# The 3 key stages to setting up and managing a bug bounty program [Part 1]

BY ANNA HAMMOND · APRIL 7, 2022 · LAST UPDATED ON JULY 14, 2025

In today's post, we're going to explore two related cybersecurity topics. First, the bug bounty process, and second, do bug bounty programs work?

First we explore how the bug bounty process involves three steps: setup, execution and reporting. Then we look at a real world example of a bug bounty program to see what benefits it brings.

If you're considering setting up a bug bounty program for your organization but are hesitant about complexity, this article is a great place to start. We'll see how bug bounty programs don't require expertise to get up and running. Additionally, we'll learn how surprisingly affordable bug bounty programs are, especially if you're used to the high ticket price of pentests.

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

## Understanding the bug bounty setup process on a bug bounty platform

The setup process for a bug bounty program generally involves four  key steps:

1. Configuring your bug bounty program
2. Running your bug bounty program
3. Processing reports and payment
4. Continuously optimizing for success.

While we can't speak for the details of every bug bounty program out there, let's examine what the setup process looks like for Intigriti clients.

### 1. Configuring your program

We've done our best to streamline and simplify the bug bounty program setup process because we want security to be available to all sizes of business with all levels of IT skill on-staff. Our platform is remarkably user friendly.

Within your Dashboard, your first steps will be to configure three things:

1. The scope of what you want tested
2. The price you'll pay for discovery of vulnerabilities based on severity

3. Whether you want your bug bounty program to be public or private.

The **scope** of your bug bounty program will establish whether you want very focused testing or a wider approach. While what you want tested will depend on your business and technology models, our Bug Bounty Program Settings Knowledge Base article will give you the key information you need to get started if you're working in the Intigriti platform.

**Price**—or bounty—is only one of the factors that motivate ethical hackers, but it's an important consideration. Our publicly listed bug bounty programs page 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.

A **private** bug bounty program will only be listed to selected cybersecurity experts and will not appear in public listings. This can be a great first step for organizations wanting to dip their toe into bug bounty programs without too much initial exposure. Private programs are also great for when you have a specific testing scope, like mobile OS hacking, for example.

After these steps, you'll be ready to hit launch on your bug bounty program. Before you do, however, you might want to check out our Bug Bounty Program Launch Checklist. It's useful no matter what your level of experience is.

## 2. Running your bug bounty program

Many users new to a bug bounty program think this is where they sit back and wait. And then, before they've even got their feet up on the desk, they get a surprise.

The truth is, even businesses with strongly enforced security protocols and great security postures are often taken aback by how quickly vulnerabilities are discovered in their attack surface by our crowdsourced security experts.

Discovery of vulnerabilities isn't an indication of poor security so much as vindication of the effectiveness of crowdsourced security testing. As an example, Port of Antwerp received 135 vulnerability submissions from security researchers from Intigriti within a few months of launching. As Europe's second largest port, they had regularly run pentests and had very robust security practices in place.

At Intigriti, we often see the first valid vulnerability reports arriving within 24 hours and will get it to our customers soon after that. So what's going on out there before your report arrives in your inbox? The process is as follows:

- Crowdsourced researchers begin searching for vulnerabilities
- When a researcher finds a vulnerability, they prepare a well written report
- Researchers submit their found vulnerabilities to the platform's triage team – every report *must* go through this process to check its quality
- The Intigriti triage team communicates with researchers ensuring the quality of the submission
- The triage team applies further quality assurance steps

### What does the triage team do?

When selecting a bug bounty platform, it's worth checking whether triaging services come with the cost of your subscription. At Intigriti, triaging services are offered on all program types by default. These dedicated security experts validate every vulnerability report is valid, in scope and not a duplicate before passing it on to the customer. This is a huge time saver for organizations running a bug bounty program. As Yannick Herrebaut, Cyber Resilience Manager & CISO of Port of Antwerp, says:

> **"I cannot overstate the importance and the value that the triage team offers to us. The researcher sees or notices something, documents it, and publishes it on the platform. It then goes through the triage team as a quality check before we receive it. Our developers know that any vulnerability that makes it through this step is important and in need of remediation. The value is immense for us."**

Finally, as you run your bug bounty program, you might want to take a look at our article dedicated to helping organizations get the most of bug bounty programs.

### 3. Processing reports and payment

Once you receive your first vulnerability reports, the remaining steps of the bug bounty process are simple. First, you will be notified that a vulnerability has been discovered. If you're working with Intigriti, you will receive a report deemed in-scope, valid and unique that clearly outlines the vulnerability.

Once you've been through the report, you can accept or reject its findings. You may also have additional questions, in which case you can message the researcher or researchers (if they are collaborating on the report) through the Intigriti platform. This has proved very valuable to Intigriti customers.

We have a knowledge base article on handling the reports. The process is almost always easy as the reports have been pre-vetted by the triage team. If you accept the bug report, payment will be automatically processed through the bug bounty platform.

You can then get to work patching the vulnerability. And if you're happy with the results from your bug bounty program, you can easily expand its scope or start a new program with a different scope and/or crowd at any time!

Finally, if you've chosen Intigriti as your bug bounty platform, any time you have questions, our Knowledge Base is a great starting point. Support is also on-hand and ready to help. And a dedicated success manager will check in with you regularly to make sure you're getting the results and service you require.

That just about covers the steps in the bug bounty process, but before you invest time and money into any platform, there's probably one burning question we should address here...

## Do bug bounty programs work?

On the Intigriti website, we've posted many customer case studies and other resources that give a good idea of how effective—and affordable—a bug bounty program can be.

One detailed customer case study is for Port of Antwerp—Europe's second-largest port and a major lifeline for the Belgian economy. We put together a three minute video about Port of Antwerp and their bug bounty program success. You can check it out here:

And if you prefer the tl;dr version, here's 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.”
- “Early on into the program’s launch, we could already see it was a success. For that reason, we decided to go ahead with the program next year, and the years after that!”

## Article Series: What to expect from the bug bounty process, from setting up to post-launch

We hope you’ve enjoyed this article and are happy to discover that it is the first in a series of four articles that address the subject, *What to expect from the bug bounty process, from setting up to post-launch*.

The series is as follows:

1. The 3 key stages to setting up and managing a bug bounty program [*This article*]
2. How to prepare for launching a bug bounty program
3. Launching a bug bounty program
4. Optimizing your bug bounty program for success

We’ll update links here as we release each article. See you back here soon!

### Learn more

Want to know more about bug bounty programs? Get in touch to request a demo with a member of our team today.