



The Ethical Hacker Insights Report 2022

ETHICAL HACKING: THE RISING CAREER PATH FOR INFORMATION SECURITY PROFESSIONALS IN 2022





Not enough time? Watch the webinar!

Scan this QR code to watch the webinar or go via this link <https://go.intigriti.com/ethical-hacker-report-webinar-22>



Page 4

¹ <https://go.intigriti.com/Ethical-Hacker-Report-2022-esecurityplanet-trends>

² <https://go.intigriti.com/Ethical-Hacker-Report-2022-medcitynews-talent>

³ <https://go.intigriti.com/Ethical-Hacker-Report-2022-globalxetfs-threats>

⁴ <https://go.intigriti.com/hr2021>

Page 6

⁵ <https://go.intigriti.com/hr2021>

Page 13

⁶ <https://go.intigriti.com/Ethical-Hacker-Report-2022-Female-Hackers>

⁷ <https://go.intigriti.com/Ethical-Hacker-Report-2022-Donate-to-Women>

⁸ <https://go.intigriti.com/Ethical-Hacker-Report-2022-1337UP-Live>

⁹ <https://go.intigriti.com/Ethical-Hacker-Report-2022-WiCys-Women-in-Cybersec>





Table of contents

- 4 Executive Summary
- 5 Key terms
- 6 Bug bounty is a fast-growing community
- 8 Where are they?
- 12 Who are they?
- 13 Driving more female hacking talent at Intigriti
- 14 The rise of bug bounty hunting as a career choice
- 20 Security testing methods through the eyes of penetration testers
- 22 Vulnerability reporting preferences and habits outside of a bug bounty platform
- 24 Self-hosted programs vs bug bounty platforms
- 30 What can you take from this report?





Executive Summary

In 2022, becoming an ethical hacker is an increasingly popular ambition amongst information security professionals worldwide. According to our survey of 1,759 security researchers*, 96% would like to dedicate more time to bug bounty hunting in the future and 66% are considering it as a full-time career.

When combining the [cybersecurity skills shortages](#)¹ with the ongoing [war for talent](#)², it's essential that organizations pay attention to this trend. Concerningly, the findings show that this generation of professionals aren't getting what they need from employers to keep their skills and knowledge up to date, despite [rising cybersecurity threats](#)³. For information security, for

example, 50% of respondents say they turn to bug bounty hunting to learn the most relevant and useful knowledge.

However, these respondents aren't novices when it comes to security testing. As well as bug bounty hunting, 65% of respondents said they also have hands-on penetration testing experience, and 73% have contributed to a Vulnerability Disclosure Policy (VDP). Taking the opportunity to dive deeper into their opinions on traditional security testing techniques, the response on penetration testing was undivided. According to our survey, 90% of respondents agreed or strongly agreed that

- a penetration test cannot provide
- continuous assurance that an
- organization is secure year-round.

What you'll learn from this report

As well as continuing our work of [demystifying ethical hacking](#)⁴, with a deep dive into researchers' drivers, motivations, and ambitions, we're highlighting:

- ✓ The views of ethical hackers around bug bounty programs, penetration testing, and VDPs
- ✓ How companies can use bug bounty hunting as an educational tool for internal training
- ✓ How organizations can work with a globally distributed community of ethical hackers.

But before we dive into these topics, read on to understand some key terms we'll use throughout this eBook.

*See the full survey methodology for this survey on page 35.



Key terms

Bug bounty concepts explained

Bug bounty platform

A bug bounty platform, like Intigriti, facilitates the creation and management of bug bounty programs. Most security researchers choose to report vulnerabilities through a bug bounty platform because it provides the best infrastructure and legal framework for them to be successful. Security researchers can engage and communicate with companies in a safe, structured, and reliable way, while receiving live updates and communications.

Similarly, companies find bug bounty platforms to be one of the most reliable and stable ways to set

up programs. When you sign up to Intigriti as a client, for example, a customer success manager will help you define a clear scope for your program and advise on aspects like what you'll compensate researchers and how you'll manage budget flow.

Bug bounty program

A bug bounty program allows independent security researchers (also known as ethical hackers) to report bugs to an organization in a legally compliant manner.

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.

Bug bounty hunter

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

Bounty

If the submission is accepted by the organization it relates to, the researcher is paid a reward or compensation which is better known as a 'bounty'. The reward or compensation can be monetary or reputation points, but also gifts like goodies and swag.






Bug bounty is a fast-growing community

Since the release of [Intigriti's Ethical Hacker Insights Report 2021⁵](#), the number of security researchers signed up to the platform has increased by 43% and the average amount of vulnerability submissions per month also rose by 43%. During the same period, the number of live bug bounty programs on Intigriti's platform increased by 48%, which according to 23% of our community was a key driver in them dedicating more time to bug bounty hunting since the pandemic began.

The data collected for this section of the report is based on activity on Intigriti's platform between May 1, 2020 to April 1, 2021 and May 1, 2021 to April 1, 2022.



