Visma's Bug Bounty Program Manager speaks to Intigriti about the practice of running a successful program

BY ANNA HAMMOND · AUGUST 24, 2022 · LAST UPDATED ON MARCH 6, 2025

Visma is a leading provider of cloud software solutions in Europe and Latin America. With around one million public and private sector customers for their software solutions across the Nordics, Benelux, Central and Eastern Europe, and Latin America, the organization works continuously to maintain a robust security posture.

In this interview, we speak to one of the keystones of Visma's security policy—Ioana Piroska, also known to many as the "Mother of Hackers." We previously talked to Ioana at the end of 2021 after the 1337UP1121 live hacker event, which Visma hosted in partnership with Intigriti. In today's interview, we discuss Visma's security program and how bug bounty programs have become essential to Visma's security posture.

Intigriti interviews Visma's Bug Bounty Program Manager, Ioana Piroska (Mother of Hackers)

Intigriti: Hi Ioana, can you start by introducing yourself and explaining your role at Visma?

Ioana: Sure! I work as a security engineer and I'm also the Bug Bounty Program Manager in the security team at Visma. Regarding the team, our job is to help all our many internal teams improve the security of their products. We do this through a security program called VSP (Visma Security Program).

We have many services in VSP: training and awareness, code scanning SAST and DAST (static and dynamic application security testing), internal pentesting, threat intelligence, log management, incident response, and more.

Bug bounty and responsible disclosure (RD) are an essential part of VSP, and it's the final layer of security verification we can do for our applications.

Intigriti: You have an unusual nickname, "Mother of Hackers." Where does it come from?

Ioana: I work with hackers every day and try to maintain their engagement by being fair, always explaining my decisions, and being consistent. In other words, I behave like a mother! That's why my colleagues started calling me the "Mother of Hackers." It was made official with a Twitter account where I post the latest updates and news about our bug bounty programs.

Intigriti: What were your most significant security pain points before setting up a bug bounty program?

Ioana: Number one was being able to find vulnerabilities that pentests or automated tools (such as vulnerability scanners) cannot.

Visma is a huge company with many different software solutions, from ERP systems to school and healthcare systems. We have software and services running in the private and public sectors. Given our size, automation and scaling are very important, but the security of our products is also absolutely crucial.

Running a bug bounty program was seen as an important way of scaling our security program beyond the limitations of automated scanners as Visma continues to grow.

Today, having a bug bounty program has helped us to improve our security posture a lot.

What was your biggest challenge in starting a bug bounty program?

Ioana: As I mentioned a moment ago, Visma is a very large and diverse company with many offerings. Consequently, the big challenge is finding a product's owners, which is especially true with the responsible disclosure program, where everything that Visma owns is in scope.

Intigriti: How did you overcome this challenge?

Ioana: The first step was to create awareness about our bug bounty programs and to create an onboarding process for new teams wanting to join.

We have automated some of the processes related to this. For example, our red team has created a framework that updates our Visma-owned assets database daily. We maintain a clear and up-to-date overview of our attack surface by utilizing new assets and software and by discovering new vulnerabilities.

We have developed a tool for all our security services that facilitates the onboarding process of the internal teams. Additionally, we use this to gather information about assets, products, and infrastructure to find who is responsible for what more easily. That's the advantage of having all services recorded in one place.

Intigriti: Why did you choose to work with Intigriti?

Ioana: Several reasons. First, Intigriti is based in Europe, like Visma. This makes things like managing the money pool and invoicing process easier. Since Intigriti is Europe's number one bug bounty program provider, we decided to get in touch.

We were also convinced of Intigriti's enormous potential, and this is evident in the company's growth in the two years we've been working together. Finally, we liked that Intigriti was very personal and willing to fulfill our needs and collaborate continuously.

Intigriti: You came to Intigriti from another service provider. What differences do you see working with Intigriti?

