



# The Ethical Hacker Insights Report 2024

STRENGTH IN NUMBERS: UNLOCKING THE VALUE OF CROWDSOURCED SECURITY





# Table of contents

3	A note from Inti, Intigriti's Chief Hacker Officer	11	Researcher spotlight: @Itsirkov	21	Getting the financial incentive right and staying competitive
4	Methodology	12	A strong preference for bug bounty platforms	22	Determining your bounty budget
5	Return on Security Investment (ROSI)*	13	The power team behind Intigriti's platform: community enablement	23	Balancing speed and security: Personio's bug bounty program enables agile development
6	Glossary	15	A community that believes in being thorough	24	Key takeaways
7	Demographics: Uncovering the people behind the craft	16	Going beyond point-in-time testing	25	About Intigriti
8	Exploring the unique skillsets of this dynamic community	17	Hybrid pentesting	27	Contact us
9	What makes a bug bounty program attractive?	19	Retesting vulnerabilities		
10	From novice to expert: The educational power of bug bounty programs in cybersecurity	20	Financial gain continues to remain the primary motivator		



# A note from Inti, Intigriti's Chief Hacker Officer

## Crowdsourced security has officially earned its stripes in security testing.

This is evidenced by major brands such as Microsoft, Nestle, Coca-Cola, Monzo and Intel, all of which have adopted Intigriti's bug bounty platform in recent years. Their engagement underscores the solid reputation that this form of security testing has established over the last five years, definitively proving its value within the cybersecurity community.


A major force behind this trend is the challenge CISOs globally face to ensure continuous security coverage of assets, particularly during periods of rapid business growth or change. Further, in recent years cybersecurity teams have had to operate with **reduced budgets<sup>1</sup>**, fewer staff and limited resources according to Enterprise Strategy Group. They needed a solution that could extend their capabilities, and many adopted crowdsourced solutions found on platforms such as Intigriti.


Crowdsourced security testing means CISOs can leverage a global community of security researchers to continuously test for new and undiscovered vulnerabilities on one platform. This approach not only maximizes their Return on Investment (ROI) but also enhances their return on Security Investment (ROSI)\*, enabling them to invest less now to avoid higher costs in the future.


With this Ethical Hacker Insights report, you'll get access to a demographic breakdown of Intigriti's ethical hacking community. Plus, we'll offer practical strategies for cybersecurity leaders to do more with less.

**Knowledge is the best defense against malicious actors. Are you ready to outsmart them?**

### Keep reading to unlock:

 **How ethical hacking communities become an extension of your team:** Access to the most current and competent security specialists in the world.

 **Tactics to elevate your security testing strategies:** Transition away from traditional point-in-time testing and bring in greater incentivization.

 **Strategies to enhance the appeal of your program:** Drive engagement and get more results.



**Inti De Ceukelaire**  
CHIEF HACKER OFFICER

<sup>1</sup>[go.intigriti.com/reduced-budgets](https://go.intigriti.com/reduced-budgets)



# Methodology

**Intigriti collected the responses of 550+ security researchers over the course of April 2024.**

To qualify for the survey, respondents must have hunted for a bug bounty at least once in their life. We also analyzed more than 640 bug bounty tables across multiple industries to help organizations benchmark against their industry peers and make an informed decision about how to reward security researchers for reporting vulnerabilities.



**550+**

responses from security researchers were collected for this report



**640+**

bug bounty tables across multiple industries were analyzed by Intigriti

RESEARCHER

**youngvanda**





# Return on Security Investment (ROSI)\*

**“Return on Security Investment” (ROSI) is a strategic concept that quantifies the value derived from allocating resources to cybersecurity measures.**

It emphasizes that the budget spent on cybersecurity should not only be viewed as an investment but as a crucial prevention tactic against potentially costly and damaging cyberattacks.

➤ ROSI calculates the financial value that security measures contribute by reducing the risk and potential costs of security incidents. ROSI helps organizations determine the effectiveness of their security spending by comparing the cost of security implementations against the financial losses prevented. This calculation supports strategic decision-making by highlighting the economic benefits of investing in robust security systems.





# Glossary

**Bug bounty programs often come with a set of terminologies and jargon specific to the field of cybersecurity and ethical hacking. Here are some common terms used within this report:**



## Q Security researchers

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

## Q Bug bounty program

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

## Q Bounty

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

## Q Triage

Completed by a highly experienced team of security analysts, the triage process validates submissions based on defined criteria. The purpose is to filter out duplicate reports and 'out of scope' submissions, as well as reproduce the vulnerability, based on the information presented by the researcher. The vulnerability's severity rating is also suggested by triage during this stage.

## Q Crowdsourced security testing

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



# Demographics: Uncovering the people behind the craft

The majority of ethical hackers are in full (37%) or part-time (8%) employment. Yet, 12% are now hunting for bounties full-time, with 83% of this group spending time hacking daily.

**37%**

of Intigriti's community **are in full-time employment**

**12%**

are **full-time bug bounty hunters**

**68%**

have an **undergraduate or master's degree**

**19%**

have a Certified Ethical Hacker (**CEH**) **certificate**



We look at the researcher community as our partners, not as our adversaries. They have a very different way of looking at our attack surface compared to those who are internal and potentially building the product itself.

