Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem

Omer Akgul • Taha Eghtesad • Amit Elazari • Omprakash Gnawali • Jens Grossklags
Michelle Mazurek • Daniel Votipka • Aron Laszka

UNIVERSITY OF MARYLAND

PennState

UNIVERSITY of HOUSTON

Tufts UNIVERSITY

Technical University of Munich

Berkeley UNIVERSITY OF CALIFORNIA

Bug bounty programs

Bug bounty programs

Bug bounty programs

Images from flaticon.com

Bug bounty programs

Images from flaticon.com

Bug bounty programs

- Crowd-sourced vulnerability discovery systems

3

Bug bounty programs

- Crowd-sourced vulnerability discovery systems

  - Bug bounty hunters find vulns.

Images from flaticon.com

3

Bug bounty programs

- Crowd-sourced vulnerability discovery systems

  - Bug bounty hunters find vulns.

  - Companies learn vulnerabilities.

Images from flaticon.com

3

Bug bounty programs

- Crowd-sourced vulnerability discovery systems

  - Bug bounty hunters find vulns.

  - Companies learn vulnerabilities.

  - Hunters get recognition/compensation

Images from <u>flaticon.com</u>

3

Bug bounty programs

- Crowd-sourced vulnerability discovery systems

  - Bug bounty hunters find vulns.

  - Companies learn vulnerabilities.

  - Hunters get recognition/compensation

Images from flaticon.com

Bug bounty platforms

Bug bounty platforms

Images from flaticon.com

Bug bounty platforms

Bug bounty platforms

- Platforms that help connect bug bounty programs with bug bounty hunters

Bug bounty platforms

- Platforms that help connect bug bounty programs with bug bounty hunters

- Can help standardize the hunter-manager process

Images from flaticon.com

Bug bounty platforms

- Platforms that help connect bug bounty programs with bug bounty hunters

- Can help standardize the hunter-manager process

Bug bounty platforms

- Platforms that help connect bug bounty programs with bug bounty hunters

- Can help standardize the hunter-manager process

6

Why care about bug bounties?

Why care about bug bounties?
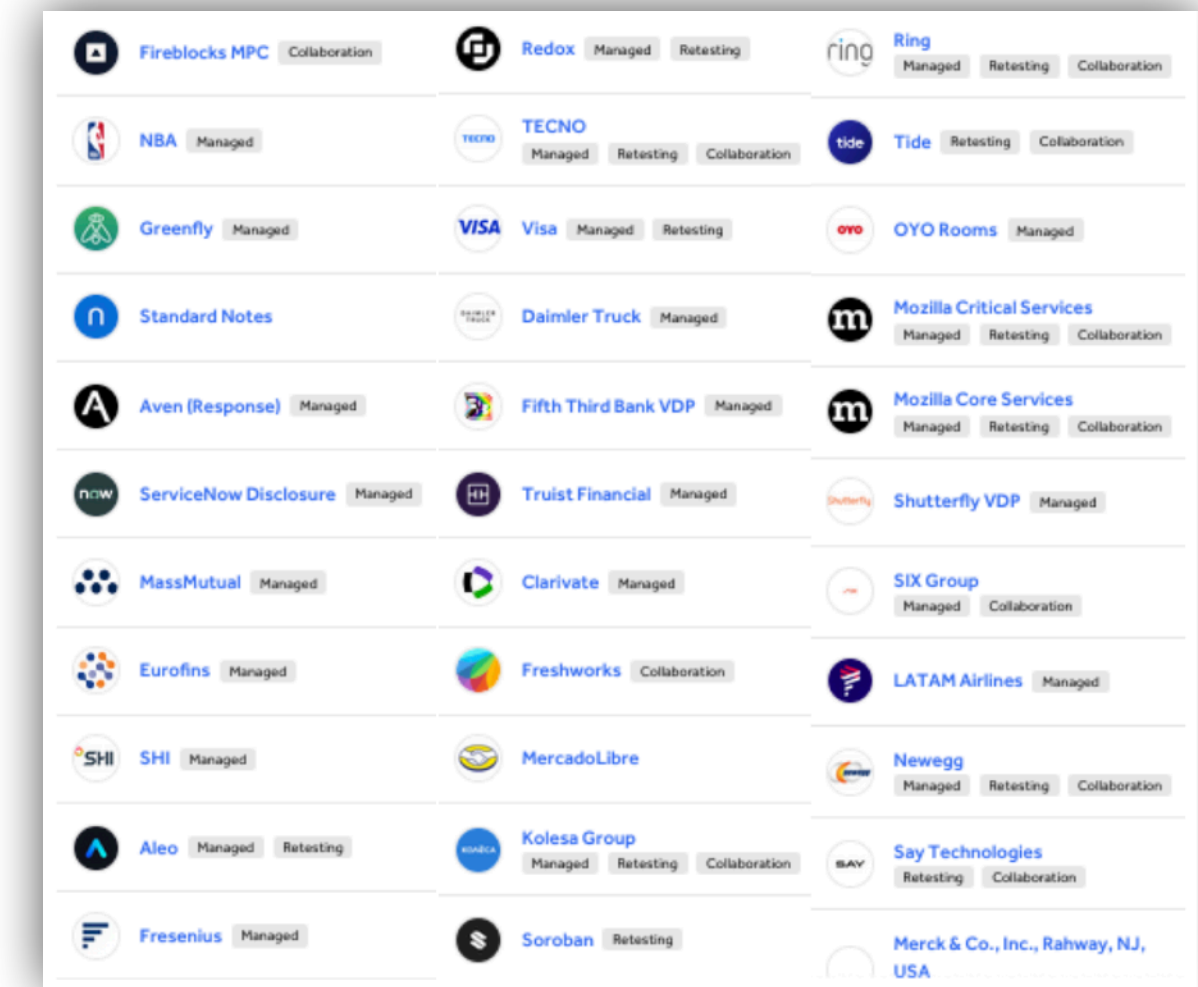
- Works great for organizations!

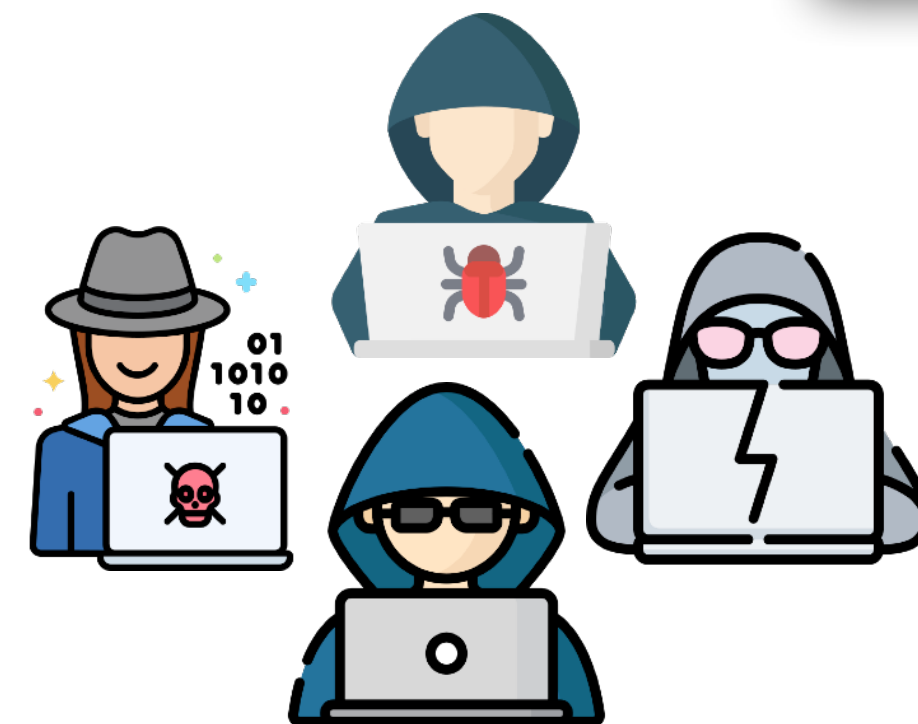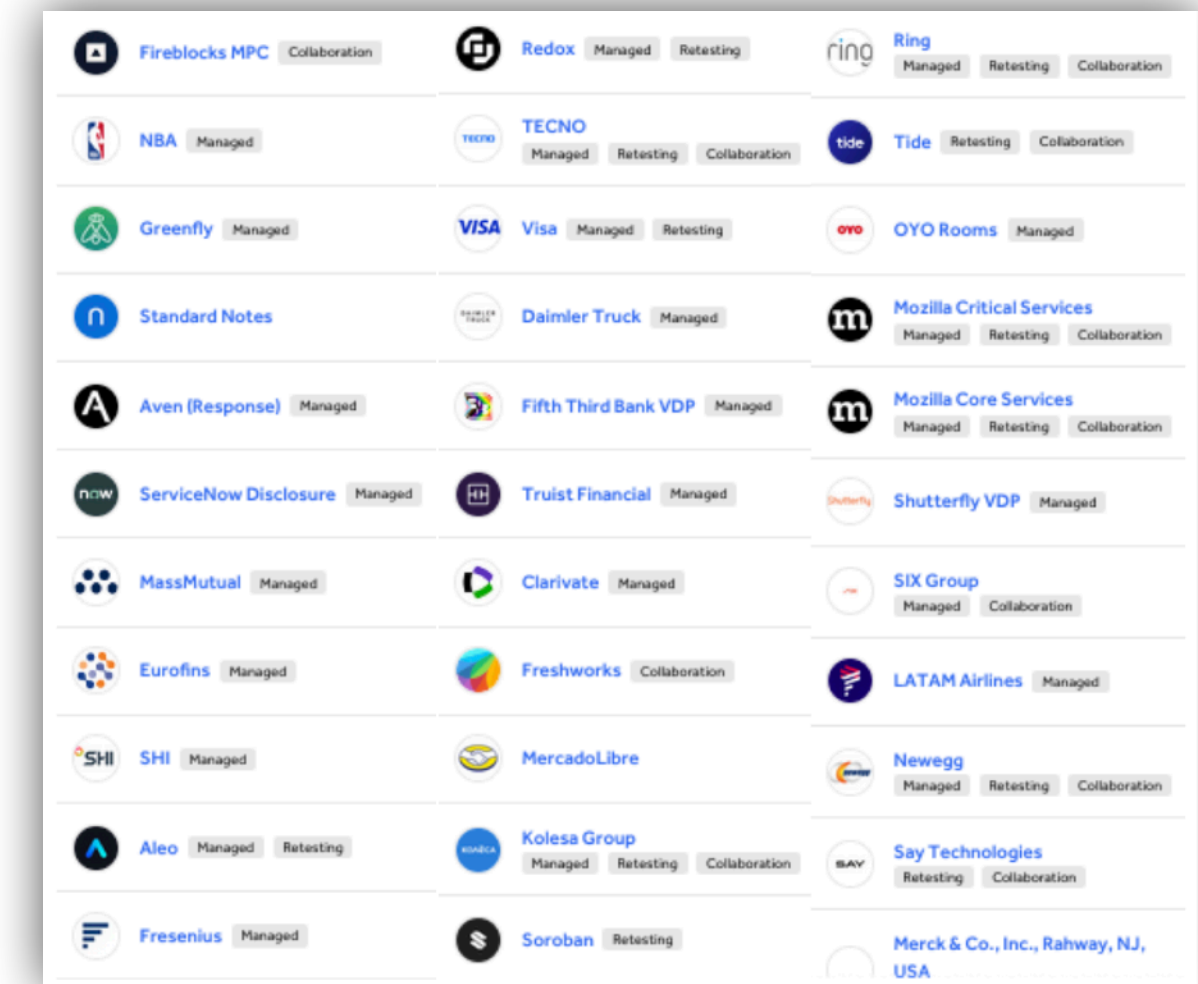# Why care about bug bounties?

- Works great for organizations!

  - Cheaper to run than in house team

7
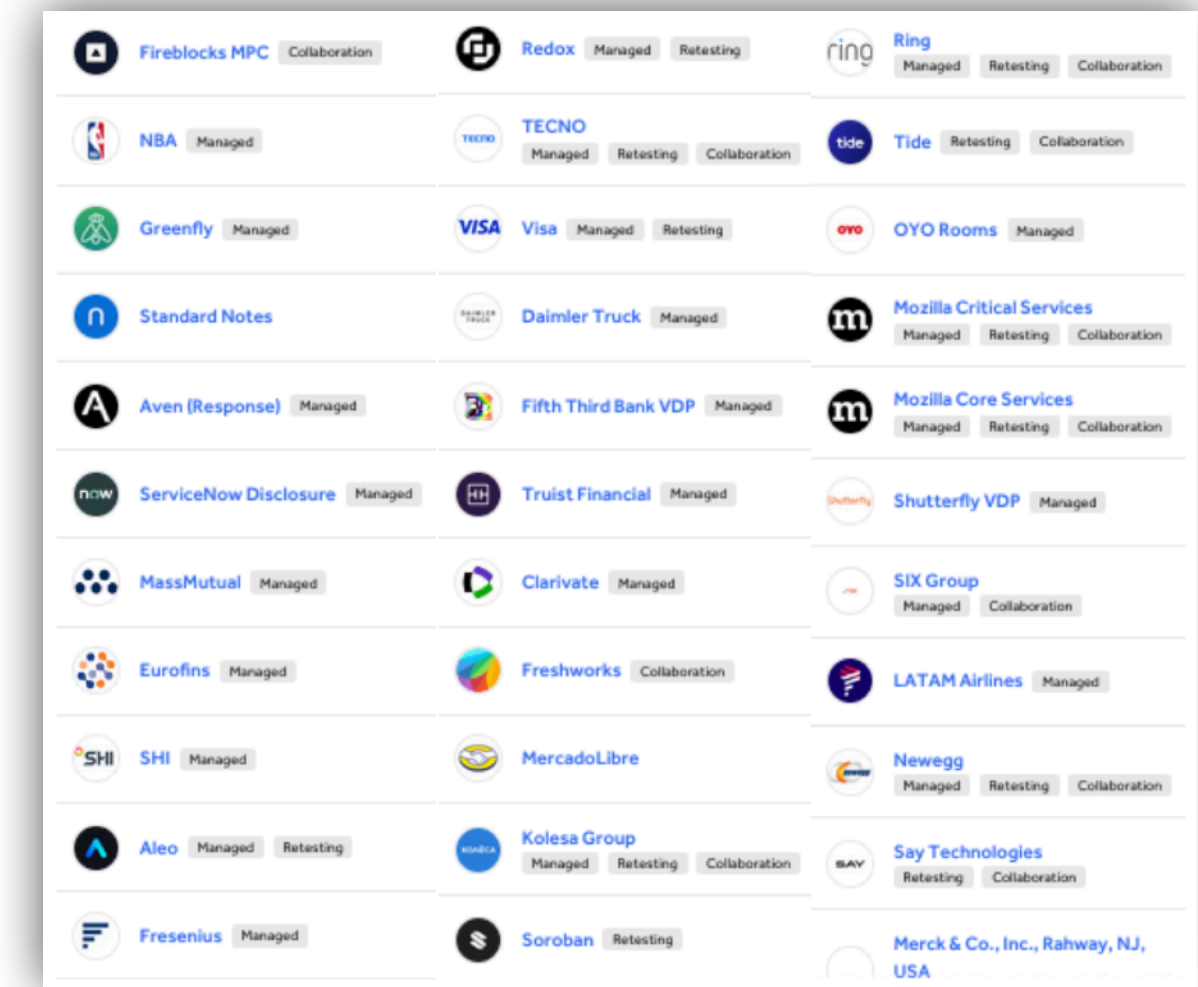
Why care about bug bounties?

- Works great for organizations!