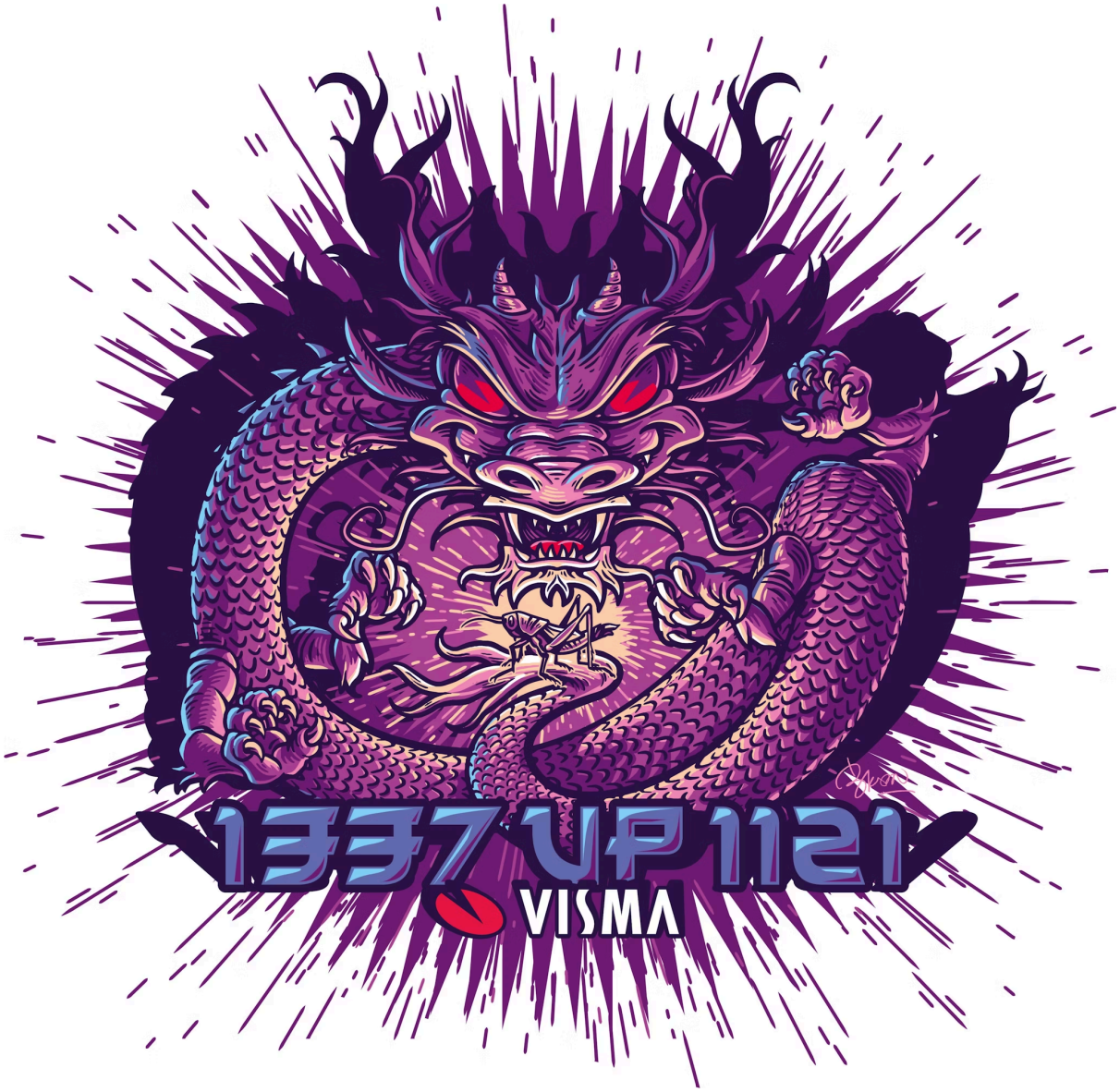
Ioana: Our previous vendor was one of the first and is very big. Intigriti is smaller and more personal. They are much closer to their customers.

Intigriti is based in Europe. That means we have no hassle with money pools. The money is immediately available.

We also have personal and direct contact with our Success Manager, Neil. He's very approachable via Slack and replies almost instantly.

The product team is also great. They listen. Several features have already been developed after we requested them.

Finally, when we organized a virtual live event, Intigriti's involvement was remarkable. They provided the infrastructure for the swag store, sending swag and dealing with complaints from people who didn't receive their swag. Intigriti took that pain away.



Visma's virtual live hacking event, 1337UP1121

Intigriti: Which goals did you set for your bounty program? Did you achieve them?

Ioana: The initial goals were as follows:

- Onboard new product teams continuously
- Launch the responsible disclosure program on the platform
- Onboard our marketing websites to the bug bounty program
- Be fast to triage, pay and resolve

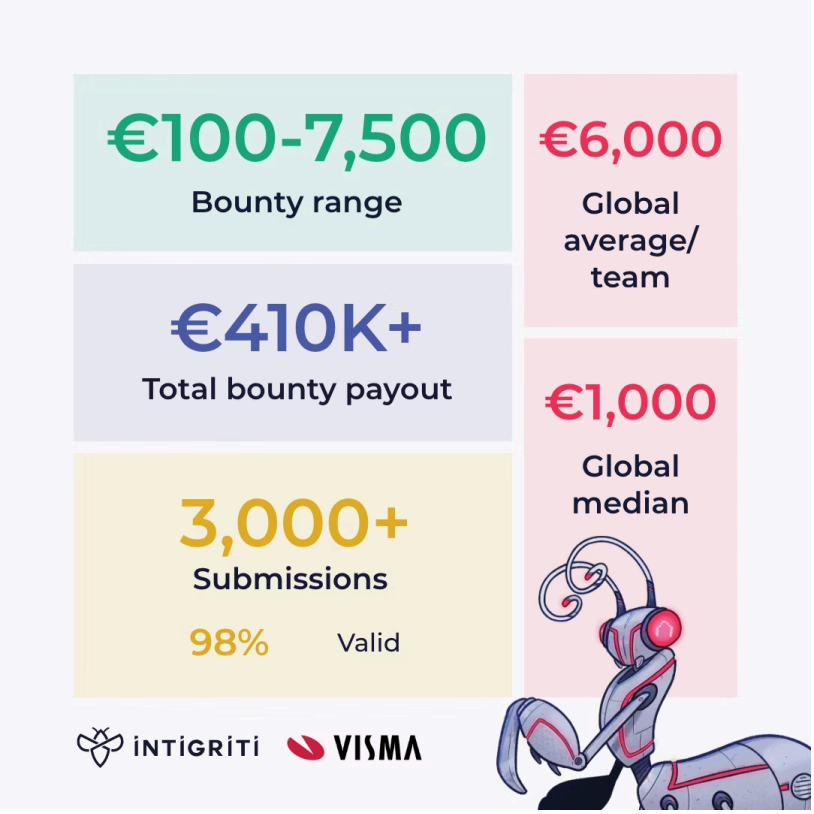
All these goals were achieved. We brought more than 50 product teams onboard, along with over 80 marketing websites. Our responsible disclosure program was launched at the beginning of 2022, too.

