YES WE HACK

yousign

YOUSIGN

Private Bug Bounty Program

CASE STUDY

YES WE HACK

yousign

WHY DID YOU CHOOSE BUG BOUNTY?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

There are a number of platforms out there, mostly U.S.-based. We requested certain guarantees from the hunters invited to our programs, and YesWeHack offered those guarantees and the confidence to launch a bug bounty program.

WHAT VALUE DOES BUG BOUNTY BRING COMPARED WITH TRADITIONAL CYBERSECURITY SOLUTIONS, SUCH AS PENETRATION TESTING?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

It offers diversity in terms of perspectives and skills. Every hunter has his own approach, his way of doing the thing: a unique approach that makes a particular attack. This is different from penetration testing, and it provides a much stiffer challenge. With bug bounty, we left the penetration testing world behind, in order to benefit from 10, 20, or 30 different views and really challenge our teams.

It is also interesting that not all hunters are necessarily 'cybersecurity professionals'. The entire ecosystem is represented here, and we can pick up individuals based on their nationality, skill set, and ranking on the platform.

However, the primary value of bug bounty is the continuity, recurrence, and 'annualisation' of the tests: as soon as we release a new version, we integrate the existing program and receive immediate feedback on the security of the new version. We don't need to wait a year for the next penetration test to check on the security of our update. This approach is embedded within our project lifecycle.

Our scope evolves 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 these in time. It helps us monitor our services almost constantly, which is very reassuring. It would also be impossible financially to do a penetration test on each delivery, although we would need to.

The return on investment is compelling too. Yousign carries out one penetration test 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.

yousign

DO BUG BOUNTY PROGRAMS SPELL THE END FOR PENETRATION TESTING? OR WILL THEY REMAIN COMPLEMENTARY?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

For Yousign, the two will continue to be complementary. It could mean the end of penetration testing 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 only using bug bounty.

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.

HOW DO THE RESULTS COMPARE BETWEEN PENETRATION TESTING AND BUG BOUNTY?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

I've had the same reports from both, but there are many more reports from bug bounty than from penetration testing. Moreover, after we have carried out a penetration test on a given scope, running bug bounty always brings additional vulnerabilities.

One of the problems with penetration testing is that results mainly depend on the expertise of the penetration tester. Our last penetration test showed up some relevant things, but when you compare the results with those of the bug bounty program we launched afterwards, there was no comparison.

> **"After we have carried out a penetration test on a given scope, running bug bounty always brings additional vulnerabilities.**

HAVE YOU SEEN ANY CHANGES AMONG YOUR TEAMS SINCE USING BUG BOUNTY?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

Yes, definitely. I initially managed the programs on my own, but soon afterwards involved the development teams so that they could manage processes like replying directly to hunters and fixing bugs. Most reports concerned the applications team, so they had to face up to reality and take things forward.

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, but they also started to 'think' differently, always keeping in mind the security aspects. You could say that they are not only delivering for clients, but for the hunters too!

WHAT'S NEXT?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

The next step is to extend the use of bug bounty. Besides the current programs in our production and 'staging' environments, we want to embed bug bounty within our CI/CD workflow to add to our battery of functional and unit tests. This should make us even more agile. Bug bounty is certainly a key component of our CI/CD approach.

In time, we may move to a public program.

ABOUT

YES WE HACK

Founded in 2015, YesWeHack is a Global Bug Bounty & VDP Platform.

YesWeHack offers companies an innovative approach to cybersecurity with Bug Bounty (pay-per-vulnerability discovered), connecting more than 25,000 cybersecurity experts (ethical hackers) across 170 countries with organizations to secure their exposed scopes and reporting vulnerabilities in their websites, mobile apps, infrastructure and connected devices.

YesWeHack runs private (invitation based only) programs and public programs for hundreds of organizations worldwide in compliance with the strictest European regulations.

In addition to the Bug Bounty platform, YesWeHack also offers: support in creating a Vulnerability Disclosure Policy (VDP), a learning platform for ethical hackers called Dojo and a training platform for educational institutions, YesWeHackEDU.

⟶ CONTACT US

⟶ VISIT OUR WEBSITE

yousign