5 ways to maximize hacker participation in your bug bounty program

BY ANNA HAMMOND · AUGUST 2, 2021 · LAST UPDATED ON MARCH 6, 2025

Our customer success team at Intigriti is often faced with the same question: How can we maximize ethical hacker participation in our bug bounty program?

To answer this query, we asked our security researcher community what their top reasons were for picking a bug bounty target as part of our Ethical Hacker Insights Report 2021. To help provide a little context, we're going to break down the numbers within this article and highlight five ways companies can make their bug bounty programs more attractive.

What makes a bug bounty program attractive to ethical hackers?

1. The scope

Every bug bounty program comes with a scope. This section details what ethical hackers can and cannot test. It also covers aspects like what vulnerabilities the program most wants to receive. Having a scope provides hackers with clarity—and the more precise it is, the more likely your program will receive high-quality reports.

So, what kind of scope appeals to ethical hackers the most? Ethical hackers are inquisitive people who enjoy a challenge. Remember, not all bug bounty hunters use bug bounty platforms to earn—70% use Intigriti's platform to develop their skillsets and 40% use it to discover new challenges.

What motivates ethical hackers to hack? [Source: The Ethical Hacker Insights Report 2021]

For this reason, the scope is a big attraction point. Within our report, 68% of security researchers said they seek out programs that offer a lot of scope. Similarly, 43% said they're most interested in programs with fresh scope, such as recently added elements to the bug bounty program.

How can you apply this to your program?

A scope that is overly prescriptive and strict may mean some researchers lose interest in the program. Alternatively, it may fail to appeal to researchers in the first place. A scope that includes more systems or assets to test, on the other hand, is an appealing target for ethical hackers. There are a few reasons for this:

1. Ethical hackers prefer to work with all available scope, including non-authenticated scope, so that they can mirror the activity of a malicious hacker.
2. It gives them the chance to learn whilst challenging their existing capabilities.
3. As they hack, they'll understand more about your organization, as well as your ecosystems and structure. The more they discover, the more intel they can gather into where your vulnerable security spots are.
4. You're providing them with more ways to find crown jewels.

Adding new targets and functionalities to test is a proven way to keep hold of the community's interest, and continuously engage them. Unlike penetration test solutions, enlarging your bug bounty program's scope is free on Intigriti and can be done at any moment. Additionally, we highlight newly released features to the community through regular email updates.