  - Cheaper to run than in house team

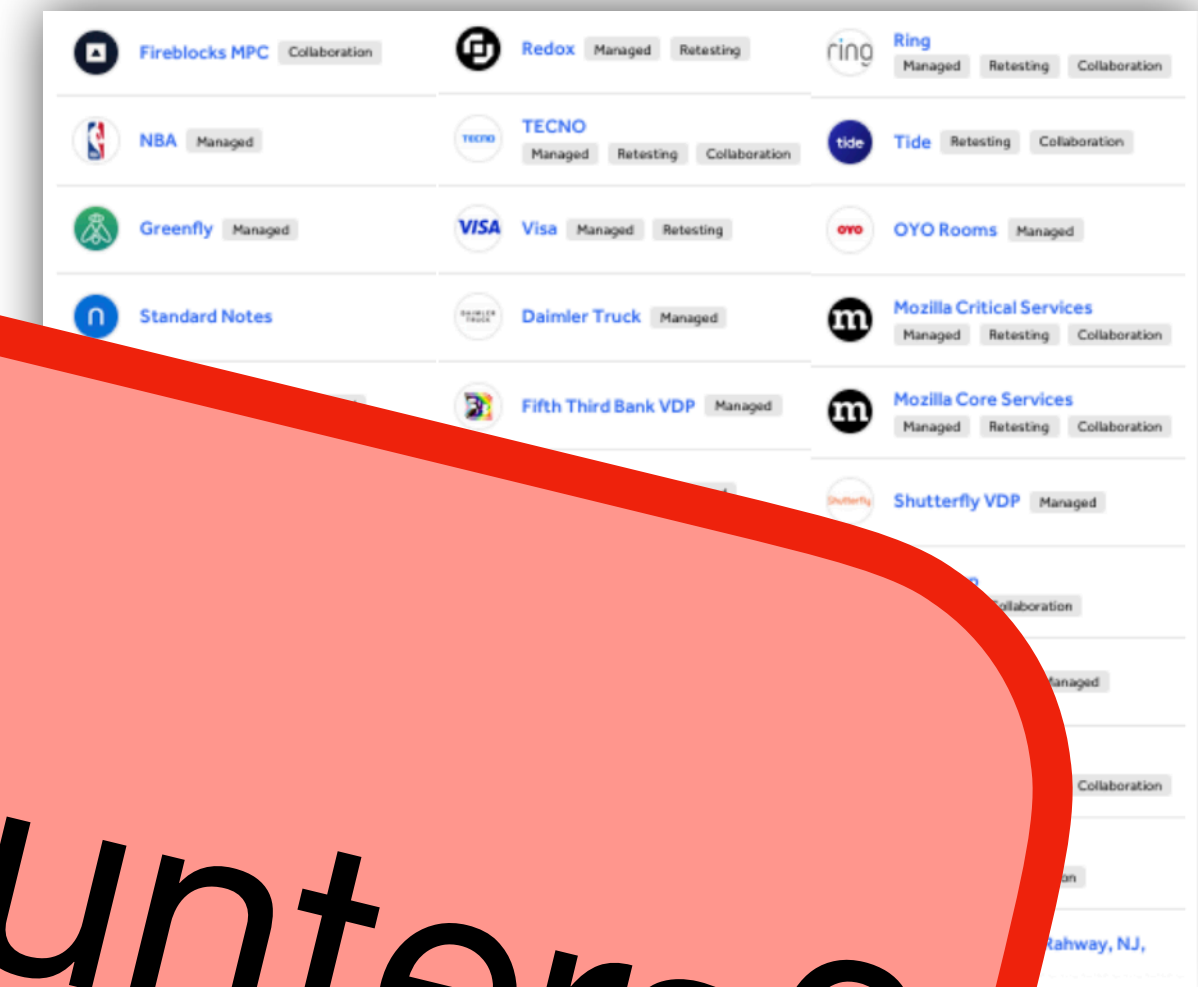 - Access to diverse skills
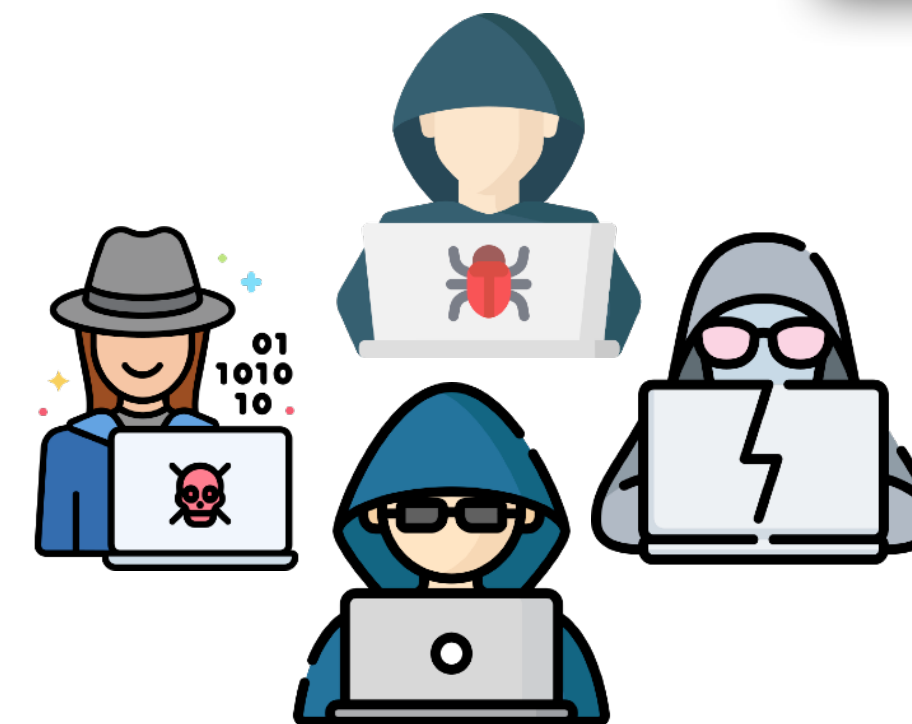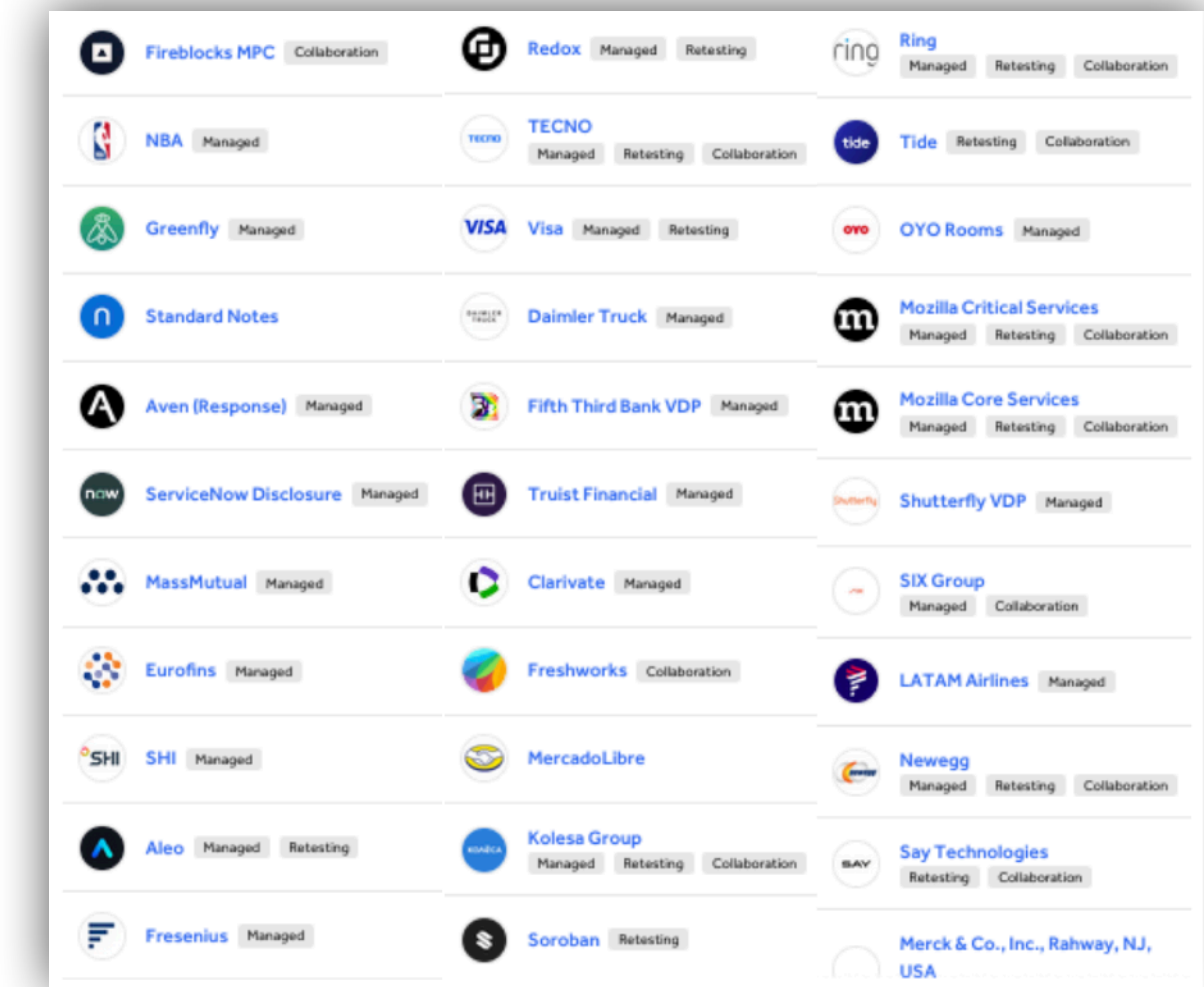
Why care about bug bounties?

- Works great for organizations!

  - Cheaper to run than in house team

  - Access to diverse skills

  - 400K+ valid vulns foun

Images from flaticon.com and hackerone.com

Why care about bug bounties?

- Works grea

  - Cheaper t

  - Access diverse skill po

  - 400K+ valid vulns foun

What about the hunters?

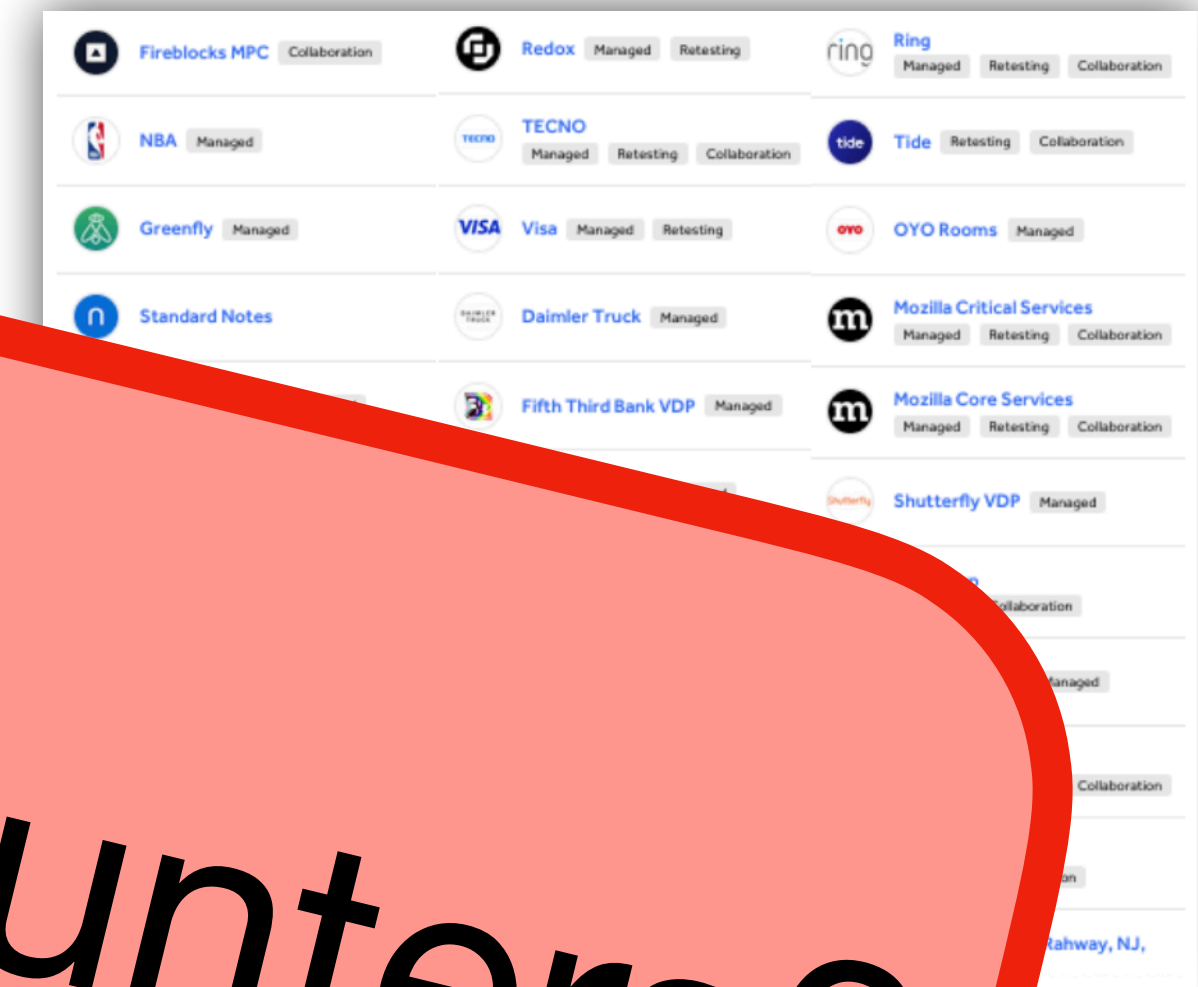Images from flaticon.com and hackerone.com

Why care about bug bounties?

- Works grea[...]

  - Cheaper t[...]

  - Access diverse skill po[...]

  - 400K+ valid vuln[...]

What about the hunters?

Their experience?

The hunters' perspective

The hunters' perspective

✔︎ What are the benefits?

The hunters' perspective

✔️ What are the benefits?

❓ Factors in choosing programs?

Program			Launch date	Reports resolved	Bounties minimum	Bounties average
U.S. Dept Of Defense			11/2016	8892	-	-
Verizon Media	Managed		02/2014	6398	$50	$400-$500
Mail.ru			04/2014	3618	$100	$250-$300
AT&T	Managed		07/2019	2985	$100	$300
Adobe	Managed		02/2015	2628	-	-
IBM	Managed		07/2018	2067	-	-
Ford	Managed	Retesting	01/2019	1693	-	-
Uber	Managed		12/2014	1515	$500	$500-$750
Twitter			05/2014	1194	$140	$420-$560
Sony	Managed		10/2017	1168	-	-
Magento	Managed		01/2019	1092	$100	$290-$690
Slack			02/2014	1073	$100	$500
Ubiquiti Inc.	Managed		01/2015	1002	$150	$175-$250
Starbucks	Managed		05/2016	999	$100	$250-$375

The hunters' perspective

✔️ What are the benefits?

❓ Factors in choosing programs?

✳️ What are the challenges?

Program		Launch date	Reports resolved	Bounties minimum	Bounties average
U.S. Dept Of Defense		11 / 2016	8892	-	-
Verizon Media	Managed	02 / 2014	6398	$50	$400-$500
Mail.ru		04 / 2014	3618	$100	$250-$300
AT&T	Managed	07 / 2019	2985	$100	$300
Adobe	Managed	02 / 2015	2628	-	-
IBM	Managed	07 / 2018	2067	-	-
Ford	Managed Retesting	01 / 2019	1693	-	-
Uber	Managed	12 / 2014	1515	$500	$500-$750
Twitter		05 / 2014	1194	$140	$420-$560
Sony	Managed	10 / 2017	1168	-	-
Magento	Managed	01 / 2019	1092	$100	$290-$690
Slack		02 / 2014	1073	$100	$500
Ubiquiti Inc.	Managed	01 / 2015	1002	$150	$175-$250
Starbucks	Managed	05 / 2016	999	$100	$250-$375

The hunters' perspective

✔️ What are the benefits?

❓ Factors in choosing programs?

💢 What are the challenges?

🧰 Which platform utilities are useful?

Program		Launch date	Reports resolved	Bounties minimum	Bounties average
U.S. Dept Of Defense		11 / 2016	8892	-	-
Verizon Media	Managed	02 / 2014	6398	$50	$400-$500
Mail.ru		04 / 2014	3618	$100	$250-$300
AT&T	Managed	07 / 2019	2985	$100	$300
Adobe	Managed	02 / 2015	2628	-	-
IBM	Managed	07 / 2018	2067	-	-
Ford	Managed Retesting	01 / 2019	1693	-	-
Uber	Managed	12 / 2014	1515	$500	$500-$750
Twitter		05 / 2014	1194	$140	$420-$560
Sony	Managed	10 / 2017	1168	-	-
Magento	Managed	01 / 2019	1092	$100	$290-$690
Slack		02 / 2014	1073	$100	$500
Ubiquiti Inc.	Managed	01 / 2015	1002	$150	$175-$250
Starbucks	Managed	05 / 2016	999	$100	$250-$375

9

The hunters' perspective

✔️ What are the benefits?

❓ Factors in choo...

💥 W...

🧰

Which factors are most important?

