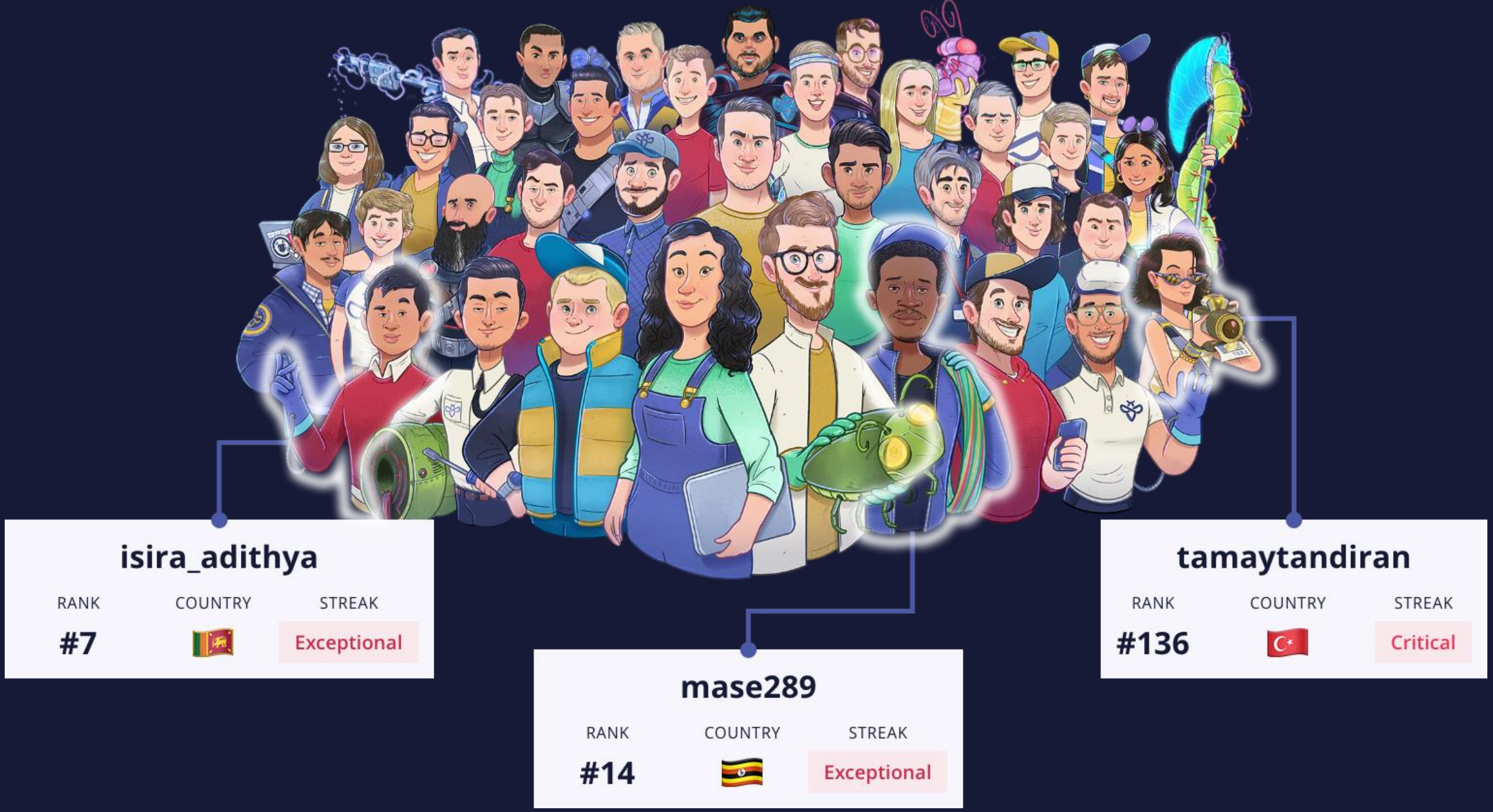
INTIGRITI



isira_adithya

RANK	COUNTRY	STREAK
#7	🇱🇰	Exceptional

mase289

RANK	COUNTRY	STREAK
#14	🇺🇬	Exceptional

tamaytandiran

RANK	COUNTRY	STREAK
#136	🇹🇷	Critical

Crowd Security is the **best kept secret**!

what is your **biggest challenge** in pentesting?