Now we're working hard to expand the program's scope. Our long-term goal is to add everything Visma owns to the bug bounty program scope.

Intigriti: What have you discovered from running bug bounty programs on Intigriti?

Ioana: We discovered that even though we have a pretty strict onboarding process and do security tests internally before teams join the program, we still see many vulnerability findings thanks to the bug bounty program.

Since we launched, we've seen more than 3,000 submissions, most of which have been valid. The submissions amount to more than €410K spent on bounties. However, we are more secure as a result of the bug bounty programs we run on Intigriti.



Visma's bug bounty program success overview

We realized that the most common type of vulnerability that we have at Visma is Insecure direct object references (IDOR) or access control problems. More than 50% of the bugs that we get are of this type.

These are bugs that cannot be found with the automated tools for scanning. You need to understand the application flow to identify them, and only the human mind is capable of doing this. I believe this is one of the most important added values bug bounty programs bring.

Intigriti: What impact does running a bug bounty program have internally? Have you seen any specific benefits? Do you have examples?

Ioana: The bug bounty program has had an immense impact internally at Visma! Our internal teams feel more confident about cybersecurity after onboarding to Intigriti, and once they've fixed the vulnerabilities reported by the bug bounty program, their confidence grows even more.

They've seen how hackers think and how they were able to find specific types of vulnerabilities. This has helped them develop their products as "secure by design."

They've also learned a lot from the reports. These are a great way to see their mistakes and learn how to avoid them in the future. It's an ongoing process.

As for findings, the most impactful ones are the critical or severe ones, of course. We rarely get them, but yes, we've received some. And because we try to be as transparent as we can to help others, here's a shortlist of the most impactful bugs we've seen:

- HTTP request smuggling

- Remote code execution (RCE)
- Account takeover through different creative methods

Vulnerabilities like these could have had huge consequences if they had not been surfaced and fixed as a result of our bug bounty program. So, in general, we've increased the security awareness internally due to VSP, but especially because of our bug bounty program.

Intigriti: What would you say to someone considering starting a bug bounty program?

Ioana: The benefits of having a bug bounty program are immense. For Visma, it has proved itself as one of the best ways to minimize risks and secure our assets in a fast and controlled way.

This came with some costs, yes. But those costs are nothing compared to how much the company would have lost in the case of a successful security breach. Espen Johansen, our Security Director, says:

> **"$1 spent on a bug bounty program is $10 – $100 saved later."**

I completely agree with him and consider that having a bug bounty program is worth the effort and the costs. Just allocate a budget and start doing it. You will immediately see results!

Intigriti: What do you think of responsible disclosure as a standard?

Ioana: I think responsible disclosure is the minimum that a company can do to secure its assets with the help of ethical hackers. You don't even need a platform for this. You can publish the policy on your website and start doing it.

It's a great way of improving security by taking advantage of the skills of security researchers around the world. Responsible disclosure should be a standard nowadays, definitely.

Intigriti: In addition to security, what are the other benefits to running a bug bounty program you've experienced?

Ioana: We always had a lot of support from management at Visma around security. But since we've been running our bug bounty program, we have even more support because they see and understand the risks better.

We've also seen increased customer trust. We try to be as transparent as possible about the findings and lessons learned from our bug bounty program. Customers appreciate this openness.

The reports from the bug bounty program also provide fantastic learning tools for us in the security teams and our developers. Finally, the continuous nature of the teamwork and collaboration is a real advantage for cybersecurity.

Learn more

Intrigued by what you have read? Want to know more about bug bounty programs? Get in touch to request a demo with a member of our team today.

About Ioana

Ioana Piroska is a Security Engineer at Visma Software, based in Timisoara, Romania.

She is the Bug Bounty Program manager at Visma, helping the service delivery teams during the onboarding process and throughout their Bug Bounty journey. Her goal is the success of the program by making sure the hacker's engagement is maintained.

As a mother of two, she balances work life and family life very well, always finding some free time for her hobbies such as reading, sports, and baking.