**Madeline Eckert**

**SENIOR PROGRAM MANAGER ON THE RESEARCHER INCENTIVES TEAM**



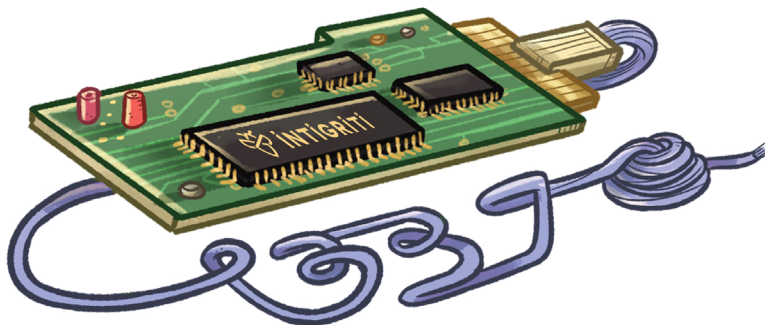


# Exploring the unique skillsets of this dynamic community

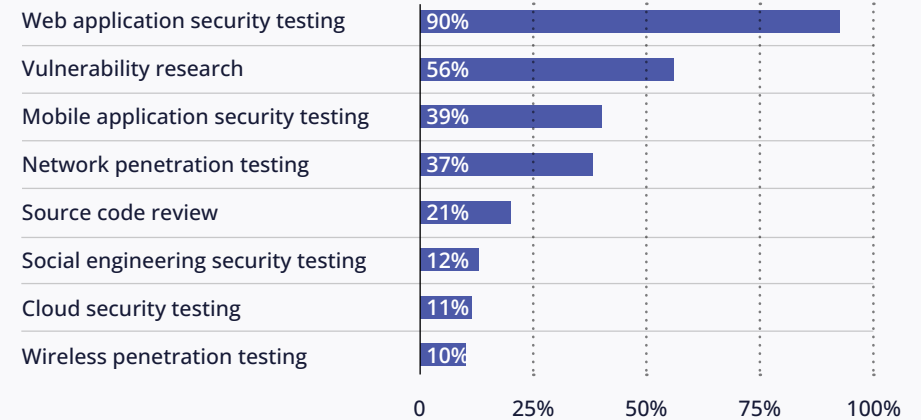
The strongest area of expertise from the community is web application security testing with 90% citing this as their strongest skillset—which perhaps makes it unsurprising that this is also the area which the community focuses most of their time on.

API (53%) and Linux (30%) testing are also leading areas of focus, suggesting a robust capability in identifying and addressing security gaps across different platforms.

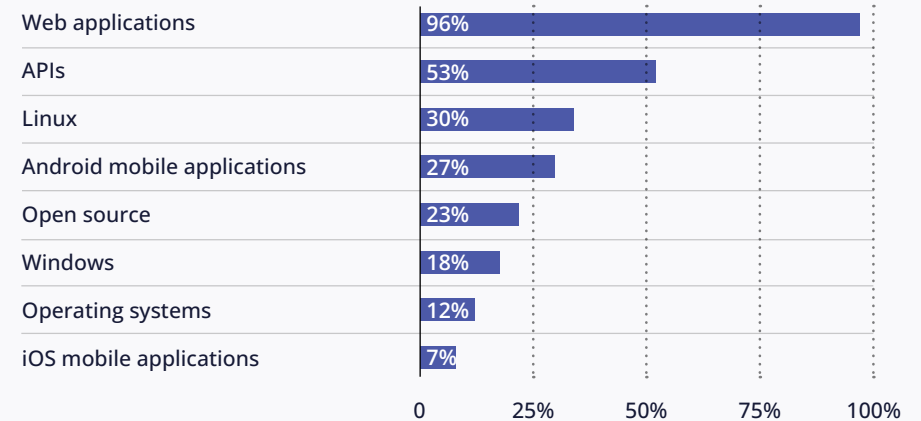
Lower engagement in areas like iOS mobile applications and wireless penetration testing reflects a more niche focus within the community.



## Top 8 skills from our community:



## Top 8 areas of focus from our community:







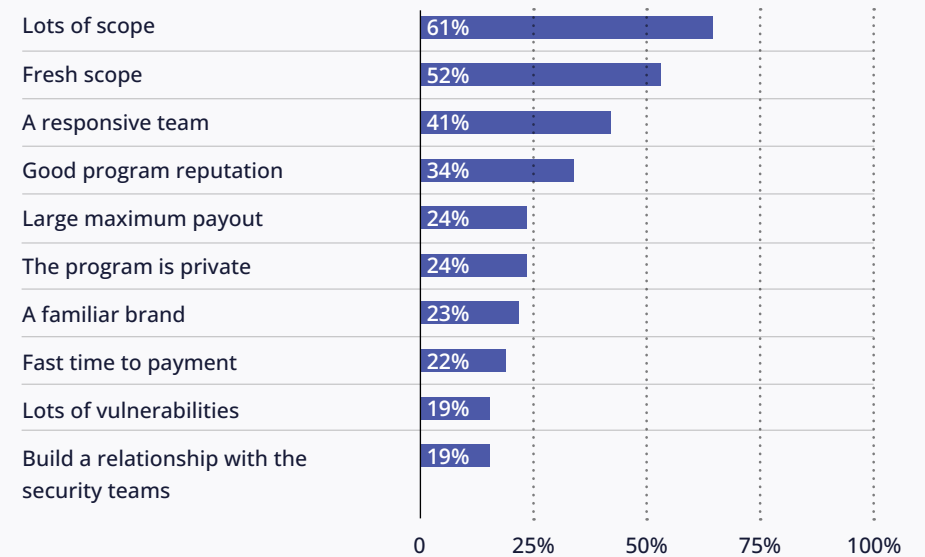
# What makes a bug bounty program attractive?