”I **need** to be secure”

vs

”I **want** to be secure”

pentests are defined by **budget** and **time** pentests are a **snapshot** of a **dynamic** environment pentests are **not** the result of **creativity** and **impact**

you can’t force
a hacker to **be creative**

do your magic!

do your magic!

now, please!

do your magic!

now, please!

c’mon, start hacking!

it doesn’t work like that

hackers like to **recon**

hackers like to **research**

hackers like to **break stuff**

hackers like to **think**

outside the box

hackers like to **hack**

not to write dull reports

What with those reports?

It is only shared with one person.

What happens when someone leaves the company?

How do you ensure that the recipient understands?

What about interaction with the people that fix it.

pentesting is **dead**!

we now have

crowd security

yes, **but**

crowd security can be **opportunistic**

Pentesting

- Control over timeframe
- Guarantee that someone spent time
- Certainty of a methodology
- Pay for time
- Specific reporting format (PCI DSS)
- Isolated environments / ICS

Crowd Security

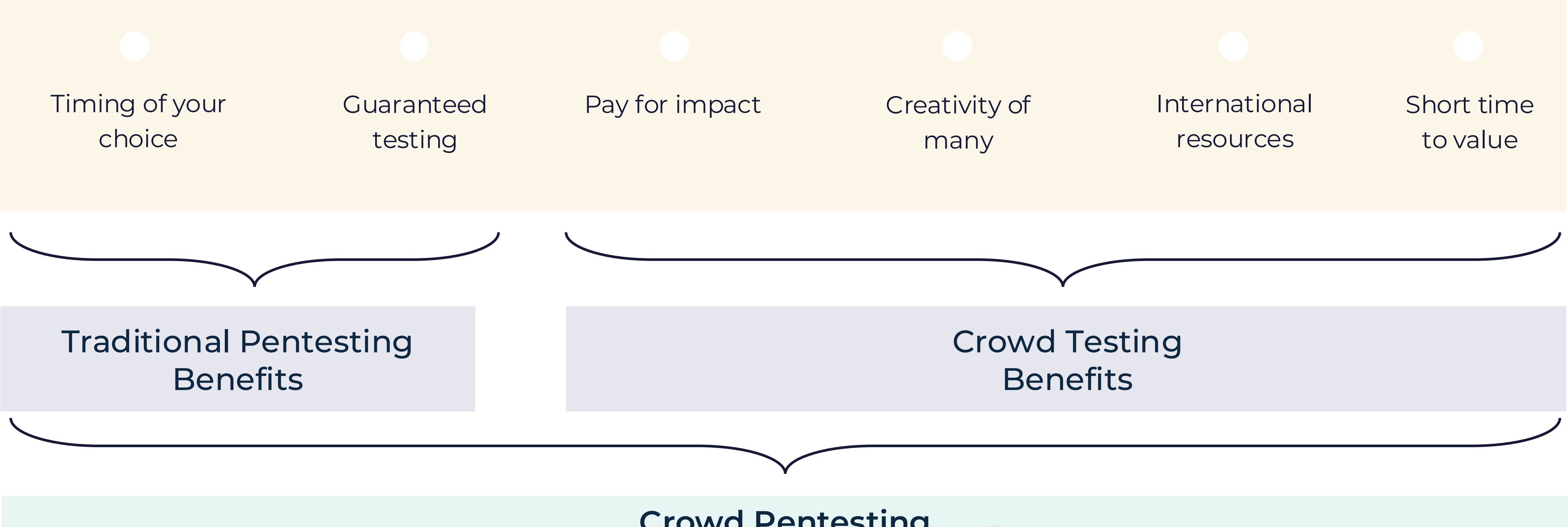
- Continuous testing
- No negative results
- Creativity
- Pay for impact
- Interactive reporting
- Public facing environments

Crowd Pentesting

Combining the pay for impact approach of bug bounty programs with the dedicated resourcing approach from classic penetration testing.

