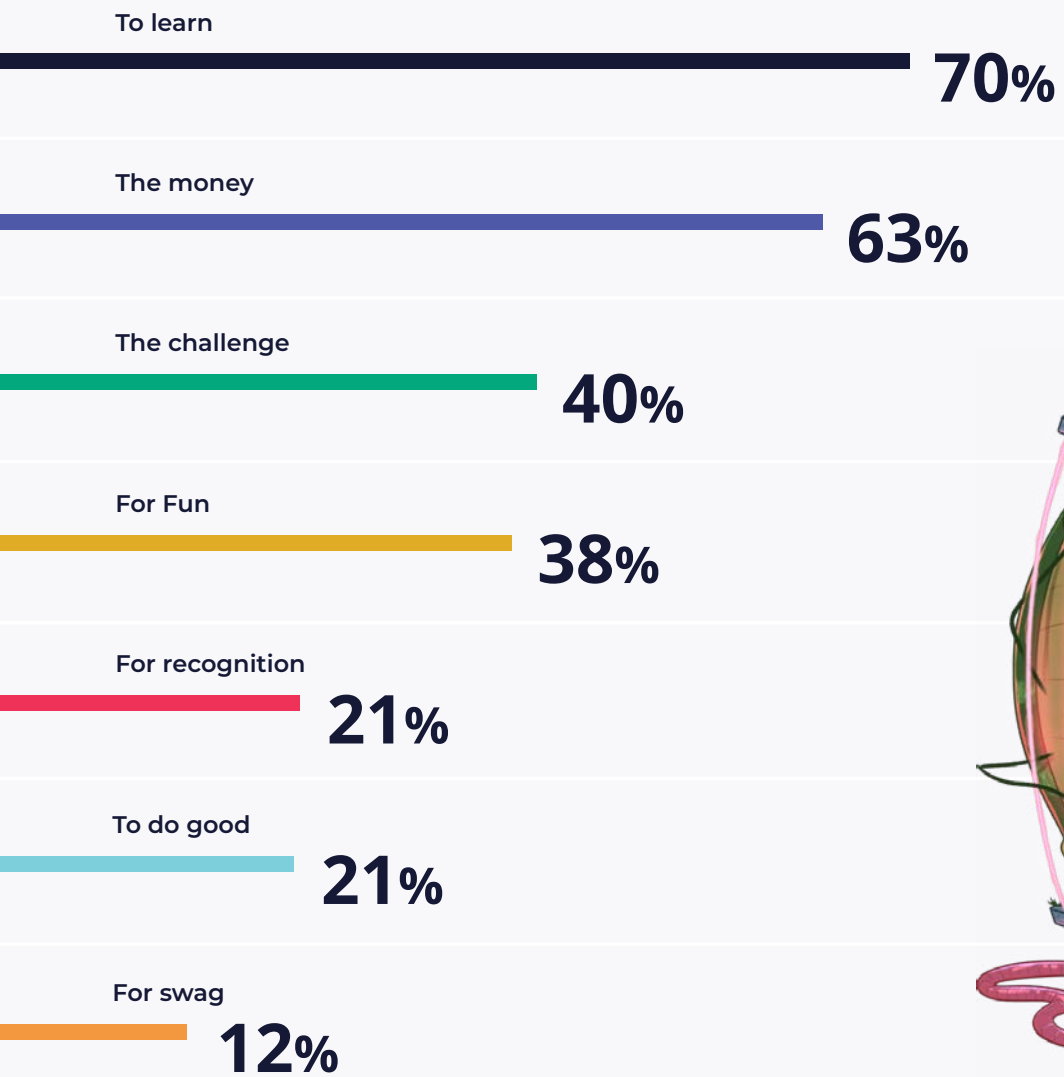
**Pentesterland:** I like focusing on bug classes that scare me the most, for the challenge. If I can get a handle on them, I can do and learn anything else. Once I have found enough of one class of vulnerabilities, I'll switch to a different one I want to master.

I am not very selective about targets. I work on public and private programs, and open scope isn't a requirement.

“ I am not very selective about targets. I work on public and private programs, and open scope isn't a requirement.







## Why they work

70% of our community are here to learn

RESEARCHER

Pieter



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



## Natural Curiosity

Think of hackers as explorers of the digital arena — they're eager to develop their knowledge of the fast-moving and ever-changing security landscape. 70% of our hackers are on the Intigriti platform to learn and develop their skills, and 40% are driven by the challenge.



