combell

CUSTOMER STORY

How a webhosting company works with Intigriti to test infrastructure

CHIEF TECHNICAL OFFICER

Wesley Hof

Digital version?
Scan the QR code or go to
go.intigriti.com/combell-story

INTIGRITI

How a webhosting company works with Intigriti to test infrastructure

Wesley Hof is CTO at Combell — Belgium's largest web hosting company and part of hosting giant team.blue, which actively serves more than 2 million customers in 10 European countries. Combell offers two main product groups: shared hosting services for webspace, databases, SSL certificates and email, and cloud consultancy where they design, build and maintain infrastructures in a public, private or hybrid cloud environment.

The challenge

Infrastructure security testing through traditional penetration testing

When Combell wanted to improve their security testing, they found that many automated tools and platforms are focused on testing web applications. As a hosting company, Combell needs to also test infrastructure — and their shared hosting offer was an additional challenge. As multiple customers log in on the same system, it is important that customer A is not able to reach the data of customer B, for example. Data must always stay segregated.

Hof concluded:

> "To test our security, we needed to take the same approach as a malicious hacker: someone who creates an account, logs in on our systems and then tries to bypass virtual boundaries to reach the data of other customers. This type of strategy is very hard to accomplish with automated tools or through other platforms."

The solution

Crowdsourced security testing

Combell's specific need to test security with a hacker mindset led Hof to investigate crowdsourced security testing. He looked for a way to tap into the knowledge of external security researchers who use the same methods as a malicious hacker would.

Combell decided to start with an ethical hacking program managed by a bug bounty platform. Such platforms act as a facilitator between ethical hackers and internal IT teams.

Three main obstacles had to be overcome before starting with a bug bounty program.

> "The biggest challenge was that I had to convince my colleagues that bug bounty is the legal way to allow unknown people to try and ethically hack our platform. The second challenge was to reassure people that the amount we would pay for vulnerabilities wouldn't go through the roof. This leads to the third obstacle I had to address: the concern about the impact of the vulnerability reports on our DevOps team.
>
> The truth is, no matter how secure your infrastructure and your web applications are, ethical hackers will find vulnerabilities. You need to set time aside for your development teams to address the issues and fix the problems. It took some time and effort on an operational level to allocate time to solve issues when they would inevitably be found."

In the end, Hof and his team managed to convince their colleagues that bug bounty was the way to go, and the stage was set to get started.

Implementation and getting started with Intigriti

The positive experiences of Intigriti's existing customers made Hof want to try the bug bounty platform to see if it was a better fit for their security testing needs. Intigriti, which is headquartered in Belgium, also has a strong European presence — which was an added value for Combell as a Belgian company.

The setup process for launching a bug bounty program on Intigriti was straightforward for Hof and his team:

> "After we became a customer, we had a meeting to flesh out exactly how we wanted to scope the security testing and pentesting program, and then we started."

> The infrastructure side of things now gets tested, not just the web applications like with most security testing tools.

WESLEY HOF
CTO COMBELL

combell

INDUSTRY
Web hosting

EMPLOYEES
1,000

REVENUE
275 million EUR

The result

an increase in infrastructure vulnerability reports and better feedback

Once the program was up and running, the first vulnerability the researchers found was in relation to the infrastructure.

> “This reinforced that we had made the right decision”, Hof explained, “but we also now receive twice as many vulnerability reports in total on the application side as well. We also continuously get actionable and well-structured feedback from Intigriti’s triage team. The platform is intuitive to work with and reports are detailed (proof of concept is always included) which is very convenient for us.”

Clear communication between Combell and researchers results in faster fixes

Hof makes it clear that the value of Intigriti extends further than the quality and quantity of the vulnerability reports received through the platform:

> “Intigriti also encourages us to fix bugs within a decent time frame. If we don’t react to important bug reports quickly enough, someone from Intigriti will give us a call urging us to act immediately. With this kind of motivation and clear communication from Intigriti, our engineers can pick up security issues more quickly and solve bugs in production faster.”

Budget control for peace of mind

The initial concerns people at Combell had regarding the budget to set aside for bug bounty were quickly eased by Intigriti. Hof’s team periodically uploads a set amount of budget to the platform, and they cannot go over it:

> “When the funds are depleted, the vulnerability reports stop coming in. That’s a good way to keep the budget in balance.”

Intigriti as part of a connected, company-wide security approach

> **Intigriti is an entire part of our process now. We’re looking at rolling out Intigriti at other companies in the team.blue holding. We believe Intigriti is a great security tool for hosting companies.**

TAKE YOUR FIRST STEPS

- Request a demo intigriti.com/demo
- Visit the website intigriti.com
- Get in touch hello@intigriti.com

- 90,000+ researchers
- 400+ live bug bounty programs
- GDPR compliant
- Strong global presence

INTIGRITI

Information from Q1/2024. We are constantly growing, so please contact our sales department or see our website for an accurate number.