Farahhawa

Combining best of both worlds



Timing of your choice

Guaranteed testing

Pay for impact

Creativity of many

International resources

Short time to value

Traditional Pentesting Benefits

Crowd Testing Benefits

Crowd Pentesting

Formerly founder of tSF
Security consultancy and pentesting

CEO.Founder of Intigriti
Crowd Security

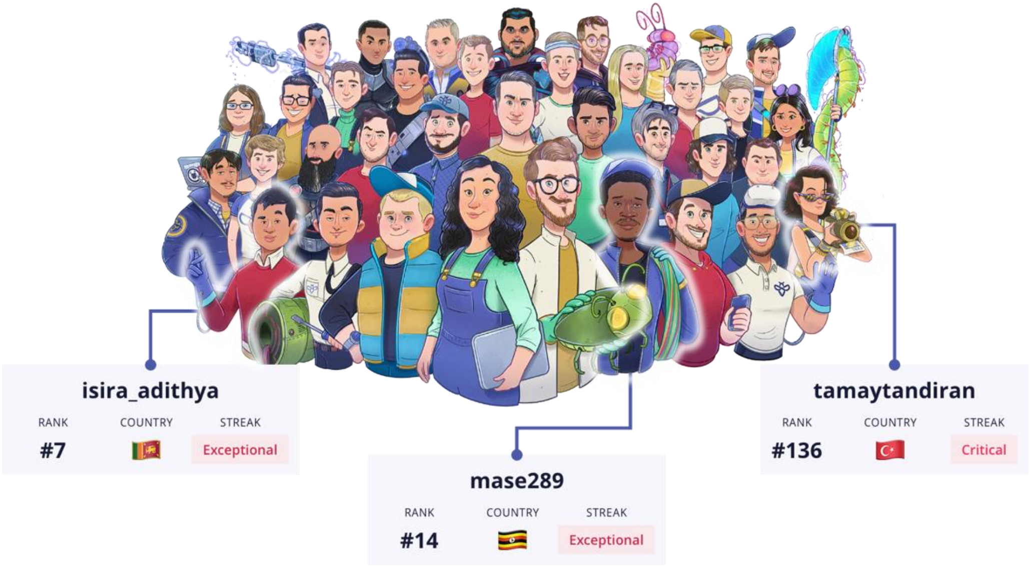
Stijn Jans

INTIGRITI

About Intigriti

- Connecting **125,000+ ethical hackers** with companies
- Crowd security testing, **pay for results**
- Founded in 2016 with offices in **Antwerp and London**
- **12 skillsets** including web, mobile, open source, IoT, network, hardware ...
- **500+ bug bounty programs**