RESEARCHER
Alicanact60 

+200

Companies on Intigriti

↑ **100%**

+300

Active **programs**

↑ **48%**

+50,000

Registered **researchers**

↑ **43%**

4 M €

Total bounty **pay-outs**

↑ **65%**

1,600

Average vulnerability **submissions** per month

↑ **44%**



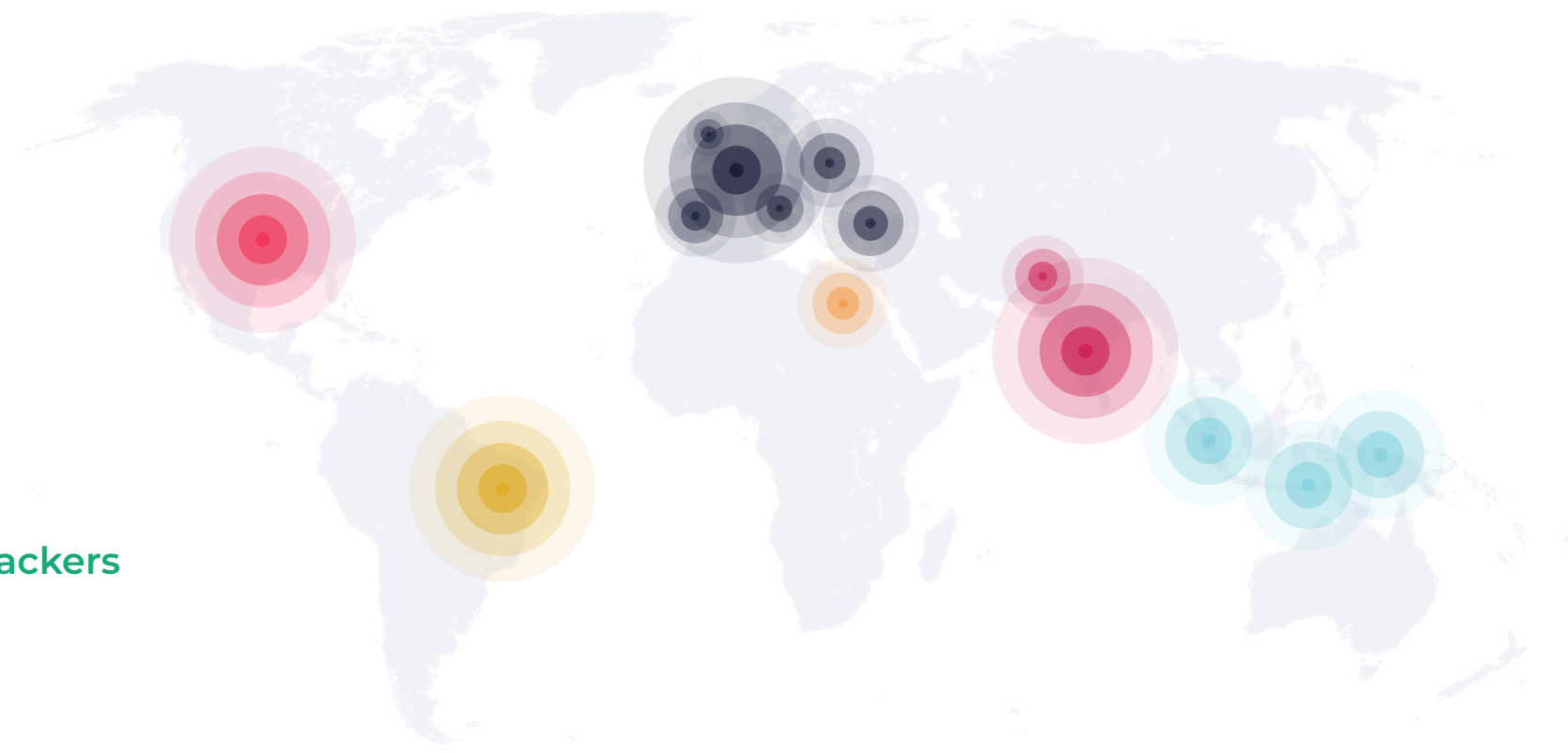
Total cybercrime costs saved since launch: \$71.7million

What is the true cost of Intigriti's bug bounty platform and services? Some would say \$71.7 million, as this is the total cybercrime costs, we have saved our customers since launch. Based on the average cost of a data breach (USD 4.24million, according to IBM) and total number of triaged reports by Intigriti.

23%

of vulnerability reports submitted via the Intigriti platform in the last year were deemed high impact.





Where are they?

A truly global community of hackers

We have security researchers representing us across the world, and since our last report release (May 2021), the number of countries that the platform has received reports from increased by 36%.

Researcher residency location

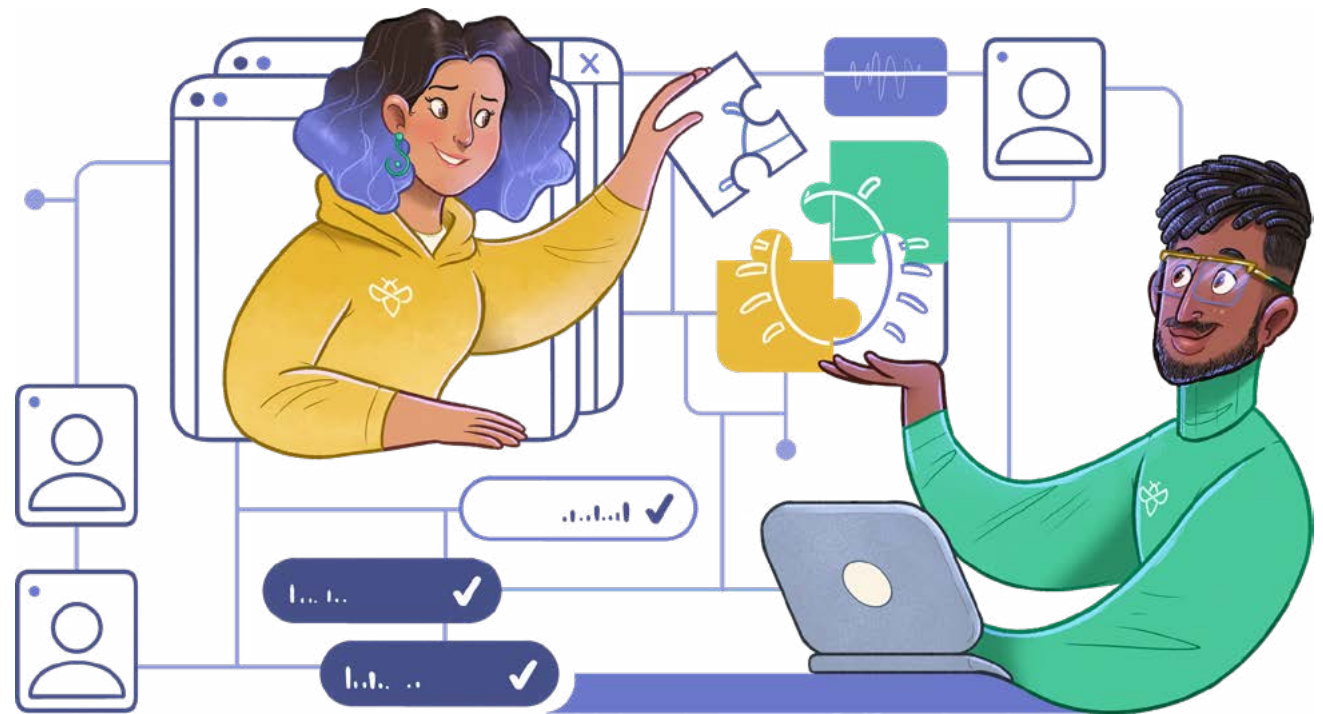
- | | |
|---------------------------|---------------------|
| 01. India | 06. Germany |
| 02. United States | 07. The Netherlands |
| 03. Belgium | 08. France |
| 04. Brazil | 09. Turkey |
| 05. United Kingdom | 10. Pakistan |

