GLOBAL INSURANCE GROUP

Private Bug Bounty Program

CASE STUDY

CAN YOU INTRODUCE YOURSELF QUICKLY?

I am the Group CISO of a multinational insurance firm. My team's mission is to set up a "cyber shield" for the group and all its subsidiaries, by offering new security services to our subsidiaries – including Bug Bounty.

WHY DID YOU DECIDE TO LAUNCH A BUG BOUNTY PROGRAM?

I discovered Bug Bounty following discussions with CISOs from major financial institutions. Having a recommendation from organizations like these with demanding security needs was a key factor in my decision. We started small and the results were conclusive, so we gradually opened several Bug Bounty programs. It's a new approach, which implies a learning curve.

YES WE H/CK

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

First of all, Bug Bounty offers the guarantee of continuous checking – and not just punctual testing, which is what you get with 'traditional' penetration testing. If I run a two-week penetration test every year, it implies that we remain 'unprotected' for the other 50 weeks, which is no longer acceptable. As a complement, automated tests can also be useful, but are not sophisticated enough. With Bug Bounty, I have researchers working permanently on my scopes.

This continuity is essential, especially when you have frequent deliveries in an increasingly agile development context.

Bug Bounty also allows us to be more flexible. For example, I need to test environments which are still in development, or in validation phase, before going into production. Again, this is challenging to do consistently using traditional penetration testing.

The YesWeHack platform enables us to adjust the rules for each program, including the bounty grid, according to the specific phase of each project.

I would also mention responsiveness and availability: it is increasingly difficult, if not impossible, to find skilled penetration testers at short notice, when you need them most, i.e. when you have a new release.

> **"With Bug Bounty, you just 'press a button', and it starts: you can run tests at any time and get confirmation of remediation in the process very quickly.**

With Bug Bounty, you just 'press a button', and it starts: you can run tests at any time and get confirmation of remediation in the process very quickly.

Finally, we have been amazed by the diversity of reported vulnerabilities. We uncover more 'real-life' scenarios: for example, researchers have found 'bits' of vulnerabilities whose combination made unprecedented attacks possible. Vulnerabilities like these were not addressed until then, as they were not brought to our attention. We are now able to correct them in depth.

Bug Bounty really puts yourself in the head of a hacker.

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

For me it is complementary. The reality however is that there are too few audit firms to keep pace with the number of testing that must be carried out. Hence the key value of Bug Bounty. Moreover, penetration testing shows various limitations and constraints: they must be scheduled in advance, with a start and end date, and they demand project management.

This synchronization is a real headache, especially with agile developments. If a delivery is two days late on a given scope, the pentesters are no longer available, which poses a real stewardship problem.

What I also like about Bug Bounty is the remediation check. With traditional penetration testing, you almost never receive a remediation check. Following an audit, if a developer tells me, 'I fixed the bug', I only have his word. Bug Bounty allows me to delegate this control to the researcher, who is entirely objective.

This enables me to fix a vulnerability and validate the correction in the process – unlike a traditional cross-verification, which I should run once all my vulnerabilities have been addressed. Now, when a serious or critical vulnerability is discovered, I know it is fixed quickly, and I can sleep soundly! (Laughs)

YES WE HACK

HAVE YOU SEEN ANY OTHER CHANGES SINCE YOU STARTED THE BUG BOUNTY PROGRAM?

There is certainly more awareness now, but the major point I'm observing is the acceleration of the patching rate / frequency. Our developers fix much faster.

Responding to researchers, rewarding them, closing reports, etc. require developers to react more quickly. This, in turn, leads to much shorter time-to-remediation.

AND IN TERMS OF AGILITY?

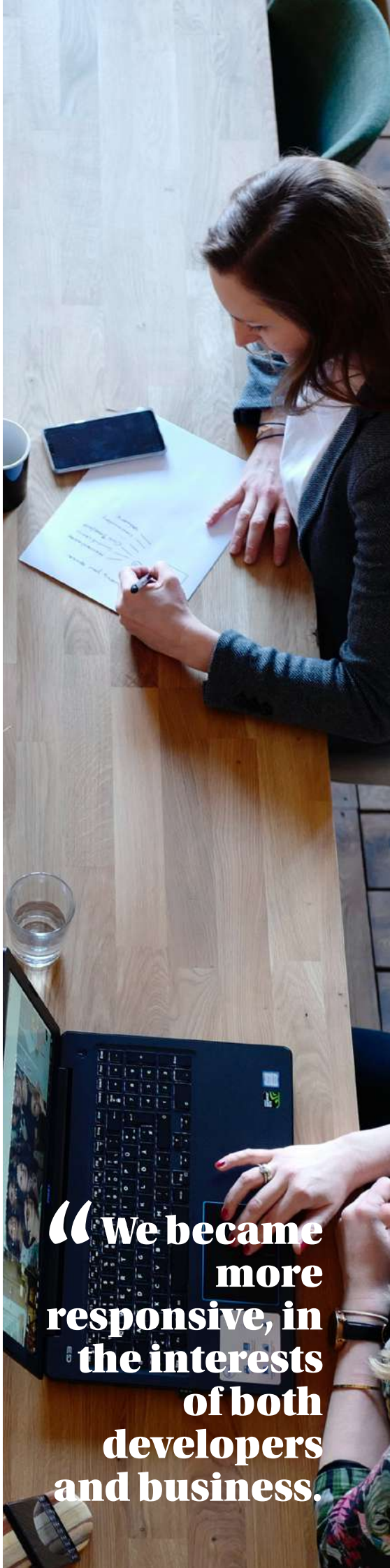
As mentioned earlier, we have implemented specific programs dedicated to test environments, before their release. We therefore detect and fix vulnerabilities further upstream of projects. Firstly, this allows us to train our developers 'on the fly'; second, it accelerates our deliveries since there are fewer patches to manage in the validation and release phases.