Our multi-pronged approach

Our multi-pronged approach

Factor free listing (n=56)

Our multi-pronged approach
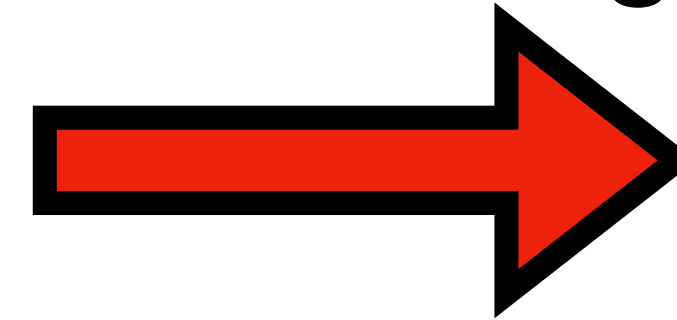
Factor free
listing (n=56)

Qual coding

Our multi-pronged approach

Factor free listing (n=56)

Qual coding

Our multi-pronged approach

Factor free listing (n=56)

Qual coding

Our multi-pronged approach

Factor free listing (n=56)

Qual coding

Factor rating (n=159)

Our multi-pronged approach

Factor free listing (n=56)

Qual coding

Factor rating (n=159)

Quant Analysis

Our multi-pronged approach

Factor free listing (n=56)

Qual coding

Factor rating (n=159)

Quant Analysis

Our multi-pronged approach

Our multi-pronged approach

Interviews (n=24)

Factor free listing (n=56)

Qual coding

Factor rating (n=159)

Quant Analysis
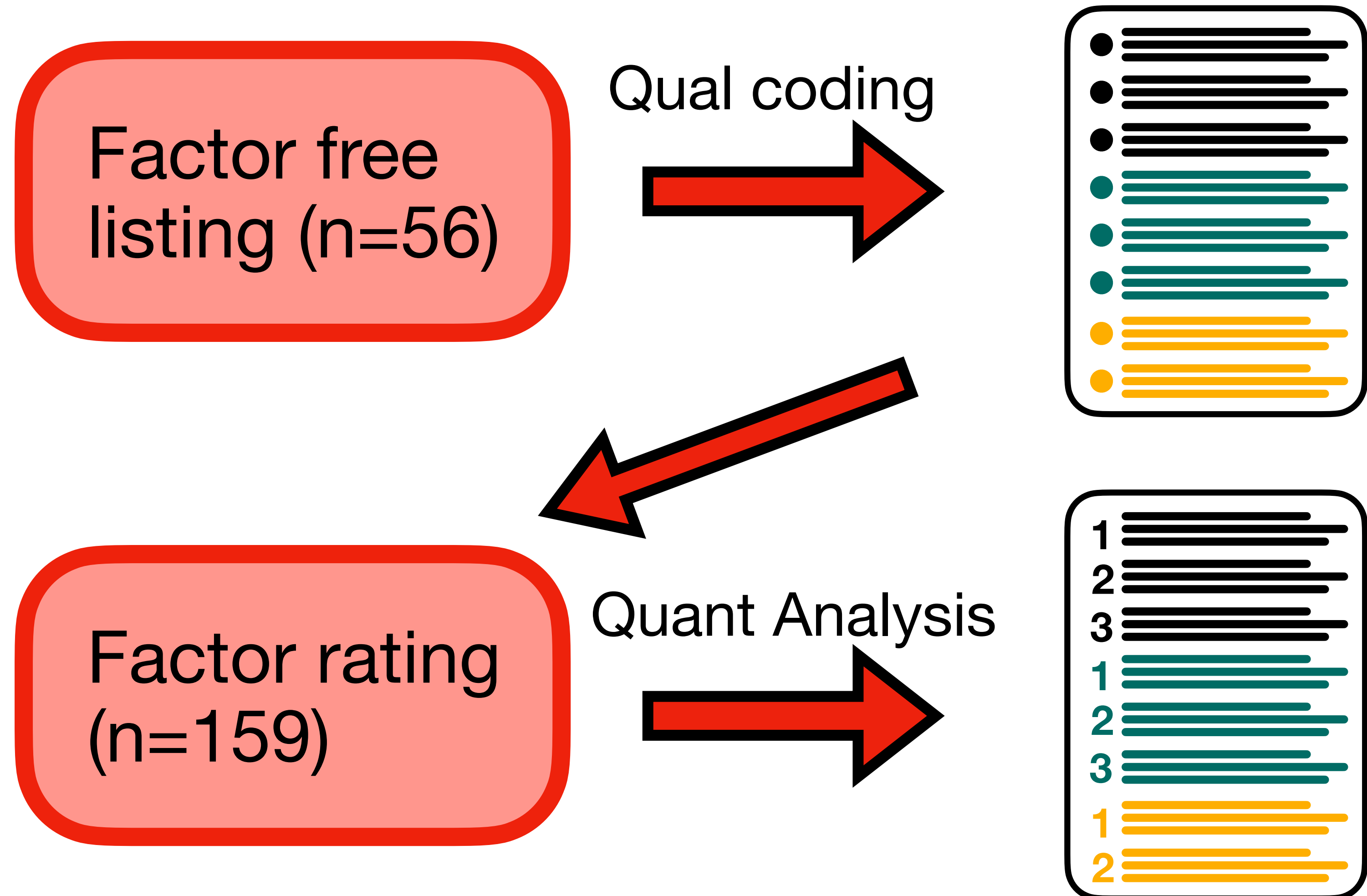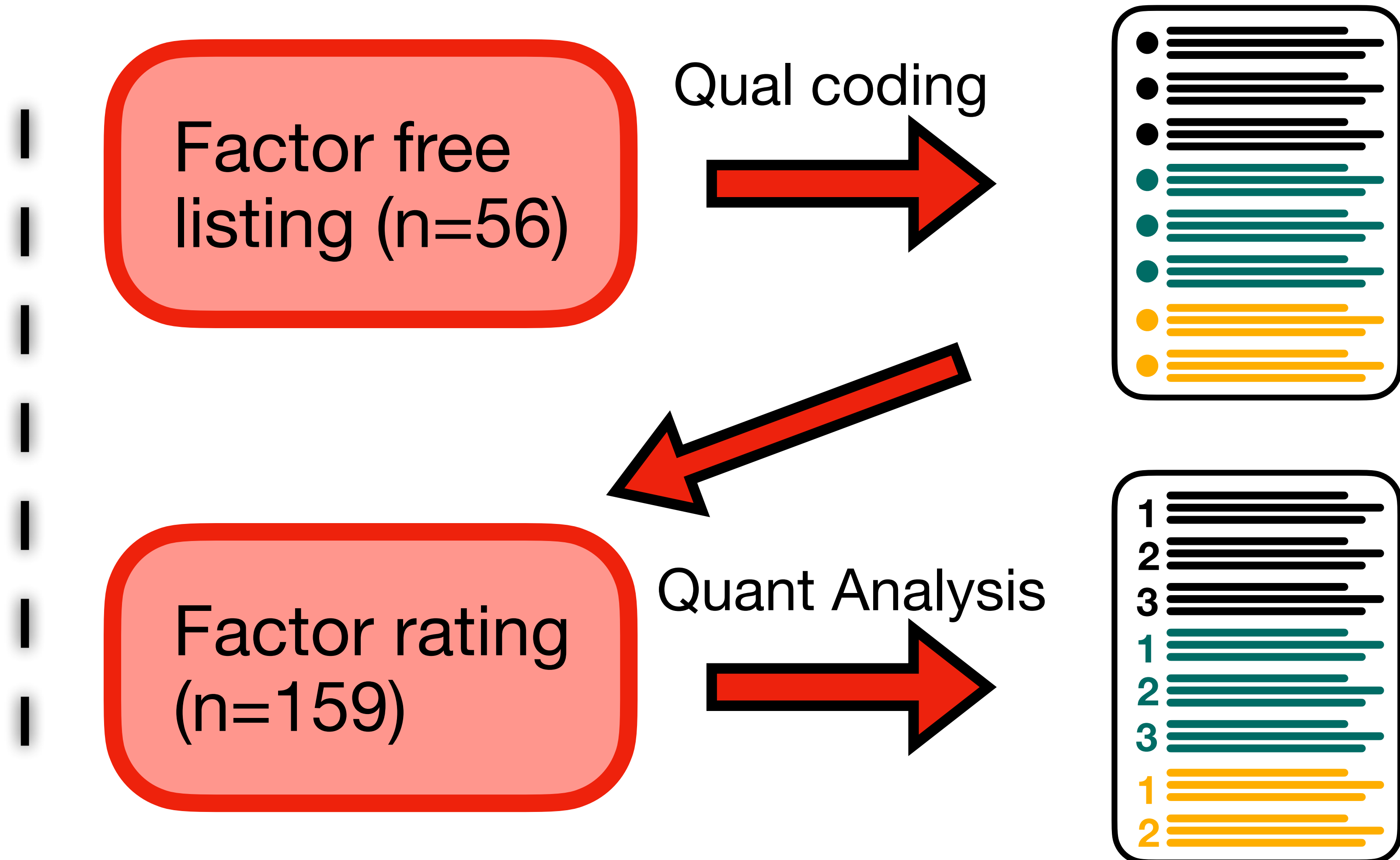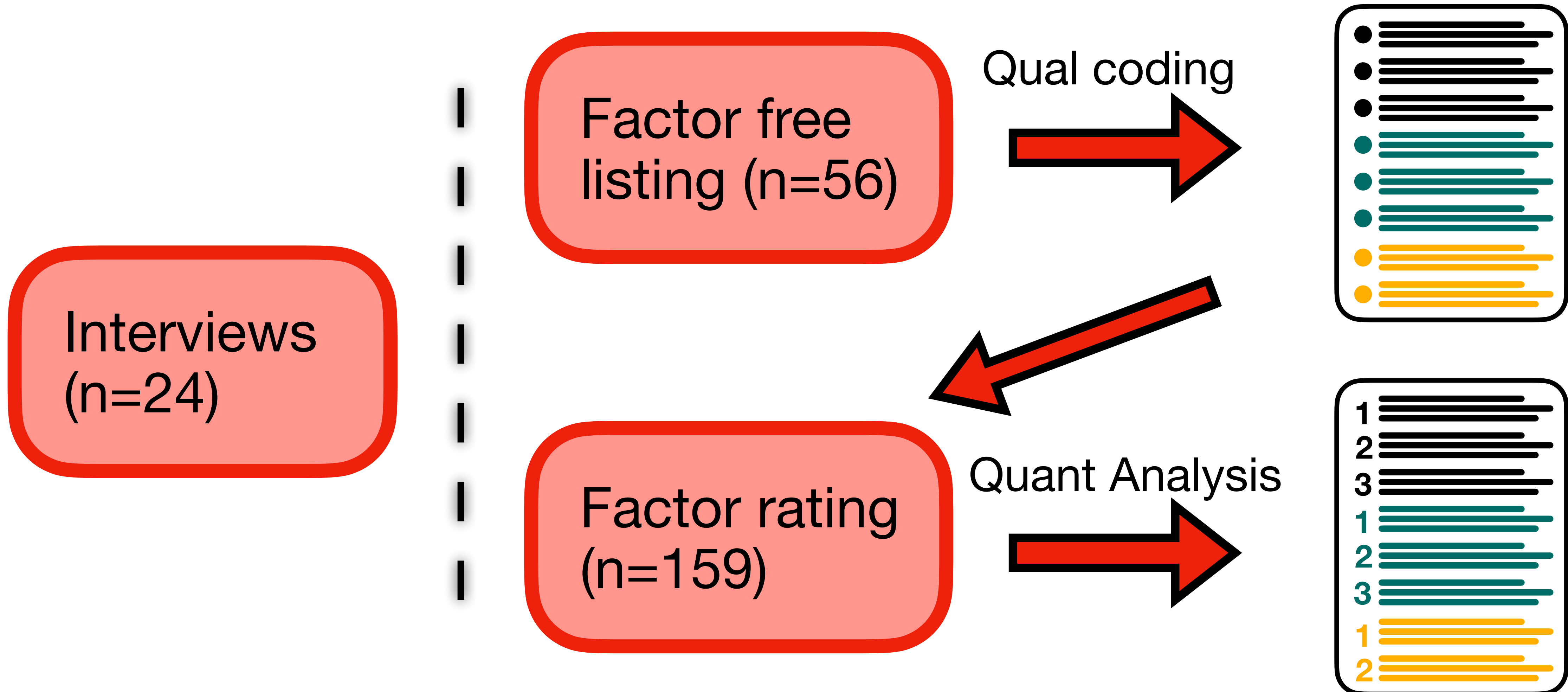
Our participants

Our participants

- Wide range of participants

Our participants
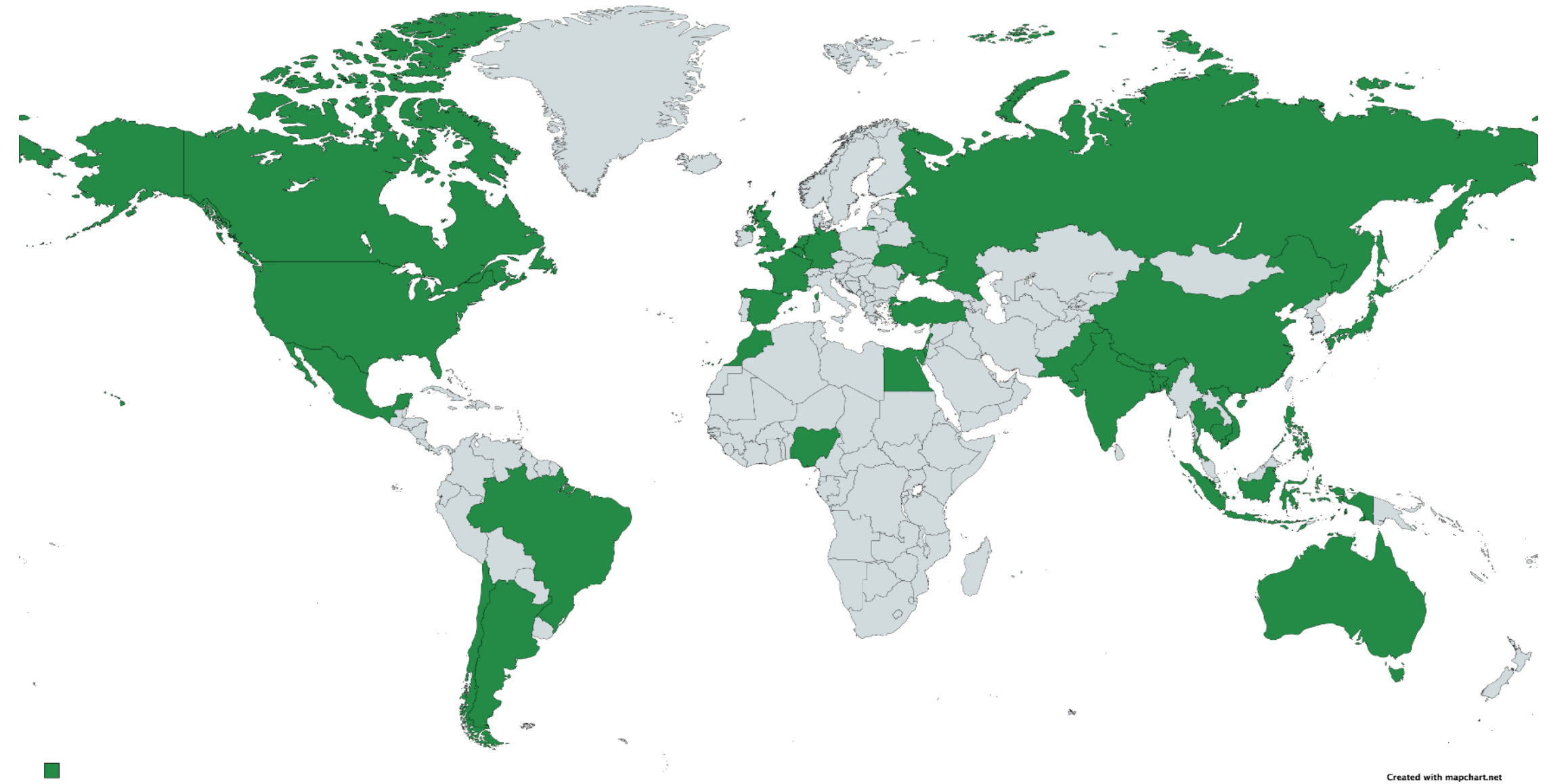
- Wide range of participants

