HR software giant Personio takes its bug bounty program to the next level

BY ANNA HAMMOND · MARCH 2, 2023 · LAST UPDATED ON MARCH 6, 2025

Arnau Estebanell, senior application security engineer at Personio, discusses the important role bug bounties can play in the security of SaaS businesses.

Personio is a European tech company that develops software to simplify HR management processes.

Following a successful invite-only bug bounty that launched last year with Intigriti, the company has taken the next step in its crowdsourced security journey by opening its program to all ethical hackers registered on the platform.

We caught up with Arnau Estebanell, senior application security engineer at Personio, for the details:

Hi Arnau! Tell us a little bit about Personio and your new bug bounty program

Arnau Estebanell: Our mission at Personio is to give HR teams time to focus on what matters: people. We help automate people processes and free up time for more strategic work, enabling HR to go beyond HR.

Since we started our journey in 2015, we've helped 8,000 HR teams across Europe focus less on administrative tasks and more on the people that drive their business forward.

We launched a private bug bounty program with Intigriti in September 2021. Following a successful launch, we moved to an application-level program. Now, after nearly 18 months and numerous submissions, we can confidently go to the next stage with a registered bug bounty program.

As your researchers know, a registered program is not publicly advertised on the Intigriti website, but is visible to anyone with an Intigriti account. This is one step away from a fully public bug bounty program.

Personio has opened up its bug bounty program to all researchers that are registered on the Intigriti platform

What drove your initial decision to launch a security bug bounty at Personio?

AE: Ensuring the safety of the data of our customers is the number one priority for Personio's Security team. As a growing startup, we must spend our time wisely and focus on what matters most. The great thing about bug bounty is that whenever a vulnerability is reported by a researcher, the impact is often clear due to the accompanying proof of concept. This means we can fix the vulnerability quickly and aren't dealing with 'theoretical' bugs, but ones that have proven impact.

On a personal note, I am an advocate of bug bounties. I have hunted in different programs in the past, and now I see the other end of it, helping Personio manage their BB program.

I was recently speaking at an InfoSec meetup, and someone asked me the question, 'What security solution gives you the best ROI?' The answer was clear to me, bug bounty.

When a researcher reports a critical or exceptional vulnerability, the value is immense. This is a vulnerability that could really hurt your company, and you are able to manage it and fix it with the confidence that the researcher is acting in good faith, while also rewarding them appropriately.

DON'T MISS Nurturing program engagement: Easy steps you can take to keep your bug bounty program ticking

Why do you feel it's important for an HR software – or indeed any SaaS company – to venture into the world of bug bounty or crowdsourced security?

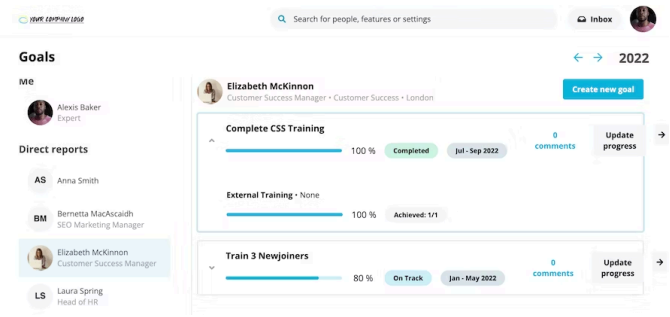
AE: Human resources teams often handle sensitive employee and company data, including salary details, healthcare information, and medical documents. As such, our customers need to know that their software provider can be entrusted with this information, so from our perspective, the more people that check our systems, the better.

Five years ago, Personio had around 30 employees. At that stage, and although security is something that has always been a top priority for us due to the sensitivity of the data we manage, there was no dedicated

security representative – this all landed with the developers, who also worked on the platform's security.

Nowadays, we have around 1,700 employees, and we keep growing, including the security team. The pace of growth that we've seen is quite the challenge, and that is why it is of paramount importance to find security solutions and providers that are able to scale with you.

Having a pool of 70,000 researchers available to help test the security of a SaaS platform not only gives you more eyes on the code, but it also helps an organization scale its security team in a realistic way, by focusing on vulnerabilities based on impact.



Personio's HR software solution is used by SMEs around the world

What impact has your bug bounty program had on your internal security and development teams?

AE: When you receive a critical or exceptional vulnerability, it is clear for the development teams that there's an issue that needs to be fixed. With a bug bounty, proving the impact of the vulnerability is never a challenge.

Having a third party discover these bugs can really shake things up internally, in a positive way. Vulnerabilities reported on the bug bounty are often fixed in a matter of hours. It is not one colleague telling a dev team that something is wrong, it is external researchers showing you how they could harm your company.

One particular thing that I like about the bug bounty and the triage team from Intigriti, is that in terms of signal-to-noise ratio, there is no noise and all the vulnerabilities that get to our vulnerability board have been previously verified.

READ MORE Empowering hackers through bug bounty and crowdsourced security

From a technical perspective, what has your bug bounty program helped you to achieve that other security testing services might have missed?

AE: One example that immediately comes to mind is when we started receiving multiple cross-site scripting (XSS) reports from a single researcher. We had three reports that were all very similar, and the researcher kept using certain characters in his payloads. It was clear that this researcher knew something about our system.

We started an internal investigation and soon realized that the issue had to do with a flaw in the way we were performing input sanitization. This researcher had a lot of experience with a particular framework and their reports allowed us to fix the issue at its source. If we only had one submission of this type, it's unlikely that we would have fixed the underlying issue.

What's next for Personio? Are you considering launching a fully public bug bounty program at some point?

AE: We look forward to seeing the results of our newly launched registration-level bug bounty, which allows anyone with an Intigriti account to view and work on our program.

Who knows, once this program has bedded in, we may well launch a full public program further down the line.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com