
YES WE HACK
deezer
DEEZER
Public Bug Bounty Program
CASE STUDY

WHY DID YOU DECIDE TO LAUNCH A BUG BOUNTY PROGRAM?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

About two years before we launched our Bug Bounty program, we started internal security audits on our code, which had never been done before at Deezer. These tests allowed us to make a first pass and fix some obvious vulnerabilities.

Then we became interested in Bug Bounty and YesWeHack. The ease of use of the platform convinced us of launching a program. Following the launch, we very quickly received interesting vulnerabilities, everything went smoothly, so we decided to continue and expand our perimeters.

WHAT VALUE DOES BUG BOUNTY OFFER COMPARED TO TRADITIONAL CYBER SECURITY SOLUTIONS, SUCH AS PENETRATION TESTING?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

We typically perform an annual audit on several of our services, which lasts between one and three weeks. But this approach is expensive, focuses only on a few services, and over time, doesn't really deliver interesting results.

Bug Bounty gives us ongoing feedback throughout the year, on various scopes, and detects bugs very quickly.

In terms of ROI, Bug Bounty is also very interesting: we decide ourselves the reward we assign to each vulnerability.

> **"Bug Bounty gives us ongoing feedback throughout the year, on various scopes, and detects bugs very quickly.**

Moreover, Bug Bounty guarantees us a diversity of testing skills. With penetration testing, each consultant is ultra-specialized, so we tend to guide him or her on what we want from the test. With Bug Bounty, we were surprised by some researchers' reports. They gave us results of original scenarios, which we had never seen before.

Finally, I appreciate the quality of the reports on the flaws reported through YesWeHack. You sense the researchers are really trying to offer a functional and reproducible POC, that we can easily retest.

The reports of our usual audits are generally quite accurate, but we also find the equivalent quality with Bug Bounty, when the researchers are good and 'play the game'. It's very pleasant to receive reports illustrated with screenshots and videos, which greatly facilitates their understanding, validation, and also their communication to the teams concerned.

deezer

DO YOU GET HELP FROM RESEARCHERS TO ANALYZE AND FIX THE BUGS RECEIVED?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Yes, the researchers help us in the bug reproduction phase. In some cases, we ask them to check whether the vulnerability has been fixed. We also have a large team of developers in-house who can take care of this patch management.

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

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

For me the two remain absolutely complementary. Bug Bounty is a tool that goes further and deeper than the audit. We use penetration testing on new services, or on scopes where we already know there are problems.

deezer

HAVE YOU OBSERVED ANY CHANGES TO YOUR TEAMS SINCE YOU BEGAN USING BUG BOUNTY?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

We clearly see an increased awareness of security. Bug Bounty reports helped us trigger some major security projects. Our cybersecurity vision and posture have evolved, and Bug Bounty is one of the drivers of this change.

In terms of organization, we adapted our process to collect, sort, and validate reports. Then, based on the elements of each validated report, an internal ticket is created and assigned to the relevant team for processing with a varying degree of priority.

DO YOU CONSIDER BUG BOUNTY AS A SIGN OF CONFIDENCE TOWARDS THE MARKET?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Yes. Using a public Bug Bounty program, we can demonstrate and highlight our concerns about security and transparency. We also assume the fact of exposing ourselves to 'controlled' attacks, and to consider the valuable feedback from the researchers' community.

At Deezer, we also have a team dedicated to fraud: indeed, artists and labels are paid according to the audience of the tracks. In order to guarantee their income, we have to protect them from any fraud relating to the platform. So, this is a crucial part of our cybersecurity strategy – and within the scope of our Bug Bounty program.

> **"Using a public Bug Bounty program, we can demonstrate and highlight our concerns about security and transparency.**

YES WE HACK

WHAT'S NEXT?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

For the time being, we are pursuing our current strategy, regularly reviving the program when activity is declining. Generally speaking, the amount of feedback often depends on how visible Deezer is in the news. When we communicate more or launch campaigns, researchers are attracted to our program.

As a next step, we will consider an increase in bounties to encourage researchers to find more complex vulnerabilities.

