How to prepare your internal team for launching a bug bounty program

BY ANNA HAMMOND · JULY 27, 2022 · LAST UPDATED ON MAY 5, 2026

Bug bounty programs are an excellent way for organizations to find and resolve cybersecurity vulnerabilities. However, to maximize success, it's important to include this essential pre-step: the need to prepare internal teams when launching a bug bounty program launch.

To help guide you through the process, this article covers all the steps in getting your internal team ready to launch a bug bounty program. Thankfully, it is simple and falls into two categories:

- What your team should expect when implementing a bug bounty program
- What will vulnerability reports mean in terms of work and responsibilities

Let's take a look!

What your team should expect when launching a bug bounty program

A significant part of bug bounty programs' value comes from a continuous cybersecurity process. This means vulnerabilities could be discovered more quickly and regularly than your team is used to. It's precisely why huge names like Intel, Apple, and Google run programs.

In the modern workplace, cybersecurity is a necessary practice for every employee. Ideally, you should discuss the following points with *all* your internal teams before launching your bug bounty program to avoid any misapprehensions:

1. Get ready for speed

Let your team know they are probably going to see vulnerabilities come in thick and fast. This is actually a benefit! You're staying ahead of malicious hackers. Still, it can feel overwhelming if you're not ready for it.

Bug bounty programs are highly effective. However, if you sense some nervousness from your team, share a couple of success stories from other organizations that show why continuous cybersecurity is an excellent approach.

2. Bug bounty culture isn't about blame

A bug bounty program will almost certainly uncover vulnerabilities. Let your security team know that this won't lead to a blame game. The goal is to harden security and to learn how to improve it, not point fingers.

3. Bug bounty programs are the right approach

Crowdsourced security testing is perfectly suited to the modern reality of agile development, SaaS platforms, cloud storage, and more. This continuous method of testing can keep up with the pace of development cycles and software updates. It is something vulnerability scanners and irregular pentests cannot do as effectively.

4. Not all hackers are malicious

The word "hacker" can send a shiver down the spine of IT departments. Make sure to explain the benefits of working with crowdsourced "ethical hackers"— also known as "security experts", "security researchers," or in this case, "bug bounty hunters."

You could even quote Thomas Colyn, CISO of DPG Media, on this:

> *"By launching a [bug bounty] 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."*
>
> **Thomas Colyn, CISO of DPG Media**

5. Bug bounty programs are another layer of cybersecurity

Bug bounty programs are a great way to harden security, but they don't make your company immune from attacks. Make clear the scope of the tests you are running. Also, stress that other good security practices are still essential.

6. There will be learning opportunities!

Development, engineering, and IT teams can all learn from high-quality vulnerability reports. Bram D'hooghe, Director of Security, Privacy & Compliance at Showpad, explains: "*Intigriti vulnerability reports provide examples we now use in our training for our engineering team so that they get this information upfront in their development life cycle.*"

Showpad discusses it's bug bounty program with Intigriti

What will vulnerability reports mean in terms of work and responsibilities?

Your internal security team is going to need to process the reports you receive. This will include getting fixes scheduled and completed. But you should also keep in mind that the launch of your program may be felt beyond your IT department.

For example, in Europe, you could see GDPR-related considerations that arise from the discovery of vulnerabilities. Does your Legal team know you're about to launch a program?

Bug bounty programs are also a solid way to send a message to your customers and stakeholders that your organization takes security seriously. With that in mind, is your PR and marketing team aware of the program launch? They may want to make some noise around announcing the launch.

In short, make sure that everyone in your organization knows what is around the corner. This is not just the Program Managers, Engineering, and IT departments.

Prioritize your vulnerabilities

Finally, when the first reports come in—and they almost certainly will—you should have a plan of action in place that lays out priorities and how team resources will be used to assess and fix vulnerabilities. Let's look at that now.

Is your internal security team ready to receive their first vulnerability report? The answer is yes if they could answer these questions quickly about any reported vulnerability:

- Is it in scope?
- What is its severity level?
- Who will fix it?
- When will they fix it?

Note: if you're running on a bug bounty platform, like Intigriti, that provides triage services, the first two items above are already taken care of.

Prioritize your responses

So, what about fixing those bugs? This is usually the work of the Engineering or IT department. Can they answer this critical question: *How do we handle each level of severity in terms of time and resources?*

Security decisions shouldn't be made on the fly, so you should work through these with your teams *before* your launch:

- Are we clear on the security threat levels we have established?
- How will we handle each level of reported security threat?
- What is the timeframe to fix each type of vulnerability?
- Which resources will be assigned to each type of vulnerability?
- Are we ready for high severity risks?
- Who will spend the weekend working if a high-severity bug comes in on a Friday afternoon?
- How will we respond if we are suddenly inundated with more serious vulnerability reports than we can handle?
- What's the internal feedback process for fixed vulnerabilities?

If your team can provide clear answers to these questions, it will ensure your bug fixing goes smoothly when the reports start arriving.

Experience is the great teacher

Your internal teams will no doubt encounter unforeseen issues in launching your first bug bounty programs. But if you follow the above steps, you'll be out the gate running. The result should be that you will quickly see improved cybersecurity in your organization with minimal friction. Good luck!

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.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com