The scope of a bug bounty program is a significant factor for ethical hackers, with 61% citing lots of scope and 54% choosing fresh scope as motivation for engaging with a program. Additionally, 19% reported a variety of vulnerabilities were important. This indicates a preference for programs that offer a wide and evolving range of targets for testing.

Additionally, the interaction of security teams is highly valued, with 41% of respondents attracted to programs with a responsive team and 19% emphasizing the importance of relationship building. This underscores the importance of interaction and feedback in the bug bounty process.

The reputation of the program and the potential for high rewards also play crucial roles, with 34% of respondents attracted by a good reputation and almost a quarter (24%) by large maximum payouts.

What attracts you to a particular bug bounty program on Intigriti?





# From novice to expert: The educational power of bug bounty programs in cybersecurity

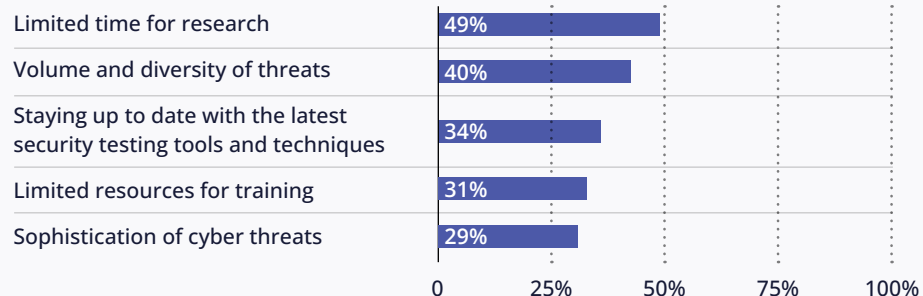
## Fast facts:

- 18% of respondents have secured a job opportunity with a company from participating in their bug bounty program.
- 74% of respondents participate in bug bounty programs to learn.
- 65% of respondents who have participated in a Vulnerability Disclosure Program (VDP) do so because they are an effective way to practice and learn.

More than two-thirds (68%) of Intigriti's community feel confident or very confident staying up to date with emerging security threats, despite 45% of respondents stating they receive no formal training from their employers.

When asked about the most effective way to learn about emerging threats, 46% of respondents identified bug bounty hunting as the top method. This was closely followed by personal research and training (44%). In contrast, only 6% considered on-the-job training as the best way to stay informed about new threats.

## The challenges they face with keeping up with threats:



RESEARCHER

**tamaytandiran**





## Researcher spotlight: @Itsirkov

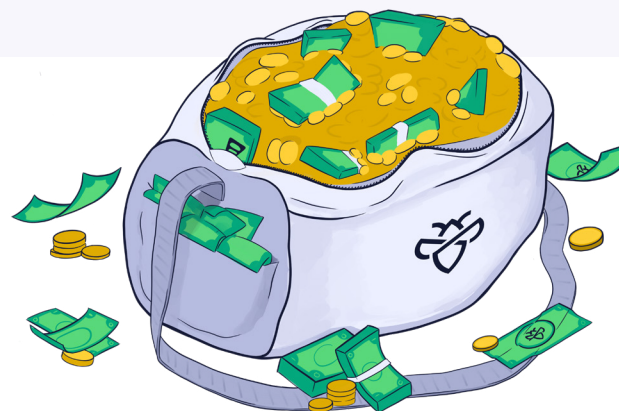
**My greatest achievement in ethical hacking was when I was invited to a private bug bounty program, and during my participation, I discovered 18 critical vulnerabilities within 30 days of hacking.**

Demonstrated impact included exploiting vulnerabilities of different categories, such as broken access control issues, server-side injections and common misconfigurations.

As a result of my findings, I was awarded €57,250 and was ranked #1 on the private program and monthly leaderboard. Here, I'd like to highlight that I had the opportunity to collaborate with an amazing security team on this program that took security of the organization very seriously and fully engaged with my reports.

Collaboration between ethical hackers and internal security teams can be incredibly impactful.

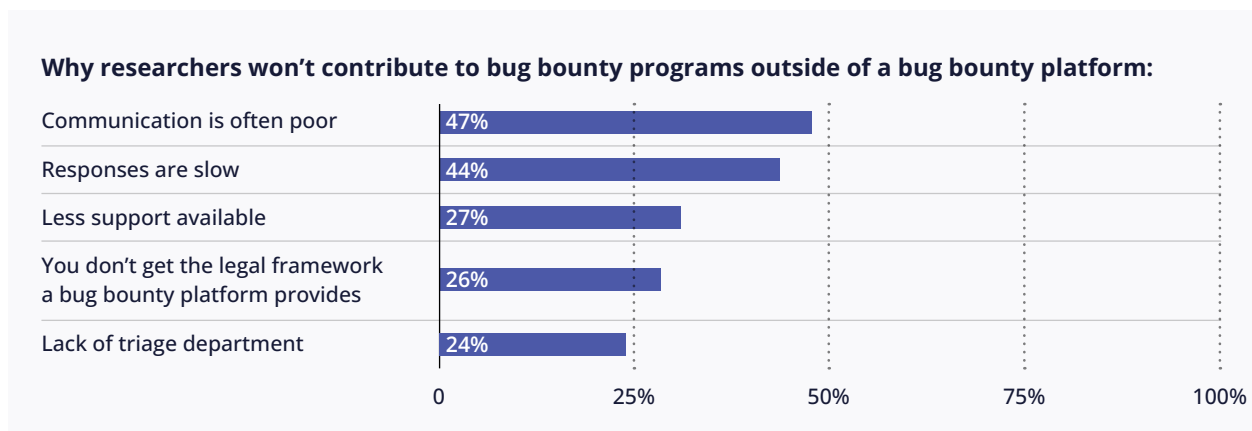
I personally believe that we will see more bug bounty programs launch in the coming years due to the effectiveness of the model and access to talented ethical hackers on platforms, like Intigriti. The community has already grown a lot in recent years.





