yousign

CASE STUDY

PRIVATE BUG BOUNTY PROGRAM

EUROPEAN LEADER ON THE ESIGNATURE MARKET

November 2019

YES WE HACK

YOUSIGN

Why did you decide to go for such a new and disruptive solution as Bug Bounty?

There are a number of platforms out there, which - mostly US based. We asked for certain guarantees on the hunters invited to our programs, and it seemed to us that YesWeHack offered those guarantees and the confidence to launch a Bug Bounty program.

What value you think Bug Bounty can add compared to traditional cyber security solutions (e.g. pen test)?

Diversity in terms of perspectives and skills. Every hunter has his own approach, his way of doing thing, **a unique approach that makes a particular attack.** This is different from pentesting, and it provides a much stiffer challenge. With Bug Bounty, we kind of left behind the pentest world, in order to benefit from 10, 20 or 30 different views and really challenge our teams.

What is really interesting, is that not all hunters are necessarily "cyber security professionals". The entire ecosystem is represented here, and we can pick up individuals based on their nationality, skill set, ranking on the platform, etc.

Yet Bug Bounty's main value, is the continuity, recurrence and "annualization" of the tests: as soon as we release a new version, we integrate the existing program and get immediate feedback on the new version's security level.

CONTINUITY

KEY SELLING POINT

We don't need to wait a year for the next pentest to check on the security of our update. This approach is embedded within our project lifecycle. Our scope evolve constantly, and bugs evolve at the same time. Security flaws turn up every day, not just once a year, and Bug Bounty enables us to detect and fix them in time.

It helps us monitor our services on a practically constant basis, and that is very reassuring. It would also be impossible financially to do an pentest on each delivery, although we would really need to, etc.

And then there is ROI. Yousign carries out one pentest each year. And this is quite expensive, compared to a Bug Bounty program. **It's a bit crazy when you think about it: they cost more or less the same, but Bug Bounty covers an entire year, whereas an audit only lasts a week...**

Is Bug Bounty the end of pen testing? Or will it always remain complementary?

For Yousign, it will continue to be complementary. It could mean the end of the pentest in some industries, but not in ours: as a trusted third-party provider we are required to carry out regular audits. In a less stringent regulatory environment, I would probably consider about using Bug Bounty only.

However Bug Bounty is very important for our sales and marketing : it's clearly a differentiator to large prospect accounts.

We mention it systematically in our request for proposal submissions as it's seen by the market as a quality hallmark.

YOUSIGN

What are the differences between the results of a pentest and Bug Bounty?

I've had the same reports from both, but there are clearly many more reports from Bug Bounty than from pentest.
And after having carried out a pentest on a given scope, running Bug Bounty always brings additional vulnerabilities. One of the problems with pentests is results mainly depend on the expertise of the pentester. Our last pentest showed up some relevant things, but **when you compare its results with those of the Bug Bounty program we launched afterwards... there's no comparison.**

Have you seen any changes in your teams since you have been using Bug Bounty?

Of course. To start with, I managed the programs on my own, then fairly soon afterwards I got the development teams involved so that they could directly reply to hunters, fix bugs, etc. Most reports concerned the applications team, so they had to face up reality and take things forward, if I can put it like that.

What's more, we quickly saw that their interactions with the hunters affected their delivery and working methods: not only do they integrate security into their development work more effectively, they actually started to "think" differently, always keeping in mind security aspects.
You could say that they are not only delivering for clients, but for the hunters too (laughs).

What's next ?

The next step is to use Bug Bounty even more. In addition to the current programs on our production and "staging" environments, we want to fully embed Bug bounty within our CI/CD workflow to add to our battery of functional and unit test. This should make us even more agile and bug bounty a key component of our CI/CD approach.

And later on, we might move to a public program.

Kevin Dubourg
Bug Bounty Program Manager

yousign