YES WE HACK

OUTSCALE

OUTSCALE

Public Bug Bounty Program

CASE STUDY

WHY DID YOU IMPLEMENT A BUG BOUNTY PROGRAM?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

We've been ISO 27001 certified since 2014 and are mandated to use penetration testing to seek out vulnerabilities. At first, the penetration testing proved useful. Over time however, they produced fewer exciting outcomes. We quickly realised that owing to the limited duration of an audit (2-3 weeks), the penetration tester didn't have the time to identify more severe vulnerabilities. At best, he or she had hunches, but then we needed to work on them.

We also saw that, for several years, bug bounty had been working well in the U.S. Household name brands were using the approach.

We explored red team and bug bounty, with researchers coming from diverse backgrounds to test our scopes and discover new vulnerabilities.

If we'd gone with red team, we'd have encountered the same problem we had with the classic penetration testing I mentioned before. So, we chose to launch a bug bounty in the belief that, although the penetration testers were no longer finding anything, that didn't mean there weren't other problems.

We started with a private program collaborating with approximately 15 hunters because we weren't 'sure' about our applications. The hunters identified some significant vulnerabilities. We gradually invited more hunters before finally going public with two scopes: our infrastructure service and our customer portal.

CAN YOU DESCRIBE THE EVOLUTION AND DEVELOPMENT OF YOUR PROGRAM?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

It was reasonably quick – one year – to implement the program. When we went public, we didn't experience a sharp spike in vulnerabilities: we started with a grid of very reasonable bonuses, which we gradually increased to reactivate hunter activity on our program to reach our current 'cruising speed'.

DID SOVEREIGNTY INFLUENCE YOUR DECISION TO WORK WITH YESWEHACK?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Yes, definitely. When we considered bug bounty, we were aiming for both the ANSSI SecNumCloud qualification and the HDS certification. It therefore seemed more opportune for us to work with a French partner, giving us solid guarantees on how our data is managed.

IS WORKING WITH A SOVEREIGN PLATFORM AN ASSET FOR YOU IN THE WAY YOU APPROACH YOUR MARKET?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Yes, the concept of sovereignty is essential to our French and European customers. Those include public and para-public organisations, as well as organisations of strategic importance (*OIV or Operators of Vital Importance; abbreviated as per its French naming*), that are sensitive to the issues of sovereignty and control of their data. In the context of cloud services provisioning, partnering with a sovereign platform like YesWeHack assures our customers that the end-to-end vulnerabilities processing chain is controlled effectively.

In a broader sense, bug bounty offers Outscale a competitive advantage because it guarantees active security: where we once performed biannual penetration testing and periodic scans, we're now looking for vulnerabilities continuously. The moment a hunter signals a vulnerability, we're able to include it in our correction cycle automatically. Our customers are reassured, knowing that we don't wait for updates from vendors to fix our vulnerabilities. Also, we're able to detect and fix vulnerabilities in our products we develop in-house.

WHAT IS THE TRUE VALUE OF BUG BOUNTY?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

First, hunters don't face any time constraints. They can take the time they need to detect sophisticated vulnerabilities, further develop an exploit, suggest remediation, and write up a detailed report. By contrast, penetration testing often results in a few scans and two or three CVEs, without any concrete proof of exploitations.

The diversity of the community is another advantage: I can exchange with hunters specialising in UI, for example, and others in application services. Each of them offers different, complicated things that a 'non-specialised' auditor could never find. Sometimes, I think you have to be crazy to notice stuff like that! I have access to a wealth of expertise. They find things that no-one else could.

My team are familiar with different approaches, through talking to people with different approaches to vulnerability management. We sometimes have to explain that a finding isn't a vulnerability, but rather a misuse at their end and so on.

Last but not least, a bond builds up over time with individual hunters. If a researcher has found significant vulnerabilities, and he or she wants to test more complex things, then we give them the resources or access to do more exciting stuff. This in-depth, collaborative approach is impossible to achieve with penetration testers who are consistently overwhelmed and caught up with their tight deadlines.

> **"I have access to a wealth of expertise. They find things that no-one else could.**

YES WE H/CK

3DS OUTSCALE

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

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

In my opinion, they are two completely approaches: I use penetration testing for their certifying value and to comply with specific standards, which allows me to satisfy customers requiring these certifications. Meanwhile, bug bounty meets the need for more operational security and to focus on all the things that penetration testing and classic scans aren't able to detect.

HAVE YOU SEEN ANY CHANGES IN YOUR TEAMS SINCE OUTSCALE BEGAN USING BUG BOUNTY?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

At the SOC (security operations centre), we manage the existing programs, bonuses, and relationships with the hunters, the creation of new programs, and any changes in the scopes. The bug bounty reports come to my SOC team, which then qualifies each vulnerability.

In 90 percent of cases, they are non-critical vulnerabilities that are quickly qualified. If there is any doubt, we discuss it in-house. If the vulnerability is particularly interesting, the person in charge of managing it presents it to the team. We then talk about its potential impact, the solutions we can use, the hunter's recommendations, and how we can ensure it doesn't come up again. These exchanges increase the skills of the entire team.

