What Telenet, UZ Leuven and an ethical hacker say about Intigriti's ethical hacking and bug bounty platform.

BY INTIGRITI · MAY 5, 2020 · LAST UPDATED ON AUGUST 8, 2026

Want to read the latest version? Visit the link below:

https://www.intigriti.com/blog/customer-stories/what-telenet-uz-leuven-and-an-ethical-hacker-say-about-intigritis-ethical-hacking-and-bug-bounty-platform

> *Unfortunately, or fortunately, the researchers already found a couple of things. For me, that proves working with an ethical hacking platform is an important part of our security process, and we'll keep working with ethical hackers in the future.*"
>
> – Reinoud Reynders, IT-Manager Infrastructure and Operations, UZ Leuven

About

Telenet: Telenet, a provider of media, telecommunications and entertainment services, employs 2,300 people and has a revenue of over 2.5 billion euro.

https://www.youtube.com/watch?v=yHR0pHhynv8&rel=0UZ Leuven: UZ Leuven is a renowned university hospital with around 2,000 beds and over 9,000 employees. The information technology department is of strategic importance, as the hospital and its staff heavily rely on IT for medical and administrative applications.

Arne Swinnen: Arne Swinnen is a security expert who has been hunting IT security bugs on both public and private bug bounty programs as an ethical hacker since 2016.

It takes two to tango

That saying goes for ethical hacking as well.

Ethical hackers are independent IT security researchers who strive to make companies more secure by finding vulnerabilities in systems before these become problematic. It takes relentless searching and a creative mindset to be a researcher. When their work results in finding an issue, researchers receive a reward, called a bug bounty.

Back to the tango. Preventing breaches through bug bounty is like an intricate choreography between a company's IT team on the one hand, and the ethical hacker or researcher community on the other.

In this dance, Intigriti's ethical hacking platform acts as the choreographer. The platform manages the communication between internal and external IT security people, and makes sure everybody is dancing to the same song.

To honour the complementary nature of ethical hackers and internal IT security teams, we asked members of both groups to talk about what it's like to work with the Intigriti platform.

Speaking for the researcher community, we have Arne Swinnen. Representing companies' internal IT specialists, we talked to Reinoud Reynders, IT-Manager at UZ Leuven and Eric de Smedt, Manager Cyber Security at Telenet Group.

What is Bug Bounty?

Arne Swinnen, ethical hacker:

"The bug bounty concept allows ethical hackers to investigate company systems via a platform like Intigriti. Vulnerabilities are reported so they can be fixed."

Security in the age of continuous development

Why does a university hospital work with ethical hackers?

Reinoud Reynders, IT-Manager Infrastructure and Operations, UZ Leuven: Security is very important for UZ Leuven. We do a lot of classical testing, like pentesting and vulnerability tests, but that wasn't good enough for us. Our apps are continuously being updated. It turned out impossible to use only classical pentesting to secure them.

How does UZ Leuven benefit from Intigriti?

It's much easier to secure fast-evolving apps through an ethical hacking platform. The researchers on the platform look for bugs and security leaks on a continuous basis.

Ethical hacking through the eyes of a Senior Cyber Consultant

What is it like to work with a community of people who you don't know in person?

Eric de Smedt, Manager Cyber Security at Telenet Group: Intigriti offers an international platform, where ethical hackers have to register. That makes it more trustworthy for us as clients. They also offer a platform for ethical hackers to get recognition. There's a hall of fame (Intigriti's leaderboard) for where ethical hackers earn points for reporting issues and get a ranking accordingly.

Ethical hackers: motivated by looking for problems

Arne Swinnen, ethical hacker: I see it as a challenge to look for problems in company systems in a responsible way. You also get rewarded, which makes it interesting as well. The fact that I can find problems for certain companies is good for my résumé too.

Bug bounty vs pentesting

What are the biggest differences between traditional security testing methods and ethical hacking?

Reinoud Reynders: An ethical hacking platform is interesting budget-wise. You only pay if an ethical hacker manages to find something. A pentest is commissioned for 10 days (give or take), but you don't

know what the result will be.

Eric de Smedt: Intigriti also offers the possibility to put up public projects that can then be tested. You can also create specific projects for more focussed security tests, and even invite certain ethical hackers to work on a specific project.

The community of ethical hackers

Arne Swinnen: Every researcher has a speciality. That's the strength of the concept: when more eyes are looking at a company system, more problems will be found.

Bug bounty as an extra layer of security for many types of companies

Who would you recommend Intigriti to?

Eric de Smedt: Every company that offers online services can make use of this platform. In particular eCommerce brands and applications whose business model involves customers ordering things.

Finding vulnerabilities: part of the security process.

How have ethical hackers helped you?

Reinoud Reynders: Unfortunately, or fortunately, the researchers already found a couple of things. For me, that proves working with an ethical hacking platform is an important part of our security process, and we'll keep working with ethical hackers in the future.

Do you want to know more?

Our team is ready to answer all your questions about IT security testing, the Intigriti platform, pricing or anything else. Get in touch to request a demo.

REQUEST A DEMO	VISIT THE WEBSITE	GET IN TOUCH
intigriti.com/demo	intigriti.com	hello@intigriti.com