About Intigriti



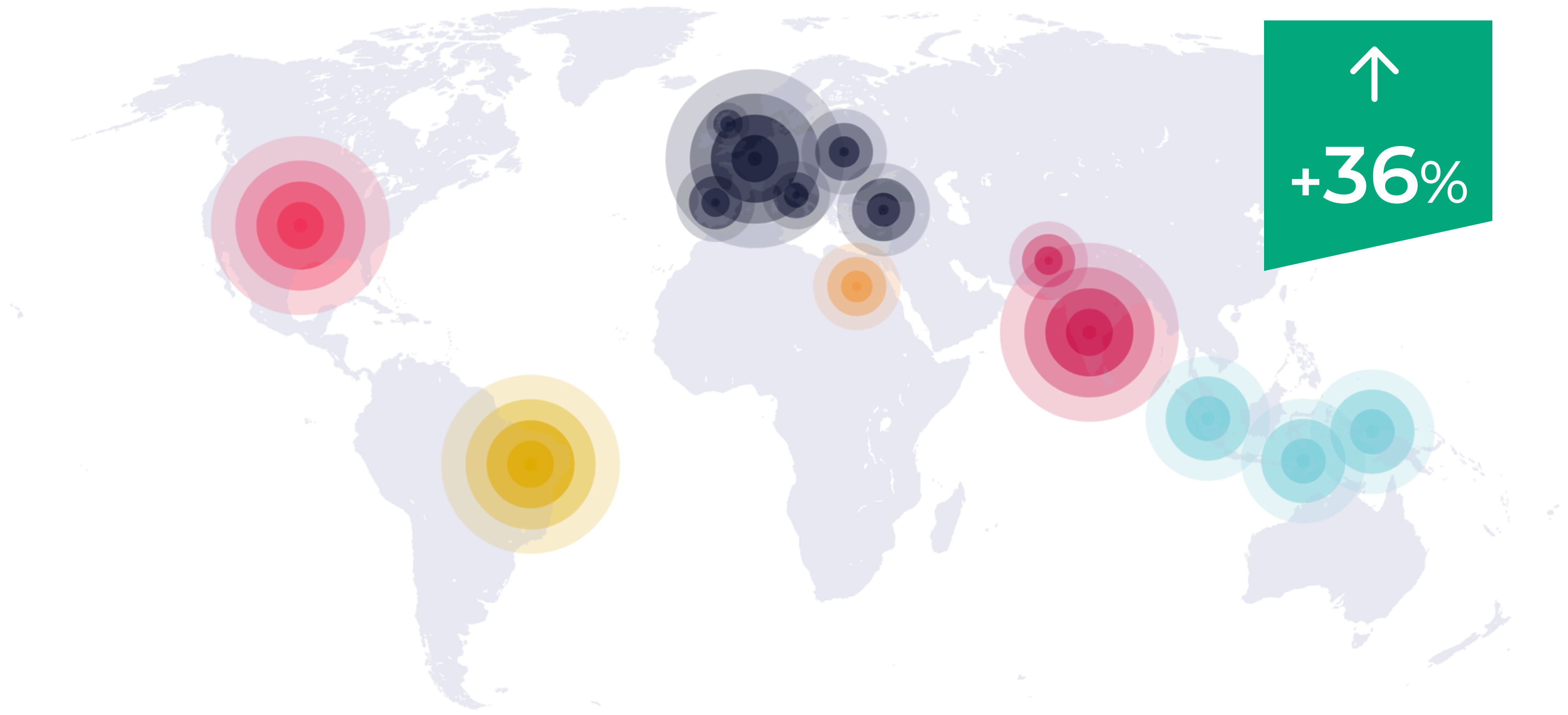
We are trusted by a worldwide crowd and the world’s largest organizations

Microsoft intel. UBISOFT Coca-Cola Red Bull Nestlé VISMA

The “ethical” hacker

- Independent security researchers
- Get paid for impact, not for time
- Ad-hoc or Full time
- Mainstream for a decade, growing popularity

