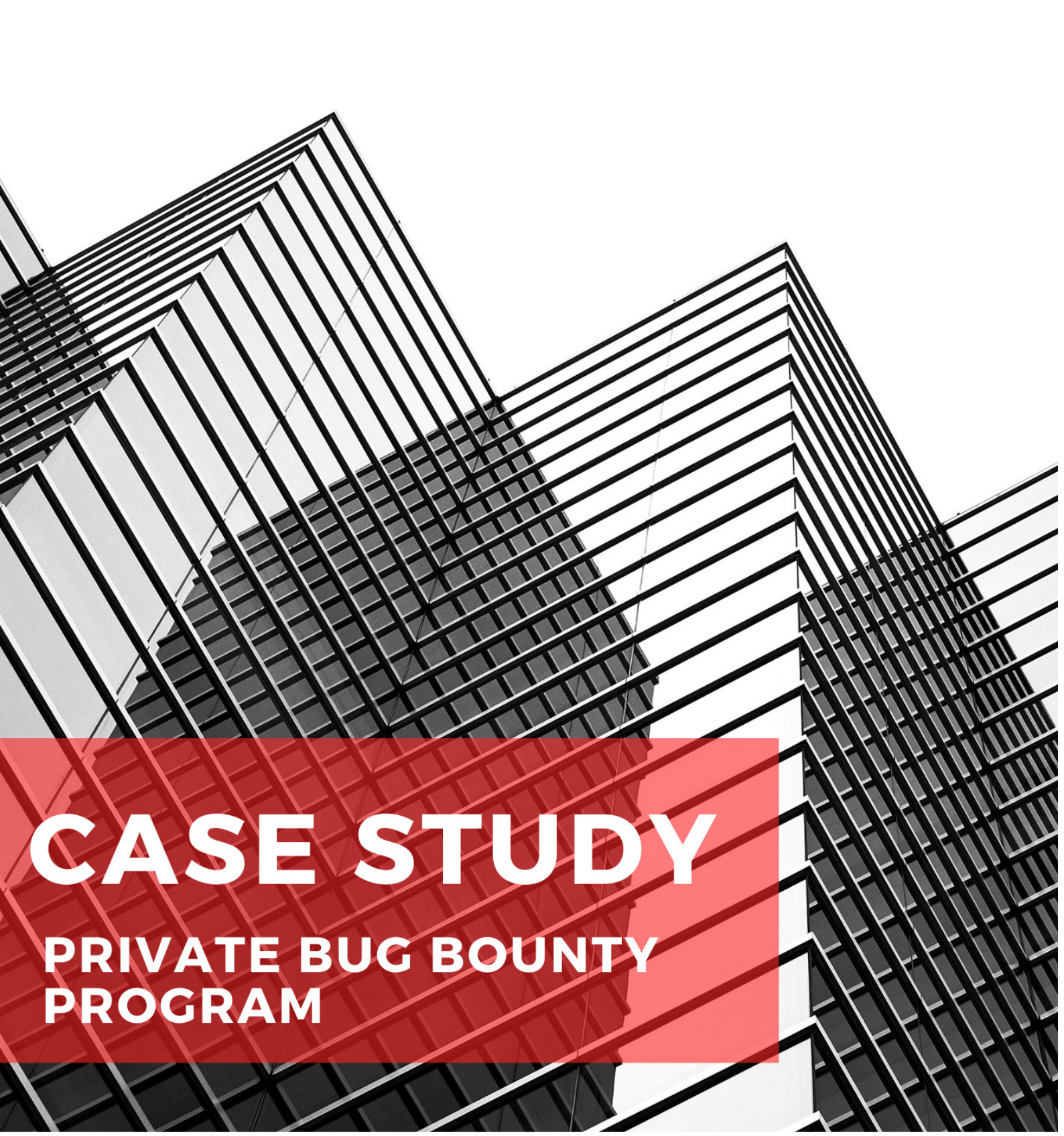

CASE STUDY

PRIVATE BUG BOUNTY PROGRAM

GLOBAL INSURANCE GROUP

YES WE HACK

November 2019

GLOBAL INSURANCE GROUP

Can you introduce yourself quickly?

I am the Group CISO of a multinational insurance firm. My team's mission is to provide a «cyber shield» for the Group and all its subsidiaries, by offering them new security services – including Bug Bounty.

What made you decide to launch a Bug Bounty program?

I discovered Bug Bounty by discussing with several CISOs from major financial institutions. The recommendation of such demanding organizations in terms of security was obviously 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.

What value can Bug Bounty add compared to traditional cyber security solutions (e.g. penetration testing)?

First of all, **the guarantee of continuous checking** – and not just punctual, as with "traditional" penetration testing. If I run a two-week penetration testing every year, it implies that we remain «unprotected» for the other 50 weeks, which is no longer acceptable these days. 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 developments context.

CONTINUITY

Bug Bounty also allows us to be more flexible: I need to test environments which are still in development, or in validation phase, before going into production, etc. Again, this is challenging to do the same through traditional penetration testing.

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 on 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.

FLEXIBILITY

REACTIVITY

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

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

DIVERSITY

GLOBAL INSURANCE GROUP

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

For me it is still complementary. But the reality is that given the number of testing that must be carried out, the availability of audit firms is not sufficient... Hence the key value of the Bug Bounty. Moreover, **penetration testing show various limitations and constraints: they must be scheduled in advance, with a start and end date, implies project management, etc.**

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 a lot about Bug Bounty **is the remediation check.** With traditional penetration testing, you almost never get a remediation check. Following an audit, when a developer tell me "I fixed the bug", I only have his word. Bug Bounty allows me to delegate this control to the Researcher, who is perfectly 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 will be able to sleep soundly. (Laughs)

Have you seen any other changes since you started the Bug Bounty program?

There is more awareness, that's for sure, 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 and lead to much shorter time-to-remediation.

Acceleration of the patching rate / frequency

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 more and more upstream of projects, which allows 1/ to train our developers «on the fly» and 2/ to accelerate our deliveries - since there are much fewer patches to manage in the validation and release phases.
We became more responsive, in the interests of both developers and business.

The next steps?

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

Second step, where we are now, is to make the service available to our subsidiaries worldwide, by offering them something different and forward-thinking, allowing them to renew their vision of cybersecurity and audits.