# A strong preference for bug bounty platforms

The survey highlighted that 40% of respondents won't contribute to bug bounty programs outside of a bug bounty platform:



## Communication is key

These responses highlight the importance of communication in bug bounty programs. Nearly half (47%) of respondents reported poor communication as the top reason for not working with programs outside established platforms.

Additionally, 44% of respondents cite slow responses as a major deterrent, indicating the need for timely feedback and acknowledgment.

A lack of such leads to frustration and demotivation, reducing continued engagement. Yet, on the contrary, effective communication clarifies doubts, provides updates, and ensures participants feel valued.



## Streamlined processes and triage provide efficiency

A sizable portion of respondents (36%) are put off by the lack of streamlined procedures in independent programs. Without well-defined workflows, contributors find it difficult to navigate the reporting and validation processes.

Moreover, 24% note the absence of a dedicated triage team as a barrier, which can lead to chaotic and inefficient handling of reports.

## Legal frameworks support collaboration

A lack of legal protections and frameworks, noted by 26% of respondents, falls short of providing a safe and compliant environment for security researchers and organizations to collaborate.

## Researcher support enables contribution

Furthermore, 27% feel there is insufficient support outside of formal bug bounty platforms, hindering effective contribution and issue resolution.

**i** Fostering transparent communication, providing clear guidelines, and ensuring responsive support are crucial for the success of bug bounty programs.



# The power team behind Intigriti's platform: community enablement

## Intigriti's community enablement team bridges the gap between our researchers and our customers.

The aim is to empower our researchers so that they feel motivated and excited to hunt on our customers' programs. The team achieves three main goals:

- 🕒 Expand our community through multi-faceted marketing activities and provide the resources and support to help researchers grow.
- 🕒 Drive engagement on Intigriti's platform through a combination of enticing bug bounty programs, live hacking events, and competitions.
- 🕒 Elevate and amplify the profiles of high-performing researchers, particularly those pioneering ground-breaking vulnerability research.

### Community development

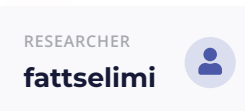
At Intigriti, we prioritize the development of our community because we know that this leads to more engaged researchers and better results for our customers. We regularly deliver free training materials, monthly challenges, conferences, and live hacking events.

### Community support

With an average response time of one hour, our support reps are ready to assist researchers all through the week. They ensure uninterrupted workflow, enabling researchers to swiftly submit vulnerability reports to programs. This unmatched responsiveness increases our reputation, brings more hackers to our platform, and drives results for our customers.

### Unrivalled triage

Intigriti's triage team is the glue between our researchers and our customers. As security analysts themselves, they are perfectly suited to facilitate communication and provide support to both parties, ensuring seamless collaboration and enablement in both directions.





“ The incredible triage team at Intigriti may not be listed as a feature, but they are certainly our favorite aspect. Numerous times, after assessing a researcher’s submission, I’ve turned to the internal chat with a question, only to discover that the team had already proactively addressed my concerns without me even asking.

**Arnau Estebanell Castellví**  
LEAD SECURITY ENGINEER

*Personio*



“ After two and a half years of #bugbounty, I can say that Intigriti is the best platform. It’s where I feel at home, and it has literally changed my life.

**Leorac**  
INTIGRITI SECURITY RESEARCHER



“ I really enjoy the personal touch Intigriti’s researcher support has. I feel seen and cared for as a hacker.

**Renniepak**  
INTIGRITI SECURITY RESEARCHER



## A community that believes in being thorough

**Intigriti's researcher community is extremely diligent, as indicated through the survey results. An impressive 88% of researchers retest vulnerabilities after they have been resolved, demonstrating a robust verification process. This practice ensures that fixes are effective and sustainable.**

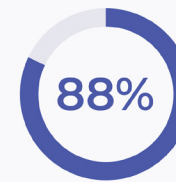
The outcomes of these retests are mostly positive, with 65% of researchers finding that the vulnerabilities are generally fixed. However, 14% noted that the vulnerabilities required further remediation steps, and 21% discovered new issues during retesting. This encapsulates the dynamic nature of cybersecurity, where fixing one issue can sometimes reveal others.

The efficiency of the retesting process is notable, with 38% of researchers completing their retests in less than an hour and 30% taking less than two hours. This quick turnaround highlights the agility and value that bug bounty programs bring to organizational security, ensuring rapid verification of fixes and continuous improvement of security measures.



LESS THAN  
**2 hours**

The majority of researchers take less than 2 hours to complete a retest



of researchers retest vulnerabilities after they have been resolved



always retest



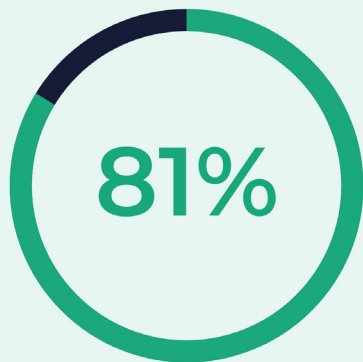
retest when they can



## Going beyond point-in-time testing

The survey responses indicate that security researchers see real limitations of traditional point-in-time penetration testing in providing continuous security assurance. A significant 81% of researchers believe that such testing fails to ensure year-round protection.