  - Across the globe

Our participants

- Wide range of participants

  - Across the globe

  - Weekly hours

11
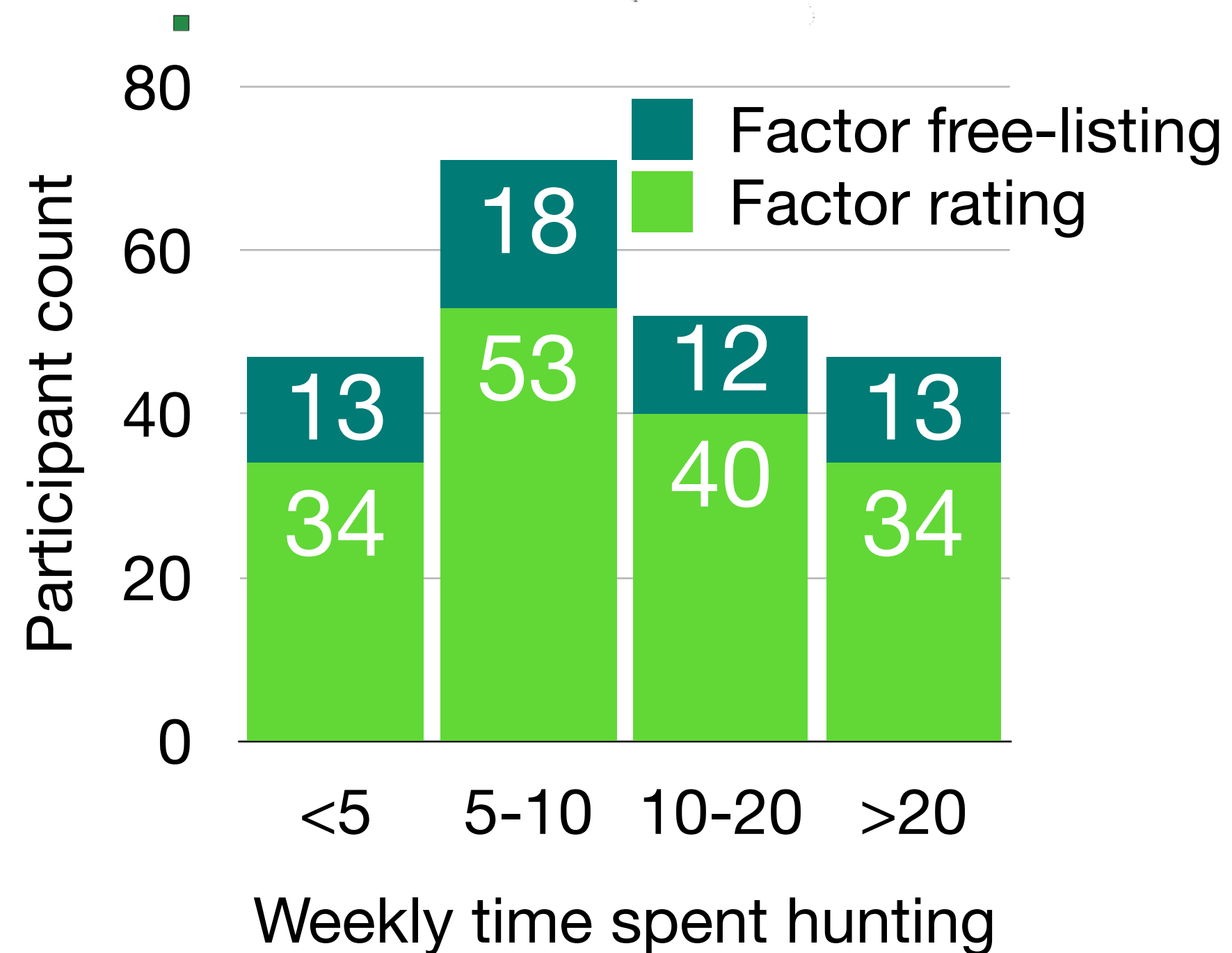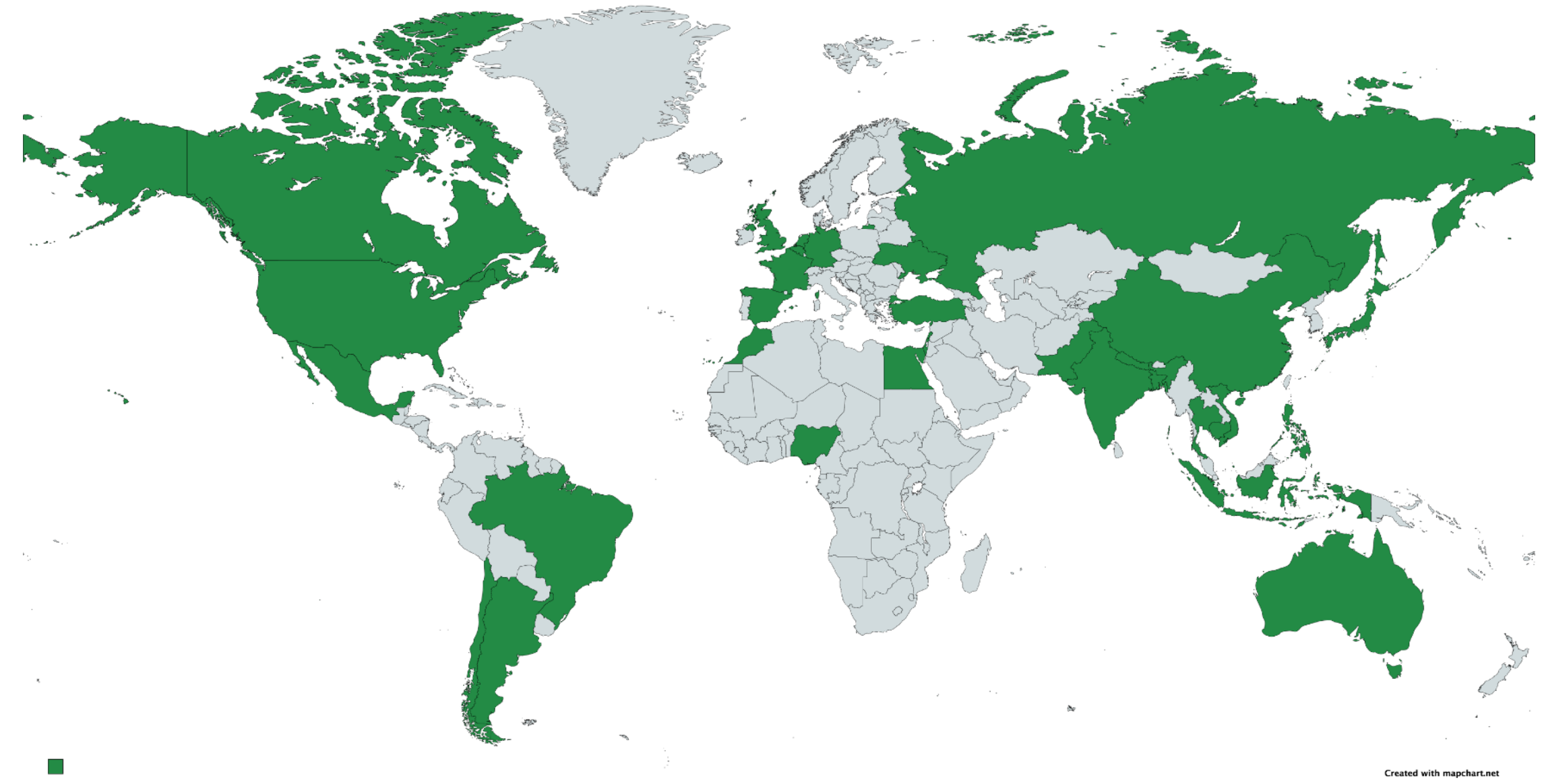
Our participants

- Wide range of participants

  - Across the globe

  - Weekly hours
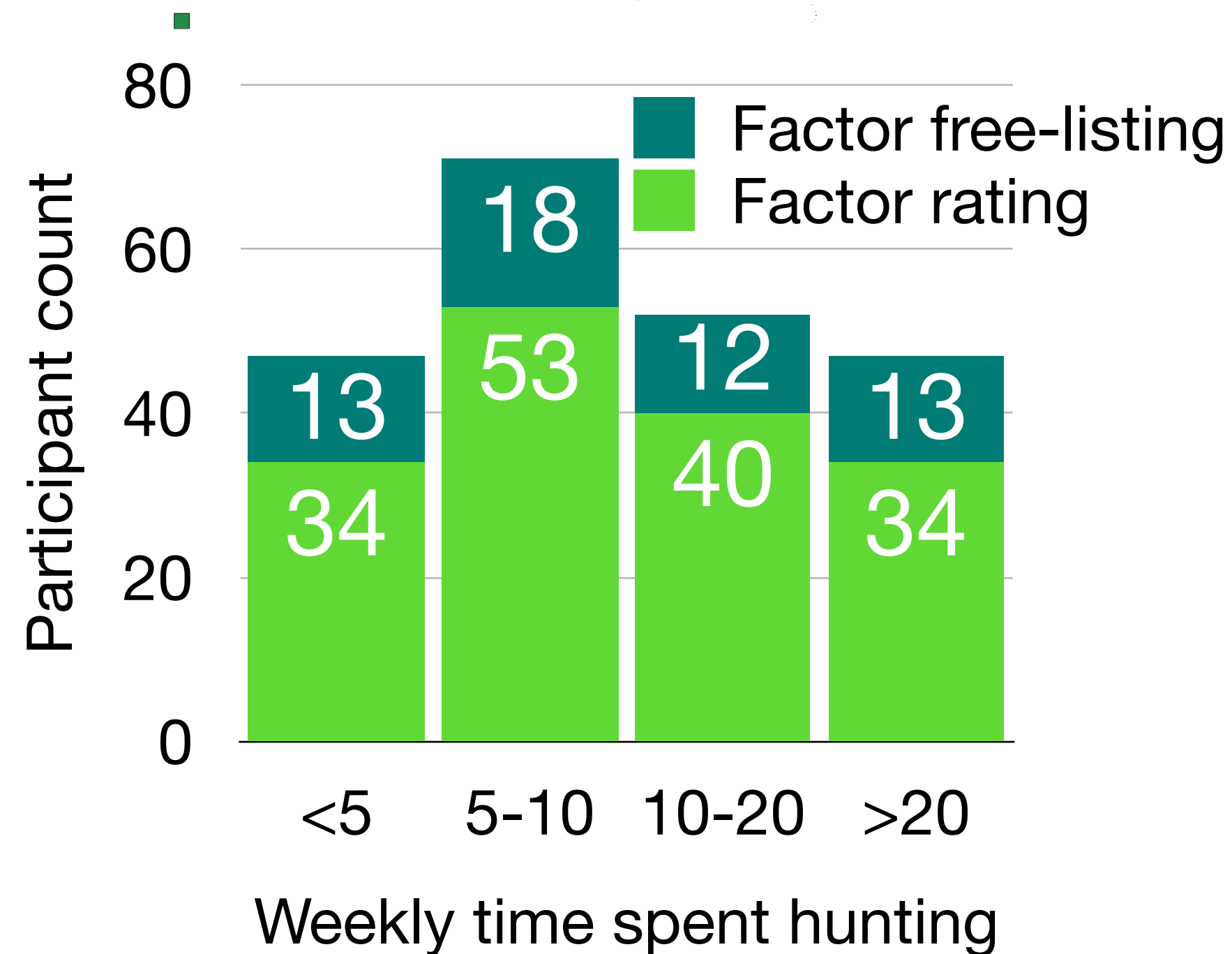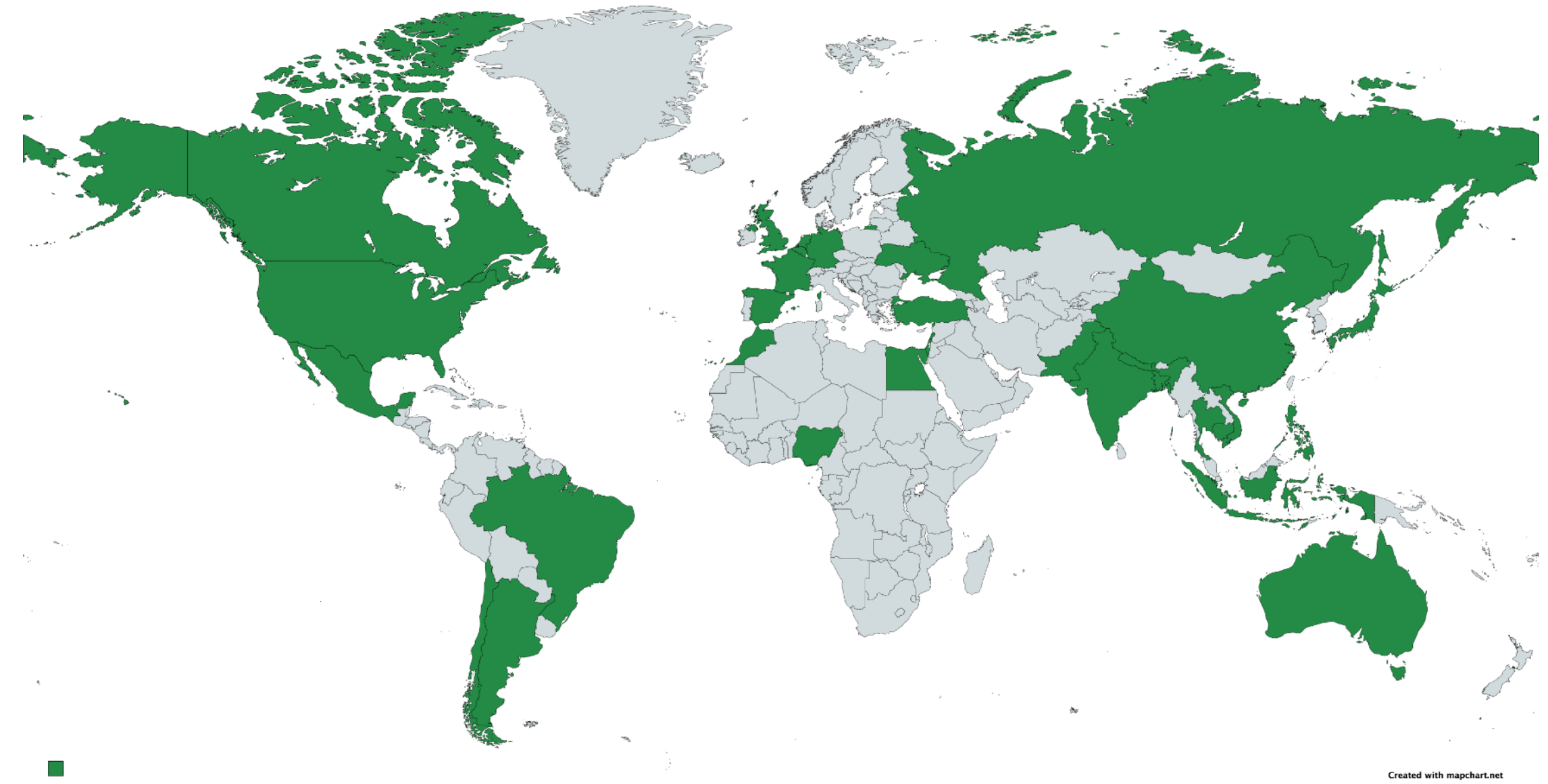
  - # of bugs found