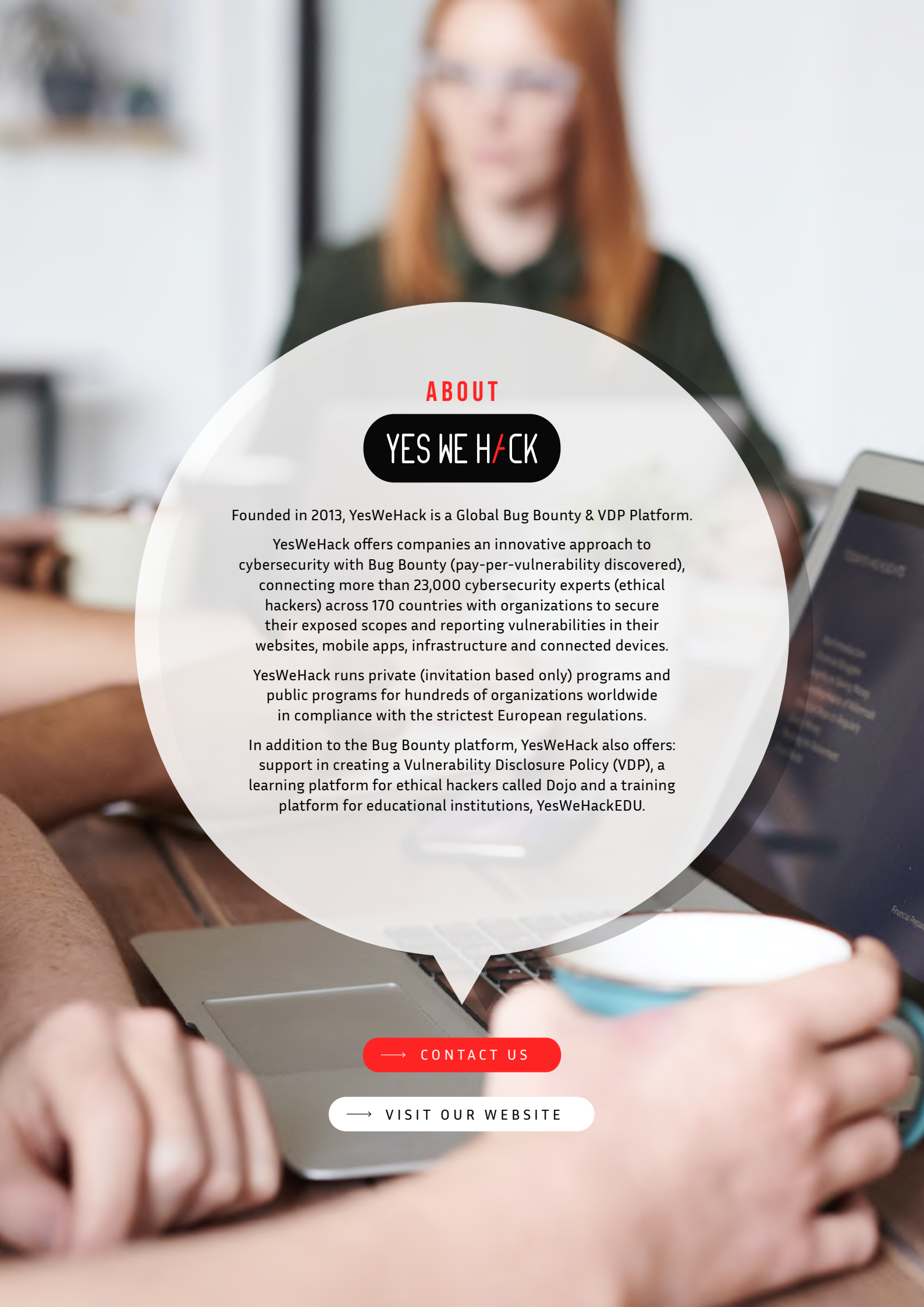
We became more responsive, in the interests of both developers and business.

WHAT'S NEXT?

Our first step is to gradually expand the Group's assets under Bug Bounty. And on these scopes, to gradually move from black box to grey box.

The second step, where we are now, is to make the service available to our subsidiaries worldwide. We want to offer them something different and forward-thinking, allowing them to renew their vision of cybersecurity and audits.





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