Furthermore, only 32% of these researchers think that traditional pentesting would identify many of the same vulnerabilities uncovered during bug bounty hunting, suggesting that bug bounty programs are more effective in finding diverse and unexpected issues in a more creative way. This highlights the necessity for more dynamic and ongoing security measures.



of researchers say that point-in-time testing cannot provide continuous assurance that an organization is secure year-round.



RESEARCHER  
**deleite** 





# Hybrid pentesting addresses these gaps

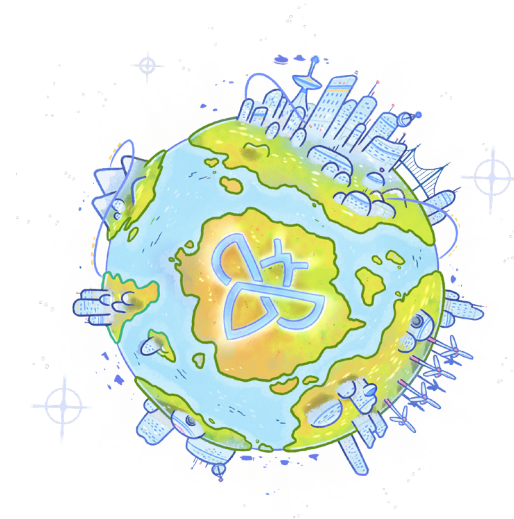
**Intigriti's hybrid pentesting effectively merges the incentivization elements of bug bounty programs with the structured, time-boxed methodology of traditional penetration testing. This model not only ensures a consistent income for researchers but also promotes exhaustive testing.**

Under this approach, researchers receive a fixed base bounty for each day of testing, complemented by the chance to earn extra rewards from a bounty pool for identifying vulnerabilities. This structure further incentivizes researchers to conduct thorough and diligent testing.

Notably, 81% of survey respondents indicated they would be more motivated to find vulnerabilities in a hybrid pentest scenario compared to traditional pentesting.

The hybrid model not only boosts ROI by introducing competitive and incentivized efforts but also significantly improves the Return on Prevention (ROP).

By integrating continuous and proactive security measures, organizations can better prevent costly and damaging cyberattacks, thereby reducing potential financial losses and enhancing overall security posture.



“ Intigriti's annual hybrid pentest solution gives us a cost-efficient solution with a higher quality specifically aimed at our custom software. The innovative approach also fits in well with our ISO27001 policy and we are convinced that it mitigates more risks than a traditional pentest.

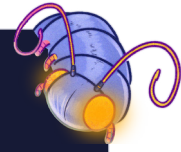
**Robert Van Bloem**

**DEVELOPMENT MANAGER**





	<b>Traditional pentesting</b>	 <b>Bug bounty programs</b>	 <b>Hybrid pentesting</b>
<b>Objective</b>	Focused testing for regulatory compliance and proactive security measures	Thorough and continuous testing to maintain proactive security	Focused testing for regulatory compliance and proactive security measures
<b>Approach</b>	Methodology-driven, time-bound	Creative testing, ongoing	Methodology-driven and creative testing, time-bound
<b>Results</b>	Predictable and almost immediate, can range from low to exceptional severity	Continuous pulse of immediate reports, can range from low to exceptional severity	Predictable and immediate, can range from low to exceptional severity
<b>Incentives</b>	Paid for time, no competition amongst testers	Paid for results, high competition among testers	Competition among testers, paid for time and paid for results
<b>Duration</b>	Point-in-time, repeated at regular intervals	Continuous	Flexible, on-demand and scalable