Hacker origins



↑ +36%

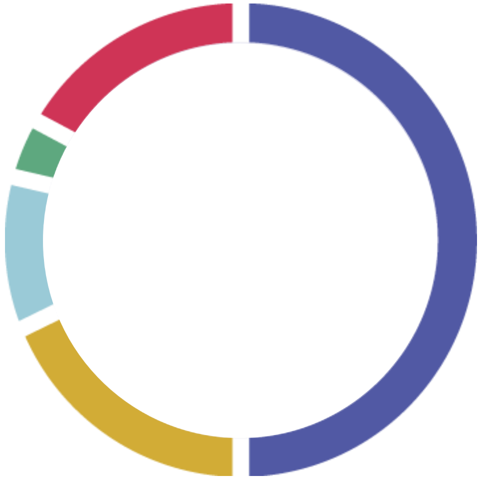
Researcher residency location

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

Best performing researchers

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

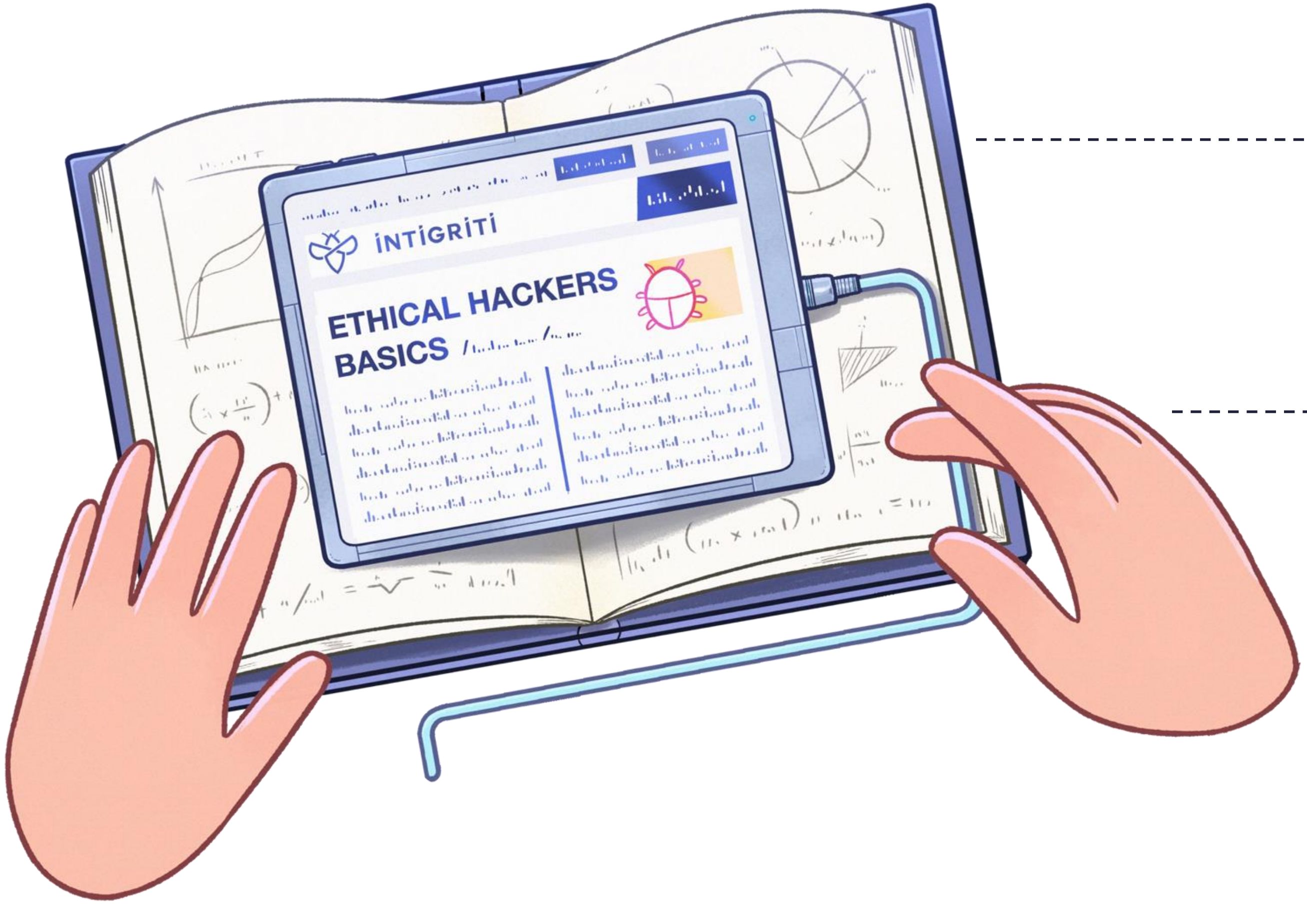
73% of hackers fall under the age of 30



Community breakdown by age

4%	19%	50%	20%	7%
18- years old	18 – 20 years old	21 – 29 years old	30 – 39 years old	40+ years old

Crowd Security as a career choice



96%

of the community would like to dedicate more time to crowd security testing in the future

66%

would consider crowd security testing as a full-time career.