Our participants

- Wide range of participants

  - Across the globe

  - Weekly hours

  - # of bugs found

  - Years of experience
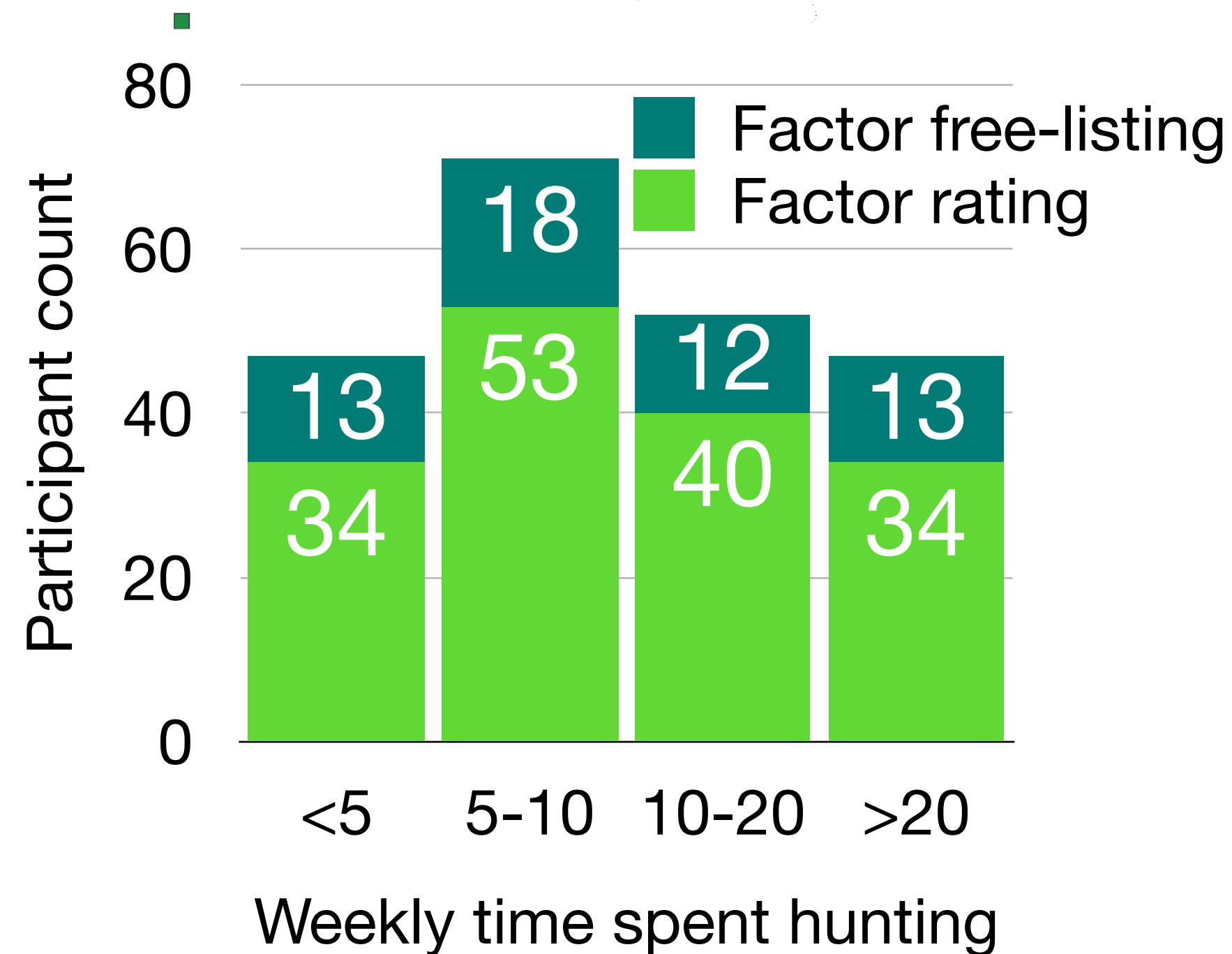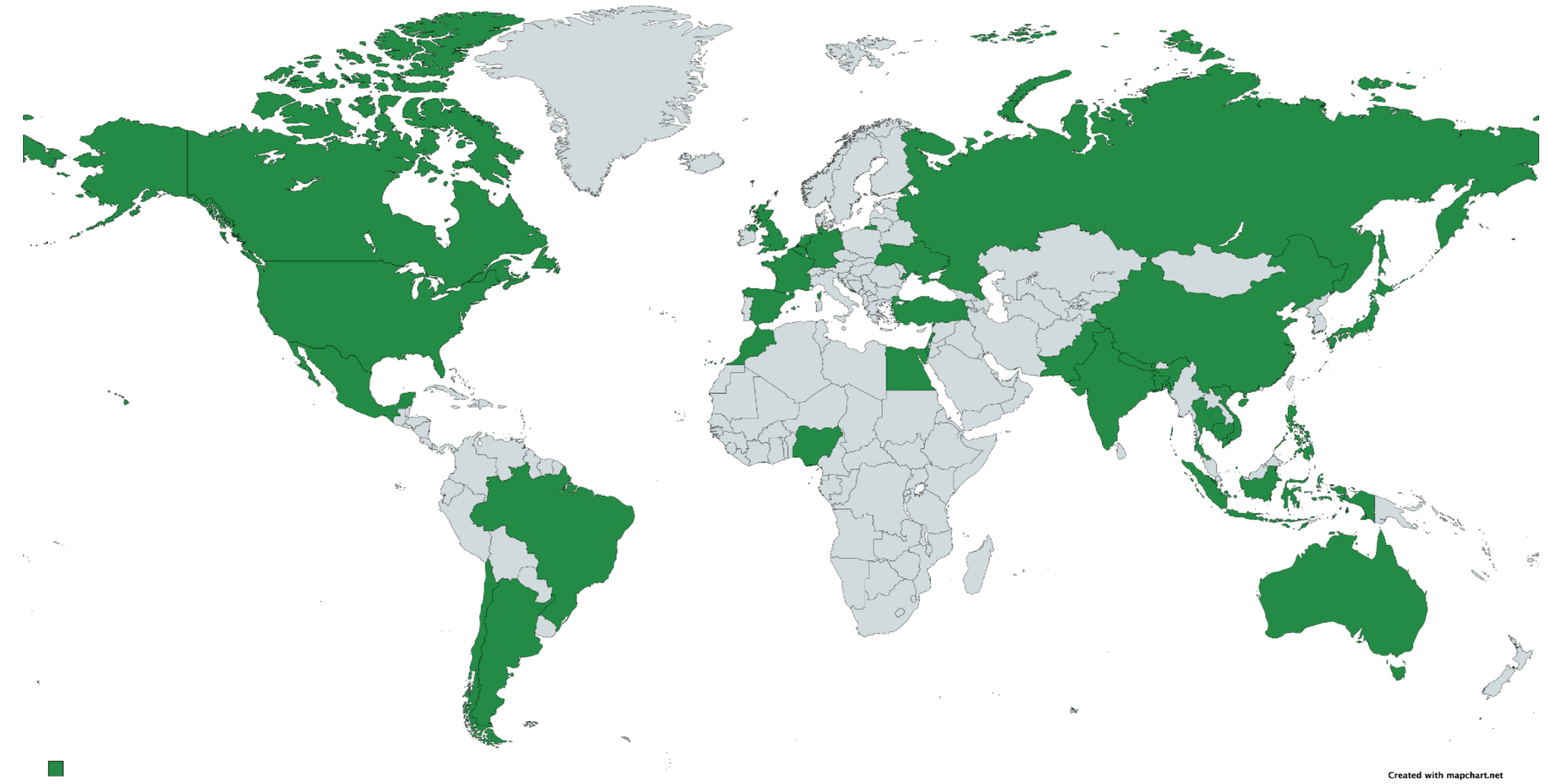
Our participants

- Wide range of participants

  - Across the globe

  - Weekly hours

  - # of bugs found

  - Years of experience

- Similar to bug bounty platform reports.

Created with mapchart.net

Legend:
- Factor free-listing
- Factor rating

Y-axis: Participant count (0, 20, 40, 60, 80)

Bars:
- <5: 34 (rating), 13 (free-listing)
- 5-10: 53 (rating), 18 (free-listing)
- 10-20: 40 (rating), 12 (free-listing)
- >20: 34 (rating), 13 (free-listing)

X-axis: Weekly time spent hunting
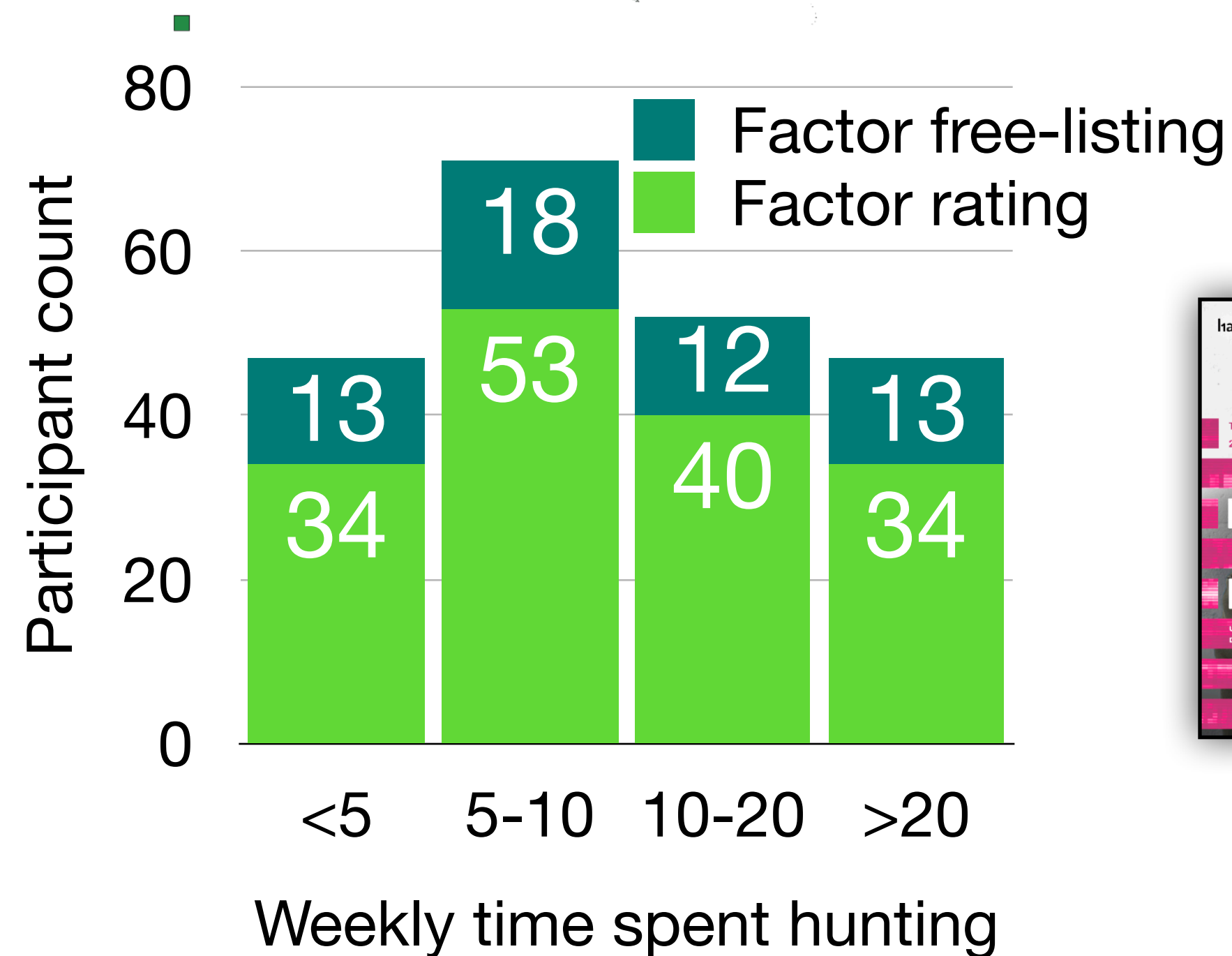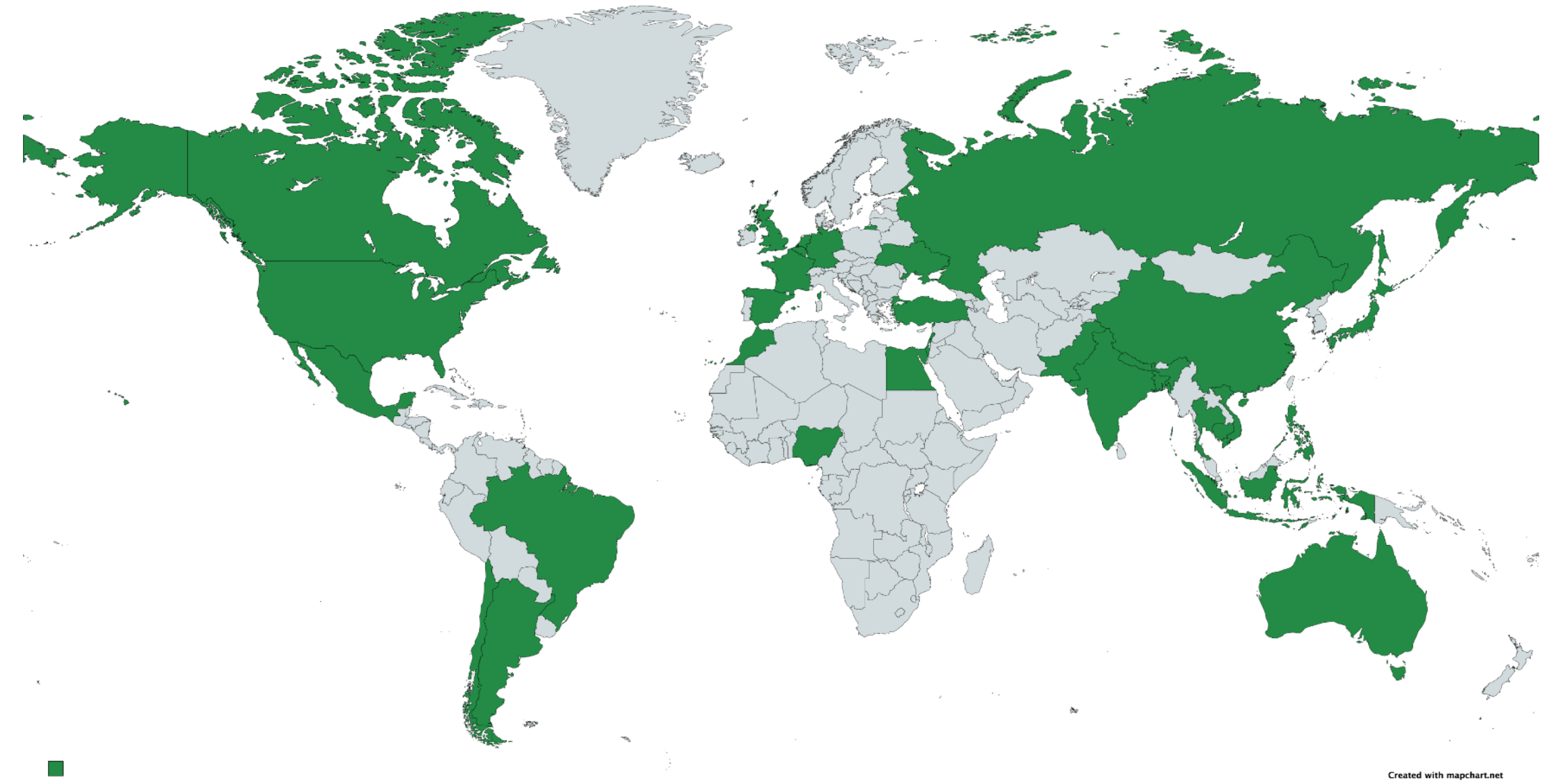
What are the factors?

What are the factors?

✔️ What are the benefits?

What are the factors?

✔️ What are the benefits?

❓ Factors in choosing programs?

What are the factors?

✔︎ What are the benefits?

❓ Factors in choosing programs?

✖︎ What are the challenges?

What are the factors?

✔️ What are the benefits?

❓ Factors in choosing programs?

💢 What are the challenges?

🧰 Which platform utilities are useful?