Best performing researchers

- | | |
|----------------------------|--------------------|
| 01. Belgium | 06. Germany |
| 02. The Netherlands | 07. Turkey |
| 03. France | 08. Finland |
| 04. India | 09. United Kingdom |
| 05. United States | 10. Vietnam |

Despite much of the world's organizations getting 'back to normal', remote working culture is here to stay. According to experts at Owl Labs, around 62% of employees aged 22 years-old to 65 years-old want to continue working remotely at least occasionally. Bug bounty hunting creates opportunities for researchers to work from anywhere, at any time, and pick their targets. These aspects are increasingly appealing to those that desire the remote work lifestyle.

i 62% of employees aged 22 years-old to 65 years-old want to continue working remotely at least occasionally.





Bug bounty hunters: Who are they?

Most bug bounty hunters are part-time

More than half (54%) of the community are in full-time employment elsewhere and 32% are students. With this in mind, it's unsurprising that much of the community (86%) define themselves as part-time bug bounty hunters. Even so, just over a fifth (22%) of this group gets more than a quarter of their total income from bounty pay-outs.

With regards to work, a large part of the community (65%) say they have hands-on penetration testing experience (they are currently, or have previously been, a penetration tester). Considering that the average base salary for a penetration tester in the UK is £38,624 (€46.060/USD \$50,903) per annum, according to PayScale, an additional 25% of income is a significant increase for part-time bug bounty hunters.

Are full-time bug bounty hunters

14%

Are part-time bug bounty hunters

86%

Spend less than 5 hours per week on bug bounty hunting

40%

Spend 6-20 hours hunting for bugs per week

45%

Have hands-on penetration testing experience

65%

RESEARCHER
Kapytein



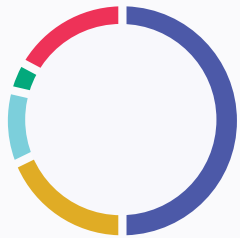


The dominating age group is 21-29-years-old

The majority (73%) of survey respondents fall under the age of 30-years-old, indicating that since the last Ethical Hacker Report, Intigrity is still a young community. However, looking at the habits of the respondents over the age of 30-years-old, 52% said they have dedicated

more time to bug bounty since the pandemic began. While digital natives were the early adopters of bug bounty, older generations are quickly following their lead.

i 73% of survey respondents fall under the age of 30-years-old



Community breakdown by age

4%

13 - 17 yrs old

19%

18 - 20 yrs old

50%

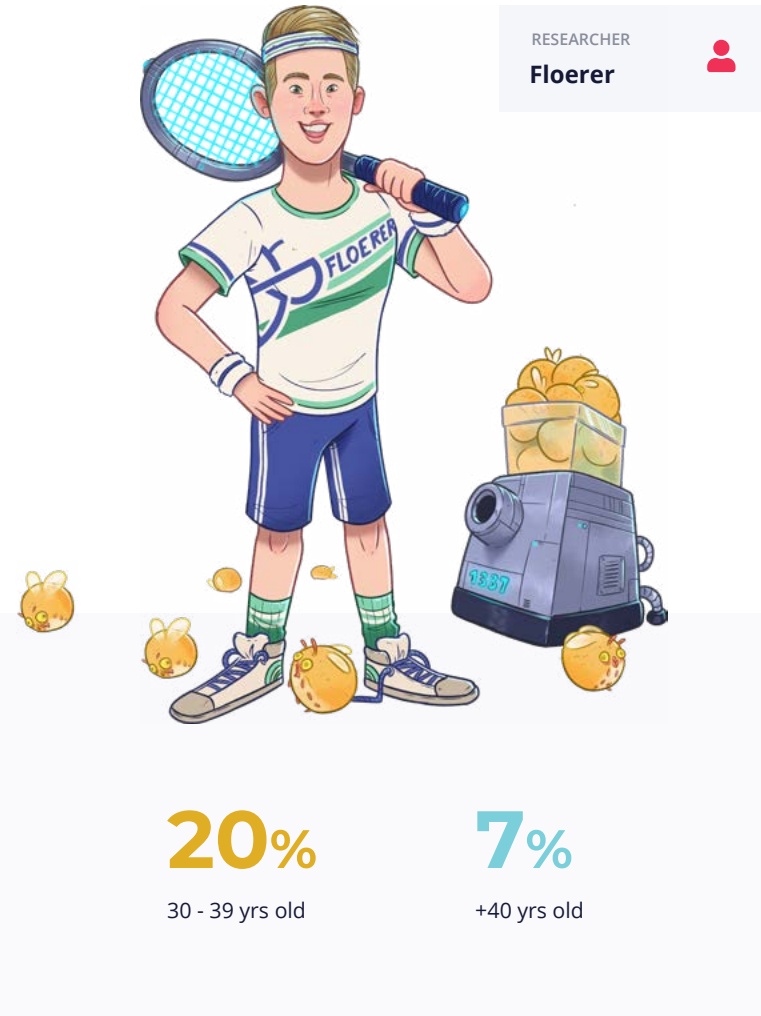
21 - 29 yrs old

20%

30 - 39 yrs old

7%

+40 yrs old



RESEARCHER

Floerer





Driving more female hacking talent at Intigriti

It's well-known that there is a shortage of female tech talent. Being part of this world, we understand this better than anyone. Within the bug bounty community alone, 95% of hunters are male — but we're trying to change that. One way we can help diversify the industry is to influence the next generation of female security talent by bringing those already [defying stereotypes](#)⁶ to the forefront. In addition, we [donated all of our sponsorship money](#)⁷ from our virtual live bug bounty conference in March ([1337UP LIVE](#)⁸) to [Women in Cybersecurity \(WiCyS\)](#)⁹.