95%

of hackers would (or have already) convinced a friend to take up hacking.

The pandemic drove more infosec talent towards crowd security platforms

74%	35%	23%	53%	32%
Grow their hacking skills	Got better at hacking	Say the crowd security programs have gotten more interesting	Earn more through crowd security	More time to dedicate to hacking

Let me tell you a story about a trip to Lisbon

53

Average number of **vulnerabilities** submitted in the first week

24h

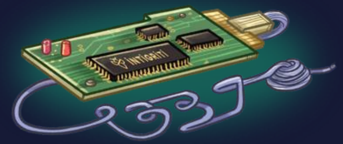
Average time Triage takes to **review, and accept or reject a report**

23%

of our registered hackers submit **at least one report every month**.

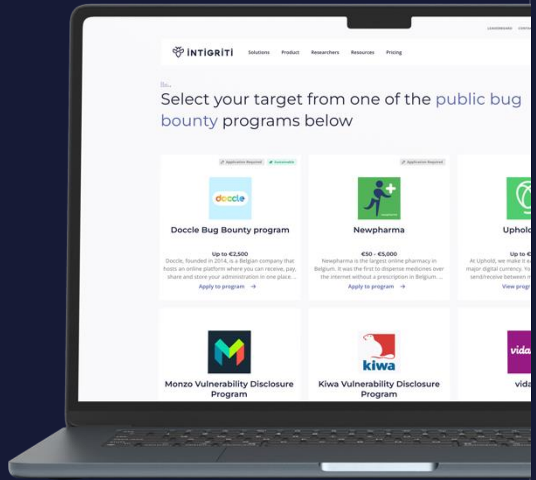
37

Average number of submissions that are accepted within the first week



2 days

Average time for customers to accept or reject a report (if escalated)



INTIGRITI Solutions Product Researchers Resources Pricing

Select your target from one of the public bug bounty programs below

Application Required Sustainable

Doccle Bug Bounty program

Up to €2,500

Doccle, founded in 2014, is a Belgian company that hosts an online platform where you can receive, pay, share and store your administration in one place. ...

Apply to program →

Application Required

Newpharma

€50 - €5,000

Newpharma is the largest online pharmacy in Belgium. It was the first to dispense medicines over the internet without a prescription in Belgium. ...