## Earning money to have fun, follow dreams & afford a better lifestyle

Like in all professions, there is, of course, a financial motive. When asked what motivates them to hack, 63% said they hunt for vulnerabilities to earn more money. However, rather than using the cash to earn a living, most do it to allow them to live the lifestyle they desire.

More than half (52%) of our community say their bug bounty earnings contribute less than 10% to their total income. Yet, for 10% of our community, bounty earnings make up their sole income.

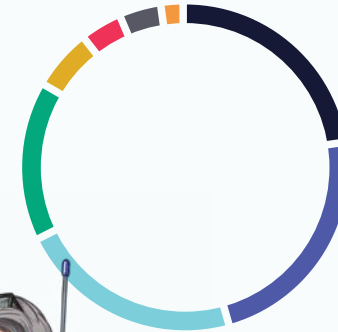
With bug bounty being an untraditional career choice, none of our community says they learned about the concept through school or career teachers. Most of our hackers learned about bug bounty hunting through friends (22%), during an internet search (22%), or social media (21%).

Given that home-working trends are growing, Intigriti expects this number to grow significantly over the next few years. In a [FlexJobs<sup>1</sup>](#) survey, 65% of respondents reported wanting to transition to working remotely full-time post-pandemic, and 31% desire a hybrid remote work environment. Bug bounty platforms allow security professionals to work from anywhere — which makes it an attractive option to candidates who can't get this level of flexibility elsewhere.

**i** For 10% of our community, bounty earnings make up their sole income.

### Most popular ways to discover the world of bug bounty

- 22% were recommended by a peer
- 22% found it via a search engine
- 21% via social media
- 15% via blog posts
- 6% via news articles
- 4% via online chats
- 4% via workshops
- 2% via vendors



RESEARCHER  
\_jca\_



<sup>1</sup> <https://www.flexjobs.com/blog/post/remote-work-statistics/>



## How they spend their earnings

### Goal-driven rewards

In August 2020, Intigriti hacker, @MattiBijnens, reached a very exciting milestone. Having set himself a challenge to earn enough bug bounties to be able to afford a Tesla, he finally reached his goal. So, what did he do with the money?

He bought the car. And what does he plan to do next? Hack it.



### Spending money to earn money

The laptop on the left is how it started, and the laptop on the right is how it's going for Intigriti's hacker, @\_D3LT4\_. He took to Twitter in November 2020 to showcase his newly purchased laptop, monitor, and keyboard (right), which he bought entirely through bug bounty rewards.

The way he sees it, the purchase was a case of spending money to earn more money.



RESEARCHER  
hg\_real



## What is the coolest thing they've done with their bounty money?



For a long time, I just put all my earnings from bug hunting and work in a savings account. Then, I wanted to treat myself for the first time. I bought a ticket to an onsite training day on advanced usage of Burp Suite, and booked everything from plane tickets to hotel.



**PentesterLand**

Intigriti Cybersecurity Researcher



Any bounty money goes directly to my kids' education. I don't have anything cooler to report there, unfortunately!



**Pudsec**

Intigriti Cybersecurity Researcher



Travel the world! I spend two days a week hunting for vulnerabilities on the Intigriti platform. This allows me to earn enough income to live off and do the things I want to do in life, like go travelling.



**Kuromatae**

Intigriti Cybersecurity Researcher



RESEARCHER

**\_p4fg\_**







## Doing good for the sake of doing good

There are obvious benefits to taking the legal route to disclose vulnerabilities: The money, the credit (21% enjoy the recognition they receive), and the free swag. But ultimately, ethical hacking is about being part of a community that defends against cybercriminals. That's why for 21% of our community, their primary goal on the platform is to do good.

① **Ethical hacking** is about being part of a community that **defends against cybercriminals**.





## Hacker highlights from @Pudsec

### Hi Pudsec! Tell us a bit about yourself.

**Pudsec:** I'm 38, married with 3 kids, and living in Australia. I've been working in the IT industry since high school and have worked in most fields.

### What does your life look like?

**Pudsec:** I work full time as a Linux system administrator and Python/PHP software developer. With the family, sports and work, it's hard finding spare time to hunt for bugs so it's more of a hobby at the moment. I'll usually hunt when I get home from work and the kids are occupied with homework. Then after their bedtime, I'll try and fit in another hour or so.

