How to prepare for launching a bug bounty program [Part 2]

BY ANNA HAMMOND · MAY 4, 2022 · LAST UPDATED ON JULY 14, 2025

If you came here from our first article in this series on the bug bounty process, we'll assume you're now preparing for launching a bug bounty program.

In this second article in the series, we're going to set out the seven simple steps you should take to get ready for launching a bug bounty program. And, as we said in the first article, don't be daunted: using a modern, SaaS-based, bug bounty platform like Intigriti can actually be fun!

Note: This is the second in a series of four articles on "What to expect from the bug bounty process, from setting up to post-launch."

The 7 simple steps for launching your bug bounty program

1. Define objectives

Your first step in preparing your bug bounty program will be to define your business objectives. One organization's goals in running a bug bounty program may differ greatly from another's, so you need to be clear what *you* want to achieve.

Here's one good example of clear business goals from an Intigriti customer, Bram D'hooghe, Director of Security, Privacy & Compliance at Showpad:

> "*Customer trust* ***for us is key. If we don't have customer trust, we won't sell our product. Therefore, we need to be on top of our game with regards to our privacy and security.***"

"Trust" is an important business objective for many SaaS companies that store a lot of sensitive and mission critical customer data. Other typical areas to consider are data security and business viability. For example:

- "We need ***continuous security testing*** that can match the pace of our agile development release cycle." Or;
- "As an organization that stores rapidly changing essential logistics data, we need to ***protect against data breaches*** that would disrupt the supply chain."

Remember that security today is both mission critical and a hot zone for potentially serious reputational damage. Your first bug bounty program is going to help protect your mission and your reputation. So, what areas of your business do you most need to protect straight away? Write those goals down and keep them beside you—we'll return to them as we progress.

2. Prepare your systems with standard security procedures

You should run standard cybersecurity procedures and tests *before* starting your bug bounty program. Doing so will ensure you patch obvious and overseen security loopholes that shouldn't need a bug bounty attached to them.

The first step will be to make sure all of your software is up-to-date and patched with the latest security fixes. Additionally, you should run automated vulnerability scanners, and if your budget permits it, you could run a pentest as well. Perhaps you have internal procedures for maintaining security? Make sure those are up-to-date too.

Essentially, you want your organization's cybersecurity running at its highest level. Only then, should you invite crowdsourced ethical hackers to start testing your attack surface.

One Intigriti customer who quickly grasped the value of this approach was CISO of Brussels Airlines, Jean-François Simons:

> *"I see pentesting as a security test that you take before going to a bug bounty program. It's like a cleanup. If you start with bug bounty straight away, you might be in for an unpleasant surprise."*

Remember, a bug bounty program involves pitching your cybersecurity against crowdsourced, real human ingenuity—and there are some things humans still do better than machines.

3. Decide on a platform

Your next step will be to choose a platform for your bug bounty program. Some companies choose to host their own programs but most will choose a dedicated bug bounty platform. There are some significant benefits to using a platform, like Intigriti, over a self-hosted platform:

- **Program engagement** is very active. Security researchers are continuously engaged through bounty opportunities, points and reward systems, leader boards, hacking events, education, and more.
- **Vulnerability disclosure policy requirements** are advised but not required because a good platform simplifies and guarantees the submission process.
- **Validating submissions** (in the case of Intigriti) is handled by an internal Triage Team. This can save internal teams hours, if not days, sorting through vulnerability reports.
- **Handling communications** is done within the Intigriti platform, making it easy for clients to ask questions. A triage department works as the go-between for client and researchers, but companies can also directly message researcher(s).
- **Budget allocation & payment processing** is handled by the platform and processed automatically after a submission is accepted by the organization. Payment and administration are taken care of by the platform, saving admin time and also maintaining good relationships between customer and ethical hackers.
- **Disclosure agreement** is set within the platform as part of the Community Code of Conduct. Researchers must agree not to disclose reports publicly unless given permission. In short, you know you can trust the hackers working on your bug bounty program.

4. Define the Program Scope

Now we get into the nitty-gritty of preparing your bug bounty program for launch. This is where having clear business objectives (see step one) will help.

It would be impractical to outline every possible parameter companies might consider test-worthy in this article, but here are some broad suggestions to help get you started.

Private or public

A public bug bounty program is openly published and invites all registered security experts to take part. A private program is not made public and only a select group of hackers are involved in the security testing. Private programs are perfect when you have a specific testing scope, such as mobile app hacking.

The attack surface areas where security experts should focus

You need to be very clear here. It's a good idea to speak to your entire security and IT team, if possible, and make sure that you have a complete picture of your attack surface. Once you've done this, you should establish a list of security priorities based upon your business objectives and where you think the greatest areas of cybersecurity weakness lie.