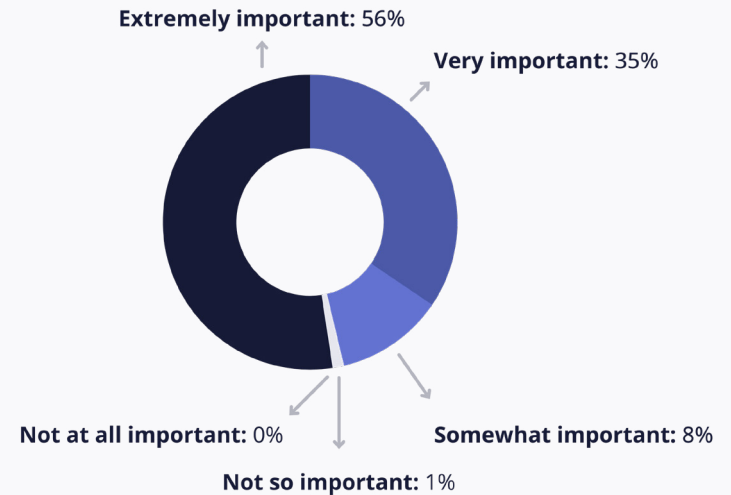
# Retesting vulnerabilities

## Proactively inviting researchers to retest a vulnerability they submitted provides another layer of assurance

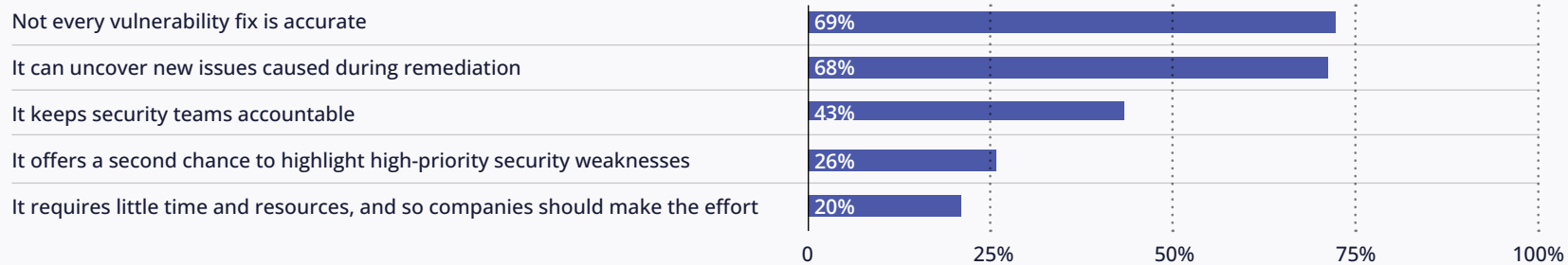
A significant 95% of the community are likely or very likely to retest a vulnerability they submitted if requested, indicating a high level of engagement and willingness to contribute to continuous security improvement.

The survey results also highlight the critical role of retesting in vulnerability management in the eyes of our community, with 99% of respondents affirming its importance to a varying degree. This consensus reinforces that retesting provides a crucial layer of assurance in maintaining robust security practices.

The importance of businesses asking hackers to retest vulnerabilities after they've been fixed according to hackers:



The value in retesting vulnerabilities according to researchers:



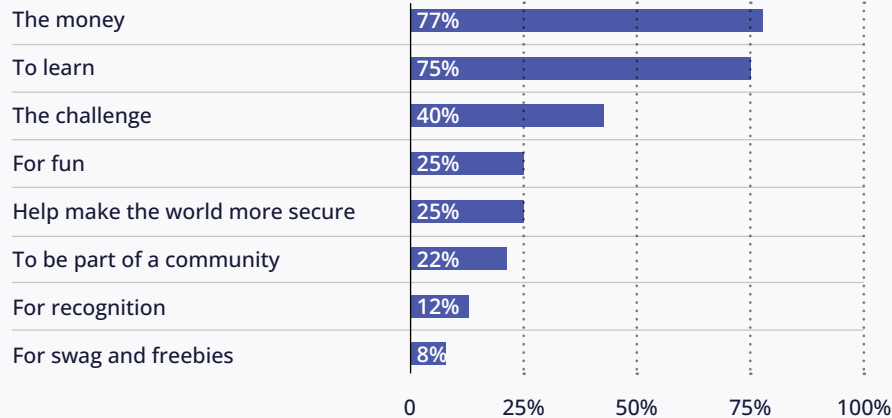


# Financial gain continues to remain the primary motivator

Three-quarters (75%) of the community participate in bug bounty programs because they value the learning opportunities, 40% enjoy the challenge, and 25% wish to contribute to global security.

However, the driving force behind the participation of 77% of researchers in bug bounty programs is financial rewards.

