Vulnerability Disclosure Programs Vs Bug Bounty: Which Is Best?

BY ANNA HAMMOND · MAY 19, 2021 · LAST UPDATED ON MARCH 6, 2025

Ethical hackers dedicate significant amounts of time to discover and report security flaws to businesses. Creating a stress-free and sensical way for them to disclose security vulnerabilities to you is critical. Not only does it encourage responsible disclosure, but it maximises the success of their contribution. In turn, this irons out the bottlenecks in the process and allows you to fix bugs faster.

There are several ways you can choose to receive and manage vulnerability disclosure reports. But, if we condense down the various options, it ultimately narrows down to two main options:

- Self-publish a Vulnerability Disclosure Policy
- Publish and host through a third-party vendor, such as a bug bounty platform.

We break down the difference between vulnerability disclosure programs vs bug bounty programs, as well as the challenges and benefits of both. By the end of this article, you should have a clear indication of which method fits your business needs best.

Vulnerability disclosure programs vs bug bounty programs

Self-publishing contact details

This method of vulnerability disclosure involves publishing your contact information on your website via a vulnerability disclosure policy. Security researchers can use this information in good faith to alert you to vulnerabilities they've found in your system.

Of course, outlining the process via a vulnerability disclosure policy is only half the battle for a triumphant vulnerability disclosure program — it's the execution and integration that counts. For this, communication is key. To avoid potential frustration from both sides, it's important to:

- Respond to initial requests to acknowledge receipt
- Keep an open line of communication for when you need additional information
- Provide a timeline to carry out triage
- Confirm or reject the vulnerability
- Provide a timeline to introduce patch
- Confirm details of a reward or bounty
- Request for retests from the researcher, if relevant

- Update the researcher once the issue is fixed.

Of course, you need to ensure that you also pay or reward researchers on time and for the right amount.

The benefits

As well as mitigating the risk of security issues going undetected, having a VDP helps businesses to:

- Streamline their vulnerability reporting process
- Show a commitment to information security and data protection
- Build trust among stakeholders and customers
- Establish a set of rules for hackers to follow when testing your service.

It also encourages researchers to put in the effort to disclose a vulnerability in the first place. Plus, as part of the safe harbour agreement, they'll feel safe in the knowledge that no legal action will be taken against them.

Challenges of self-managing a VDP

The main struggle with hosting and managing a VDP yourself is that it requires significant time and energy investment. For example, the responsibility to manage and triage incoming reports lies with your internal security team. Many companies receive a large influx of reports when first launching a disclosure program. However, after the hype dies down, so do the high-quality submissions because the most skilled community members won't look outside bug bounty platforms. This can lead to more time being spent on time-wasting reports.

Managing the successful vulnerabilities also requires a time investment. For example, you need to ensure researchers receive the right bounty amount within the time they were promised. This is critical to maintaining good working relationships.

Finally, companies can have issues with submissions reaching the right person through various VDP contact routes. For example, many companies will provide researchers with an email address to report bugs. However, it's not unusual for mailboxes to mistake well-intentioned vulnerability reports for spam.

Vulnerability disclosure through a bug bounty program

Whilst a VDP allows security enthusiast to submit reports, bug bounty programs actively encourage a community of researchers to carry out security tests. Researchers are outreached to and incentivised by a potential earning structure, based on impact and quality.

Benefits of working with a bug bounty platform

Companies that encourage vulnerability disclosure through a bug bounty program tap into tens of thousands of verified security specialists eager to test their systems. Many ethical hackers choose to hunt for vulnerabilities via an official bug bounty platform because they offer a clear and managed way

to submit reports and get rewarded. They also provide a reliable infrastructure and legal framework for them to be successful.

Another major benefit of launching a bug bounty program through a third-party vendor is the client support that comes with it. For example, every client will have access to a customer success team as well as a triage team.

What does a customer success team do?

A customer success team helps businesses optimise their program for maximum success. For example, they'll work with you to define a clear scope for your program and advise on aspects such as what you should compensate researchers and how to outline the severity of a security flaw. They can also help you choose between launching a public program (where anyone can contribute) or a private program (where the business hand selects who can participate.)

