How Visma uses Intigriti to protect an ever-expanding attack surface

About Visma

Visma is a leading provider of cloud software solutions in Europe and Latin America, with over 1 million active customers. They provide solutions that simplify and digitize core business processes. Their vision is to shape the future of society through technology by building and delivering software solutions in the private and public sectors.

The challenge

Providing complete cybersecurity for a vast and rapidly evolving attack surface

Visma has a roster of over 6,000 talented developers pushing out software on agile timeframes from multiple entities. Visma is also growing fast. On average, they acquire a new company at the staggering rate of nearly one per week. These factors make a well-organized and scalable cybersecurity strategy for their attack surface essential. However, they also make it very challenging.

As Visma's Security Engineer & Bug Bounty Program Manager, Ioana Piroska has a key role in ensuring onboarding and continuous security assurance for the internal teams at Visma.

> "Our job in the security department is to help all these internal teams improve the security of their products. We do this through a security program called the Visma Security Program (VSP). VSP includes training and awareness, code scanning SAST and DAST (static and dynamic application security testing, internal pentesting, threat intelligence, log management, incident response), and more."

CASE STUDY

Although this thorough approach achieved good results, it wasn't sufficient in protecting against specific security threats that Visma faced. As Ioana explains:

> "There are bugs that automated tools for scanning cannot pick up. For these, you need to understand the application flow. Only the human mind is capable of doing this. So, while our automated tools are vital, they can't cover all the required bases."

Visma, therefore, knew they needed a human component that would complement and complete their security testing.

VISMA

COMPANIES
200+

COUNTRIES
37

DEVELOPERS
6000+

INDUSTRY
International conglomerate

ACQUISITIONS/YEAR
40+ new
1 every week

The solution

Using the Intigriti bug bounty platform to leverage human skills

Scanners and other automated cybersecurity testing tools are renowned for finding common vulnerabilities in systems and software. However, they have their limits, so Visma turned to the Intigriti bug bounty platform to supplement their automated testing.

Rapid scalability was a must for such a large and diverse company, as was high-quality support as they quickly grew their presence on the Intigriti platform. Ioana explains why the partnership with Intigriti immediately worked so well:

> "Intigriti is very close to its customers. We have personal and direct contact with our success manager, who answers our questions almost instantly via Slack. At the same time, the product team listens, and we've seen several features implemented on our request."

> Our Security Director has a simple rule of thumb. He says $1 spent in bug bounty is between $10 and $100 later — and I completely agree with him.

IOANA PIROSKA
SECURITY ENGINEER & BUG BOUNTY PROGRAM MANAGER, VISMA

Continuous onboarding and security testing

Ioana's team is responsible for security onboarding and providing continuous security support for all the internal teams. Sometimes the scale of the operation and the pace of new acquisitions make knowing what digital assets each entity owns a challenge:

> "Our bug bounty is an important way of scaling our security program while the company grows. With so many companies in our organization, gathering information about all the assets, products, and infrastructure on our attack surface can be challenging. So, we started to create awareness about our bug bounty program and developed an onboarding process for the new teams that want to join."

This onboarding encouraged newly added and existing companies to bring their assets and solutions forward for testing via a bug bounty program. This, in turn, helped to increase attack surface visibility throughout the organization, while also providing all the advantages of crowdsourced bug bounty programs.

The result

Hitting security goals

When Ioana and her team set up their Intigriti bug bounty programs at Visma, they had some clear goals in mind. These included continuously onboarding new product teams; onboarding their marketing websites; launching a Responsible Disclosure program on the platform; and making sure they had a fast process in place to triage reports, pay bounties, and resolve bugs.

They hit every goal and saw a significant improvement in cybersecurity as a result.

Beyond scans and pentests

Pentests and other automated scans remain a critical part of VSP at Visma. However, Ioana is clear that bug bounty programs need to complement these processes to provide additional cybersecurity testing:

> "With bug bounty programs, your tests are performed continuously, compared to a normal pentest which takes place once or twice a year. Add to this the advantage of the number of testers you have through crowdsourcing. In a bug bounty program, hundreds of testers can look at your digital assets simultaneously."

Ioana also worked with her Intigriti Success Manager to tailor private bug bounty programs to Visma's specific needs for the initial onboarding of products:

> "With Intigriti, we were able to run private programs where we could choose which specialized hackers to invite to cover all programming languages, web apps, and mobile apps. As a result, the quality of the reports is outstanding."

Greater visibility and security awareness internally

Using bug bounty programs as a core component of VSP has paid dividends for security at Visma. Since launch, the program has already received over 3,000 submissions, 98% of which are valid. As Ioana explains:

> "More than 50% of the vulnerabilities discovered are IDOR or access control problems, which are bugs that automated scanning tools cannot find. In my view, this is one of the highest values of bug bounty programs in general. Some of these findings could have had huge consequences if they were not surfaced and fixed as a result of the bug bounty program."

Beyond these timely findings, Ioana has seen other significant benefits to running a bug bounty program through the Intigriti platform:

> "The reports we receive are great learning materials for our internal teams. They see their mistakes and learn how to avoid them in the future. They also learn how hackers think, and this helps them create products that are "secure by design." There's no doubt that security awareness has elevated because of the program. Today our teams feel more confident about security."

The team's time to fix vulnerabilities also decreased as a result of these factors.

Looking forward

As expansion at Visma continues apace, so too will the need for continuous security testing. Ioana is certain that as the company grows, bug bounty programs will become even more integrated into the business.

> **Bug bounties are a critical part of VSP. It's the final layer of security verification that we can do for our applications before and after release day. We will continue to expand the scope, and our long-term goal is to eventually have everything that Visma owns added in the bug bounty scope.**

IOANA PIROSKA
SECURITY ENGINEER & BUG BOUNTY PROGRAM MANAGER, VISMA

TAKE YOUR FIRST STEPS

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

- **50,000+ researchers**
- **400+ live bug bounty programs**
- **GDPR compliant**
- **Strong European presence**

intigriti

Information from Q2/2022. We are constantly growing, so please contact our sales department or see our website for an accurate number.