The rise of bug bounty hunting as a career choice

Bug bounty hunting is a highly desirable career choice amongst young people

As well as 96% of respondents stating that that they want to increase the amount of time they spend hunting for bounties, two thirds (66%) would even go as far as to consider the practise as a full-time career. This is particularly true

for respondents under the age of 30-years-old, with more than three-quarters (77%) of this age group saying they'd consider bug bounty hunting full-time.





96%

of the community would like to dedicate more time to bug bounty hunting in the future.

66%

would consider bug bounty hunting as a full-time career.

77%

of these respondents were 30-years-old or younger.

i The biggest appeal of full-time bug bounty hunting to respondents is the money, with 48% declaring this as their number one attraction point. The desire to be their own boss and ability to work their own hours closely follow, with 45% of respondents listing these points as appealing aspects.

RESEARCHER

IsiraAdithya





What aspects of full-time bug bounty hunting appeal to respondents?

48%

The money

45%

To be their own boss

45%

To work their own hours

41%

The work is interesting

36%

To help companies be more secure

29%

To work from home

Other reasons respondents are attracted to full-time bug bounty hunting include the ability to work on any company target in the world (23%), and the ability to outsmart malicious hackers (10%). Another 10% also said that working alone is a desirable aspect.

*Respondents could select more than one answer.

Word-of-mouth recommendations is resulting in more ethical hackers

Encouragingly, 96% of the community members would, or have, convinced a friend to take up ethical hacking. Word-of-mouth recommendations remain to be the biggest driver for the expanding ethical hacking community, indicating that there is an elevated level of trust. In other words, these professionals see the practice as a sustainable security testing solution and career choice.

i 96% of the community members would, or have, convinced a friend to take up ethical hacking



The pandemic drove more infosec talent towards bug bounty platforms

Responses to the pandemic, such as social distancing rules and temporary job retention schemes, opened more time for people to pick up the hobby they always wanted, or to spend more time on the tasks they never had time for. In the case of our community, that hobby was ethical hacking — and it's clear the hobby stuck. In comparison to before when the pandemic began, 59% of all respondents said they are spending more time bug bounty hunting.

Leading their biggest motivation for dedicating more time to bug bounty hunting, 74% wanted to increase their skills while just over half (53%) had a financial motive to earn more.

*Respondents could select more than one answer.

Top 5 reasons why include:

74%

Grow their bug bounty hunting skills

53%

Earn more through bug bounty hunting

35%

Got better at bug bounty hunting

32%

More time to dedicate to bug bounty hunting

23%

Say the bug bounty platforms have got better



RESEARCHER

Ethic_Yuki



Bug bounty hunting is helping to tackle the cybersecurity skills shortage challenge

It's the responsibility of security teams to protect their organization's networks, information, systems, and assets while also managing defenses against potential cyber threats. It's no secret that this is an arduous task, especially since cyber threats are always evolving and increasingly sophisticated. So, how do security professionals keep up?

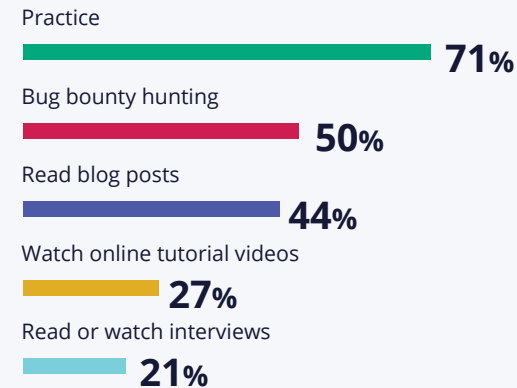
Bug bounty hunting was listed as the second most popular method to develop their general security skills and knowledge. In fact, with 50% of respondents choosing bug bounty hunting as their first choice, this was voted a significantly better avenue to learn than through their jobs (11%).

When it comes to resources of the most relevant and useful information about security, 78% of respondents chose bug bounty hunting as the best option, compared to 8% that said they learned more in an official education environment (in school, college or university.)

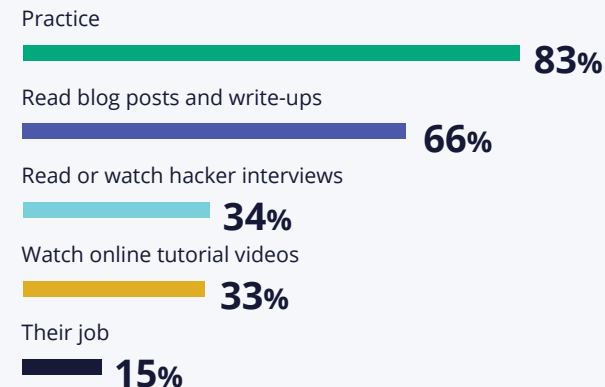
*Respondents could select more than one answer.

Top 5 tactics respondents use to develop their:

General information security



Ethical hacking skills and knowledge



Ethical hacking communities are often first discoverers of evolving security threats

Since May 2021, 64% of Intigriti's ethical hackers have encountered a vulnerability they've not previously come across before. Of this group, a third (33%) don't believe the vulnerability had the potential to be picked up through a traditional penetration test. As attackers shift tactics, cyber defences must too. The only way to test their effectiveness is to apply continuous pressure against them.

Taking into account the answers of all respondents that met our criteria, 90% said they agreed or strongly agreed that "a penetration test cannot provide continuous assurance that an organization is secure year-round."