What are t

✔ What are the

❓ Factors in ch

❌ What are the

🧰 Which platfo

Images from flaticon.com

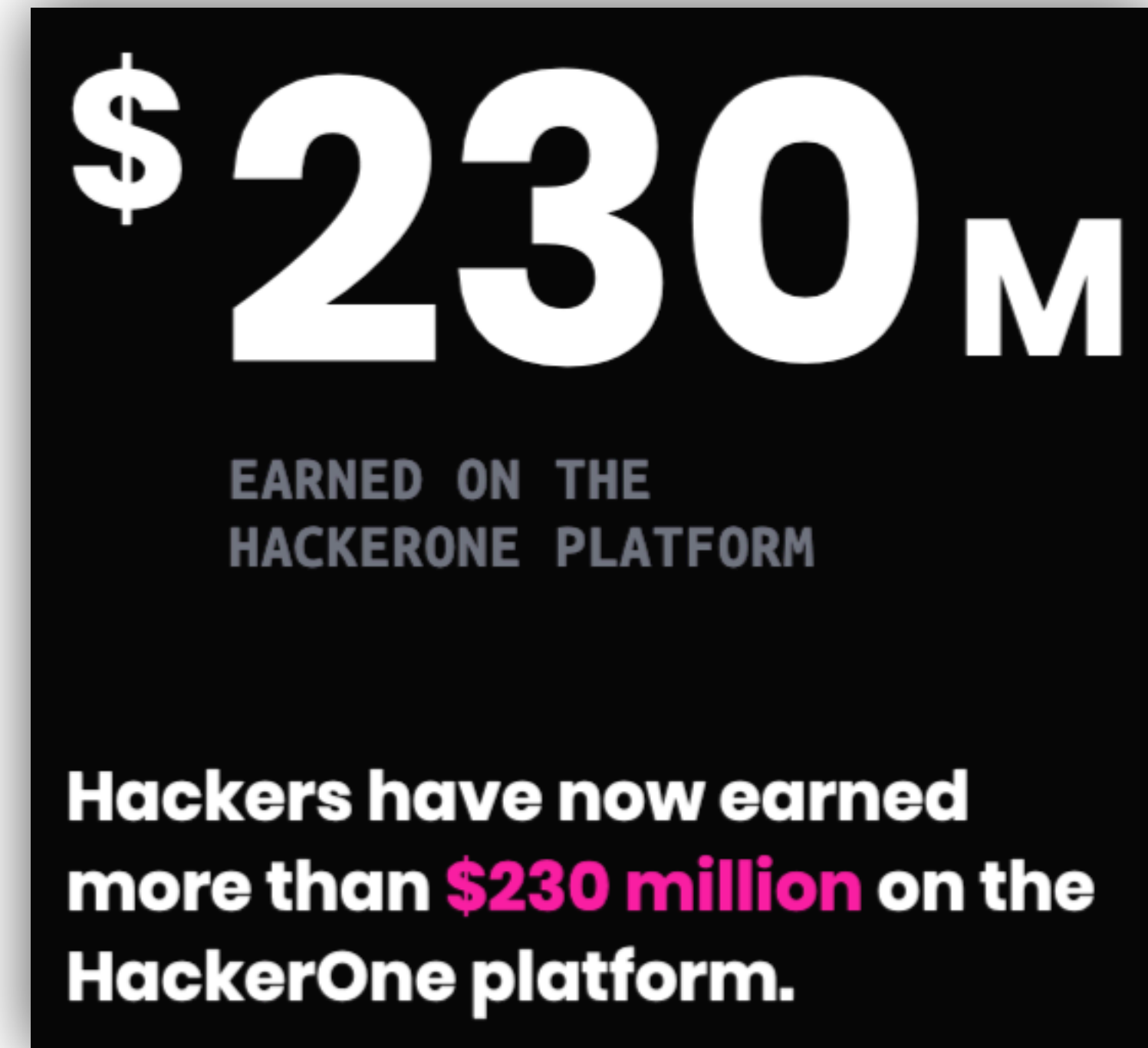| Question	Code Name	Description	FL	μ_r	Worth ( )
	Scope:	Number of domains or assets that are included in the program.	28	6.10	0.156
	Reward:	Expected monetary or non-monetary rewards (e.g., SWAG, hardware, subscription).	36	5.91	0.120
	Bounty table:	Reward rules and ranges set by the managers (e.g., $50 for low criticality bugs, but $5000 for high criticality bugs).	16	5.87	0.117
	Technology familiarity:	Familiarity with the technology of the assets (e.g., familiarity with web or iOS).	22	5.86	0.113
	Legal safe harbor:	Language of program includes a commitment to not pursue legal actions after hackers who follow the rules and/or explicitly authorizes testing conducted in accordance with the rules.	4	5.71	0.098
Choosing a program	Program repute:	Program's reputation in the community for being pleasant to work with (i.e., what other hackers say about the program).	15	5.68	0.086
	Learning opportunity:	Lack of familiarity with the technology of the assets (e.g., interest in learning crypto or Android).	1	5.35	0.064
	Private or public:	Private programs (accessible only by invitation) vs. public programs (accessible by anyone).	4	5.16	0.048
	Company familiarity:	Company behind the program is widely known, or you or your peers use its products or services (e.g., working on Uber's program because you like or use their services).	15	5.04	0.047
	Saturation:	Number of reports received or number of hackers working on the program.	8	5.17	0.047
	Career opportunities:	Future career opportunities with the company behind the program.	3	4.49	0.027
	Public disclosure:	Public vulnerability disclosure is generally allowed following the resolution of the issue, permissive NDAs.	6	4.63	0.027
	ge:	For how long the program has been running.	6	4.44	0.023
	Business domain:	Business domain of the company behind the program (e.g., social media, insurance, medical).	2	4.47	0.021
	Country:	Where the company behind the program is located.	1	3.34	0.006
	Poor responsiveness:	Lack of responses or slow responses from program managers.	30	5.39	0.130
	Dissatisfaction with responses:	Rewards are lower than promised by rules (e.g., downgraded severity, impact, disagreements with duplicates).	26	5.36	0.120
	Unclear scope:	Program scope is not defined clearly.	3	4.99	0.082
	Poor platform support	Dissatisfaction with how platforms handle issues, such as mediating between hackers and programs.	1	5.03	0.079
	Duplicates:	Too many reports marked as duplicates.	4	5.02	0.078
	ssets outside expertise	Assets are outside area of expertise, lacking certain required skills.	11	4.87	0.068
	Secure assets:	Finding bugs is too difficult.	5	4.78	0.064
Challenges of bug hunting	Stress and uncertainty:	Fear of burning out, social isolation during work, irregular income, etc.	5	4.8	0.062
	Too much labor work:	Menial tasks (e.g., CAPTCHA, waiting for timeouts, obfuscation, setting up test accounts).	12	4.62	0.050
	Boredom:	Bored of working on the program or a more interesting program launches.	8	4.62	0.050
	Unrepresentative reputation system:	Hackers' reputation points do not reflect real experience and are not transferable between platforms.	1	4.59	0.047
	Difficulty working with managers:	Bug-bounty program managers are difficult to work with (e.g., disrespectful, requiring extra work).	23	4.48	0.044
	Not enough time:	Not having enough time for participating in bug bounties.	2	4.45	0.043
	Limited vulnerability disclosure:	Restrictive vulnerability disclosure policies and NDAs that may prevent you from publishing your work following the resolution/mitigation of the issue.	2	4.49	0.041
	Legal threats:	Fear of threats of legal implication (civil or criminal).	2	3.96	0.028
	Lacking communication or language skills:	Communication difficulties because you feel that you lack language skills, experience anxiety in communication, etc.	2	3.45	0.014
	Monetary rewards:	Monetary compensation.	42	6.31	0.191
	Learning:	Learning or improving skills.	32	6.18	0.170
	Enjoyment:	Enjoyment or challenge of white-hat hacking.	20	6.08	0.140
	Legal safe harbour:	Hacking without the threat of legal actions if they obey the rules.	4	5.96	0.118
Benefits of bug hunting	Flexibility:	Work schedule and place flexibility (compared to traditional employment).	16	5.85	0.095
	Career:	Building relations and reputation with companies for employment and other work opportunities.	11	5.71	0.091
	Community:	Bug bounty creates a community of hackers.	3	5.52	0.071
	ltruism:	Improving cybersecurity for the sake of helping others, hacking to make the internet safer for everyone.	5	5.54	0.062
	Reputation:	Earning platform reputation points, building a following, etc.	14	5.36	0.048
	Non-monetary rewards:	Non-monetary compensation (e.g., SWAG, hardware, subscriptions).	4	4.35	0.013
	Ease of payment:	Receiving payments in a standardized, hassle-free way.	12	6.51	0.156
	Ease of reporting:	Easy to generate, submit, and track reports and their status.	16	6.46	0.142
	Viewing disclosed vulnerabilities:	Platform provided interface for viewing bugs found by others.	15	6.41	0.137
	Private program invitations:	Access to private programs on the platform.	5	6.28	0.107
	Program directory:	Listing many programs in one place, with statistics, details, etc. (being able to view Uber, Paypal, etc. programs on one page with statistics).	17	6.02	0.068
Useful platform features	Standardized rules:	Platform standardizing how scopes, rewards, criticality, etc. are defined.	3	5.99	0.063
	Community:	Platform making effort to create a community of hackers.	11	5.77	0.057
	Platform rewards:	E.g., platform SWAG, funded travel.	1	5.89	0.054
	Mediation:	Platform resolving disputes between hackers and programs.	13	5.77	0.051
	Platform managed disclosure:	Platform provided tools/mechanisms to publicly disclose resolved bugs.	6	5.86	0.050
	Resources for learning:	Platform providing free resources on how to hack (e.g., Bugcrowd University).	2	5.59	0.047
	Reputation system:	Platform managed reputation system for hackers.	6	5.70	0.043
	Platform triage:	Triaging managed by the platform (e.g., HackerOne triages your report instead of Uber).	5	5.06	0.023
	None:	There are no useful features that platforms provide.	4	-	-

What are the factors?

✔️ What are the benefits?

❓ Factors in choosing programs?

💥 What are the challenges?

🧰 Which platform utilities are useful?

Benefits of bug-bounty?

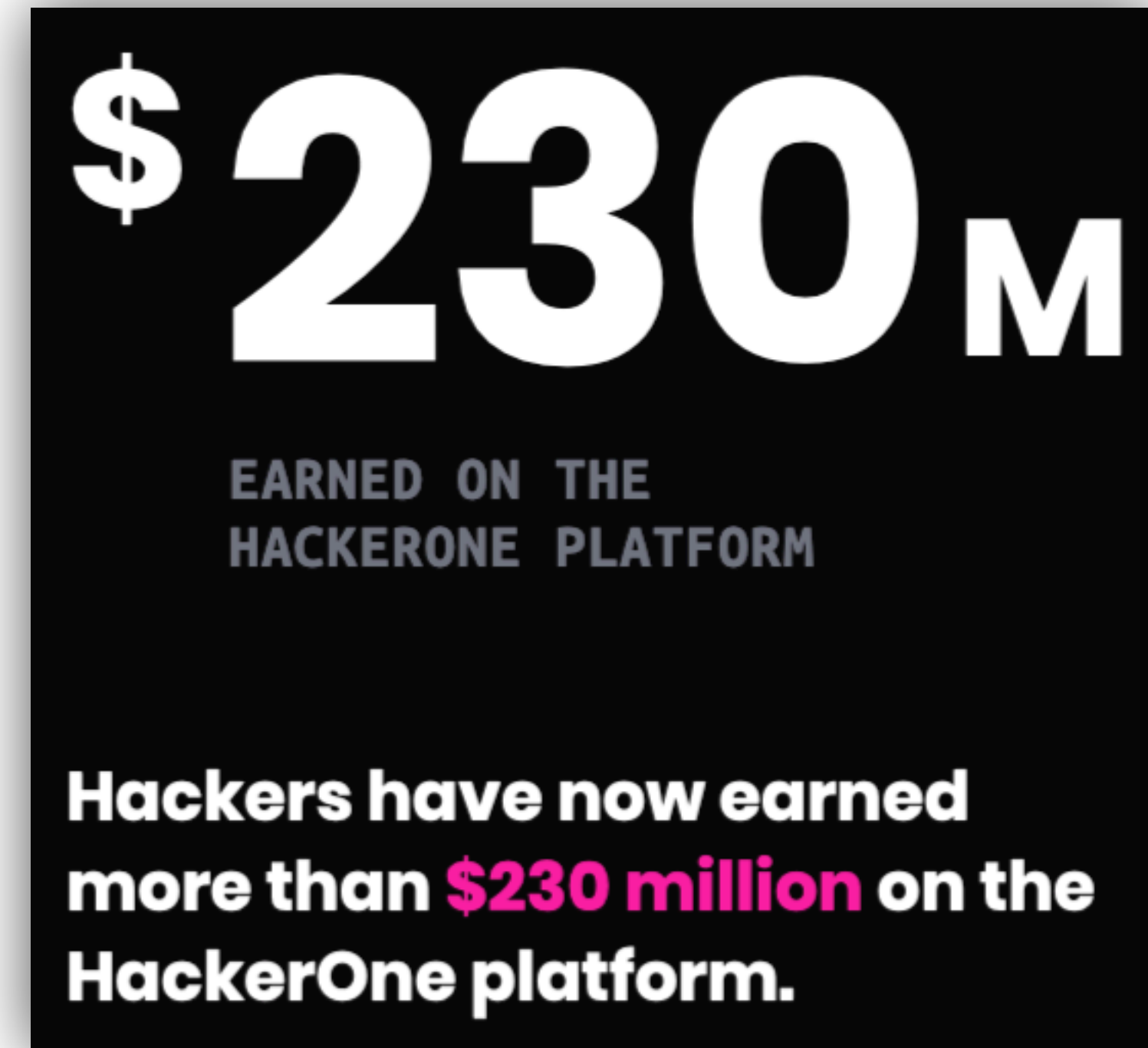Images from <u>hackerone.com</u>, <u>bugcrowd.com</u>, and <u>flaticon.com</u>

15

Benefits of bug-bounty?

✔️ Monetary rewards (#1)

$230M

EARNED ON THE
HACKERONE PLATFORM

Hackers have now earned
more than $230 million on the
HackerOne platform.

Benefits of bug-bounty?

✔ Monetary rewards (#1)

✔ Learning/improving skills (#2)

Images from hackerone.com, bugcrowd.com, and flaticon.com

Benefits of bug-bounty?

✓ Monetary rewards (#1)

✓ Learning/improving skills (#2)

✓ Fun! (#3)

$230M

EARNED ON THE
HACKERONE PLATFORM

Hackers have now earned
more than $230 million on the
HackerOne platform.

Benefits of bug-bounty?

✔ Monetary rewards (#1)

✔ Learning/improving skills (#2)

✔ Fun! (#3)

✔ Legal safe harbor (#4)

ExpressVPN

Help us improve the security and privacy of ExpressVPN users.
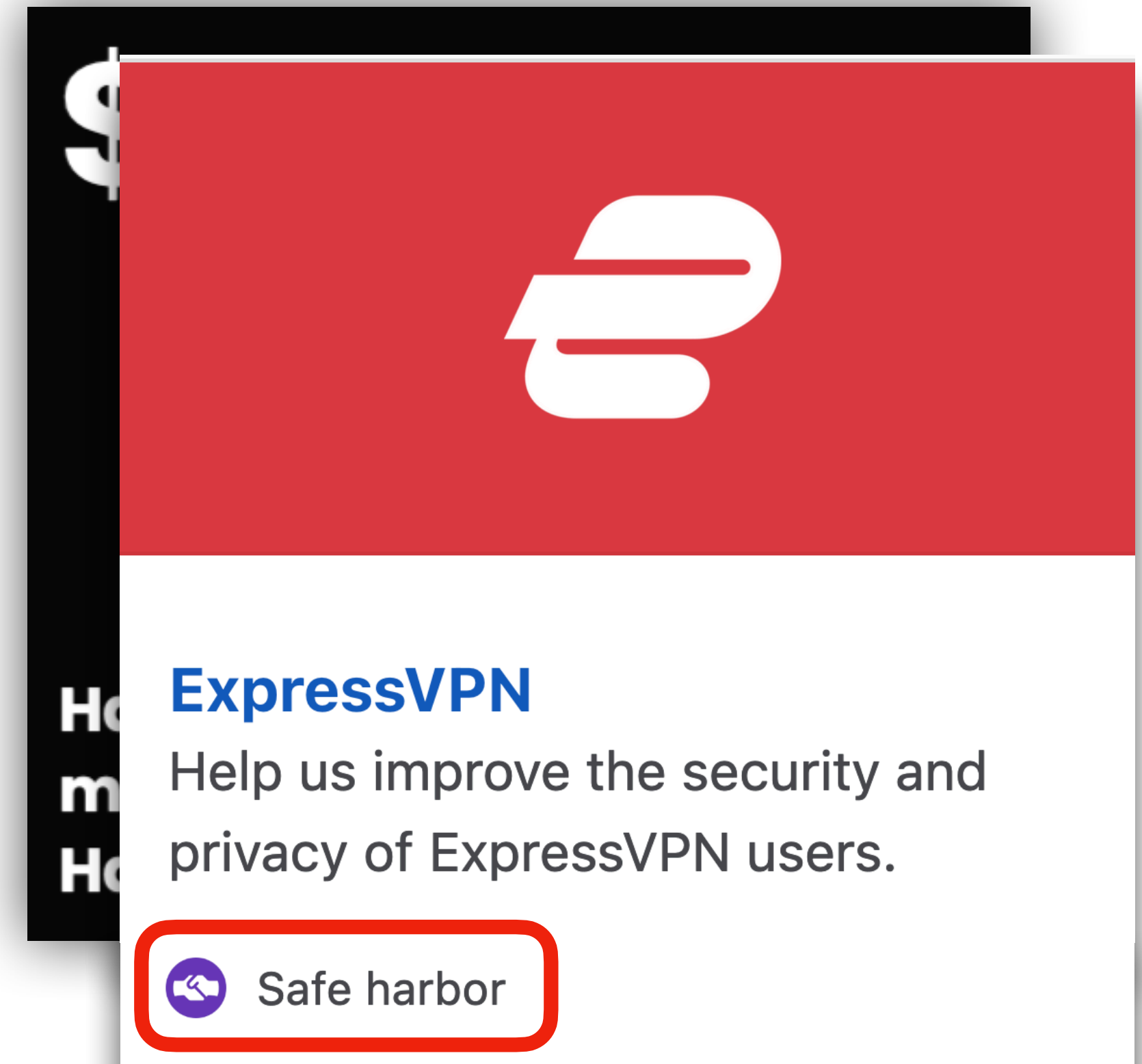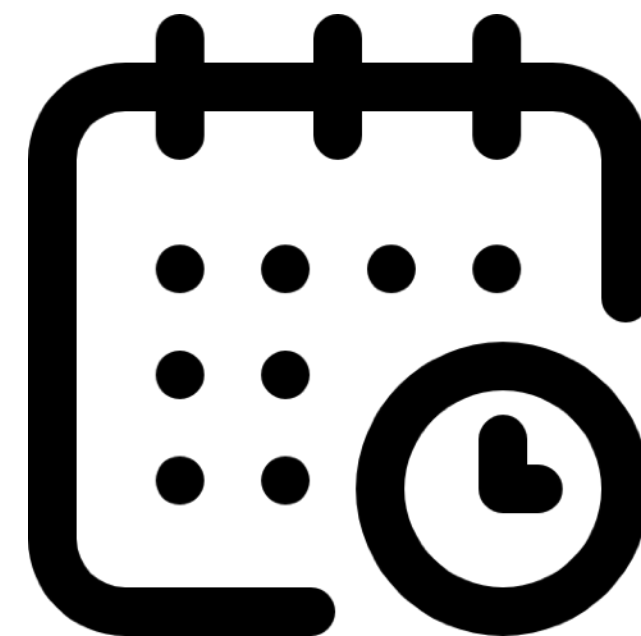
Safe harbor

Images from hackerone.com, bugcrowd.com, and flaticon.com

15

Benefits of bug-bounty?