## Why do you participate in bug bounty programs



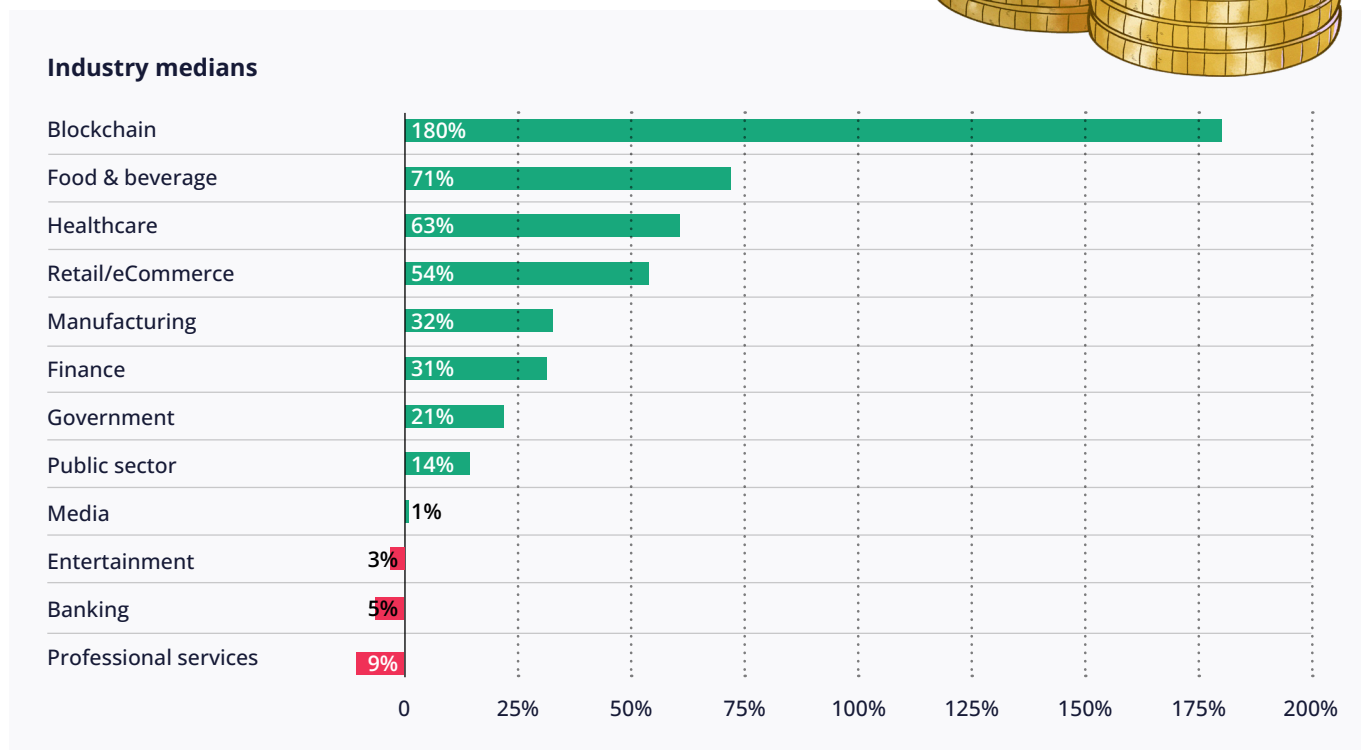


# Getting the financial incentive right and staying competitive

As part of this report, Intigriti analyzed the data of 640 bug bounty tables. Compared to March 2023, the average bounty reward has doubled. Looking at the median bounty amount, it increased by 13%.

The increases in bounty rewards across various industries reflect evolving cybersecurity priorities. In blockchain, established players are doubling down on their programs, resulting in a 180% increase in rewards. Many food and beverage companies are also increasing the median bounty pay-out after cleaning up the low hanging fruit of lower severity vulnerabilities. Healthcare has seen significant buy-in from larger players, boosting budgets and resulting in a 63% increase. Government programs are expanding as digitalization increases the industry's scope, contributing to a 21% growth.

Conversely, sectors like banking, entertainment, and professional services show small decreases, reflecting minute shifts in cybersecurity investment dynamics.





# Determining your bounty budget

A question we're often asked is what **budget organizations should allocate for a bounty reward. To make this math a little easier, Intigriti has created a tool called the Bug Bounty Calculator to estimate a recommended table for you.**

## Bug bounty table explained

A bug bounty table is a tool used in bug bounty programs to outline the rewards offered for finding and reporting vulnerabilities. It sets clear expectations for hackers and ensures consistency in reward amounts.

## Bounty tiers explained

Bounty tiers allow for different reward structures based on scope. For instance, critical sections of your website, like payment modules, might offer higher rewards to incentivize researchers to focus on them. Additionally, tiers can reflect the level of effort required or the maturity of certain scopes. As scopes mature, they may progress to higher tiers.

## Determining your bug bounty table

Several factors need to be considered to answer this question, including:

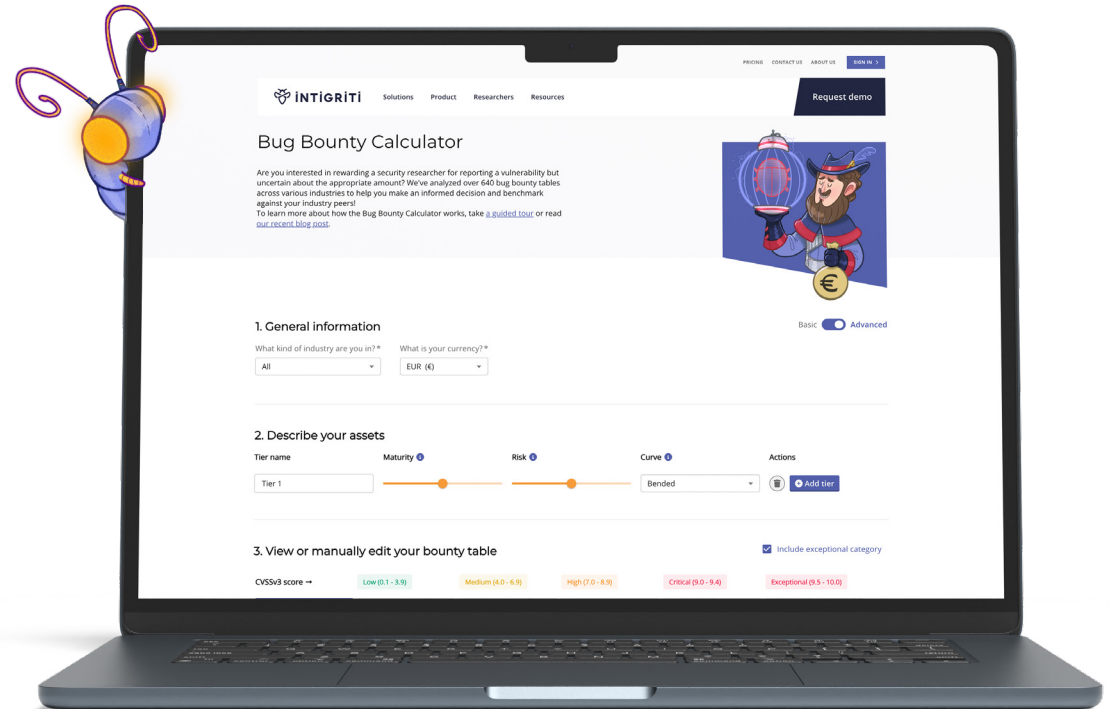
- The industry of the business the program belongs to
- Size and scope of the program
- The average cost of a vulnerability.

## Intigriti's Bug Bounty Calculator

The Bug Bounty Calculator uses the pre-mentioned factors to estimate the cost of a bug bounty reward. The severity of a vulnerability is calculated using the CVSS v3 calculator.