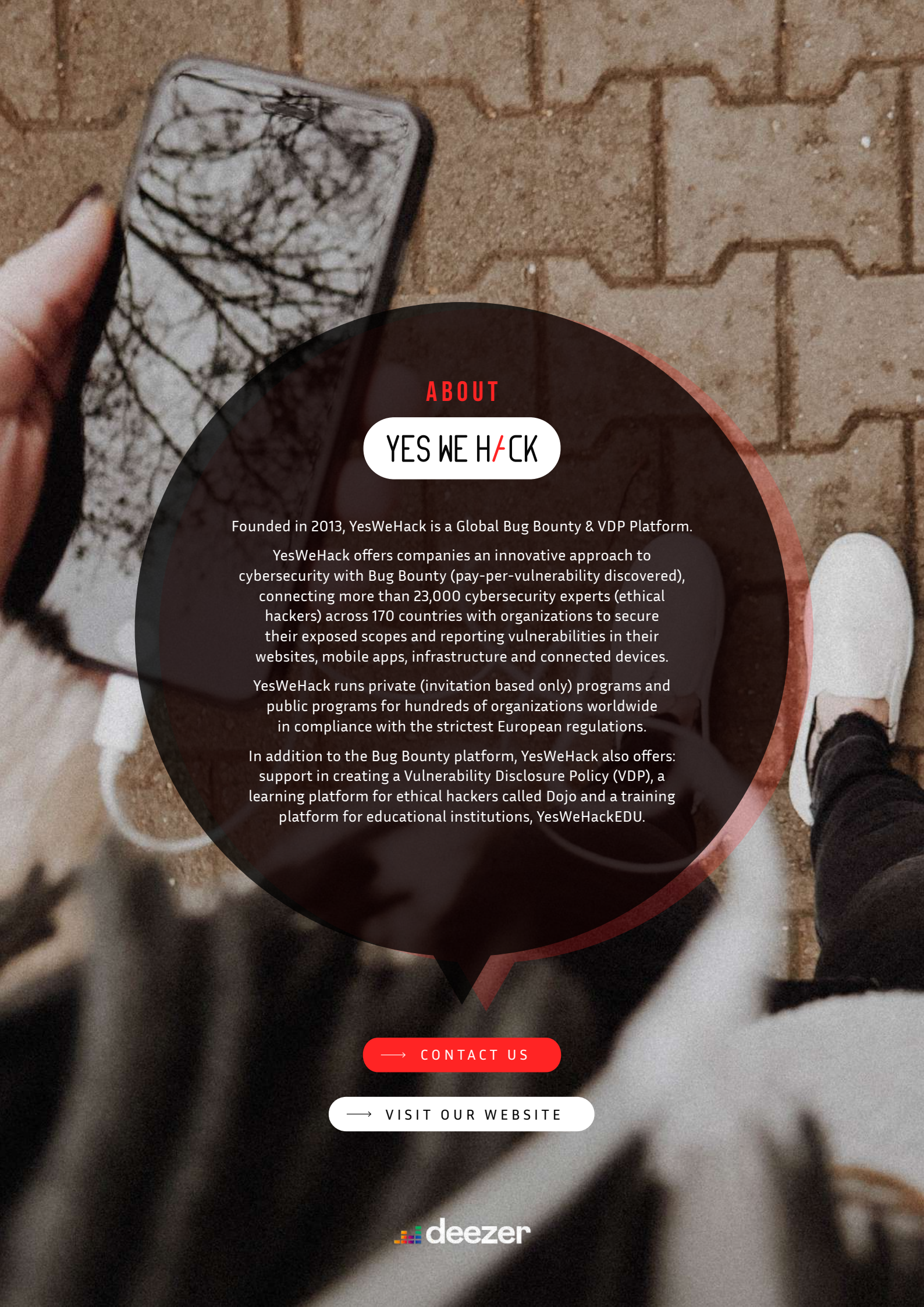
DO YOU HAVE ANY ADVICE FOR CISOS OR STARTUPS CONSIDERING BUG BOUNTY?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

As a general rule, it's better to know your security flaws when you start a project, rather than wait until there are too many to deal with, after you've made (bad) choices of architectures.

When I see what our Bug Bounty program brought us, I think it would have been better if we had taken these insights into account as early as possible.

So, I would recommend not waiting too long to implement tools such as Bug Bounty, in order to minimize the dependency on legacy systems, which are more complex to secure afterward.



ABOUT

YES WE H/CK

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

deezer