Configuring the scope of your bug bounty program in the Intigriti platform is a step-by-step process that is well documented in our knowledge base (check out the "Program management" section).

5. Set bounties

With your platform selected and your scope in place, you'll next want to set your bounties. If this is your first bug bounty program, begin by learning about what motivates ethical hackers. While monetary reward is a factor, it is not the only reason ethical hackers will join your program. Learning, reputation and swag are among the other reasons for participation.

When it comes to deciding how much to pay, take a look at our publicly listed bug bounty programs page. This will give you a good idea of the range or bounties other businesses offer.

The level of bounty you set will play a role in determining which researcher profiles your bug bounty program attracts—from beginners to full-time professionals.

Setting a bounty within a platform like Intigriti is thankfully very easy. You'll be able to apply the priorities you established in step 4 above via a bounty tiers table, where you can set rewards based on severity of vulnerability (hint: it's much simpler than it sounds).

6. Get your team onboard

In short, if you haven't prepared your team, you may rub people up the wrong way. You'll also risk putting stress on resources as the work required to patch discovered vulnerabilities builds up.

Without doubt, bug bounty programs are disruptive because they are much more effective at revealing unknown vulnerabilities than most other security methods.

If you and your team have been running a pentest once in a while and feel confident about your organization's security, a sudden flurry of vulnerability reports can be overwhelming. Also, a significant

part of the value of bug bounty programs comes from their being a continuous process. This means vulnerabilities are likely to be discovered more quickly and regularly than your team is used to.

So, here are some points to address with your internal teams *before* launching a bug bounty program:

Speed

Let your team know they are potentially going to face newly discovered vulnerabilities faster than before. This is actually a benefit—you're staying ahead of malicious hackers!

Responsibility

Bug bounty programs are highly effective at uncovering *unknown* vulnerabilities. Before going live, make it clear that the consequences of a vulnerability discovery will not be a blame game. The goal is to harden security and to learn from what is discovered.

A Modern Method

Explain that this type of security testing is well suited to the modern reality of agile development and SaaS, cloud, etc. deployments. It is continuous and delivers results frequently and rapidly. In other words, it can keep up with the pace of development and the efforts of malicious hackers, unlike vulnerability scanners and irregular pentests.

Hackers

The word "hacker" can send a shiver down the spine of IT departments. You might diplomatically decide to explain the benefits of working with crowdsourced "ethical hackers"— also known as "security experts" or "security researchers".

And if you're questioned as to why you'd want to invite a globally diverse crowd of hackers to pummel your systems, you could quote Thomas Colyn, CISO of DPG Media:

> "*[By launching a program] organizations can use the creativity of thousands of ethical hackers' minds—and that is far stronger than using automation or general algorithms to discover difficult to find vulnerabilities.*"

Cost

When it comes to asking for a budget for your bug bounty program, you might hear: "We just ran that crazy expensive pentest—why do you need more budget?" The answer is that both short and long term, bug bounty programs are more cost-effective than pentests, and they provide a higher level of cybersecurity against malicious hackers.

For a real world quote, try Yannick Herrebaut, Cyber Resilience Manager & CISO Port of Antwerp:

> "*The amount and the quality of reports from the responsible disclosure program were a lot higher than what was discovered during the pentest, and at a fraction of the cost.*"

Or better yet, share the full video interview.

Limits

A bug bounty program provides great security, but it doesn't mean your company is immune to attacks. Prepare for attacks on your program's credibility by explaining clearly the scope of your testing. For example, if you experience a security breach as a result of an out-of-scope phishing attack, it should be clear this is not a failure of your bug bounty program.

Learning

A last benefit that development, engineering and IT teams can look forward to is the quality of security reports you receive. Many organizations find these make excellent training tools. For example Bram D'hooghe, Director of Security, Privacy & Compliance at Showpad, explains:

"[Intigriti vulnerability reports provide] examples we now use in our training towards our engineering team so that they get this information upfront in their development life cycle."

7. Do your Preflight Check

Ready to launch? Not so fast! By now, everything should be set up and ready to roll. But remember the old carpenter's maxim: *Measure twice, cut once.*

Good news is, this is actually the easiest of the seven easy steps, because we have a bug bounty program launch checklist ready for you to run through in our Knowledge Base.

Ready to launch your bug bounty program?

That's it for our seven steps in preparing to launch a bug bounty program. It's straightforward and promises high dividends in terms of your organization's cybersecurity. If you'd like a refresher on how effective crowdsourced cybersecurity is, why not take a look at some customer success stories?

And don't forget to come back here soon for the third article in the series: What to consider when *launching* a bug bounty program!

Learn more

Intrigued by what you have read? Want to know more about bug bounty programs? Get in touch to request a demo with a member of our team today.