### What has been the most interesting bug you've found?

**Pudsec:** Probably one of my first ever bugs! I was browsing around on a target and discovered a private employee portal that was using Google single sign-on for authentication. I tried logging in with my Gmail account but it failed, stating it was an invalid domain. I checked out the requests it had sent and could see it was sending my Gmail address in plain text. So, I decided to try logging in again, but this time I intercepted the request and changed it to 'pudsec@' + the company's email domain. Like this: 'pudsec@CompanyName.com'. I successfully logged into the company's client portal which gave me access to all their client data.

### Why do you choose Intigriti for bug bounty hunting?

**Pudsec:** Intigriti triages very fast, and with such positive and encouraging comments. That really lifted me — especially when I was still quite new to the bug bounty world. They're very efficient too. For example, once I submitted a bug to triage, and not only did they validate it, but they went the extra mile to find a few other things to add from their end. The results of their input escalated the severity of the bug. They also took the time to explain their workings to me to help me develop as a bug bounty hunter.

“Intigriti triages very fast, and with such positive and encouraging comments. That really lifted me — especially when I was still quite new to the bug bounty world.”







# What attracts our hackers to a bounty?

## Excitability, exclusivity, and of course, earning potential

Earning potential isn't the only incentive for our community — but it's certainly an attractive aspect. Just over three-quarters (76%) of our community hack with some financial motive. For example, 20% search for low-hanging fruit by choosing what they describe as 'easy targets.' 23% seek out bounty's that offer fast payments, and a third (33%) look for vulnerability programs that offer a large maximum or minimum payment.

**i** Just **over three-quarters (76%)** of our community **hack with some financial motive.**

At the same time, hackers are inquisitive people who enjoy a challenge. For this reason, 85% of them said they seek out programs that offer a lot of scope or fresh scope. The feeling of exclusivity is another key driver. Around a third (30%) of our community said they enjoy being part of a small, select team of hackers who are personally invited to take part in a vulnerability search.

### What are the top reasons for picking a bug bounty target

**68%**  
says lots of scope

**43%**  
says fresh scope

**42%**  
says responsive team

**30%**  
says not many invited hackers

**23%**  
says fast time to payment

**22%**  
says familiar target

**20%**  
says easy target

**20%**  
says large maximum payment

**13%**  
says larger minimum payment



## Building strong, working relationships

Within our community, 42% say it's important to them that the team is responsive, which is particularly crucial to those looking to build a strong, continuous relationship with a company. On this note, more than a fifth (22%) say they like working with brands they're familiar with.

**i** Within our community, 42% say it's **important to them that the team is responsive.**

RESEARCHER  
**bitmap**



## Customer Spotlight

Red Bull utilises Intigriti's crowd of security researchers to hunt and disclose vulnerabilities in their public systems. Their focus is on maintaining communication and building strong personal relationships with their hackers, rather than only focusing on formal processes.

**They also incentivise uniquely with free cans of their energy drink and branded merchandise depending on the severity of the vulnerability. An exceptional vulnerability is even rewarded with a special surprise!**

Stefan Winkler, IT Security Manager at Red Bull: "We see the work with Intigriti's hackers as a partnership where everyone provides what they are good at on a non-monetary base. We provide a huge playground of systems and technologies for ethical hackers to explore and, of course, trays and trays of Red Bull! On the other side, we receive vulnerabilities that have been obtained by ethical hackers. A win-win."




## How they work

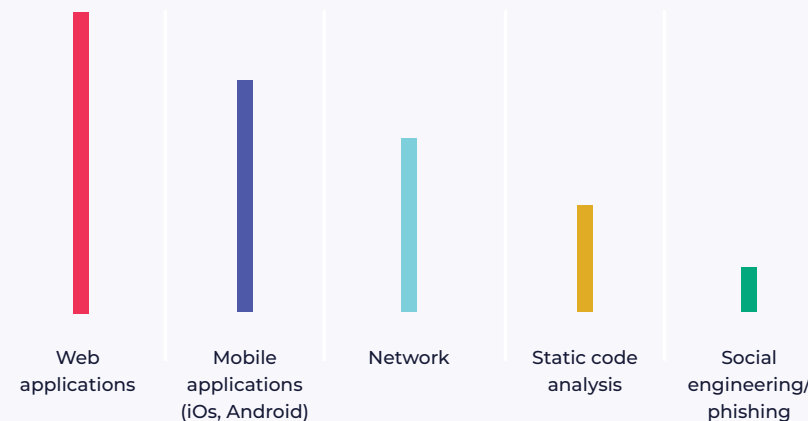
### Web application is the most popular platform to target

The most popular platform our security researchers choose to hunt for vulnerabilities is in web applications. Considering that over

80% of malicious hacks happen on web applications, our community is in the right place.