Apply to program →

Uphol

Up to €

At Uphold, we make it ea major digital currency. Yo send/receive between m

View progr

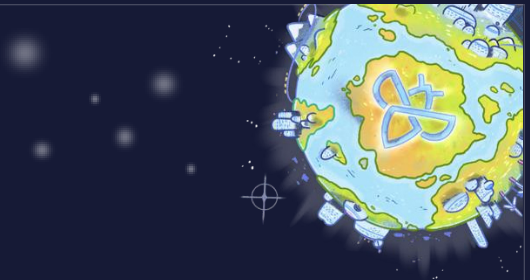
Monzo Vulnerability Disclosure Program

Kiwa Vulnerability Disclosure Program

vida

71%

of companies get a high to critical submission **within the first 48h**



32

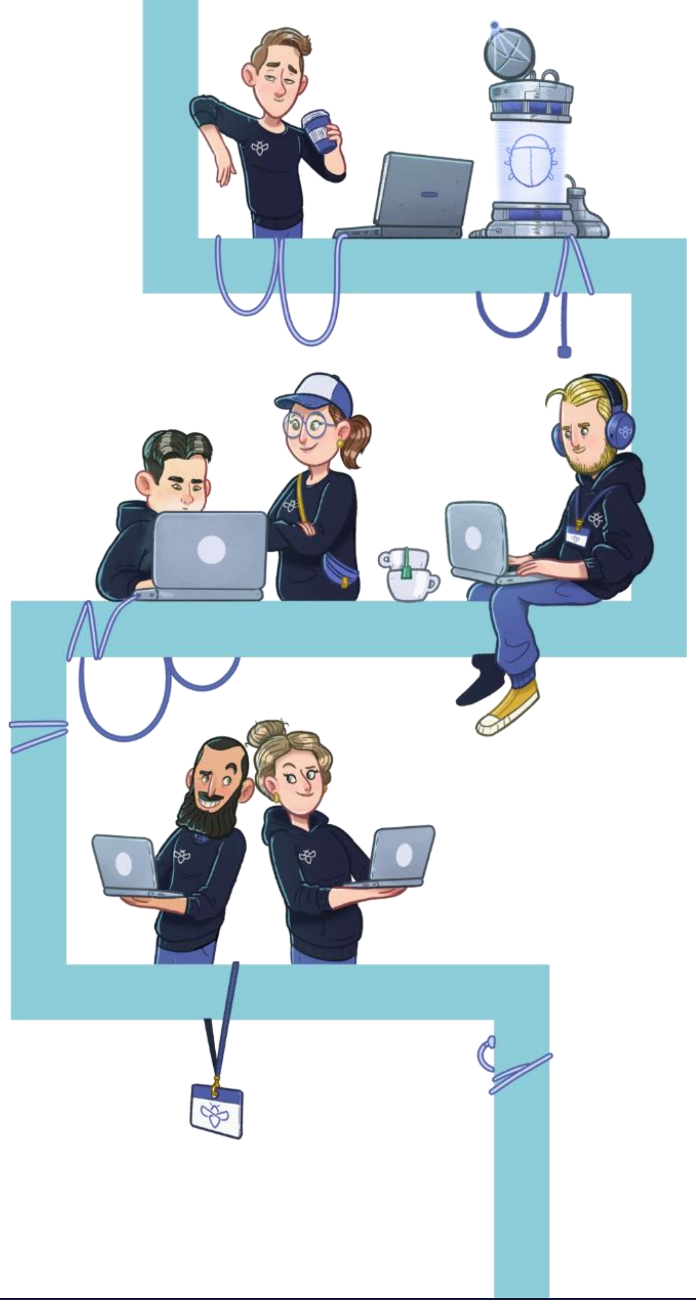
Countries serviced with our solutions

INTIGRITI

take-aways on crowd security

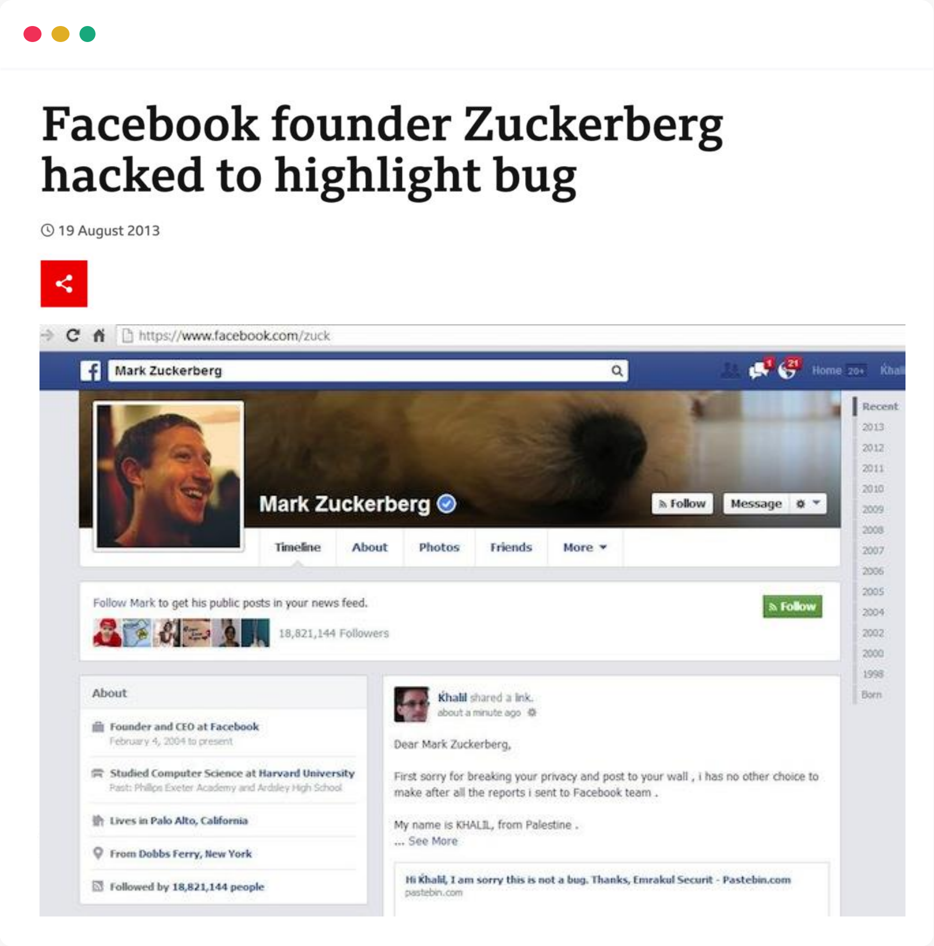
Treat hackers like partners, not scanners