Importantly, they'll ensure that your budget is managed properly. For example, at Intigriti, you decide the budget to allocate to your programs and we make sure you don't overspend. The platform also takes care of prompt payouts to the researchers who helped you.

What does triage do?

When security researchers participate in a program and find a bug, they submit a report via the platform. However, rather than submitting the report directly to your team, a triage team will first check if the report is valid, unique, and in scope. This ensures your internal team only receives actionable, valid reports.

Here's a summarised version of the steps they take before escalating reports to clients:

- Review reports
- Evaluate the impact of the security issue
- Deem whether the vulnerability is reproducible
- Ensure the bug is a valid vulnerability
- Approve the information included in the report (to ensure it makes sense to the client)
- Request more information, if necessary
- Prevent duplicate vulnerabilities from being submitted
- Decline reports that are out of scope, based on the company's program description
- Assess the severity of the vulnerability, based on impact
- Be the go-between for client and researchers.

Not only do these steps save businesses a significant amount of time, but they help build a relationship between your company and researchers that goes beyond a decent payout.

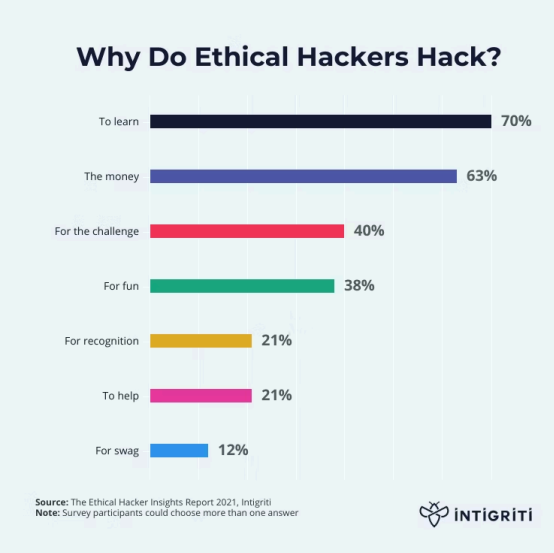
Intigriti's Program Manager and Triager, Quinten Van Ingh, gave more insight into this:

> "*"It's important that both communities feel like they are talking to a person, and not some sort of robot. Being a Triager is more than pointing out whether something is valid or not. For every decision we make, a detailed explanation must be given. We pride ourselves on being as helpful as possible."*
>
> **Quinten Van Ingh, Intigriti Program Manager & Triager "**

This helps drive researchers to your program time and time again, and in turn, build up a trusted community your business can rely on for continuous security testing.

The challenges

By nature, most researchers are on a bug bounty platform to earn cash. However, this shouldn't deter smaller companies with lesser budgets from using a bug bounty program to manage vulnerability disclosure. Money is simply just one of many motivators for bug bounty hunters. For example, the Ethical Hacker Insights Report showed bug bounty platforms are a popular place for researchers to learn and develop too.



Why do ethical hackers use bug bounty platforms?

At Intigriti, even if a program isn't offering a financial incentive, researchers are still rewarded for successful vulnerability submissions with reputation points. This allows them to earn invites for paying programs and live hacking events, and receive goodies like SWAG.

Finally, managing a vulnerability disclosure program through a bug bounty program requires contributors to sign up to the platform hosting it. However, this isn't a reason for companies to deter from this method. By signing up to a bug bounty platform to submit a report, the vulnerability enters a process of quality assurance and the researcher is given sufficient support to increase their chances of success too. It also adds an extra layer of security to working with ethical hackers because are required to pass an identity check.

Taking a coordinated approach to vulnerability disclosure

Having the right structure and tools in place is vital for a smooth collaboration. Some companies choose to manage reports via email communication and spreadsheets while others publish a VDP but point researchers towards their bug bounty program to make the report.

Vulnerability disclosure programs vs bug bounty programs: Which method you take depends on what your goals are and how you want to manage success.

Ready to streamline your vulnerability disclosure process? Speak to a member of the Intigriti team today to request a demo.

REQUEST A DEMO