 **80%** of malicious hacks happen on web applications

#### Top 5 favourite platforms to hack



#### What drives hackers to web applications?

- Nearly every company with an online presence has digital exposure, ranging from a personal website to an intranet.
- Web applications are easily accessible. All the researcher needs is a web browser.
- Successful web application hacking requires time and patience, but not high-level coding skills. This makes web application hacking accessible to all levels.



## How researchers report vulnerabilities through bug bounty platforms



## What does triage do?

The job of the triage team is to check if the report is valid, unique, and in scope. Here's a summarised version of the steps they take before escalating reports to clients:

- Review reports.
- Deem whether the vulnerability is 'exploitable'.
- Ensure the vulnerability is genuine and in scope.
- Approve the information included in the report (to ensure it makes sense to the client).
- Request more information.
- Prevent duplicate vulnerabilities from being submitted.
- Decline reports that are out of scope, based on the company's program description.
- Assess the severity of the vulnerability, based on impact.
- Be the go-between for client and security researcher.



## What do you find on Intigriti that you don't find elsewhere?



I really like the method for submitting reports on Intigriti. First, it's Intigriti's triage team who test and approve the report before they send it to the client. This is important because I know that, if it is passed along to the client, I'm sending across a good vulnerability. From the client-side, this step is valuable because they know they aren't about to have their time wasted.



**Kuromatae**

Intigriti Cybersecurity Researcher



I've used several platforms and found Intigriti's triage team to be the most effective and polite. There is always someone to answer questions or to discuss the outcome of a report. I also appreciate everything they do for the community, such as encouraging content creators and sharing bug bounty tips.



**Pentesterland**

Intigriti Cybersecurity Researcher



Intigriti triages very fast, and with such positive and encouraging comments. That really lifted me - especially when I was still quite new to the bug bounty world.



**Pudsec**

Intigriti Cybersecurity Researcher





## Bug bounty through a triager's eyes



Our priority is to give the clients and researchers a personal approach. It's important that both communities feel like they are talking to a person, and not some sort of robot. Being a triager is more than pointing out whether something is valid or not. For every decision we make, a detailed explanation must be given. We pride ourselves on being as helpful as possible.

**Quinten Van Ingh**  
Intigriti Triager



## Reaching organisations through other disclosure methods

Though a lot of organisations already understand the value of ethical hacking and actively ask for the help of our security researchers, the number of companies without a vulnerability disclosure policy in place is still much larger.

### What is a vulnerability disclosure policy?

A vulnerability disclosure policy (VDP) is otherwise known as a responsible disclosure policy. In essence, it is a set of guidelines for security researchers to follow when alerting companies to weaknesses in their digital assets. A policy provides a framework to allow hackers to communicate vulnerabilities in the correct format and through the right channel. But most importantly, it ensures their voices are heard.

A VDP must allow for open and fluid conversation between the company and the researcher. Businesses can [create their own vulnerability disclosure policy](https://blog.intigriti.com/2021/04/14/ultimate-guide-how-to-write-vulnerability-disclosure-policy)<sup>1</sup>.

### Why is a vulnerability disclosure policy important?

Having a vulnerability disclosure policy available on your website is important because it allows goodwill hackers to assist your business and protect it from exploitation. VDPs aren't specific to larger organisations — companies of any size can benefit from one.

By having a policy, businesses:

1. Reduce the risk of potential exploitations going undetected
2. Streamline their vulnerability reporting process
3. Minimise time-to-remediation
4. Show a commitment to information security
5. Build trust among stakeholders and customers.

### Disclosing vulnerabilities responsibly

Vulnerability disclosure isn't a new discussion — it's a topic that has been talked about for decades. In the late 1990s, American cryptographer Bruce Schneider said that "full disclosure is a damn good idea".

While the notion that vulnerable disclosure should follow an orderly process remains to this day, there is a greater focus now on doing this responsibly.