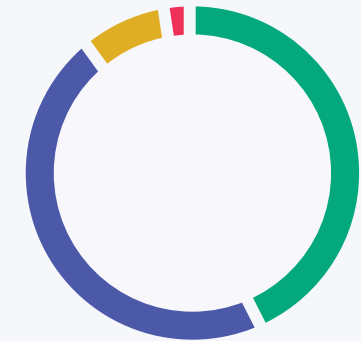
The community uses their bug bounty hunting experience to elevate their careers

Getting hands-on hacking experience is creating opportunities for the community. For example, 49% of respondents say their bug bounty experience has helped them secure an employment opportunity and 44% say, while they have not yet used their bug bounty experience to secure employment, they will use it in the future.

Do you agree with this statement?

"A penetration test cannot provide continuous assurance that an organization is secure year-round."

- Strongly agree (43%)
- Agree (47%)
- Disagree (8%)
- Strongly disagree (2%)



📌 49% of respondents say their bug bounty experience **has helped them secure an employment opportunity.**



Security testing methods through the eyes of penetration testers

How do penetration testers value penetration tests?

With 65% of Intigriti's community having bug bounty hunting experience and direct penetration testing experience, we wanted to explore their opinions on both security testing methods. Of this group, 88% agree or strongly agree that "a penetration test cannot provide continuous assurance that an organization is secure year-round." Just 14% of the pentesters believed that a penetration test would be able to find all of the same types of vulnerabilities they have found during bug bounty hunting.

When these respondents were asked about the strengths of pentesting, 79% listed 'being paid for their time' as the biggest strength of pentesting while 43% liked that the time they put in is timeboxed.

Bug bounty hunting from the perspective of a penetration tester

Of the group with pentesting experience, 95% would like to dedicate more time to bug bounty hunting in the future and around two thirds (65%) would consider bug bounty hunting as a full-time career. For those that wouldn't consider bug bounty hunting as a full-time career, 70% were concerned about not having financial security.

To further support the transition from traditional consultancy to the new way of working, Intigriti is releasing its 'hybrid pentest' offering. The solution will enable companies to attract top tech talent by providing them with a new earning channel that maintains bug bounty concepts but with heightened financial security.

Strengths of bug bounty programs, according to penetration testers

53%

like that they can earn according to the impact of their finding

46%

liked that they could choose their own target

44%

liked that they could choose their own methodology

42%

liked that they could choose when they want to work



What is hybrid pentesting?

Intigriti has developed a new and unique approach to working with our community by **COMBINING** the **"PAY FOR IMPACT" APPROACH** of bug bounty programs with the **DEDICATED RESOURCING APPROACH** from classic penetration testing. The hybrid pentest enables our clients to request dedicated security testing time from a selected researcher within a selected time window. However, it comes with the reward model, motivation, reporting and triage of bug bounty programs. **Want to know more?**

[Request a demo today](#)

RESEARCHER

Mase289





Vulnerability reporting preferences and habits outside of a bug bounty platform



A quarter of the community have found a vulnerability and chosen not to report it through a VDP where no bounties or rewards are offered

According to the survey, 60% of respondents said they participate in these types of vulnerability reporting because they are an effective way to practice and learn, and 50% feel a sense of responsibility. However, 25% have found a vulnerability and chosen not to report it through a VDP where no bounties or rewards are offered.

Top 5 reasons why researchers don't participate in VDPs

52%

believe that hackers should be paid for reporting vulnerabilities

33%

said it takes too much time

33%

simply prefer working with bug bounty programs

32%

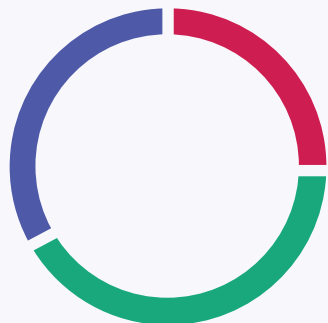
said they can't be sure the vulnerability will be fixed

27%

27% prefer focusing their time on paying opportunities

Have you ever found a vulnerability but chosen not to report it through VDP?

- Yes, I have (25%)
- No, I reported it (41%)
- No, this has never happened to me (34%)

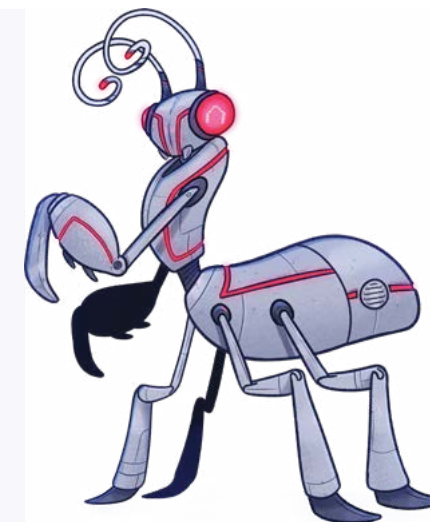


Why do you not participate in VDPs?

“

If a hacker spends their time and finds real vulnerabilities that would damage the company if in the wrong hands, *it simply doesn't seem right that they don't get paid.*

