Considerations for running an internal bug bounty program

BY ANNA HAMMOND · AUGUST 31, 2022 · LAST UPDATED ON JULY 31, 2025

Tip! *Watch my webinar for how to run an internal bug bounty program.*

Internal bug bounty programs only invite employees of the company to participate. Although, sometimes, companies will leverage their internal teams *and* external security researchers to maximize the skills base doing the testing.

As somebody who successfully set up an internal bug bounty program for a former employer, I've already given my take on the benefits of running one in a previous article. Building on that topic, we're going to now look deeper into what you should consider when setting up and running an internal program.

If you'd like to know more about the intricacies of launching, setting up, and managing an internal bug bounty program, you can find this information in my pre-recorded webinar. But, here's what we're going to cover today:

Considerations for launching an internal program

Below, I'll outline some of the key learnings I gained from running an internal bug bounty program for you to consider when launching your own. However, since I currently work as the Hacker Enablement Manager of Intigriti's wonderful community of 50,000 ethical hackers, I've also included some scenarios where Intigriti can help with specific needs.

Let's dive in!

1. Planning & defining scope

Like traditional bug bounty programs, you will still need to define a clear scope of what employees can test. For example, many internal programs will focus on testing a web application, mobile app, or network infrastructure.

Failing to make this aspect clear may lead to reports of already known vulnerabilities or ones that are unrelated to your needs.

How Intigriti can help with planning & defining scope

Not sure how to define a scope? That's the first of many reasons why some companies prefer to run their internal programs on a bug bounty platform. Intigriti, for example, presents you with a guided, step-by-step approach to creating your program scope and provides related documentation to help you understand the intricacies of the process. If you get stuck, customer success managers can answer your questions.

2. Setting up an internal bug bounty program

At this stage, you need to decide what tools you will put in place to publish your program (internally), track involvement, securely receive reports, and communicate with team members. This aspect can be challenging, especially if you're inexperienced in running a program or lack available technological resources.

How Intigriti can help with your program setup

Again, a bug bounty platform can help you to bypass these challenges quickly. Intigriti provides a cloud-based solution that enables you to publish your program to select participants and has pre-built tools for tracking their involvement. The platform securely manages communication with your team, including transmission and storage of vulnerability reports.

3. Recruiting participants

It's time to invite your employees to start hunting! You should explain:

- What's required
- How to format and submit reports
- The best way to communicate about discovered bugs.

You'll also need to let them know what type of bounties they can expect and when they'll receive payment. Additionally, let them know how they should set up their payment options.

How Intigriti can help make the communication process seamless

If that sounds like a lot of work you don't want (or don't have time) to tackle, many bug bounty platforms provide a framework for all of the above. Intigriti's platform is intuitive for the program host to set up, including sending out invites for your program.

4. Receiving submissions

Once the vulnerability reports have started coming in, there are two key elements to bear in mind:

- Reports may contain highly-sensitive information
- You may receive a lot of reports!

Given the content of vulnerability reports, you must have a secure mechanism for submission, storage, and communication about the contents of the reports. Think of the irony of trying to improve your security posture by taking dangerous steps that a threat actor could exploit!

How Intigriti can help with submission management

Once again, you can spend time and resources creating internal security tools and protocols for submitting and discussing your program. You can also use a tool designed specifically for the task: a bug bounty platform.

5. The impact of triage

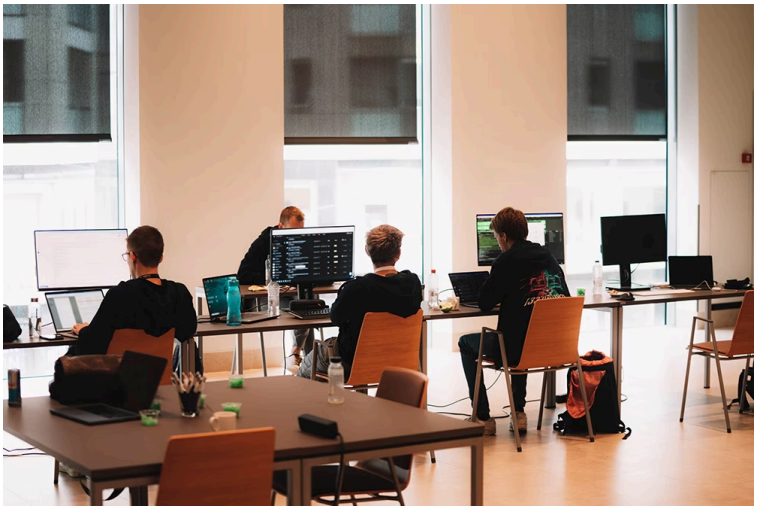
If you decide to run an internal program on your own, you'll need a triage team, and they should be aware of the following.