Today, consideration is given for the public release of vulnerability details, for example. In some cases, public disclosure can result in negative consequences for users.

### What's the difference between a VDP and a bug bounty program?

The key difference between a VDP and a bug bounty program is that a VDP follows a passive approach whereas a bug bounty is active.

Whilst a VDP allows for any goodwill security enthusiast to submit reports, bug bounty programs encourage a specific community of verified professionals to carry out vulnerability research. The latter will have access to a potential earning structure, based on impact.

Even with a bug bounty program, it's encouraged that businesses also have a VDP available on their website.



<sup>1</sup> <https://blog.intigriti.com/2021/04/14/ultimate-guide-how-to-write-vulnerability-disclosure-policy>



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

We asked our community how they report vulnerabilities outside of a bug bounty program. Concerningly, 70% have identified vulnerabilities before but found no vulnerable disclosure program to report it. Of that group, 12% didn't escalate the report. For those that did, 32% of them said the report got lost in the process or weren't sure whether it was successfully reported. That's 44% of the risks that remain undetected.

Deploying a bug bounty program will help lower the risk of a vulnerability not reaching your security team, or getting published on social media. It also acts as an additional assurance process, post-go-live, and throughout your security lifecycle.

**i** Concerningly, **70% have identified vulnerabilities** before but **found no vulnerable disclosure program to report it.**

### Most popular formats to report a vulnerability when no VDP available

**50%**

customer service

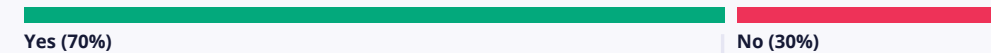
**15%**

guessing the correct email address

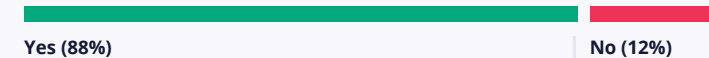
**14%**

social media

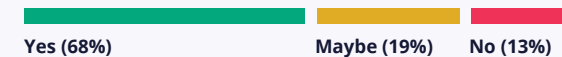
### Have you ever found a vulnerability in a company without a hacker policy?



### Did you report this vulnerability?



### Was your report successful?





## Hacker highlights from @Pieter

**What does the typical day of a full-time bug bounty hunter, like yourself, look like?**

**Pieter:** My day looks very similar to any other home-office worker. I wake up at normal hours, I try to stick to my 8 hour days, and I work Monday to Friday. The big difference is that I get to choose what I do and when I do it.

**How do you approach targets?**

**Pieter:** Normally, I'll work at a target and find four or five bugs, lose inspiration, move on, but return to it again only six months later. I'm interested to see how they fixed the previous bugs I reported and whether any new ones have appeared when they made updates.

**What advice would you give to companies listing their first program?**

**Pieter:** Make access effortless. If I get to a program and the credentials haven't been given yet or they don't work (e.g. the company has IP restrictions), I lose interest fast! If you want to have continuous attention over a longer period of time, decent payouts will help attract more people to the program.

**Do you ever stumble across vulnerabilities in companies that don't have any responsible disclosure policy?**

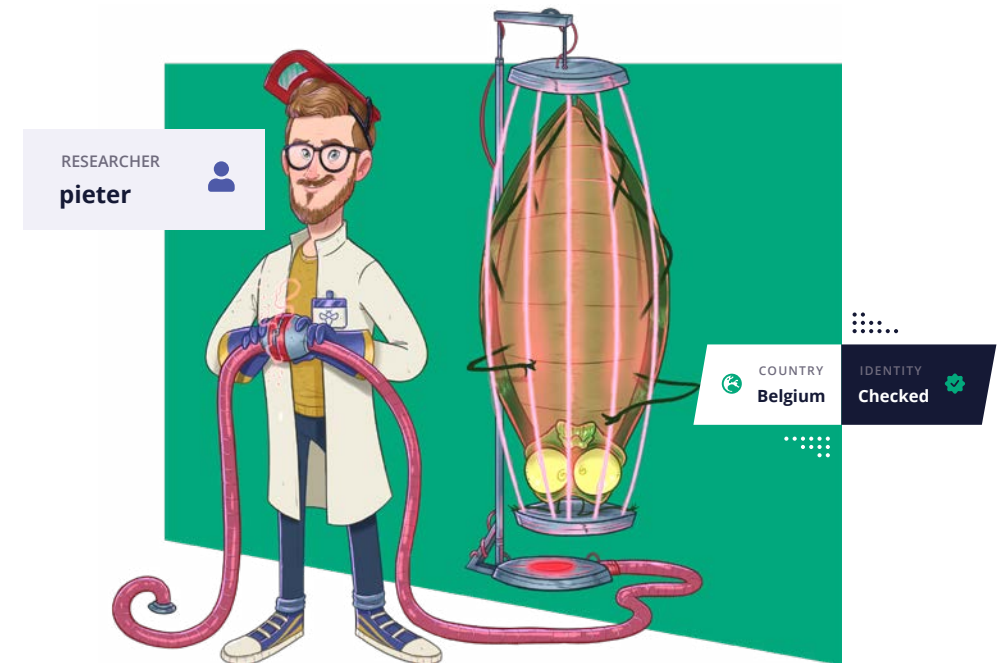
**Pieter:** Yes, 'this looks vulnerable' is a reaction I have all the time to all sorts of websites! But I don't ever target them. It can be