Leorac
Intigriti Security Researcher

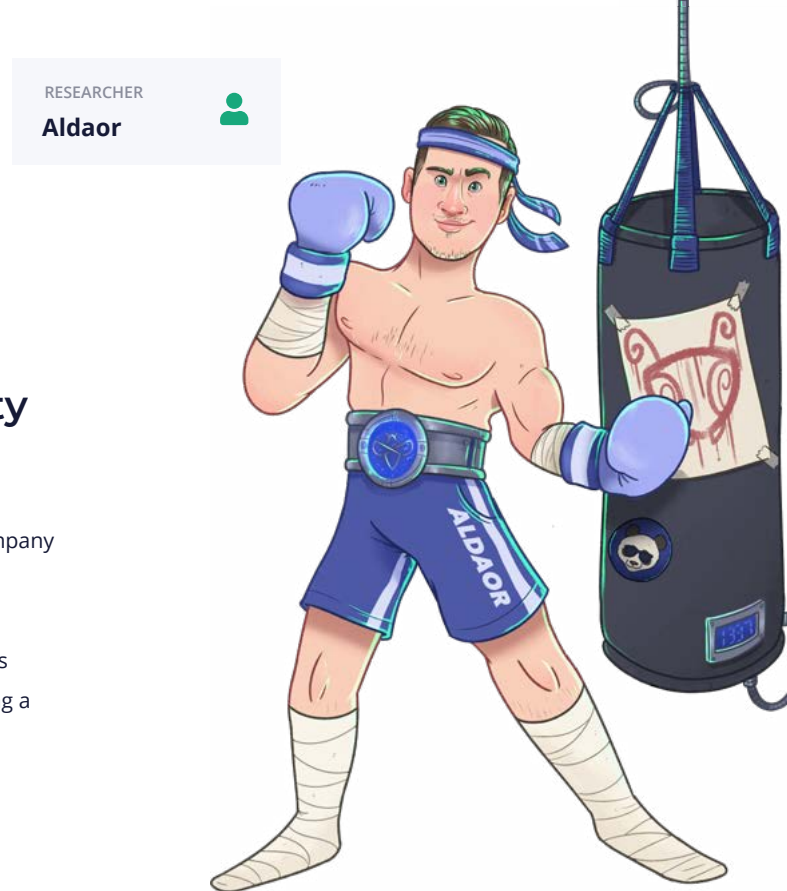




Self-hosted programs vs bug bounty platforms

Self-hosted programs vs bug bounty platforms

A self-hosted bug bounty program is exactly what it says on the tin. A company launches and manages the bug bounty program internally, relying on its own human and technological resources, and network. Before we reveal the community's feeling towards self-hosted bug bounty programs, here's some key differences between running an internal program and launching a program on a bug bounty platform.



SELF-HOSTED PROGRAMS

BUG BOUNTY PLATFORMS



Program engagement

Reactive and passive engagement
Good-willed ethical hackers will inform businesses of potential security issues.

Reactive and passive engagement
Ethical hackers are incentivized to engage with bug bounty programs through a monetary reward.



Validating submissions

Owned internally
Without enough manpower, the handling of non-valid submissions can be a time-consuming exercise.

Managed by triage
Triage teams provide a layer of quality assurance before escalating vulnerabilities to businesses.



Questions & comms

Handled internally
Managed by the internal team tasked with fixing incoming submissions.

Handled by triage
Communication is carried out within the platform. A triage department works as the go-between for client & researchers.



Payment processing

Manual
Responsibility of a finance department. To maintain good working relationships with researchers, it's important to provide payment promptly.

Automated through the platform
Processes automatically after a submission is accepted by the organisation. Payment and administration are taken care of by the platform.



Legal framework

Responsible disclosure
Researchers encouraged to perform responsible disclosure via a VDP.

Platform agreement
Researchers must agree to certain terms & conditions, providing both the company and researcher a clear legal framework.



Self-hosted programs could miss out on the contribution of almost half the ethical hacking community

Despite their desire to dedicate more time to reporting bugs to programs, more than a quarter (26%) of respondents said they do not work with companies outside of a bug bounty platform and 23% prefer not to. Considering this equates to almost half of the survey's respondents, organizations running a self-managed bug bounty program may not be achieving their potential engagement levels.

Why do ethical hackers avoid self-managed bug bounty programs?

When pressed on their reasons for avoiding or preferring not to work with companies outside of a bug bounty platform, 57% of the respondents cited it to the lack of a legal framework while 42% said the processes are less refined than a bug bounty platform. Other reasons include having less support available and a lack of a triage department (both 41%).

When we asked respondents why they would not work with companies outside of a bug bounty platform:

57%

cited it to the lack of a legal frameworks existing

42%

said the processes are less refined

41%

said there is less support available

41%

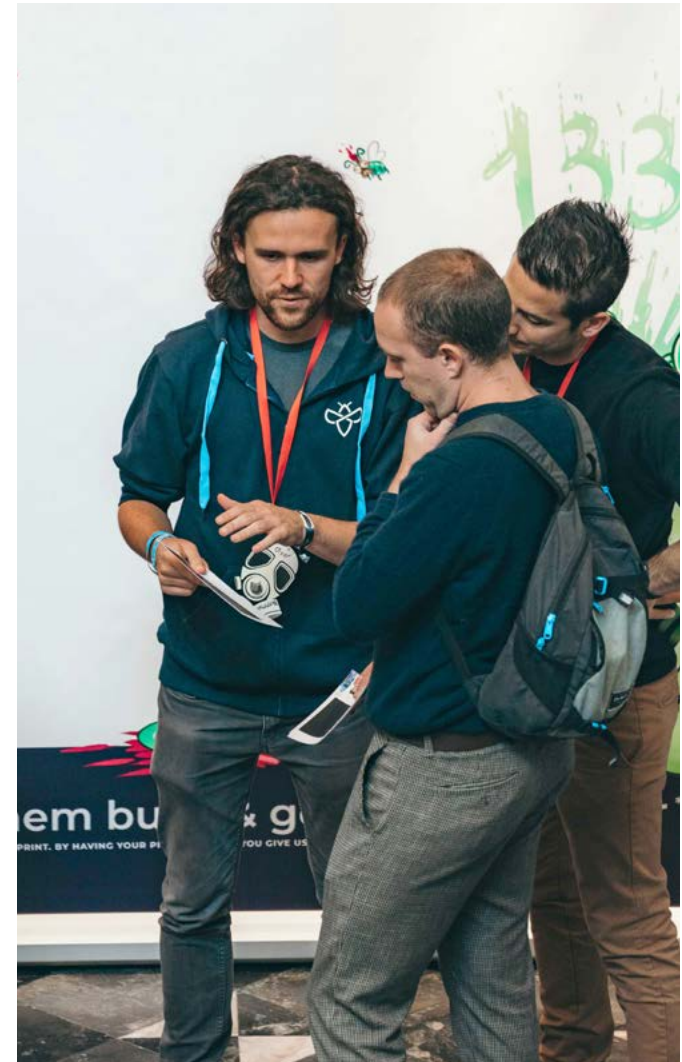
cited it to the lack of a triage department

34%

said the companies are too slow to respond

28%

said they cannot guarantee the vulnerability is fixed unless the company tells them





Customer spotlight

Showpad's bug bounty program helps drive their security development lifecycle

About Showpad

Intigriti customer, Showpad, creates a sales enablement software used by over 1,200 customers in more than 50 countries. Customer trust is critical in a data-intensive app like Showpad, and that means maintaining the highest levels of security and privacy. With their platform constantly and rapidly evolving thanks to their agile Software Development Lifecycle, continuous security testing is a must.