1. **Be ready for a lot of variability in quantity and quality:** When a report arrives, you must read, assess, and test it.
2. **Have the resources ready:** If your internal program is a success out the gate and you receive a flood of reports, you will need the time and the resources to cope with this.
3. **Vulnerability reports are often very technical:** You'll need security experts in your triage team that are skilled enough to assess and verify if risks are real and how severe they are.
4. **Letting a backlog of reports build-up is never a good idea:** Your employees will lose interest in your program if they don't receive prompt communications and payments.
5. **Duplicates will happen:** Sometimes, several reports will refer to the same bug within days or hours of each other. This occurrence is especially common for low-hanging fruit. However, it does not mean they will all submit identical reports, making them trickier to spot.

Finally, all vulnerability report submissions should have a Proof of Concept (POC) attached. However, imagine a report arrives, you run the POC, but you can't replicate it. Maybe it's your environment, so you tweak some variables—still nothing, and so you send the report back to the employee who submitted it for clarification. If this becomes a regular occurrence, quality issues in your POCs will present a huge time drain for your internal triage team.

How Intigriti's triage department can support your program

If you're already busy in your job and don't have a dedicated internal bug bounty program manager, the thought of fitting all the above into your schedule might make you a little queasy.



Intigriti's triage team live in action

Triage services streamline the process of running a bug bounty program so internal teams can focus on the cybersecurity gains and not the grunt work. They are almost always available with a bug bounty platform, but you might want to check that it is included as standard rather than an extra cost. Check out our tips for how to select a bug bounty platform provider for your business needs.

6. Motivation, payouts, and reputation

Your bug bounty program should now be in full swing. You might have seen a lot of initial enthusiasm for your program. The next thing to consider is how to sustain that enthusiasm.

While you might have a great team of highly dedicated, security-minded employees hunting for bugs, it's probably still fair to say that they'll be even more dedicated if they receive prompt assessment and payment for their vulnerability submissions. Make sure you have the capacity in place to handle payments and maximize engagement. No one likes to wait to get paid, after all.

Bug bounty programs are also a lot of fun for teams. They provide an element of competition during the hunt for bugs that gets people motivated. One way to emphasize that competition in a positive way is by creating leaderboards where you display a list of your bug hunting champions along with an avatar and a ranking based on their successful contributions.

How Intigriti can help with motivation, payouts, and reputation

Dedicated bug bounty platforms can greatly facilitate the setup of payment and leaderboard tools for you. Intigriti includes a secure and automatic payment system that ensures your security researchers are always paid in a timely manner. It also heightens competition with platform leaderboards, including per-program ones.

7. Encouraging learning

One of the big, and often unexpected, payoffs from running an internal bug bounty program is the learning they provide. To maximize this aspect of your program, share and discuss vulnerability reports once code has been patched. These can be great learning tools. Some companies even create in-house training materials from them.

Additionally, encourage dev-to-dev discussions where you discuss discoveries in vulnerability submissions. Internal teams will benefit from raised security knowledge that they can include in their code going forward.

How Intigriti can help internal teams grow their security knowledge

Platforms will often have stringent guidelines for the quality and format of report submissions they accept. This guarantees the reports your business receives contain valid vulnerabilities that are predictably presented, making them ideal for fast learning. A platform will also attract a large number of security researchers with various specialities to your program, which will amplify your opportunities for knowledge development, as they test your team's work.

Bug bounty platforms can enable internal programs

Given the complexity of systems, protocols and experience required, as well as the amount of time needed for good triage, the best approach to running an internal bug bounty program is almost always through a dedicated bug bounty platform, like Intigriti. You get the best of all worlds: a fun, educational program; improved cybersecurity; and the time-consuming process of triage handled by experienced experts!

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. Also, make sure to watch the recording of my advise on running an internal bug bounty program. It's free and available to watch immediately!

About the author:

Pascal Schulz is a Hybrid Pentest Manager at Intigriti. Together with our selected researchers, he is making sure to provide the utmost value to our customers. In his spare time, he is an avid photographer and lover of long hikes!

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com