> **Bug bounty meets the need for more operational security and to focus on all the things that penetration testing and classic scans aren't able to detect.**

DOES THIS ALSO MEAN YOUR TEAMS COLLABORATE MORE CLOSELY?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Yes, because it stimulates curiosity; people are interested and want to understand. It's always more concrete to show a real vulnerability that has taken place on the platform.

ARE YOUR TEAMS AND THE ORGANISATION MORE AGILE?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

We work in continuous integration, and bug bounty lent itself to our agile methods.

When we receive a vulnerability report, we qualify the CVSS score and, based on that score, we determine the remediation deadline. The report is then sent directly to the relevant teams for correction. The same applies to the dependencies used in the code; they're sent to R&D for analysis and version upgrade. In every case, bug bounty is an entry point like any other, and as such, vulnerabilities are managed via tickets.

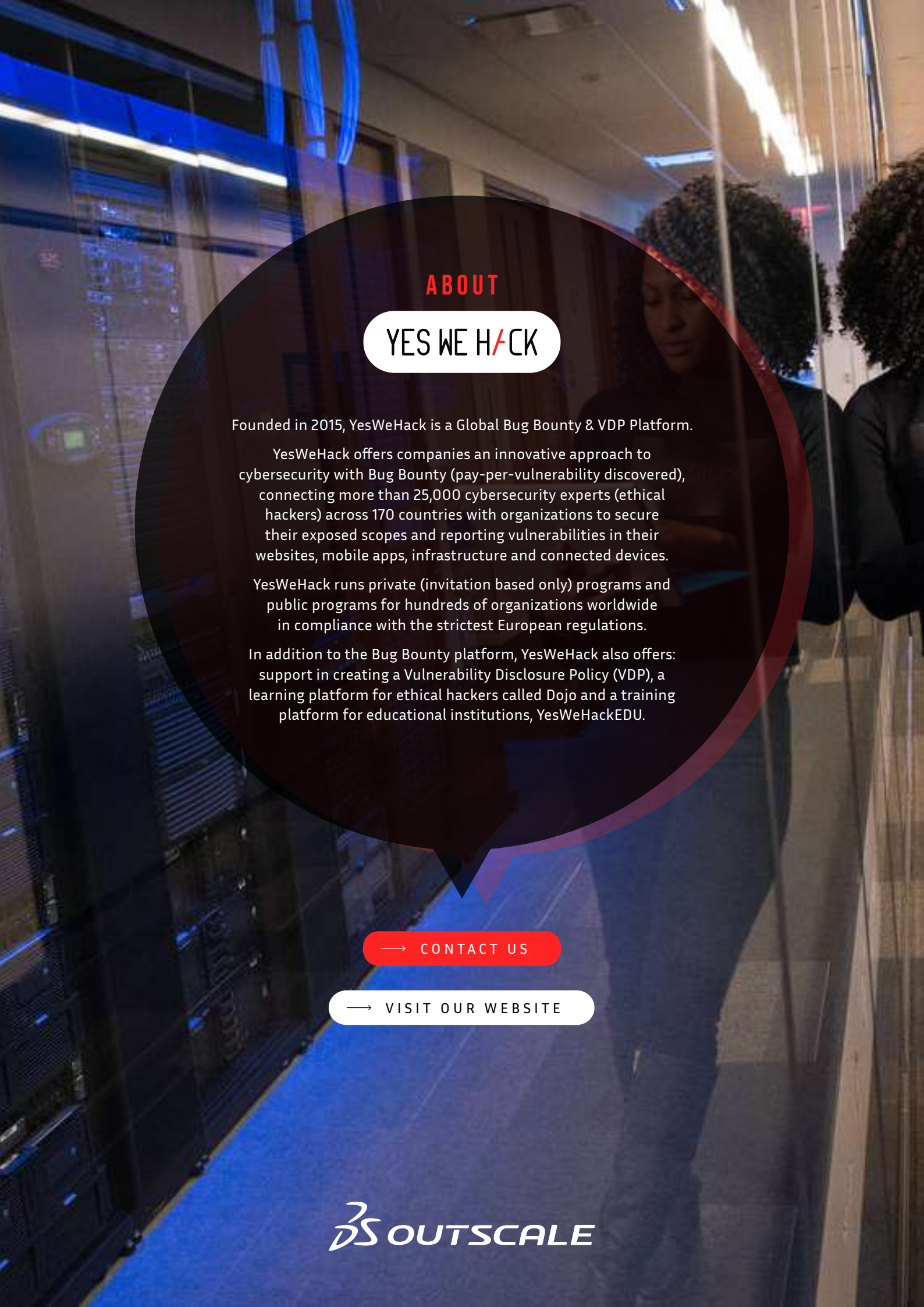
We adapt the processing according to the urgency: if a rapid correction is required, we deliver a patch immediately, to be reinstated in the next version. In this case, we create (or modify) a user story using these new elements, which will serve as a basis for developments.

WHAT'S NEXT?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

We will expand our scopes in the programs. We will also encourage hunters to 'go deep' inside our product (beyond the web-based front-end). And we will increase the bonus grid.

I'd also like to give them access to our private platforms so they can perform more stringent tests. We've already tried this once, and it produced insightful results, with hard-coded data extraction scenarios, on our test platforms. However, this involves giving hunters specific testing scopes, which is time-consuming.



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

OUTSCALE