Showpad's testing background

Showpad had used penetration tests as part of their cybersecurity practices in the past, but they provided too static an approach for the fast-development world of Showpad's Software Development Lifecycle. Upon seeking out an agile security testing solution that would continuously challenge the platform against vulnerabilities, Showpad found Intigriti's bug bounty platform:

“Comparing bug bounty and pentesting is like comparing a photograph to a film. A penetration test is like looking at a picture of what the product looks like in a certain moment in time — but it doesn't say anything about tomorrow or the next coming weeks.”



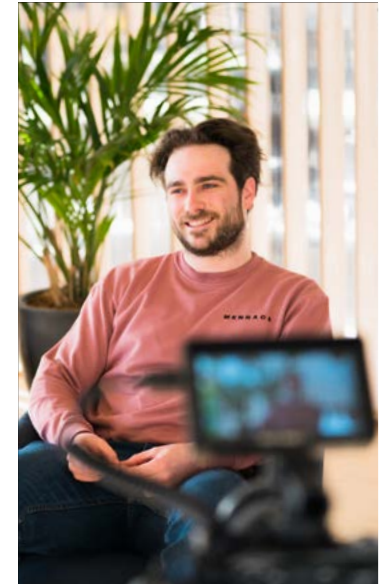
Bram D'hooghe

Director of Security, Privacy & Compliance at Showpad

Working bug bounty learnings into the Software Development Lifecycle

Since launching, Showpad has benefited from several high-quality vulnerability reports which they've been able to remediate. But they soon realized that a bug bounty program's benefits go further than catching vulnerabilities. For example, the information-rich vulnerability reports delivered to Showpad by Intigriti have been used as the basis for internal training materials. This has helped improve the engineering team's knowledge and security programming quality.

Today, Showpad builds application features designed to be secure from the offset. Furthermore, the security and development teams at Showpad now work more efficiently to build, test, and release application features. Bug bounty programs have been instrumental in this improvement and continue to help improve Showpad's cybersecurity posture on a day-to-day basis.





RESEARCHER

Putsi



What can you take from this report?

Encouragingly, more and more businesses are embracing bug bounty programs as a way to scale their security testing, accurately assess risk, and prioritize remediation. However, the findings in this report suggest that change isn't happening quick enough, resulting in a growing number of security talent moving away from traditional corporate settings and towards the more progressive opportunities that bug bounty offers. The good news is, employers can embrace the many opportunities crowd security creates for them too.

Crowdsourced security is becoming the new default for cybersecurity talent

As explored within this report, the potential for talent to shift from the traditional working environment towards crowdsourced security platforms is becoming an increasing reality for several reasons. The work-from-home culture has made employees desire more independence and has further encouraged digital nomads to pursue a remote working career. Our platform can not only facilitate this, but it also allows people to work wherever they want, whenever they want, and without having to rely on a boss to match their talent with customers or be part of a corporate hierarchy.

Significantly, this change in career preferences isn't just for younger generations. Since the pandemic began, 52% of respondents over the age of 30-years-old are spending more of their time on bug bounty platforms hunting for bounties.

A growing number of security researchers see less value in traditional security testing methods

With 90% of security researchers agreeing or strongly agreeing that "a penetration test cannot provide continuous assurance that an organization is secure year-round", it's time for employers to question whether they should still rely on them as a standalone too. Penetration tests (pentests) focus on one snapshot in time, whereas bug bounty programs are continuous. As attackers shift tactics, cyber defences must too. The only way to test their effectiveness is to apply continuous pressure against them.

Considering that an organization's security posture will change with each new feature release or update, it's not only a logical step to implement more security testing, but also critical.

On-the-job experience isn't sufficiently equipping cybersecurity professionals with the skills to handle growing cybercrime

Security teams play a potentially business-saving role in protecting and defending their organization's networks, information, systems, and assets against potential cyber threats. The responsibility is immense, and to keep up, security professionals must keep their skills and knowledge up to a constantly evolving standard. Yet, according to our survey, 50% of the respondents turn to bug bounty hunting to develop their general information security skills and knowledge rather than their employer.

Rather than viewing this finding as a criticism, employers should see it as an opportunity to create on-the-job learning opportunities that will not only increase their staff's knowledge, but also contribute to the overall security posture of the business.