- Hackers are people, not just security tools.
- A good relationship improves the quality of reports
- Show your gratitude, even when the issue is known



Communicate clearly and often

- Acknowledge reports within 48 hours and share regular updates.
- Be transparent if things take longer, they will understand
- When rejecting a report, explain why rather than sending a vague template.
- Language can be a barrier!



Facebook founder Zuckerberg hacked to highlight bug

19 August 2013

https://www.facebook.com/zuck

Mark Zuckerberg

Follow Mark to get his public posts in your news feed.

18,821,144 Followers

About

Founder and CEO at Facebook
February 4, 2004 to present

Studied Computer Science at Harvard University
Past: Phillips Exeter Academy and Ardsley High School

Lives in Palo Alto, California

From Dobbs Ferry, New York

Followed by 18,821,144 people

Khalil shared a link.
about a minute ago

Dear Mark Zuckerberg,

First sorry for breaking your privacy and post to your wall , i has no other choice to make after all the reports i sent to Facebook team .

My name is KHALIL, from Palestine .
... See More

Hi Khalil, I am sorry this is not a bug. Thanks, Emrakul Securit - Pastebin.com
pastebin.com

Define a clear scope and rules

- Create a good program design. Make clear what is exactly in and out of scope.
- Give them insights to your environment. They don’ t know it!
- Let them focus on business logic flaws and complex exploits.
- Give them a challenge!
- Include how to report, payout expectations, and legal safe harbour.

Offer fair and transparent bounties

- High-severity bugs deserve high payouts.
- Don’t downplay bugs. Don’t.
- Don’t steal their IP. Never.
- Consistency matters. Ensure to treat everybody equally.

Motivate and recognize Hackers

- Public leaderboards, “Hall of Fame,” and personalized thank-you messages go a long way.
- Give them a quote they can reuse on their LinkedIn / X / ...
- Be personal in your comms!
- Exclusive events or early access to new programs can also boost engagement.

Fix bugs fast and share progress

- Hackers love seeing their work make a difference.
- They want to see the impact
- They don’t like bugs that are open for 2 years. Show that you care about your security.
- Share remediation updates and explain how they improved your security.

Engage with the community

- Invite them to meet at bug bounty conferences
- Join Slack instances, Discord, Reddit or other places to see how hackers talk about your program. Be amongst them.
- Open them for a Friday chat. ”Ask me anything” and build that trust.
- When ready – and applicable – think about your own Live Hacking Event.

main take-away
“collaboration is key!”

connect with me
on Linkedin