Bug Bounty Q&A #3: What effort does is take to set up a bug bounty program?

BY INTIGRITI · APRIL 23, 2020 · LAST UPDATED ON MARCH 6, 2025

Bug Bounty for Business

Intigriti ceo Stijn Jans answers your questions about ethical hacking and bug bounty

—

At Intigriti, we love a good conversation. You can find us on Twitter, LinkedIn and Facebook. If the situation permits, we attend events and conferences. When the conversation turns to ethical hacking and bug bounty, some questions are commonly asked.

In this series of blog posts, we discuss these Frequently Asked Questions with our ceo Stijn Jans. This week, we'll discuss "What effort does it take to set up a bug bounty program?" Coming up next is "What is the actual role of intigriti when a company starts working with ethical hackers?"

If you have any questions you'd like to ask Stijn or anyone in the team, feel free to do so via hello@intigriti.com. We'll make sure every question gets answered, and if popular, we'll publish it here.

Question of The Week

What effort does is take to set up a bug bounty program?

This is a question that often gets asked once people start thinking about how ethical hacking could improve their own IT security.

In a conversation, people generally first want to know what bug bounty is. After explaining that it's a way to get the help of external security experts to test systems and report issues before a breach occurs, the value is usually clear.

Next, we often get asked what setting up a bug bounty looks like in practice, and what effort it takes from the internal team. Stijn Jans: "Designing an effective bug bounty program is key. A good program setup provides a structure for the effort needed."

3-step approach to start

Stijn Jans: "When asked about the effort required to start a bug bounty program, I share my 3-step approach, tried and tested over the years. It comes down to 3 basic things: defining the scope, getting the development team involved and assigning a program manager. "

1/ Define the scope

Before giving the ethical hackers the go-ahead to look for vulnerabilities, define the boundaries in which they can operate. A scope can be a single web application, a mobile application or all assets that are publicly available.

Some companies go for a wide scope and are ready to have their entire website, application or IT infrastructure tested. Others choose to be more selective and limit the scope of the program to areas where a breach could, for example, have a financial impact.

2/ Get the development team involved

To run a bug bounty program, a mature development approach is necessary, with an effective strategy in place to manage vulnerabilities.

Reports will have to be evaluated quickly, vulnerabilities prioritized and assigned to the correct remediation or maintenance cycle.

3/ Assign a Program Owner

Typically, the Program Owner will be someone who holds a security position: a CISO or Security Analyst, but it could also be an Application Manager.

Program Owners manage and monitor the program, but are not expected to resolve every vulnerability. They are the link between the ethical hackers and the internal team.

Optional: Consider involving Marketing, security testers and Security Ops

Assigning a Program Owner is absolutely necessary, but there are more valuable people and teams to include in your Bug Bounty program.

– *Marketing and PR*: running a bug bounty program enhances the trustworthiness of your company and underlines the efforts you take to improve and maintain security.

Your Marketing and PR team will communicate this positive message to all relevant parties: employees, customers, management and in some cases even the press. Many companies put a so-called 'responsible disclosure' link in the footer of their website. That webpage then refers to the company's program on the intigriti website.

– ***Security testers:*** involving your internal/external penetration testers in the bug bounty program cross-fertilizes the efforts and maximizes the return. They will learn new tips and tricks about things that they might have missed during their own testing. But they might also be able to quickly assess an incoming report and decide on follow-up actions.

– ***Security Operations***: a Security Operations Team that is fully aware of the plans to unleash bug bounty hunters in your information environment, will help to corral the hunters into the areas where they are allowed to hunt, and will also be warned upfront of potentially strange and suspect traffic and behaviour in the environment.

"Structuring the work this way, I see companies up and running on the intigriti platform and start receiving vulnerability reports in less than a week", Stijn Jans concludes. "It's usually just a matter of deciding to go for it."

Do you want to know more?

Our team is ready to answer all your questions about IT security testing, the intigriti platform, pricing or anything else. Click the button below and we'll get in touch.

Get in touch

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com