YES WE HACK

EUROPEAN FINANCIAL INSTITUTION

Private Bug Bounty Program

CASE STUDY

WHY DID YOU DECIDE TO LAUNCH A BUG BOUNTY PROGRAM?

INFORMATION SYSTEMS SECURITY EXPERT:

To be honest, I wasn't convinced at first. I imagined it was a 'patchwork' of various missions being carried out by their pentesters and not an established, focused activity.

Then I met with the YesWeHack team who presented different advantages that met my security expectations. Following this, we launched an initial Bug Bounty campaign on a site we knew well and which we had already tested multiple times before. Choosing a mature scope enabled me to control the potential program costs.

I wasn't expecting to get any feedback as we were already on our eighth penetration test on the site since I'd been on the job. And the last test had been conducted just the week before. But the results proved us wrong: we received multiple vulnerability reports, including one that was critical, just an hour after launching the program. We now know this vulnerability had existed for 18 months. In other words, two pentests had taken place without it being noticed. So, Bug Bounty instantly appealed to us! (Laughs)

> “But the results proved us wrong: we received multiple vulnerability reports, including one that was critical, just an hour after launching the program.

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

I see four main advantages.

First, you're getting something close to the real thing. By that I mean we're not trying to get a comprehensive view of the vulnerabilities. We're trying to hit right where it hurts immediately. That's very close to what a real attack would do.

Second, Bug Bounty gives us continuity – vital given the current agility trend. We continually update our internet applications (at least once a month); so, it becomes complicated and costly to pentest each deployment. Bug Bounty enables us to monitor continuously.

Third, the efficiency and quality of the work done by the hunters is exceptional. On sites that we'd tested multiple times, we systematically found vulnerabilities, some of which were critical. The hunters are paid based on results, so their goal is to find something concrete for us – and that's my goal, too. One of the problems with pentesting is that the results rely entirely on the pentester.

> **"Since we launched our Bug Bounty program, we've upped our security game: we found new vulnerabilities.**

With Bug Bounty, we work with specialists. The hunters won't necessarily look for every type of vulnerability that may exist on a web application. Instead, they go where they perform the best – and where they can be swift and effective. That's what we're looking for, too.

Since we launched our Bug Bounty program, we've upped our security game: we found new vulnerabilities. We were able to fix them, and the security of these applications is now a cut above. Ultimately, that's what a CISO should be aiming for: not just compliance, but enhanced security.

The final very important advantage is the return on investment (ROI). Between the reward budget and the cost of the platform – and given the results – over the year, it's very profitable. I have twice as many vulnerabilities reported via my Bug Bounty program than I did with pentesting, and it costs me about 50% less.

I've been pentesting critical sites for years and getting empty or nearly empty reports in return. We were paying because it was our policy, and we needed to meet our compliance requirements; but it brought us nothing, or almost nothing more, in terms of security.

> “I’m now wondering if it makes any sense to do annual pentests on applications managed in agile mode.

DOES BUG BOUNTY MEAN THE END OF THE PENTEST, OR ARE THE TWO COMPLEMENTARY?

They’re still complimentary, but it will reduce the perimeter seriously. We will aim to maintain the same number of pentests, but focus them on less critical areas.

