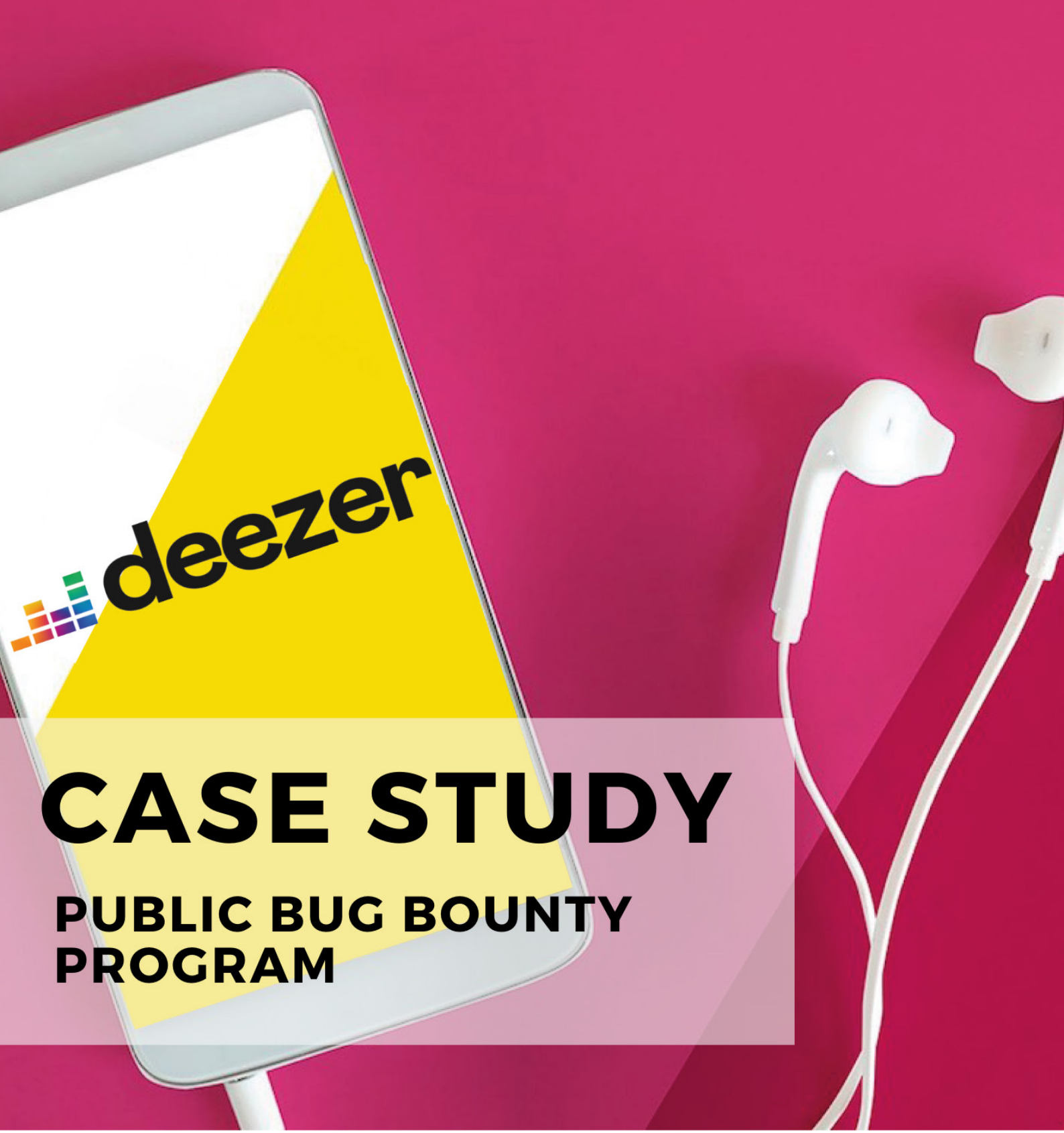

CASE STUDY

PUBLIC BUG BOUNTY PROGRAM

INTERVIEW WITH
ROMAIN LODS
HEAD OF ENGINEERING
DEEZER

January 2020

YES WE HACK

deezer

What made you decide to get into Bug Bounty?

Romain Lods, Head of Engineering, Deezer :

About two years before we launched our Bounty Bug 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 got 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 can Bug Bounty add compared to traditional cyber security solutions (e.g. penetration testing)?

Romain Lods, Head of Engineering, Deezer :

We usually perform one yearly audit on several of our services, which lasts from one to three weeks. But this approach is expensive, focuses each time on a few services only, and over time, doesn't really deliver interesting results anymore.

Bug Bounty allows us to have permanent feedbacks throughout the year, on various scopes, and to detect bugs very quickly.

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

Moreover, Bug Bounty also guarantees us a diversity of testing skills. With penetration testing, each consultant is ultra-specialized, so we kind of guide him on what we want him to test. **With Bug Bounty, we were clearly surprised by some researchers' reports who gave us results of quite original scenarios, never seen before.**

Finally, I appreciate the quality of the reports on the flaws reported via YesWeHack: we can feel that the researchers are really trying to offer a functional and reproducible POC, that we will easily be able to retest.

The reports of our usual audits are generally quite accurate, **but we also find 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.

Do you get help from researchers to analyze and fix the bugs received?

Romain Lods, Head of Engineering, Deezer :

Indeed, the researchers can help us in the bug reproduction phase. In some cases, we ask them to check whether vulnerability has been fixed.

But this remains punctual as we have a large team of developers in-house who can take care of this patch management.

Is Bug Bounty the death of the penetration testing or is it complementary?

Romain Lods, Head of Engineering, Deezer :

For me it remains absolutely complementary. **Bug Bounty is a tool that goes further and deeper than the audit**. As I was saying earlier, we use penetration testing on new services, or on scopes where we already know there are problems.

Have you been able to observe any internal changes in your teams since you are on Bug Bounty?

Romain Lods, Head of Engineering, Deezer :

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

In terms of organization, we adapted our process in order 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 certain degree of priority.

Do you consider Bug Bounty as a sign of confidence towards the market?

Romain Lods, Head of Engineering, Deezer :

From my point of view, yes: through a Public Bug Bounty program, we 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, and in order to guarantee their income, we have to protect them from any fraud or on the platform. So, this is a crucial part of our cyber-security strategy - and within the scope of our Bug Bounty program.

The next step?

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 number of feedbacks often depends on how visible Deezer is in the news. When we communicate more, launch campaigns, etc., researchers get 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 that would get into 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 could have been even 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.

Romain Lods, Head of Engineering, Deezer