YES WE H/CK

GROUPE ADP

GROUPE ADP

Public Bug Bounty Program

CASE STUDY

WHY DID YOU LAUNCH A BUG BOUNTY PROGRAM?

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

The Group Security team took the lead on this project. I had no prior experience of bug bounty, but we very quickly saw the advantages and power of the model. And although I never had any particular doubts or worries, now all I see is the benefits. The bugs reported by hunters are vulnerabilities that we and our auditors may not have seen otherwise, and which could therefore be exploited by bad guys.

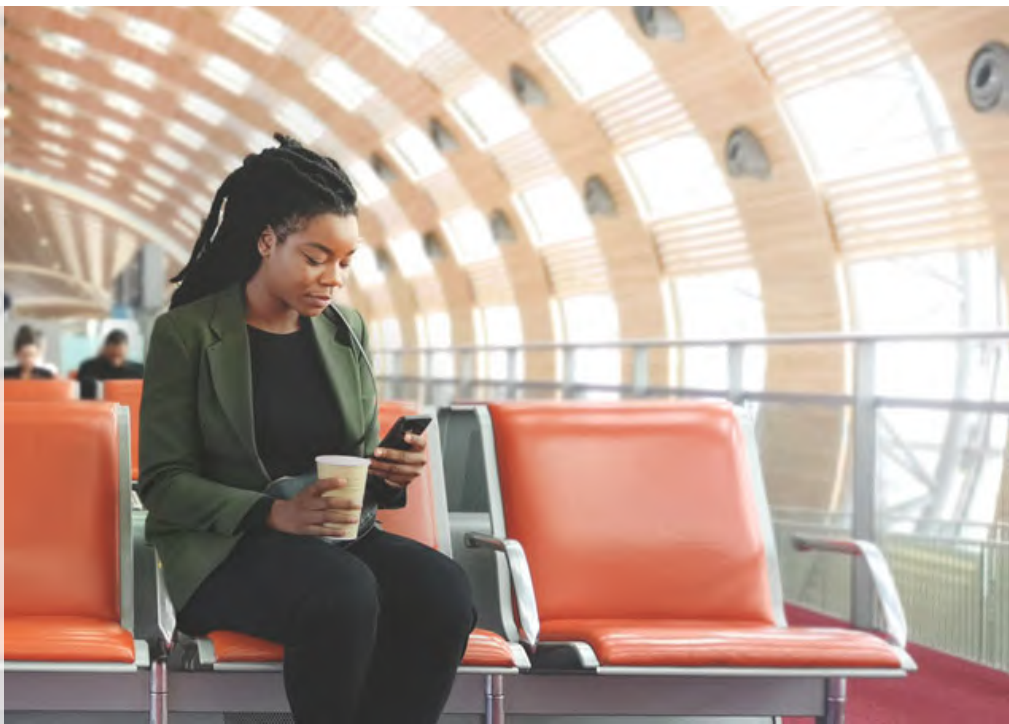
ERIC VAUTIER, GROUP CISO, GROUPE ADP:

In cybersecurity, anticipation is everything. You need to stay one step ahead of the hackers. This means keeping a close eye on market innovations. In the digital world, doing 'old-style' protection means you are clearly behind the game. And a good way to catch up is to work directly with security researchers who use hackers' methods and think like them.

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Today, bug bounty is one of the pillars of our web security strategy. Of course, it's vital to set the program rules carefully: you have to structure the tests in the right way so that the hunters don't 'disperse' their efforts. You need to identify the appropriate 'boundaries', and this is where the program setup is essential. We started with a tightly drawn scope and expanded it as we went along.

"A good way to catch up is to work directly with security researchers who use hackers' methods and think like them.



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

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Continuous testing – this is the great strength of bug bounty. Penetration tests are run at a given point in time, not following every minor delivery. By contrast, we have hunters working continuously with bug bounty. They are alert to anything new, which means they can detect whether any change creates potential vulnerabilities.

ERIC VAUTIER, GROUP CISO, GROUPE ADP:

In a perfect world we should systematically test each update on our website. This would mean running a penetration testing every week, or even more often... And everyone knows that's not feasible. Bug bounty makes this continuous verification a possibility.

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

I'm receiving reports I never had from our penetration testing. These reports are way more granular too, particularly on the website navigation experience. Auditors don't necessarily have this approach. What's more, a penetration test has a limited timeframe, whereas hunters take the time they need to go as far as possible. As time goes by, they also get increasingly familiar with our scope, which means they can go even more in depth.

ERIC VAUTIER, GROUP CISO, GROUPE ADP:

A bug bounty program can also be used to report more functional, not just technical, application vulnerabilities. For me, this is what genuinely differentiates it from the penetration test. It is a completely different angle. A penetration test often relies on automated tools, while bug bounty builds on these tools with a more human approach.

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

The interaction with hunters is interesting too. They help us understand the vulnerabilities they've found and how to fix them effectively. This way we can leverage their expertise.

For sure, bug bounty demands some investment. You have to be available to understand what the hunters have tried to do, to talk to them... But they force us to ask ourselves fresh questions: how would a bad guy get round our protection measures?