quite painful when you find a vulnerability for a company that doesn't have a VDP because I know how vulnerable they are. Yet, I have no way of disclosing it to them. Companies need to do better in that respect.

**What are your predictions for the future of bug bounty?**

**Pieter:** Looking at the past five years and projecting that into the future, I'm expecting bug bounty to grow enormously. However, I think the awareness of bug bounty platforms is going to grow fairly organically. Anyone working in an IT team today is likely to have heard about bug bounty as a possible solution already.

**“** I'm interested to see how they fixed the previous bugs I reported and whether any new ones have appeared when they made updates.





Have you ever collaborated with other hackers?

No, but I'd like to

61%

No, and I don't plan to

9%

Yes, and I'd do it again

29%

Yes, but I won't do it again

1%



## Collaborations

### Lone-wolves, team contributors, and everything in between

The stereotypical hacker may be an introvert, but our data challenges this: 91% of our researchers have collaborated with others on a program, or would like to in the future.

#### A community built on knowledge-sharing

The hacking community has one common goal: To outsmart cybercriminals. Being on a bug bounty platform, these researchers know better than anyone that cybersecurity isn't something that can be done alone.

To succeed, cybersecurity must be built on a foundation of knowledge-sharing, collaboration, and confluence.

#### Recognition is worth more than money

Of course, goodwill is enough for most to not withhold information from other hackers. However, there is another reason too. To 21% of our researchers, receiving acknowledgement for what they've contributed to the community is more valuable than a cash reward.

**i** 91% of our researchers **have collaborated** with others on a program, **or would like to in the future.**



.....

## Hacker Highlights from @Kuromatae666

### Can you tell us about yourself?

**Kuromatae:** Hi, I'm Anthony, otherwise known as 'Kuromatae', and I'm from Brittany. I used to work as a pen tester but I decided that working for an employer wasn't for me! That's when I decided to be my own boss and become a full-time bug bounty hunter.

### Do you ever work in collaboration with other hackers?

**Kuromatae:** Yes, I really like working in collaborations! What's great is that no two hackers think in the same way. When people collaborate, they end up finding some very interesting, new, and big vulnerabilities that neither of us would have ever considered otherwise!

### How do you pick your targets?

**Kuromatae:** When I pick a target, the most important aspect to me is how the company responds - including the time they take to do so. Sometimes, I only report one or two vulnerabilities at first and see how they respond before sending others. To me, first impressions count.

### How do you pick a target today?

**Kuromatae:** Who I target depends on my mood at the time but I like targeting medical companies because it helps a lot of people. I did some pen tests for a hospital recently that didn't have any reward to give. However, I only needed fifteen minutes to look into their site to report many vulnerabilities. I helped them secure their digital assets for almost nothing of my time.

### What was your quickest find?

**Kuromatae:** I think my fastest critical vulnerability find was within 10 seconds - and that was for quite a well-known company that had already done a penetration test. However, as I said before, no security researcher thinks the same. That's why I always try to play with the aspects that people don't ordinarily think about when security testing.

When it's a big vulnerability, sometimes companies will respond, fix the problem, thank me and reward me within five minutes from when I submitted the report.

“ My fastest critical vulnerability find was within 10 seconds - and that was for quite a well-known company that had already done a penetration test.