**Estimate your bug bounty table**  
Scan the QR code or go to  
[go.intigriti.com/EHR24-bug-bounty-calculator](https://go.intigriti.com/EHR24-bug-bounty-calculator)





# Balancing speed and security: Personio's bug bounty program enables agile development

## The challenge

As a rapidly evolving tech firm, Personio is constantly enhancing their existing security posture. The continuous deployment of new features meant a more dynamic and responsive method to maintain security integrity was needed.

## The solution

Personio implemented Intigriti's bug bounty program early in their application security program development. This decision allowed Personio to leverage crowdsourced security efforts, ensuring continuous and comprehensive testing of their platform. Intigriti's managed triage team provided invaluable support, handling the constant flow of bug bounty activities and integrating seamlessly with Personio's existing tools like Jira.

## The result

The collaboration with Intigriti led to significant improvements in Personio's security posture. Specific achievements included:

- > **Discovery of critical vulnerabilities:** Identifying and mitigating risks such as input sanitization issues that could lead to XSS and other vulnerabilities or misconfigured domains that could lead to subdomain takeover.
- > **Proactive security measures:** The insights from the bug bounty program initiated internal projects that not only addressed identified vulnerabilities quicker, but also improved overall security methodologies and tooling.
- > **Continuous testing assurance:** Intigriti's managed triage team ensured that Personio's platform was continuously tested by top security researchers, providing confidence in the platform's security.

## About Personio



Industry  
**Technology**



Employees  
**2,000+**



Customers  
**10,000+**



- “ The bug bounty program starts providing value from day one and can influence internal decisions in the application security program.

**Carles Llobet Pons**  
SENIOR SECURITY ENGINEER





# Key takeaways

## 1. Bug bounty programs provide a platform for relevant and timely security knowledge.

They offer practical, hands-on experience for security researchers and internal teams that traditional education and training routes cannot match. Participants value these programs for their learning opportunities, with many considering them the most effective way to stay updated on emerging threats.

## 2. The incentivization format of point-in-time security testing is shifting.

Traditional penetration testing often fails to provide continuous assurance. Hybrid pentesting, which combines traditional methods with bug bounty programs, addresses this gap by offering a base bounty and additional rewards for discovered vulnerabilities, enhancing ROI and ROP through continuous engagement.

## 3. Retesting: Very little effort required but leads to significant assurance.

Retesting vulnerabilities is a critical component of effective vulnerability management. With 95% of researchers willing to retest upon request, this process ensures that fixes are effective and helps uncover new issues, significantly bolstering security posture.

## 4. Staying competitive is vital in an already competitive world.

Using tools like Intigriti's bug bounty calculator can help organizations assess and improve their bug bounty programs, ensuring they remain attractive to top security talent and proactive against evolving cybersecurity threats.







# About Intigriti

Malicious hackers do not follow a predefined security methodology like penetration testers, and automated tools only scratch the surface. Intigriti connects the brightest cybersecurity researchers from across the globe with organizations to outmaneuver cybercriminals by staying on top of the evolving threat landscape.

## Ready to outmaneuver cybercriminals with global crowdsourced security?

[Book a meeting today](#)

Or go to [go.intigriti.com/EHR24-contact](https://go.intigriti.com/EHR24-contact)

### Trusted by the world's largest organizations



## What to expect

### Leave the hassle of triaging behind

Our expert 24/7 triage team verifies all reports, saving your team time and ensuring only valid submissions reach you.

### Security assurance

We support your compliance requirements with ISO 27001 and SOC 2 certifications. Our Trust Center provides a live dashboard where you can gain insights into our security and compliance posture in real-time.

### Easy communication

Seamlessly interact with security researchers on the Intigriti platform for updates, questions, and scoping new domains.

### Streamlined processes

Our legal framework ensures swift payment processing in days, outpacing the industry standard by weeks.

### Program oversight

Our dedicated technical customer success team is committed to attracting top-tier security researchers to your program, while conducting regular reviews to ensure sustained momentum post program launch.



# 100K+

Researchers active on the Intigriti platform



# 100K+

Total vulnerability reports have been filed

# 9.2

Net Promotor score



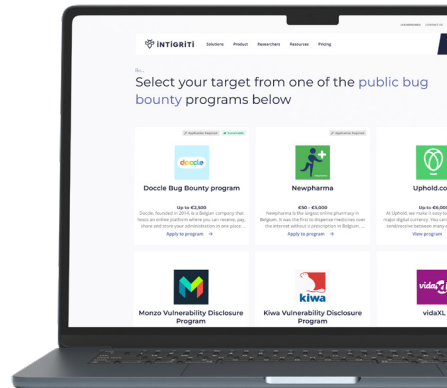
# 1.5 day

Average triaging\*



# 400+

Active programs



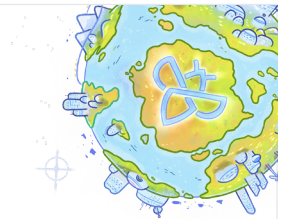
# €26M+

Rewards paid to the community



# 32

Countries serviced with our solutions



\*12 business hours is the time it takes on average for Intigriti to review and validate a vulnerability report

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



# 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](http://www.intigriti.com)

[hello@intigriti.com](mailto:hello@intigriti.com)

[in](#) Intigriti [📷](#) hackwithintigriti [✂](#) @intigriti [📺](#) Intigriti [🗨](#) Intigriti