2. The bounty pay-out

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

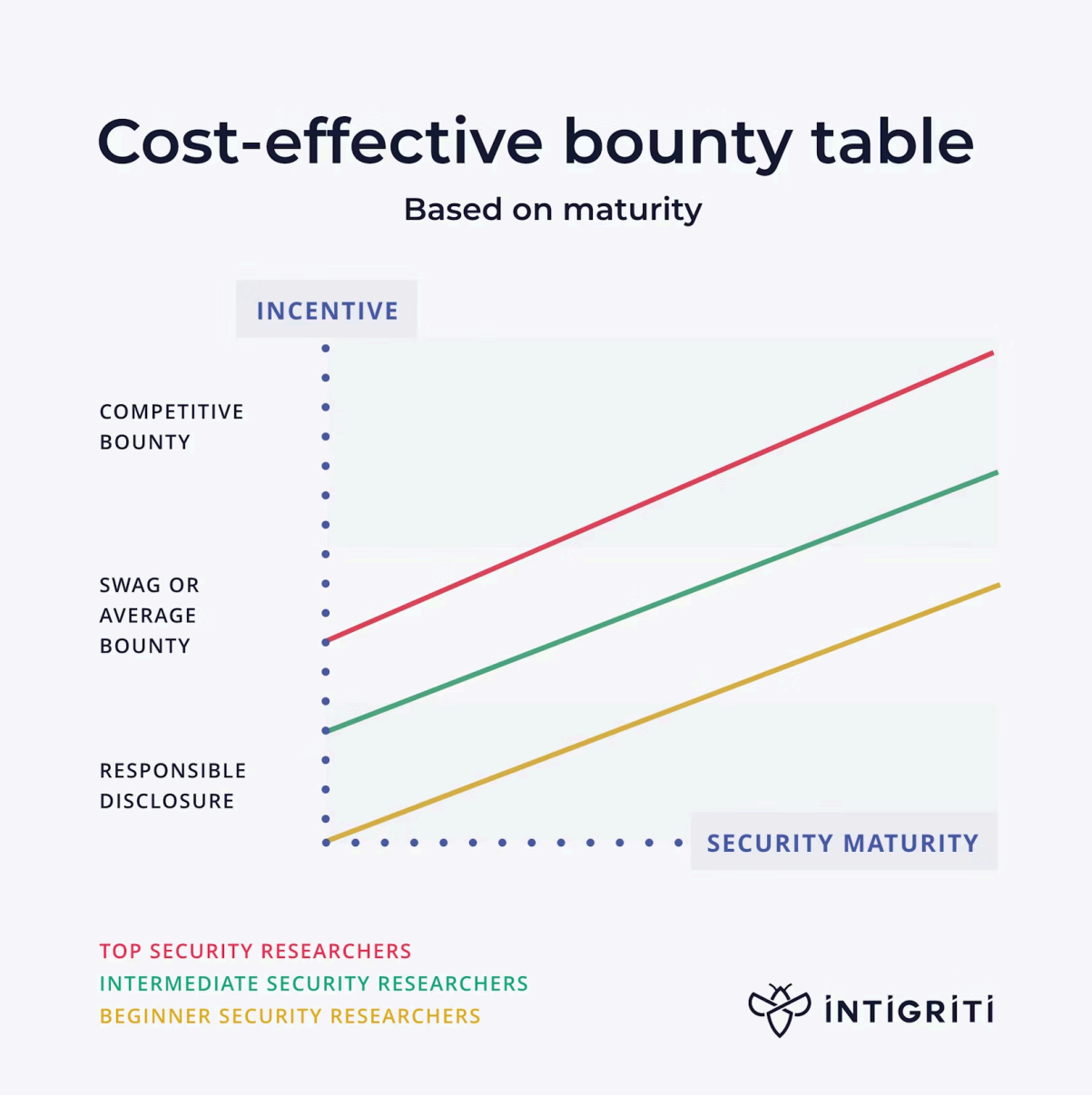
Ethical hacker money motivations [Source: The Ethical Hacker Insights Report 2021]

How can you apply this to your program?

When you're competing in the war for talent, you need to pay for value. The fastest way *not* to do this is to try and get submissions for as cheap as possible.

For researchers who know how a bug should be valued already, seeing a bounty that is far below the benchmark sends the wrong message—in other words, they perceive this as your business not taking the work of researchers seriously or understanding the value.

How to price your bounty table



Bounty table pricing based on security maturity [Source: Intigriti]

The bounty table determines what you'll pay researchers for alerting you to a low, medium, high, critical or exceptional vulnerability. This is the researcher's incentive.

Several factors need to be considered when pricing your bounty table. For example, you need to have a good understanding of the maturity of your assets. Some questions to know the answer to here include:

- Do we have a lot of low-hanging fruit?
- Do we consider our assets well-tested? How often have we had a penetration test or performed a red/blue team exercise?

- What other measures do we have in place which may make our asset mature? For example, Certifications, Scanning tools, or firewalls.

You also need to understand the bandwidth of your overall budget. We suggest spending at least the subscription amount in bounties and go as high as possible in bounty pay-outs, constantly evaluating the cost to the company if a malicious hacker would have found the vulnerability instead.

The earning potential of an exceptional bug is the crown jewel you're offering to researchers. On average, around 2% of reports are deemed exceptional, but in some cases, an exceptional vulnerability could be worth the entire budget because, if found by a malicious hacker, it could lead to a state of full compromise.

A few critical vulnerabilities are to be expected – so ask yourself what the real value of a critical vulnerability is to your business. Remember, you can choose a higher or lower bounty tier for specific assets based on their security maturity. An online retail brand may determine vulnerabilities found within its public website to be of a lower tier than the check-out section of its web-shop, for example.

3. The exclusivity

Considering that 21% of ethical hackers are motivated to hack because of the recognition they receive, it's not surprising that the feeling of exclusivity is another key driver to bug bounty programs.

