Nurturing program engagement: Easy steps you can take to keep your bug bounty program ticking

BY INTIGRITI · MARCH 1, 2023 · LAST UPDATED ON MARCH 6, 2025

How to optimize your bug bounty program for long-term success.

Bug bounty programs often have a whirlwind start. In those first few weeks, the submissions can come thick and fast. SecOps and development teams are kept busy fixing important issues. Stakeholders begin to relax as their investment becomes justified. Sound familiar?

This is often the start we see in **bug bounty programs** at Intigriti. It can be exciting to see how some of the best researchers in the world test your assets. But as the dust settles after those first few weeks, you might start to notice that activity on your program becomes a little quieter. This might initially come as a relief because it gives your team chance to catch their breath and work through the backlog of issues found. However, it will eventually be time to try and boost your program's activity again.

In this blog post, we explore how you can manage your VDP or bug bounty program in a way that delivers the greatest return on your investment. By explaining how programs on the Intigriti platform operate within an open marketplace, we will show you how to compete with other companies on the platform for the attention of the top security researchers. By making your program as enticing and interesting as possible, you can ensure you stand out from the competition.

Intigriti aims to make the growth of your program as easy as possible, and our Customer Success team is here to guide you through it every step of the way. Here are some steps you can take to build a top program:

Interest

As with any open market, bug bounty researchers have a lot of choice when picking a program to test on. Intigriti now offers hundreds of bug bounty programs, which means you need to stand out from the crowd to attract the very best researchers.

Although rewards and incentives are key, hackers also want to find their research interesting and fulfilling. When you look at growing your program further, remember the following:

- **Give the researchers plenty to test** – If your assets are mature, then you should be asking if there is any reason *not* to add them to your program. Malicious hackers who operate outside of bug bounty programs do not consider anything 'out of scope' and they do not follow any specified rules of engagement. The sooner you can get your assets onto your bug bounty program, the sooner they can be secured against these threats.

- **Reward good findings generously** – Reputational damage, downtime, and data loss are just a few of the potential scenarios resulting from a cyber-attack. One thing they all have in common is they cost a business money. Bug bounty is another tool in your arsenal to avoid these scenarios. But improving its effectiveness requires financial backing. To generate interest and earn the loyalty of the best hackers, generous bounties should not be overlooked.

- **Build a rapport with the researchers** – Since Intigriti is an open marketplace that connects researchers and companies, building positive working relationships with security researchers is essential. Engaging with researchers on submissions, speaking to them in the comments as you would fellow cyber security professionals, and letting them know you appreciate their efforts all go a long way to ensuring the best researchers favor your program above others on our platform.

- **Make your program clear and easy to understand** – Adding helpful guidance on how your tech stack works, including documentation and detailed FAQs, as well as adding information to the program on areas or vulnerabilities you particularly want to focus on, is a good way to ensure a researcher's time is spent testing the things you want them to.

Researchers are testing on your program – great! But how do you keep them coming back time and again? This is where a bit of creativity comes in. By making your bug bounty program enjoyable to work on, providing fresh scope and challenges, and marketing these effectively, researchers will keep coming back to test your assets. Here are some recommendations for how to market your program properly:

Engagement

- **Regular program updates** are a great way to keep hackers engaged. Our researchers regularly tell us what they are looking for in a program, and they want companies to keep them up to date with any new developments. Intigriti's program update tool is the perfect way to tell our community about any new feature or product releases that are in-scope. If you increase the bounties or change the terms of engagement, you should also share this with your program's community. We recommend sending an update email every month.

- **Bonus campaigns** can generate a lot of excitement for a program when they are done well. There is an inherent level of gamification built into bug bounty. Researchers compete to find the most bugs, earn reputation points, and move up the leader-board. You can channel this into your program by offering bonus rewards to the top-performing researchers on your program or running capture-the-flag competitions.

- **Social media announcements** are a quick and easy way to attract attention to your bug bounty program and keep your community of researchers informed. Additionally, we at Intigriti firmly believe that launching a bug bounty program should be something to celebrate. If you have a public program and want to explore how to make some noise on social media, speak to your CSM.

- **Join the Bug Bounty Forum on Slack** to keep your finger on the pulse of the hacking community. Researchers will often post useful information about the latest security news and trends. Keeping an eye on the Bug Bounty Forum will help you keep up to date with the newest vulnerability announcements and write-ups.

Loyalty

By harnessing interest and boosting engagement on your program, you will soon develop a loyal core of researchers. To foster loyalty in bug bounty, it is important to support a peer-to-peer relationship between your company and the security researchers. Some of the ethical hackers working on your program will be amongst the most talented and experienced security professionals in the world, and their expertise deserves to be recognized as such. To develop loyalty among the community of hackers on your program, these three things must become *your* rules of engagement:

- **Remember to respond in a timely manner.** No one wants to wait for weeks to find out if they are getting paid.
- **Explain the decisions you take on a submission.** Leave the cliff-hangers to HBO.
- **Thank researchers for their efforts.** Good manners cost nothing.

But don't just take our word for it. We speak to security researchers every day, and they often tell us what they are looking for in a bug bounty program. Here's what one of our researchers has to say about what keeps them coming back to programs time after time:

> ***"I have three things that keep me coming back to the assets of a bug bounty program: Responsiveness is important; if I get fast responses on my reports, I am eager to keep looking for more bugs. Also, I am kept engaged when a company updates their program regularly, so when new updates/features come out or when new scope is added. Making it easy to start testing is also important for when I come back to their assets, so test accounts being created for us helps, as does preventing complicated setups."***

It takes a long time to build a bug bounty program's positive reputation among the community, and only moments to destroy it. Researchers reward loyalty to them by giving up more of their time for testing on the programs they like. If they are not shown loyalty and respect by a program, they won't come back to test on it again.

The program managers who accept their responsibility to build a community on their program based on mutual respect and consideration see exponentially better returns.

Following this guidance will ensure the community you build through your program is a happy one. Here are some final insights from a top 10 hacker at Intigriti:

"For me personally there are a few key reasons I would go back to an existing program.

- *Higher bounties*
- *New scope with good bounties (Not within a Tier 3 with low bounties)*
- *A program update with a changelog of new features*
- *Addition of demo / test accounts with more features to test*

I think the most important one here is higher bounties. The existing scope has already had many eyes on it before, so the chance for us to find vulnerabilities is lower. By increasing the bounties (> 50%), it makes it worth it for us to take a second look at it. There are also some things that will prevent me from ever visiting a program again:

- *Misleading bug bounty table (Using a 'fake' Tier 1 with bounties that will be paid as a bonus at the "discretion" of the company)*
- *Bad experiences with the company (bad communication, incorrectly lowering severities of submissions, etc.)*
- *Annoying setup for accounts (having to spin up own web servers, KYC processes for signup which require manual approval, etc.)"*

RELATED: The 3 key stages to setting up and managing a bug bounty program