# Annual Hacking Events

## Bringing the world's leading and upcoming hacking talent together

Events heighten the buzz in the hacking community. They offer researchers around the globe an opportunity to come together and compete. Last year, Intigriti organised one of our biggest and best hacking events in Brussels. Thirty carefully selected individuals from around the world were asked to join us in our mission to help secure a couple of high-profile targets.

### Here's what one of our researchers had to say about the event.

"Had I been told a year ago that I would attend this live hacking event, I would have laughed. But here I am at a famous hotel in the heart of Brussels. The elevator door opens and inside are four familiar faces — they're some of the best hackers in the world! I'm used to seeing them in interviews and on Twitter, sharing advice and exploits.

### So, what led me to this point?

Two months prior, I got an email invite to an exclusive event with an RSVP form to confirm attendance.

A month later, I was added to a private messaging group together with everyone attending. The first thing I did was check the list. Imagine the Hall of Fame, and feel the fear! I was briefed around some practical details (such as how to get there and expense my journey) and asked to sign an NDA. Then, 12 days before the event, the call arrived that everyone had been waiting for: I was given information about the scope, the target, and the assets I'd have access to.

Immediately, the instant messenger group went crazy! Bug submissions also started rolling out quickly. What struck me most during this phase was that, despite this being a very

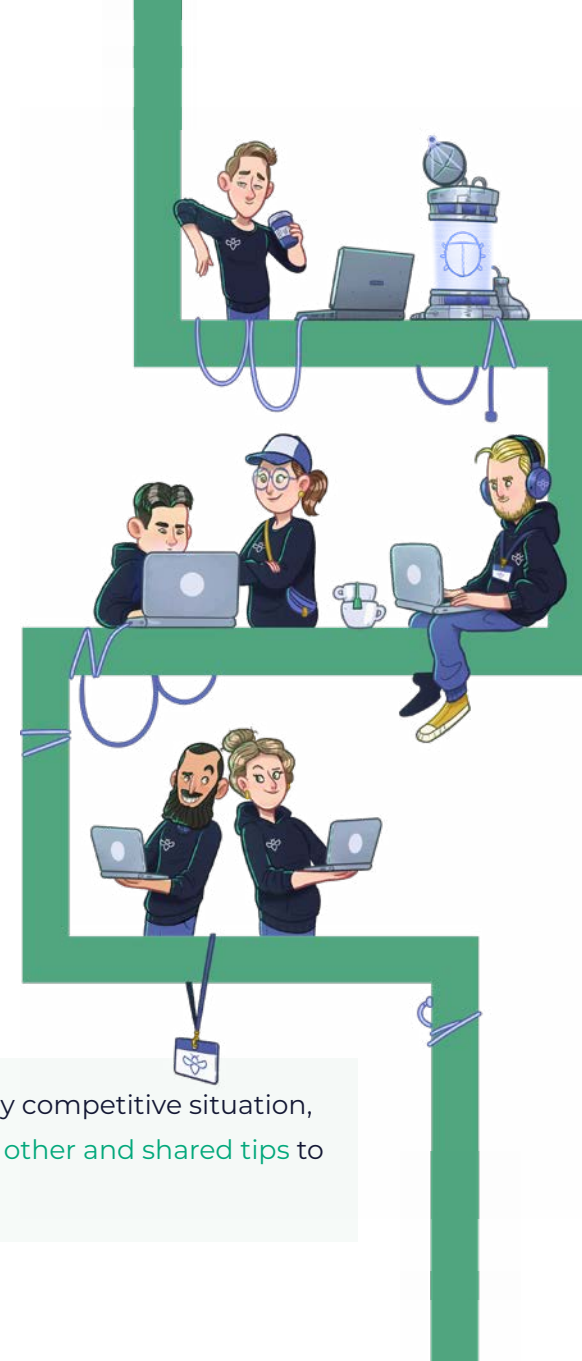
competitive situation, many hackers helped each other and shared tips to save other people time. When we finally reached the big day, everyone was already checked-in to the hotel and ready to go. I arrived at the venue around 9.20 am. After presenting myself at the reception, I was given a badge, a hoodie, and a poster to sign. Afterwards, we were guided to the 3rd floor, where all the hacking was happening.