✓ Monetary rewards (#1)

✓ Learning/improving skills (#2)

✓ Fun! (#3)

✓ Legal safe harbor (#4)

✓ Flexibility (#5)

ExpressVPN
Help us improve the security and privacy of ExpressVPN users.
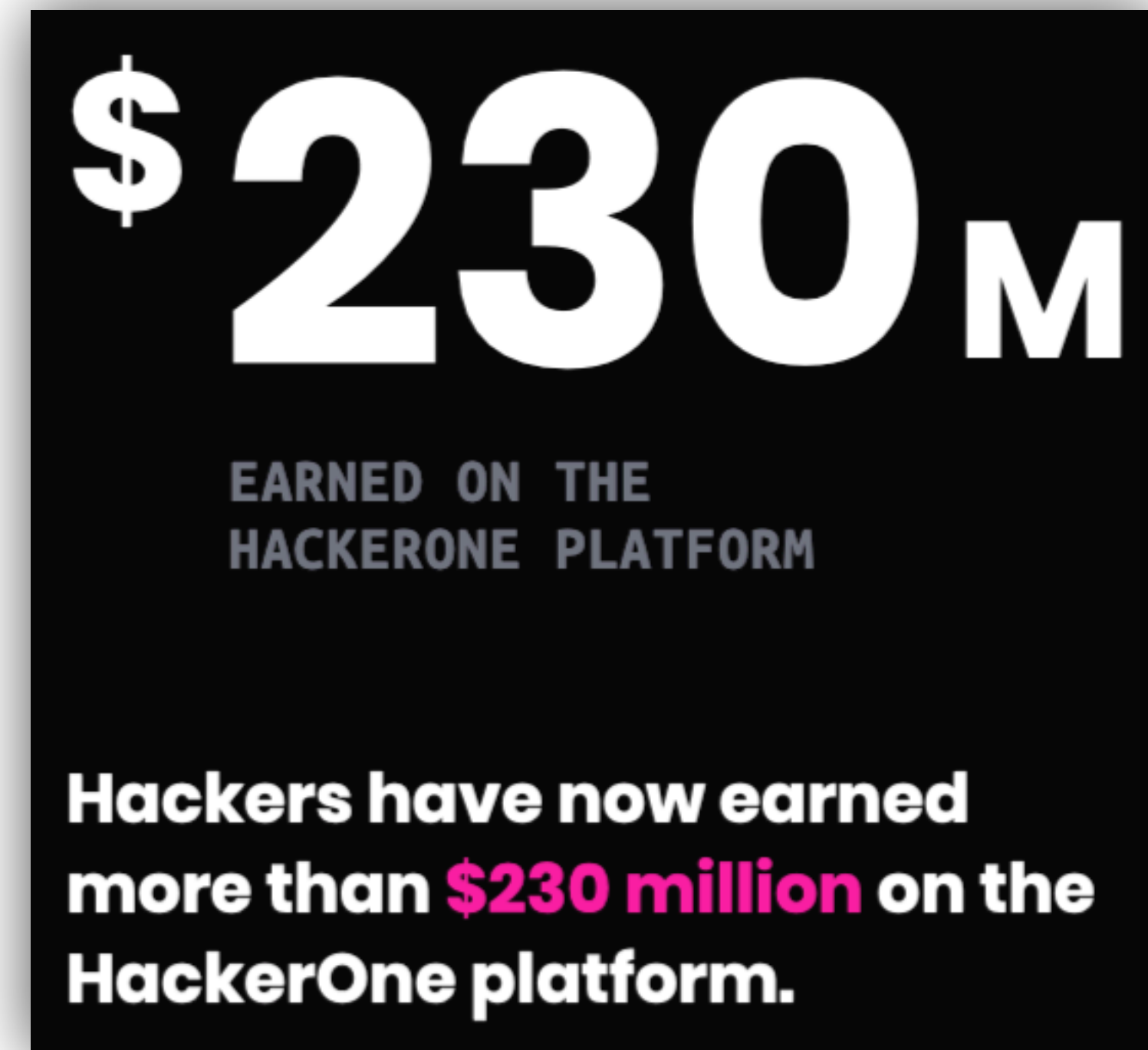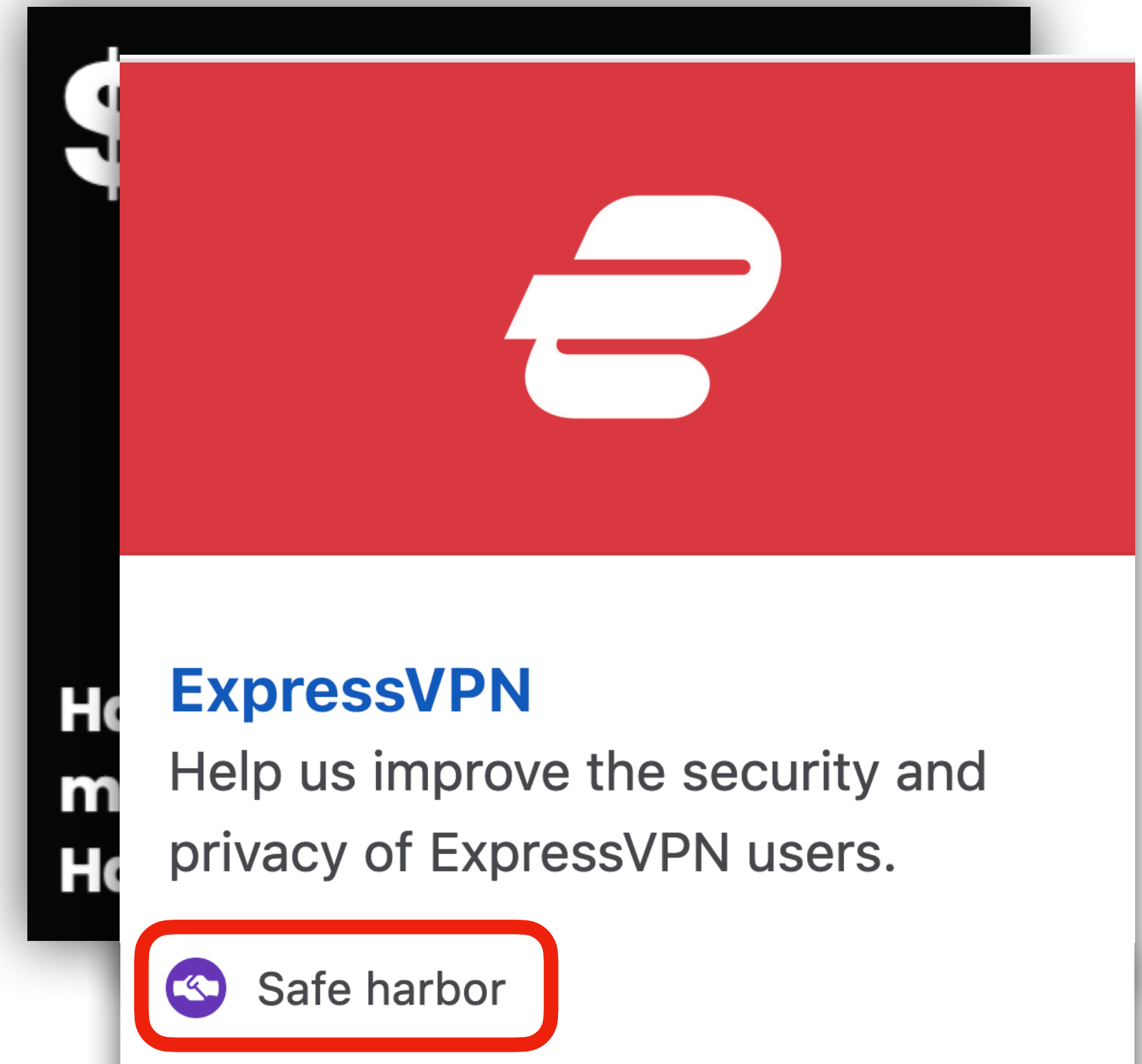
Safe harbor

Benefits of bug-bounty?

✔️ Monetary rewards (#1)

✔️ Learning/improving skills (#2)

✔️ Fun! (#3)

✔️ Legal safe harbor (#4)

✔️ Flexibility (#5)

❌ Reputation scoring (#9/10)
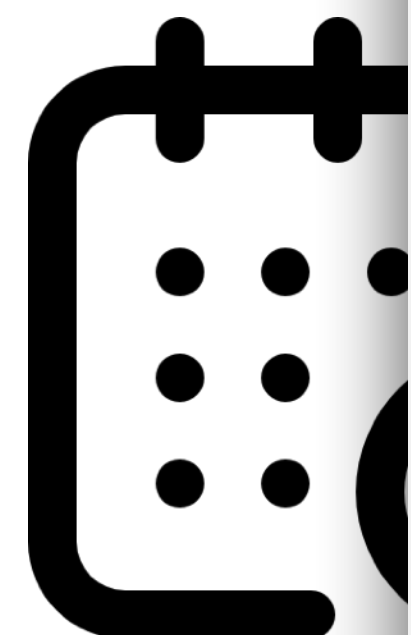
👑 All Time Reputation

Ranking is calculated based on the all time reputation earned.

			Reputation
1.		todayisnew	181685
2.		d0xing	103206
3.		try_to_hack	82217
4.		m0chan	47368
5.		sergeym	41066
6.		inhibitor181	33283

Which program to work on?

Which program to work on?

✔️ Scope (#1)

16

Which program to work on?

✓ Scope (#1)

✓ Tech familiarity (#4)

In Scope

https://hackerone.com

This is our main application that hackers and customers use to interact with each other. It connects with a...

Domain

Amazon DynamoDB   Amazon Web Services

GraphQL   JavaScript   PostgresSQL

Rails   React   Redis   Ruby   Unicorn

━━ Critical $ Eligible

https://api.hackerone.com

This is our public API that customers use to read and interact with reports. To look for vulnerabilities in this asset, create a ...

Domain

Amazon Web Services   GraphQL

PostgresSQL   Rails   Redis   Ruby

━━ Critical $ Eligible

Screenshots from hackerone.com and bugcrowd.com

16

Which program to work on?

✓ Scope (#1)

  ✓ Tech familiarity (#4)

✓ Reward (#2)

In Scope

https:/

This is
custom
connec

Domain

  Amazo

  GraphC

  Rails

https:/

read an
vulnera

Domain

  Amazo

  Postgr

Critical $ Eligible

Critical $ Eligible

Program Statistics
Updated Daily

$1,188,750
Total bounties paid

$300
Average bounty

$750 - $4,000
Top bounty range

$203,875
Bounties paid in the last 90 days

Screenshots from hackerone.com and bugcrowd.com

16

Which program to work on?

✔️ Scope (#1)

   ✔️ Tech familiarity (#4)

✔️ Reward (#2)

   ✔️ Bounty table (#3)

In Scope

Rewards

🔴 Critical	🟣 High	🟠 Medium	🟡 Low
$2,000	$750	$300	$50

Where monetary bounty is presented, eligible reports will be awarded based on our Awarding Process. For further details please review them under our policy section.

Last updated on January 14, 2020.   View changes

Eligible

Eligible

Postgre... $203,875

Bounties paid in the last 90 days

16

Which program to work on?

✓ Scope (#1)

  ✓ Tech familiarity (#4)

✓ Reward (#2)

  ✓ Bounty table (#3)

✓ Legal safe harbor (#5)

Screenshots from hackerone.com and bugcrowd.com

What are the problems?

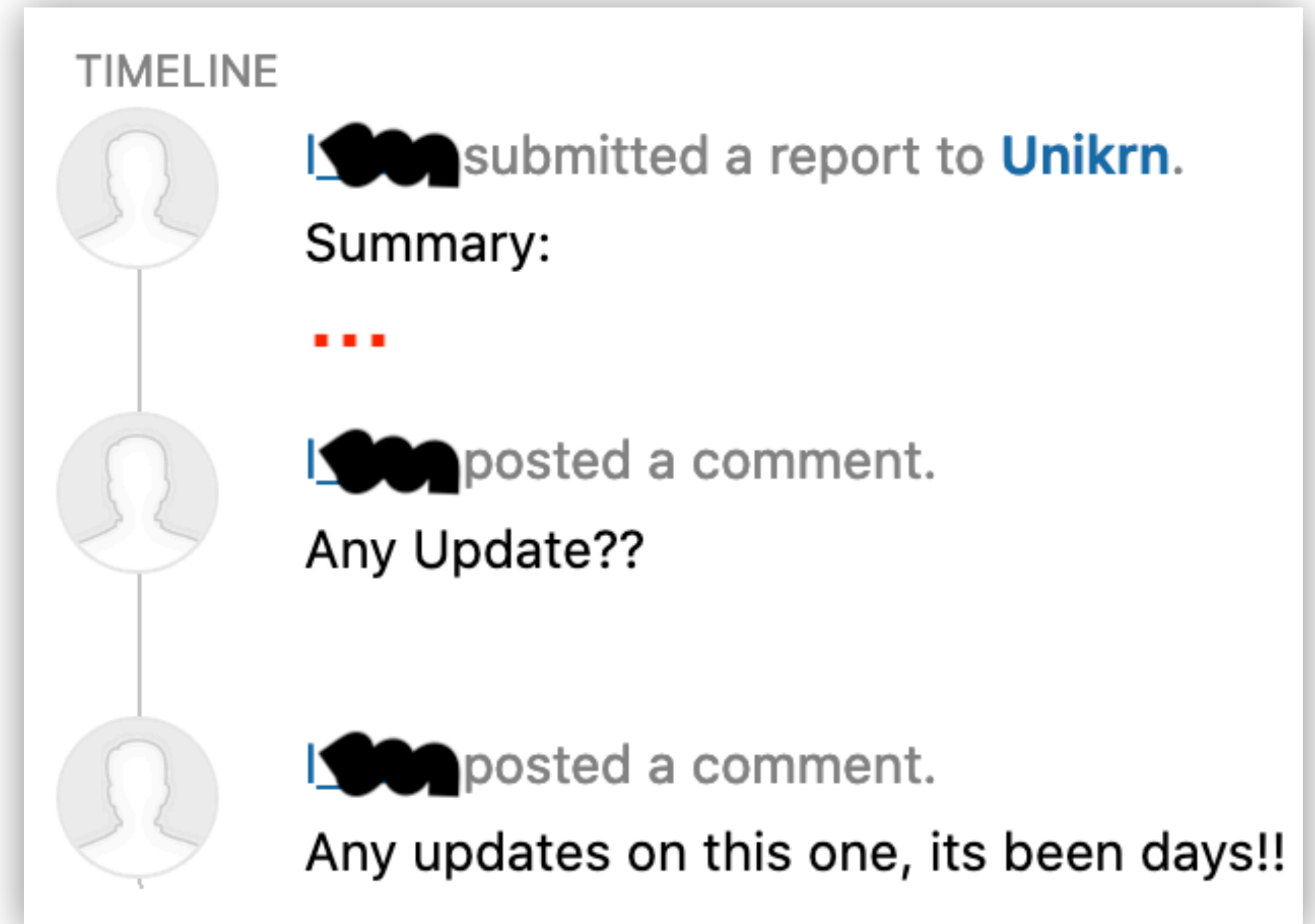# What are the problems?
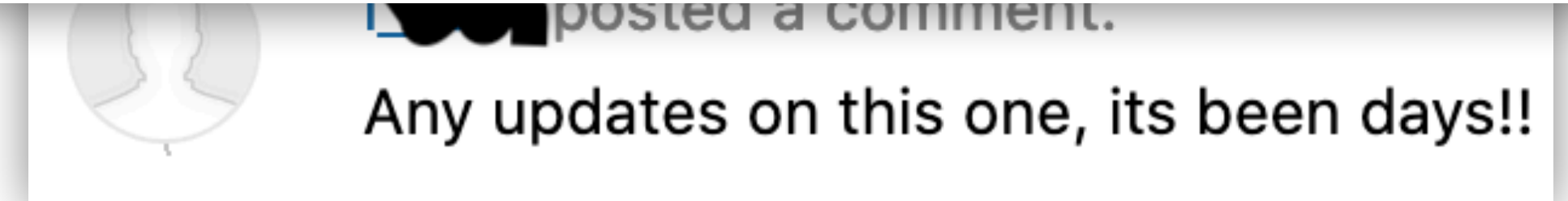
✴ Communication and disputes

What are the problems?

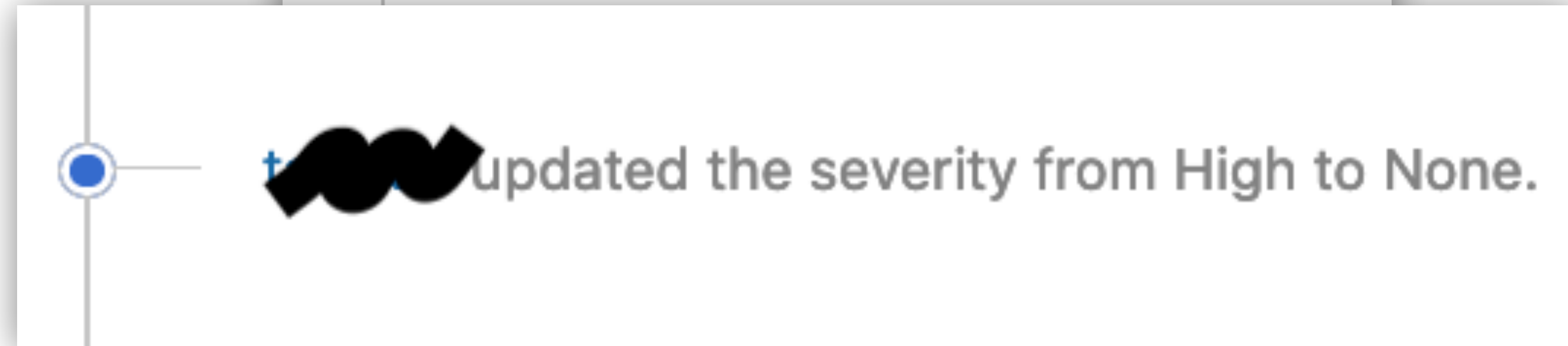✖ Communication and disputes

✖ Responsiveness (#1)

What are the problems?

✸ Communication and disputes

✸ Responsiveness (#1)

✸ Dissatisfaction with responses (#2)

TIMELINE

I⬛submitted a report to **Unikrn**.