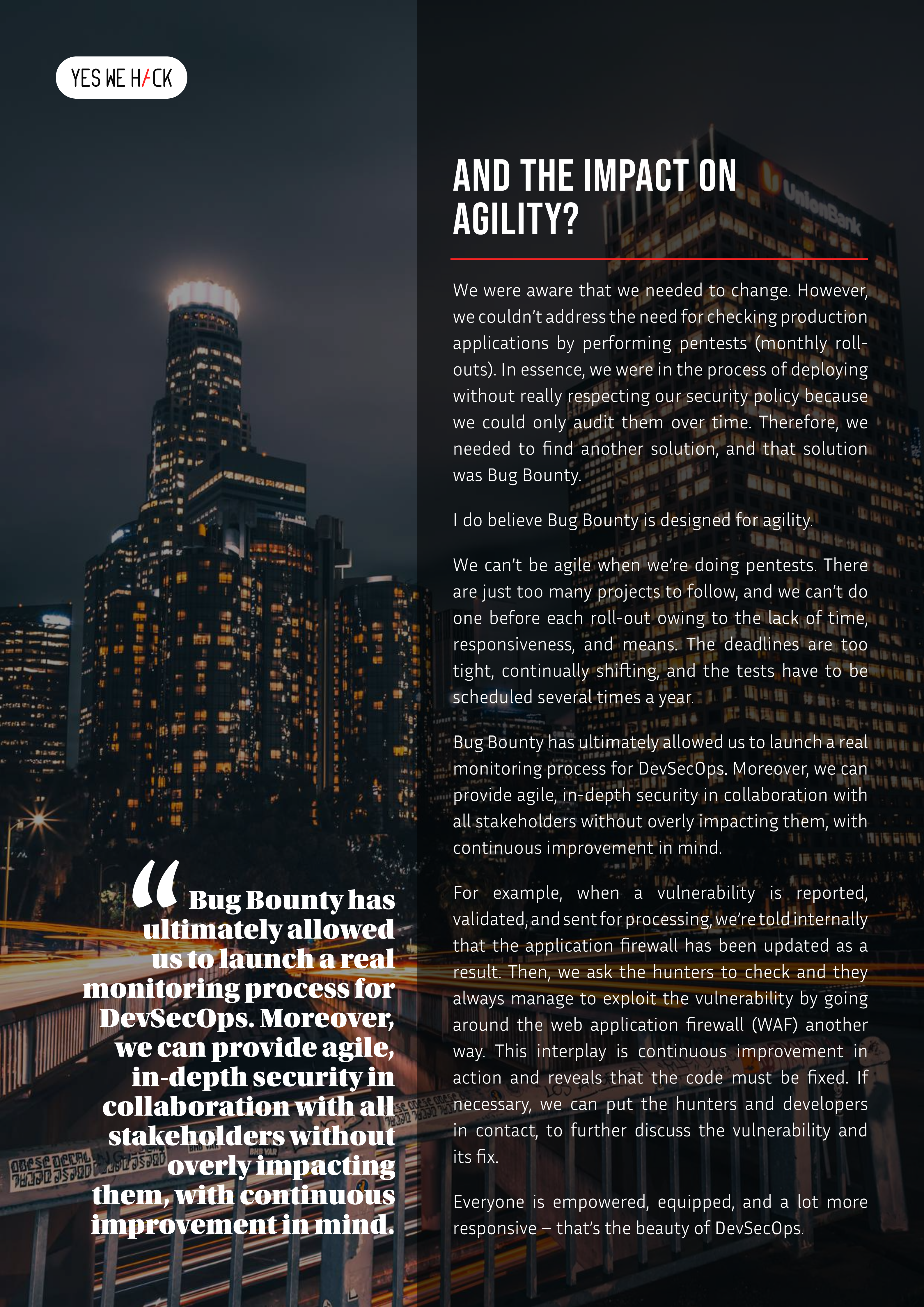
I’m now wondering if it makes any sense to do annual pentests on applications managed in agile mode. And for all the critical web-based applications, we’re moving towards full Bug Bounty.

HOW DOES BUG BOUNTY WORK IN YOUR COMPANY? HAVE YOU OBSERVED ANY CHANGES TO YOUR TEAMS SINCE YOU BEGAN USING BUG BOUNTY?

We’re in a ‘managed’ program, meaning we don’t do the vulnerability triage ourselves. But, internally, I’m in charge of overseeing the Bug Bounty program. It’s a little time-consuming at first; you need the discipline to avoid looking at every vulnerability, one by one, as soon as you get them. Once you establish your rhythm (for me, that’s once a week), it’s advantageous. Speaking of time, it’s close to that of managing a classic pentest. On the other hand, it’s a lot simpler to launch and monitor than a pentest.

We gave the Operational Security team direct access to our program. This way, our colleagues can see the vulnerabilities as soon as they’re validated. Also, our developers can interact directly with the hunters. We’ve involved them right from the launch of the project, so, they didn’t take it as a ‘punishment’, but rather like a game of offence/defence. That’s exactly how I wanted it to work; it was like: ‘Oh, they’re good, how do they do that?’. (Laughs)

Engaging with the developers has made us a lot more effective. It helps them improve and, in general, helps us make progress in terms of security.



AND THE IMPACT ON AGILITY?

We were aware that we needed to change. However, we couldn't address the need for checking production applications by performing pentests (monthly roll-outs). In essence, we were in the process of deploying without really respecting our security policy because we could only audit them over time. Therefore, we needed to find another solution, and that solution was Bug Bounty.

I do believe Bug Bounty is designed for agility.

We can't be agile when we're doing pentests. There are just too many projects to follow, and we can't do one before each roll-out owing to the lack of time, responsiveness, and means. The deadlines are too tight, continually shifting, and the tests have to be scheduled several times a year.

Bug Bounty has ultimately allowed us to launch a real monitoring process for DevSecOps. Moreover, we can provide agile, in-depth security in collaboration with all stakeholders without overly impacting them, with continuous improvement in mind.

> "Bug Bounty has ultimately allowed us to launch a real monitoring process for DevSecOps. Moreover, we can provide agile, in-depth security in collaboration with all stakeholders without overly impacting them, with continuous improvement in mind.

For example, when a vulnerability is reported, validated, and sent for processing, we're told internally that the application firewall has been updated as a result. Then, we ask the hunters to check and they always manage to exploit the vulnerability by going around the web application firewall (WAF) another way. This interplay is continuous improvement in action and reveals that the code must be fixed. If necessary, we can put the hunters and developers in contact, to further discuss the vulnerability and its fix.

Everyone is empowered, equipped, and a lot more responsive – that's the beauty of DevSecOps.

ABOUT

YES WE HACK

Founded in 2013, 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 23,000 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