We could choose between 3 rooms: One for people collaborating, one for relaxation and discussion, and one for working silently. I chose the last one. It had a big screen with a leaderboard. Then the Intigriti team explained the rules and introduced

additional scope. Hacking had officially begun! From that point, I didn't notice much apart from what was going on on my laptop's screen. However, the leaderboard was updated from time to time to reflect triage results.

At the end of the day, we had a very fancy dinner and the winners were announced! Awards were attributed to the winners, and the best bugs were briefly explained. They were high-level, jaw-dropping stuff!"

**i** Despite this being a very competitive situation, many **hackers helped each other and shared tips** to save other people time.





# Conclusion

**Ethical hackers are empowering businesses everywhere to outmanoeuvre cybercriminals by staying one step ahead.**

To bust through scalability constraints, overcome skills shortages, and stay within allocated budgets, effective security is no longer something that businesses can do alone. More and more, companies are seeing ethical hacking communities as a means to help.

For those that are considering (or new to) the concept of crowd-sourced security, Intigriti's Ethical Hacker Insights Report 2021 should have demystified who and what ethical hackers are. Simply, they are the

current and up-and-coming generation of Information Security talent working to keep your digital assets safe.

They genuinely care about making the digital landscape more secure for businesses to operate. This attitude is shown time and time again throughout this report — from consistent knowledge-sharing to choosing industries that may not have the budget to offer a reward. By helping these organisations, our community knows they're helping to keep customer data safe too.

① They genuinely care about **making the digital landscape more secure for businesses** to operate.





# Glossary

## **Bug bounty**

The concept of crowd-powered security testing, found in bug bounty platforms.

## **Security Researchers**

The cybersecurity professionals that perform the security tests. Also known as ethical hackers.

## **Bounty**

A monetary reward for researchers when they successfully reported a new, unique vulnerability for an organisation.

## **Vulnerability**

A vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack.

## **Vulnerability assessment**

Vulnerability assessments (sometimes referred to as 'scanning') are the use of automated tools to identify known common vulnerabilities in a system's configuration. Vulnerability Assessment tools scan the information systems environment to establish whether security settings have been switched on and consistently applied - and that appropriate security patches have been deployed.

## **Ethical hacking**

Hacking refers to the action of trying to bypass system limitations that are not allowed under normal operations. Since hacking is overall perceived as negative, ethical hacking is used to explain that this is done by someone with good intent.

## **Responsible disclosure**

Reporting a potential security vulnerability to the probable owner of the system

## **Vulnerability Responsible Disclosure Policy**

The process by which security researchers should alert companies to a vulnerability in their digital assets.

## **Public disclosure**

The action of publishing a or several security vulnerabilities on a public channel (such as social media or blogs) with or without permission.

## **Security breach**

The result of a successful hack by a malicious hacker.



# About Intigriti

## Agile Security Testing Powered by the Crowd

Intigriti helps companies protect themselves from cybercrime. Our community of ethical hackers provide continuous, realistic security testing to protect our customer's assets and brand.

Our highly engaged community of security researchers continuously challenges customers' security against realistic threats: we test in precisely the same way malicious

hackers do. Intigriti goes beyond traditional pentesting or bug bounty programs; our customers appreciate our advanced guidance and unmatched agility.

Our interactive platform features real-time reports of current vulnerabilities and commonly identifies crucial vulnerabilities within 48 hours.

Founded in 2016, Intigriti set out to conquer the limitations of traditional security testing. Today, the company is widely recognised for its innovative approach to security testing, impacting both customers' security awareness and security researcher's lives. Our community means everything to us. We help ethical hackers craft a non-traditional career, doing the work they love and getting paid fairly.



## Stay informed

**Intigriti blog: A one-stop source for bug bounty news and advice**

<http://go.intigriti.com/blog>

A free resource to digest important bug bounty news, interviews, and best practices.

**Bug Bytes: A newsletter curated by the community**

<https://blog.intigriti.com/category/bugbytes/>

The world of information security changes every day. It can be a challenge to keep up but here is where your weekly dose of Bug Bytes can help. When subscribing to the newsletter, you will receive a comprehensive list of all write-ups, tools, tutorials, and resources.

To stay informed, subscribe to our security newsletters today.





Already **a lot of companies** have  
joined Intigriti's platform







## 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.

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

[HELLO@INTIGRITI.COM](mailto:hello@intigrity.com)



Intigrity



hackwithintigrity



@intigrity