Summary:

...

t⬛updated the severity from High to None.

I⬛posted a comment.

Any updates on this one, its been days!!

What are the problems?

✳ Communication and disputes

  ✳ Responsiveness (#1)

  ✳ Dissatisfaction with
responses (#2)

  ✳ Scoping issues (#3)

What are the problems?

✳ Communication and disputes

✳ Responsiveness (#1)

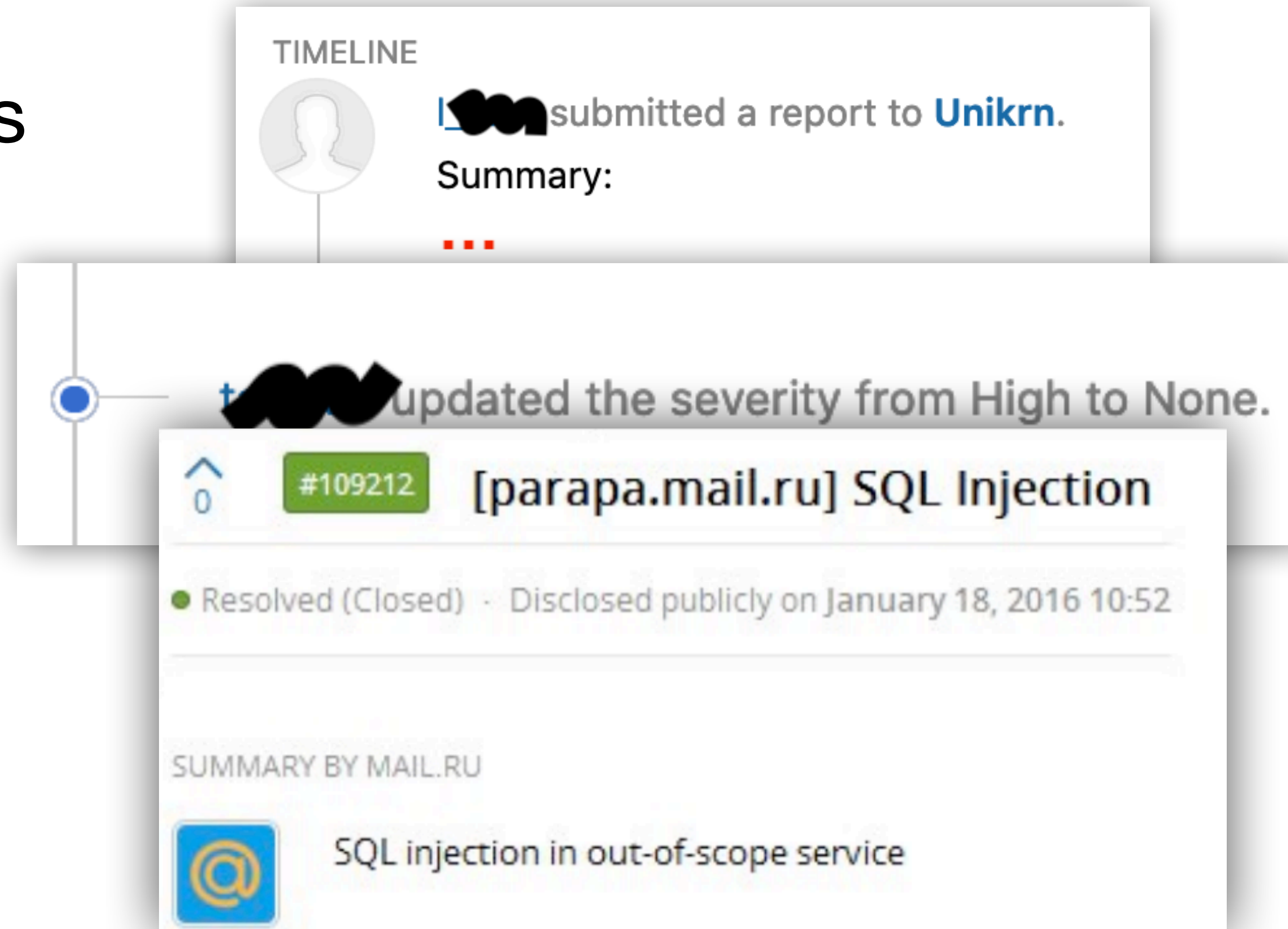✳ Dissatisfaction with responses (#2)

✳ Scoping issues (#3)

✳ Mediation dissatisfaction (#4)

TIMELINE

I███ submitted a report to **Unikrn**.

Summary:

...

t███ updated the severity from High to None.

⌃
0   #109212   [parapa.mail.ru] SQL Injection

● Resolved (Closed) · Disclosed publicly on January 18, 2016 10:52

SUMMARY BY MAIL.RU

@ SQL injection in out-of-scope service
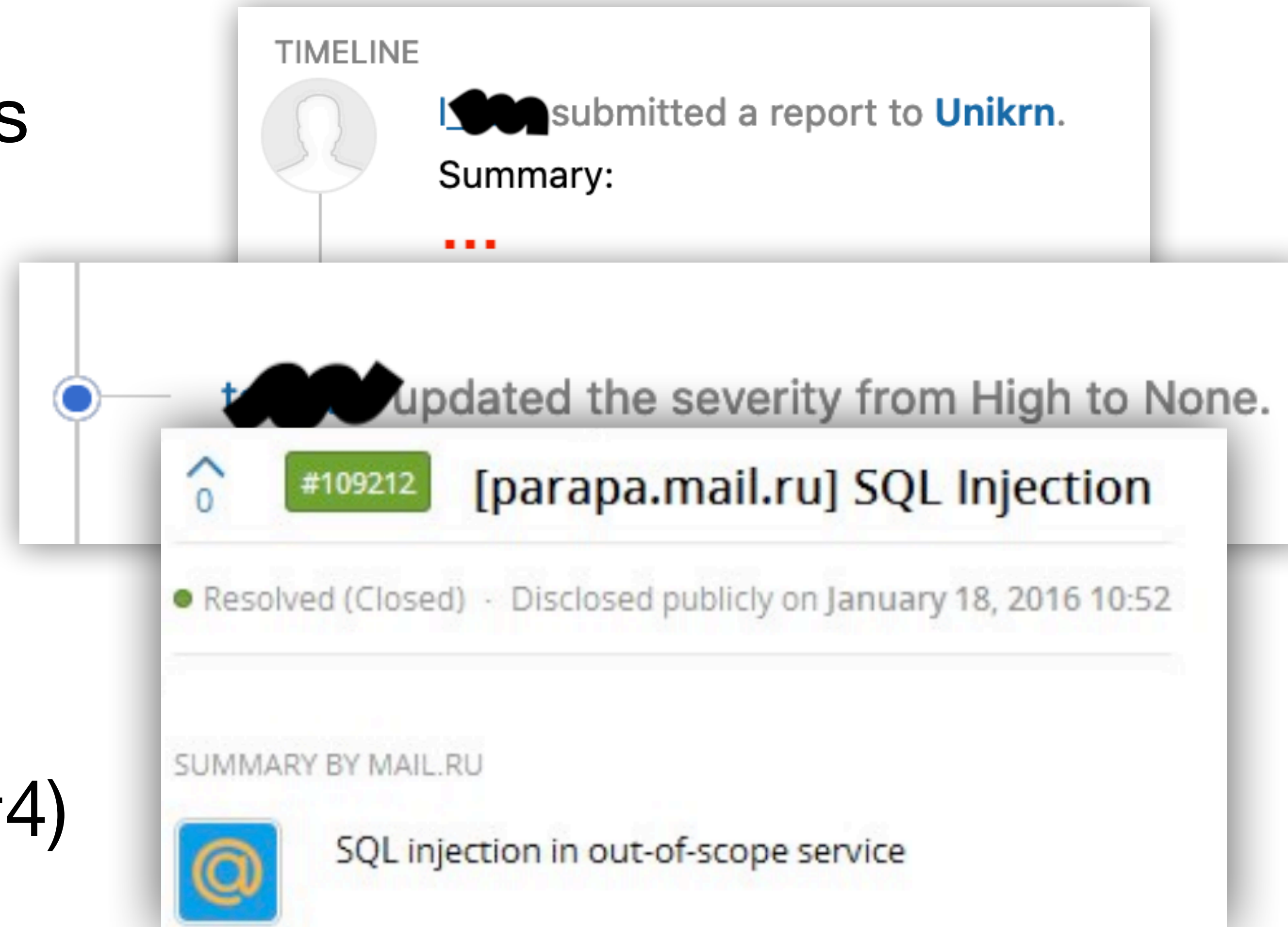
Potential troubling outcomes

Potential troubling outcomes

- From interviews:

Potential troubling outcomes

- From interviews:

  - Hunters quit/get deplatformed

Potential troubling outcomes

- From interviews:

  - Hunters quit/get deplatformed

  - Fixed but unacknowledged bugs

Potential troubling outcomes

- From interviews:

  - Hunters quit/get deplatformed

  - Fixed but unacknowledged bugs

  - Not reporting found bugs

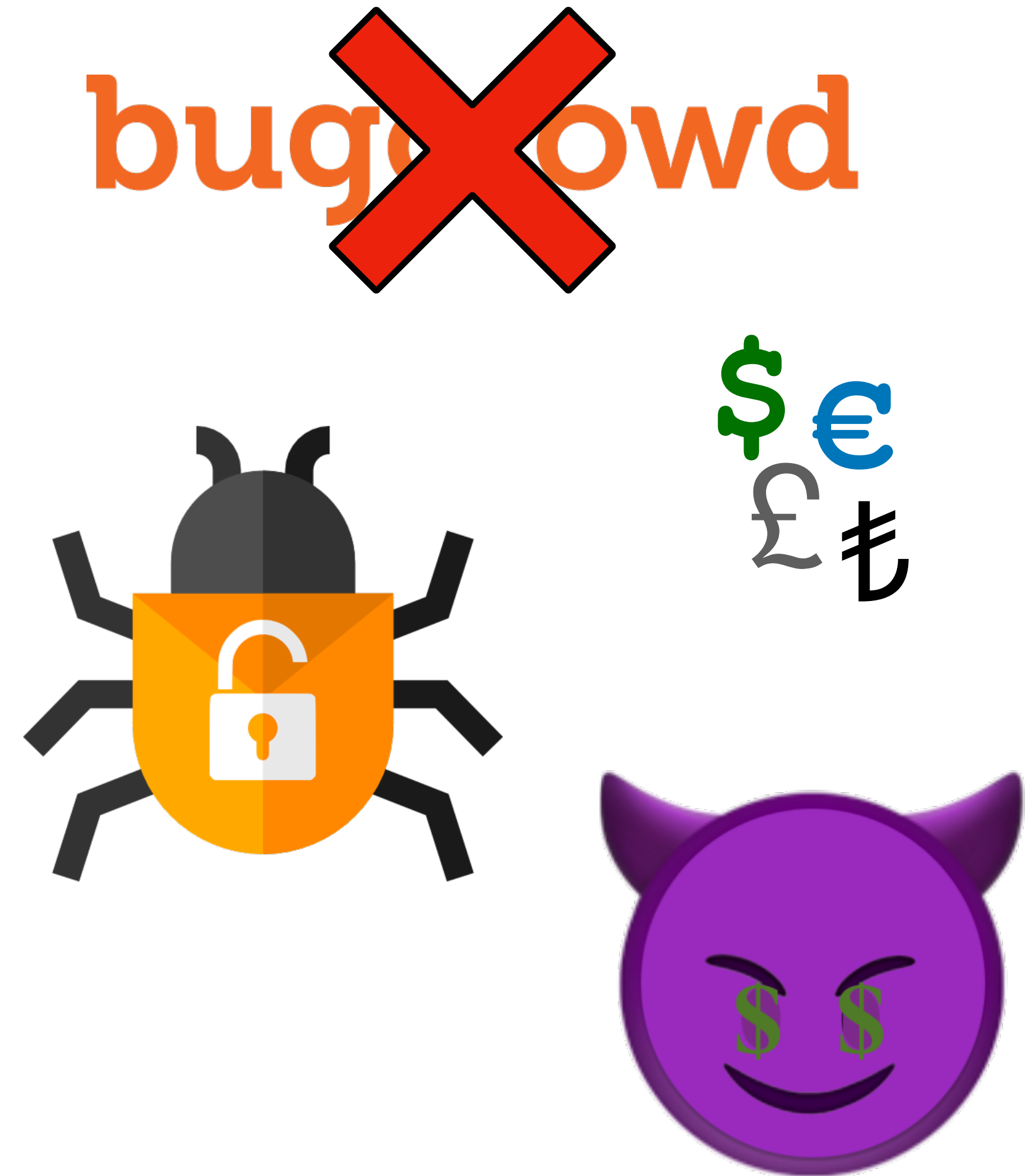# Potential troubling outcomes

- From interviews:

  - Hunters quit/get deplatformed

  - Fixed but unacknowledged bugs

  - Not reporting found bugs

  - Exploiting for fun & profit.

Some images from flaticon.com

18

What to do?

What to do?

- Bug bounty programs

Images from <u>flaticon.com</u>

What to do?

- Bug bounty programs

  - Look into impact of increased scope and rewards

Images from <u>flaticon.com</u>

What to do?

- Bug bounty programs

  - Look into impact of increased scope and rewards

  - Avoid common communication pitfalls

What to do?

- Bug bounty programs

  - Look into impact of increased scope and rewards

  - Avoid common communication pitfalls

- Bug bounty platforms

Images from flaticon.com

What to do?

- Bug bounty programs

  - Look into impact of increased scope and rewards

  - Avoid common communication pitfalls

- Bug bounty platforms

  - Perceptions of mediation

Images from flaticon.com

What to do?

- Bug bounty programs

  - Look into impact of increased scope and rewards

  - Avoid common communication pitfalls

- Bug bounty platforms

  - Perceptions of mediation

  - Focus on learning resources*

* HackEd: A Pedagogical Analysis of Online Vulnerability Discovery Exercises, S&P '21, Votipka et al.

What to do?

Policy makers?

- Bug bounty programs

  - Look into impact of increased scope and rewards

  - Avoid common communication pitfalls

- Bug bounty platforms

  - Perceptions of mediation

  - Focus on learning resources*

* HackEd: A Pedagogical Analysis of Online Vulnerability Discovery Exercises, S&P '21, Votipka et al.

Takeaways
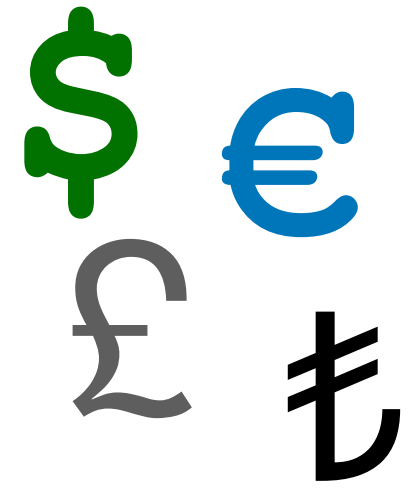
Takeaways

Bug bounty programs work
well for companies.

Takeaways

Bug bounty programs work well for companies.

What about the hunters?
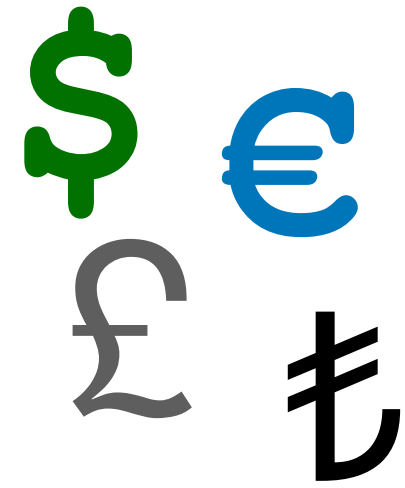
Takeaways

Bug bounty programs work well for companies.

$ € £ ₺

What about the hunters?

Rewards and learning are big motivators, reputation isn't

Takeaways

Bug bounty programs work well for companies.

$ € £ ₺

What about the hunters?

Rewards and learning are big motivators, reputation isn't

Scope is most important when choosing a program.

https://hackerone.com ━ Critical $ Eligible
https://api.hackerone.com ━ Critical $ Eligible

Takeaways

Bug bounty programs work well for companies.

What about the hunters?

Rewards and learning are big motivators, reputation isn't

Scope is most important when choosing a program.

https://hackerone.com — Critical $ Eligible
https://api.hackerone.com — Critical $ Eligible

Communication issues/ disputes are top challenges

Takeaways

 akgul@umd.edu
@_oakgul

Bug bounty programs work well for companies.

What about the hunters?

$ € £ ₺

Rewards and learning are big motivators, reputation isn't

Scope is most important when choosing a program.

https://hackerone.com — Critical $ Eligible
https://api.hackerone.com — Critical $ Eligible

Communication issues/ disputes are top challenges

20

Takeaways

Bug bounty programs work well for companies.

What about the hunters?

$ € £ ₺

Rewards and learning are big motivators, reputation isn't

Scope is most important when choosing a program.

https://hackerone.com ━ Critical $ Eligible
https://api.hackerone.com ━ Critical $ Eligible

Communication issues/ disputes are top challenges