Around a third (30%) of our community said they enjoy being part of a small, select team of hackers who are personally invited to take part in a vulnerability search. This is what is known as a private bug bounty program, rather than a public program that is open to any ethical hacker registered with the Intigriti platform.

A private program can only be seen by the ethical hackers that the client has hand-selected, meaning those hackers are recognized for their specific skill sets, experience, and expertise. By having fewer hackers involved, competition heightens—and as we already know, 40% of the community like the thrill of a challenge.

How can you apply this to your program?

If you're new to the bug bounty world, there is a real benefit of launching your first program privately. Going public straight away is not for everyone, mainly because you need to have a certain level of maturity in the field of vulnerability disclosure. A public program will gain visibility from researchers all over the world, bringing (a lot) more traffic to your systems. Without the proper mechanisms in place, this could cause some operational issues.

We typically advise our clients to start small until their team can happily handle the volume of submissions coming in, and implement patches. As your team becomes more efficient at managing this process, you can choose to switch your program to public if you desire.

4. The responsiveness of your team

According to the answers of our community, 42% look for a responsive team. Within Intigriti's interface, researchers can see an average first time to response. Having a bug bounty program is not about getting a one-time submission from individual researchers, but about building partnerships.

Kuromatae666, an Intigriti researcher who sits in sixth place on Intigriti's all-time Leaderboard, explains how he picks a target for bug bounty hunting:

> **"When I pick a target, the most important aspect to me is how the company responds – including the time they take to do so. Sometimes, I only report one or two vulnerabilities at first and see how they respond before sending others. To me, first impressions count.**
>
> *@Kuromatae666"*

Companies should want to keep their community of researchers engaged. They should encourage them to repeatedly test several aspects of their program—or even test a patch they introduced from the researcher's previous submission.

Pieter, who currently sits in second place within our all-time platform Leaderboard, provides more context on how he operates as a fully engaged hacker:

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

By working with these researchers' repeatedly, companies build trust and loyalty in their community.

How can you apply this to your program?

It's simple—ensure you respond to reports fast. To help provide some context around what "fast" means, here are some stats for you: On average, it takes less than 24 hours for Intigriti's triage team to review and accept or reject a vulnerability report. For customers to accept or reject a report, the average response time is 48 hours.

One way to get an understanding of your speed for handling submissions is to put it to the test. Start with a smaller group of researchers, and once you know you have more bandwidth, you can invite more participants. Even if you're not able to make a quick decision, ensure that you communicate with the researchers still. Thank them for their participation and let them know they'll get an update soon.

5. Your brand

If you're already a well-known brand, you have this attraction point on your side. Amongst our community, 22% seek out a familiar target when choosing a bug bounty program to participate in. However, you don't have to be world-famous to appeal to ethical hackers.

Bug bounty hunters like to hack on programs they're a customer of or heavily involved with. For this reason, we encourage clients to not only publish a program on our platform but establish a bond with the community too.

How can you apply this to your program?

You've already taken the first step in encouraging hacker participation simply by being on the platform. Intigriti ethical hacker, Pieter, explains why:

> ""This looks vulnerable" is a reaction that I have all the time to all sorts of websites. But I don't target them [when there is no vulnerability disclosure process in place].
>
> @Pieter"

However, if you want to maximize participation, there are ways you can drive engagement. At Intigriti, for example, we focus on partnerships whereby we invite local hackers to target local brands. We also drive engagement through a vulnerability reward program, leader boards, hacking events, education, and more.

The ethical hacker community also has a strong voice on social media, which can help spread your message that you're a security-first business further afield. Maintain the reputation you build by being open and communicative with your community and responding quickly.

Finally, 38% of our community are on the platform to have fun! Keep that in mind when creating your program's scope and engaging with the community.

When in doubt, your customer success team can help

These tips are a surefire way to maximize ethical hacker participation in your bug bounty program. However, we understand that it's a lot to consider. For that reason, we apply several layers of customer support for clients—no matter whether you're our newest or oldest customer. From preboarding to onboarding to triaging and program management, we're here to ensure your bug bounty program reaches its greatest potential.

Interested in inviting ethical hackers to contribute towards your security testing? Speak to a member of the Intigriti team today to request a demo.