GLOBAL LUXURY BRAND

Private Bug Bounty Program

CASE STUDY

CONTEXT

- Rapid revenue growth from digital channels
- Surge in cyber attacks in the last nine months

AN AGILE ORGANISATION

- Scale agile framework
- A DevSecOps platform
- A global 24/7 SOC team

CHALLENGES

- Align security with agile development and bi-monthly releases
- Audits may last up to a month but still don't go "deep enough"
- "Wild" vulnerability submissions through various channels

SOLUTION

- YesWeHack Private Bug Bounty program
- Deployment of a VDP with YesWeHack to follow

Our client, a global luxury goods company, was faced with a challenge common to many CISOs over the world.

The client was facing a massive increase in cyberattacks (more than one million in the last nine months), mainly due to their increased digitisation. This digital strategy encompasses more than a billion web pages, an expansion to the cloud, the opening of their information systems, and an increased use of APIs – all supported by agile development with continuous integration.

With digital change happening all around, there needed to be a parallel upgrade in security. The company realised the need for a modern, efficient security solution, better suited to their cybersecurity challenges. With new releases occurring every 15 days, that new model needed to be agile, innovative, and effective.

It was time for change and progress. Following consultation with various service providers, this world-renowned luxury brand chose YesWeHack to help implement a crowdsourced security strategy and launch their Bug Bounty programs.

This is their story: How the crowdsourced security strategy started, how it evolved, and what the future holds.

STEPS AND RAMPING UP

1 PROGRAMS DEFINITION

Our client began by launching two private Bug Bounty programs: one dedicated to their scopes in China and APAC, which feature dedicated infrastructures; the other focused on the 'rest of the world'. Their scope included a dozen URLs, several applications, and a few back-end APIs.

In terms of budget and rewards, our client accepted YesWeHack's recommendation to start small with a rewards budget of €15,000. They also concurred with our suggestion of rewards ranging from €100 to €1000 for a report.

"Unlike what U.S. providers will tell you, it is possible to begin a Bug Bounty program on a small budget." Deputy CISO, global luxury brand.

⟶ CUSTOMER'S TIPS

Leverage YesWeHack's expertise and advice to determine your perimeter and reward grid.

2 CHOOSING RESEARCHERS

For its scopes in China, our client needed local researchers that could read Mandarin. These researchers also needed knowledge of the country's local customs, owing to the specific nature of the applications, the unique approach to trading and buying, and the different tools compared to those used in Europe and the U.S.

YesWeHack connected the client a team of researchers that matched these expectations.

⟶ CUSTOMER'S TIPS

Ask YesWeHack for help in selecting your first round of researchers.

3 PROGRAMS LAUNCH

The first report arrived within 30 minutes of the program opening. After only four hours, more than eight reports had been submitted, including one critical and two high-level vulnerabilities.

⟶ CUSTOMER'S TIPS

1. *Do not launch your Bug Bounty program in the early evening if you want to sleep at night!*

2. *Be responsive. If you want researchers to be involved and stay active on your program, you need to respond quickly. Our goal is to have researchers' reports processed within three days.*

4 SEAMLESS INTEGRATION

To ensure vulnerability reports are shared quickly and reliably between researchers and development teams, our client uses the JIRA connector provided by YesWeHack. This way, tickets can be sent directly to the teams, facilitating remediation.

Learn more about how YesWeHack's bug tracking integration solution contributes to smarter DevSecOps communication and collaboration here.

5 TWO MONTHS AFTER LAUNCH

Two months on from the launch of Bug Bounty, approximately 30 reports have been submitted and 60% have been corrected. This first glimpse of the Bug Bounty model enabled our customer to realise the extent of the flaws in their infrastructure – especially in China. ***"We undertook significant penetration testing within our Chinese infrastructure. But they never uncovered the critical vulnerabilities surfaced by our Bug Bounty program."*** Deputy CISO, global luxury brand.

RISING TO THE TOP

Now that our client has a clear understanding of how a Bug Bounty program works, the team has decided to expand its scope, increase the rewards, and invite new researchers.

At YesWeHack, we always advise our clients to start small and grow step-by-step. This first phase is essential to understand how researchers work and how they think, but also how to deal with reports without being overwhelmed.

WHAT COMES NEXT

As a world-renowned luxury brand, our client receives wild reports on a regular basis, through various communication channels such as the service centre, mailings, and social networks. This makes it difficult to centralise everything, forward it to the right people, and treat it with the necessary severity.

To better manage these reports, our client is setting up a Vulnerability Disclosure Policy (VDP) with the help of YesWeHack. This allows them to:

- Centralise requests, ensuring they are sent to the right stakeholder internally.
- Reduce "noise": indeed, submissions will be completed by researchers using a dedicated and detailed online form.
- Standardise reporting formats between the VDP and the Bug Bounty program – streamlining internal processes and enabling automation at scale

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