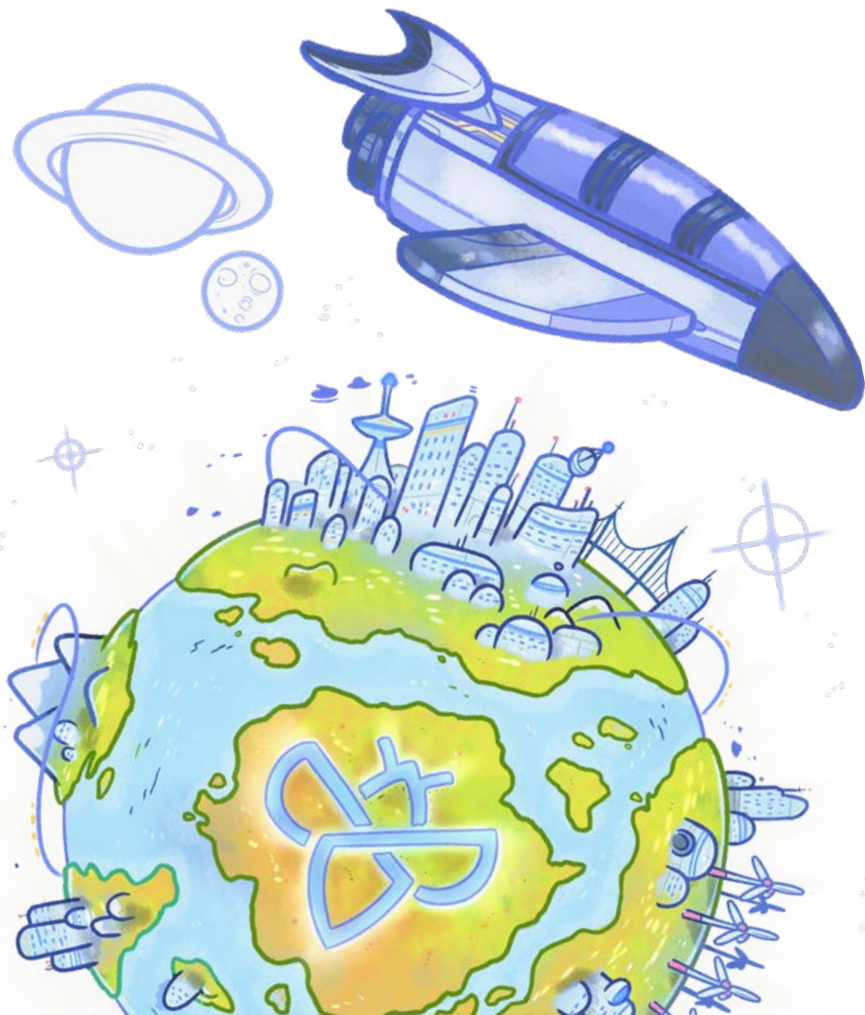
How Intigriti can help your business

Intigriti is the European leading platform for bug bounty and ethical hacking. The platform enables organizations to reduce the risk of a cyberattack by allowing Intigriti's network of security researchers to continuously test their digital assets for vulnerabilities.

Founded in 2016, Intigriti set out to conquer the limitations of traditional security testing. The interactive platform features real-time reports of current vulnerabilities, enabling organizations to obtain greater visibility over their attack surface and remediate issues faster.



Agile security testing powered by the crowd



What to expect as an Intigriti customer

01

Conquer the limitations of traditional security testing

Continuously test your digital assets for vulnerabilities by leveraging the expertise of Intigriti's 50,000 registered security researchers.

02

Industry-leading support

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

03

Reduced risk

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

04

Customized pricing

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



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

Fortnox



 Showpad

 **VISMA**

 randstad

Kahoot!


SHOP APOTHEKE
EUROPE



Survey methodology

Intigriti conducted the survey in March 2022 over a three-week period. Of the 1,759 survey respondents, we were able to identify **1,181 respondents who met our criteria.**

1 Had hunted for a bug bounty at least once in their life

2 Had participated in at least one of the following*

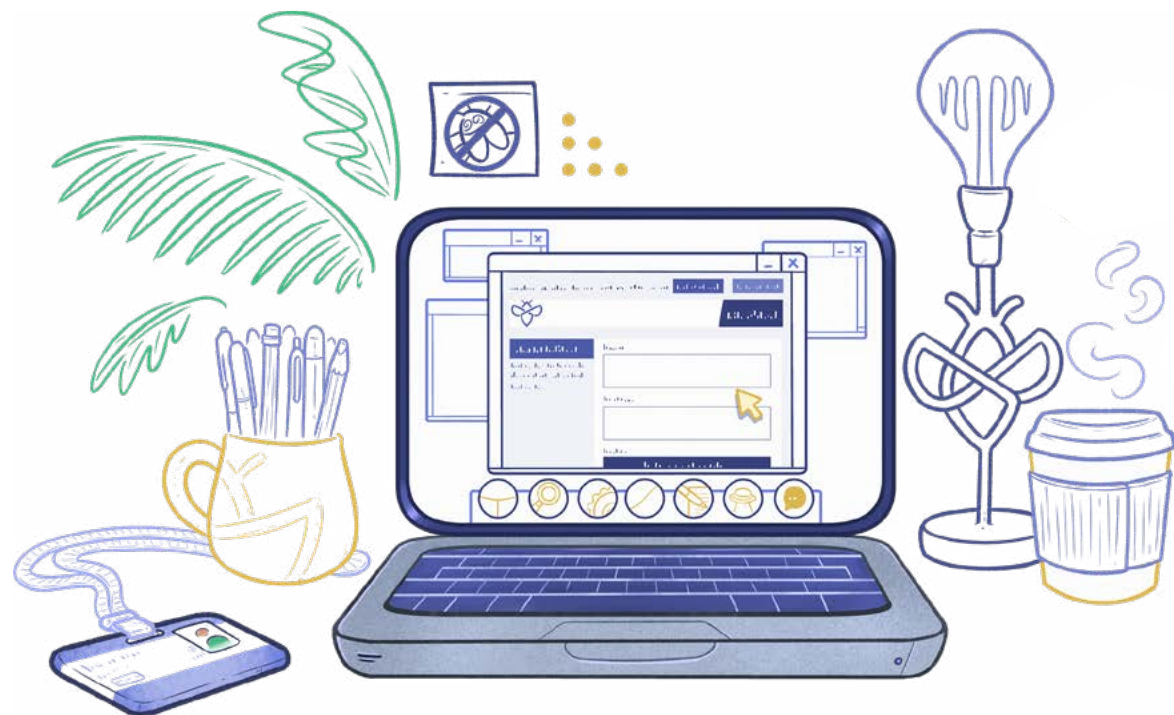
*A managed bug bounty program on a platform, an unmanaged bug bounty program on a platform, an external bug bounty program.

These criteria meant we could explore the true habits of ethical hackers who genuinely hunt for bounties. When exploring “penetration testing and bug bounty hunting through the eyes of pentesters”, **685 respondents met our criteria of having one of the following.**

1 Currently has the job title of “Penetration Tester”

2 Has previously held the job title of “Penetration Tester”

These criteria meant we could explore the opinions of ethical hackers who have hands-on penetration testing experience, as well as bug bounty hunting experience.



Contact us

Need some help getting started with ethical hackers? Our experts can help you maximize 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://www.intigriti.com)

HELLO@INTIGRITI.COM



Intigriti



hackwithintigriti



@intigriti



intigriti



intigriti