GROUPE ADP

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

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

For me, neither works without the other. On the one hand, we are not necessarily testing the same things with both. On the other, we cannot set off into the unknown without having some minimum level of certainty in advance. Bug bounty arrives at a more mature stage in the logical flow of events. You need to leverage a minimum base level of security before launching bug bounty. That said, within the current scope today, we no longer need to run penetration testing. Bug bounty is sufficient on its own. You need to set the bar at the right level at the outset, and it then becomes a recurring process.

> **“ That said, within the current scope today, we no longer need to run penetration testing. Bug bounty is sufficient on its own.**

HOW DOES BUG BOUNTY FIT WITH YOUR AGILE APPROACH?

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Like everyone, we have tools to manage sources, builds, projects, and performance analytics. We also use tools to log and track each new vulnerability report from the bug bounty program. For each sprint, we verify which relevant data we can include, so we can deal with issues as they arrive.

WHY HAVE YOU GONE PUBLIC? HOW HAS THAT CHANGED YOUR APPROACH WITH BUG BOUNTY?

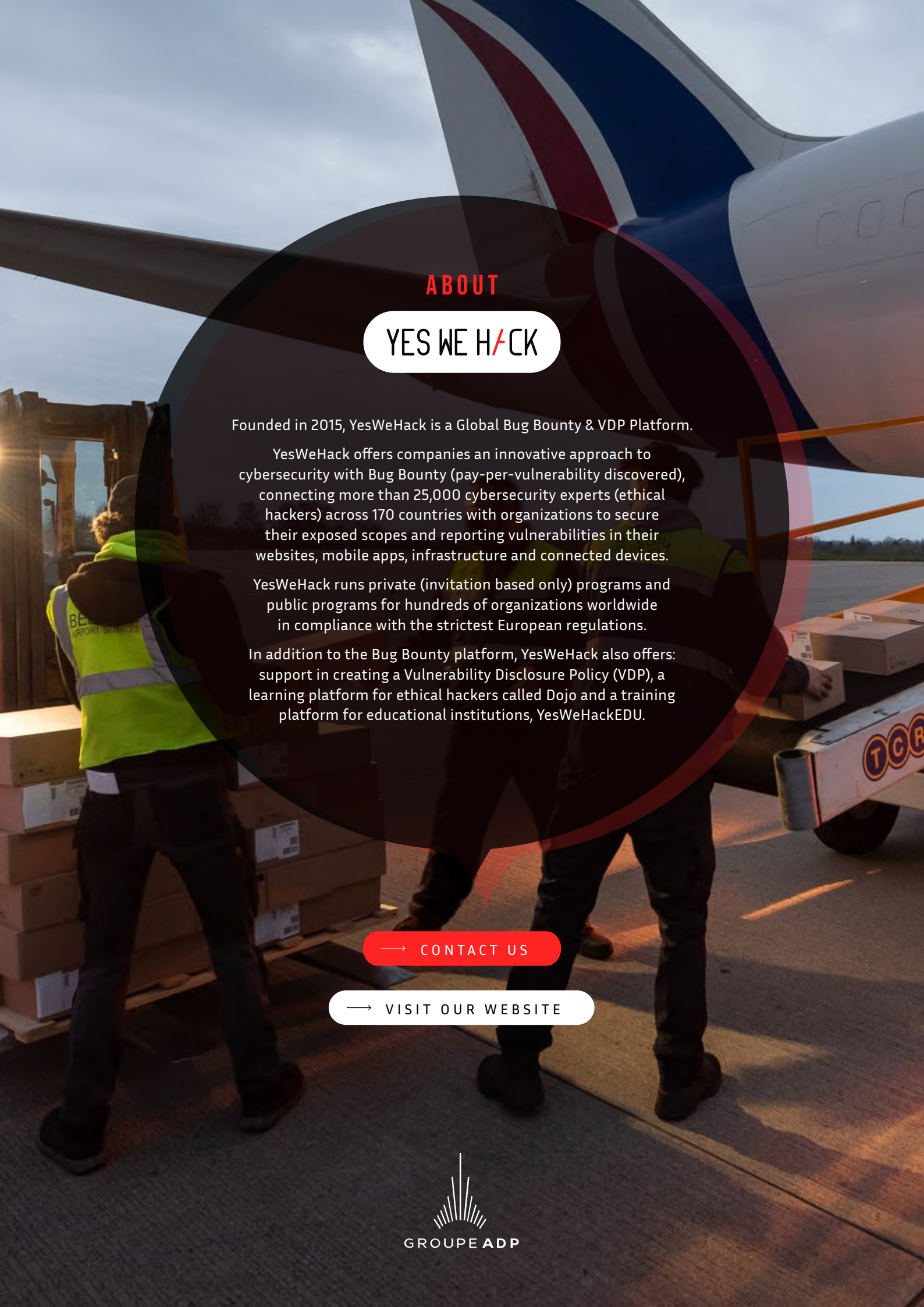
ERIC VAUTIER, GROUP CISO, GROUPE ADP:

The main advantage is to maximise our risk coverage by multiplying the number of potential tests. It also gives us a single channel for reporting vulnerabilities in our website.

WHAT'S NEXT?

ERIC VAUTIER, GROUP CISO, GROUPE ADP:

We are going to open up new scopes, on other applications, and with other business entities using the same model: a private program initially, then going public.



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

GROUPE ADP