A GUIDE TO

Navigating vulnerability disclosure for the transport and logistics industry

Continuous security testing powered by crowd knowledge

EBOOK

Table of contents

Introduction

What do aviation, maritime, automobile, freight, logistics, and supply chain industries have in common? Besides all falling under the transportation and logistics (T&L) sector, they also possess significant amounts of valuable data. Unfortunately, this makes them highly desirable targets for cyberattacks.

The T&L industry is becoming increasingly dependent on innovative technology and automation. Like most industries, with rapid digitalization comes an increase in cyber threats.

Furthermore, for interconnected industries that are part of a supply chain, the threat of a cyberattack becomes more concerning and complex. In recent years, for example, there have been several examples of cyberattacks due to a third-party supplier data loss incident.

To safeguard assets, customers and staff, state-of-the-art cybersecurity defenses and attack surface management are essential. Luckily, T&L organizations don't need to fight this cybersecurity battle alone. Worldwide, tens of thousands of security researchers are using their ethical hacking skills for good.

If you're reading this eBook, it's fair to assume that you are already facilitating the process for better security testing. In this eBook, we will explore:

- **Who** ethical hackers (security researchers) are
- **Why** the T&L industry works with ethical hackers to strengthen their cybersecurity defenses
- **What** the difference is between responsible disclosure and incentivized disclosure methods
- **How** bug bounty programs differ from traditional security testing methods

Plus, we'll cover best practices for creating a strong vulnerability reporting process.

A snapshot of noteworthy cyberattacks in T&L during the last five years

2020

EasyJet

In May 2020, EasyJet, a low-cost British air carrier, confirmed that it had fallen victim to a cyberattack in January. The cybercriminals had successfully gained access to the email addresses and travel information of around 9 million customers through a highly-sophisticated attack.

2021

Colonial Pipeline

In May 2021, a cyberattack effectively shut down the Colonial Pipeline, which provides gasoline to almost half of the east coast of the United States, for about a week. At the time, the company estimated that the cost of the ransom and the disruption to business could run upwards of $50 million.

2022

Expeditors International

Expeditors International, a global logistics company, had to shut down most of its systems worldwide following a cyberattack in February 2022. The incident cost Expeditors $47 million in extra charges for prolonged use of shipping containers at depots and terminals.

2023

KNP Logistics

KNP Logistics suffered a major ransomware attack in June 2023 which impacted key systems, processes and financial information. Unfortunately, the business went into administration shortly after the cyberattack.

[1] https://go.intigriti.com/easyjet
[2] https://go.intigriti.com/Colonial-Pipeline
[3] https://go.intigriti.com/expeditors-international
[4] https://go.intigriti.com/KNP-logistics

Hiring ethical hackers enables T&L businesses to:

- Reduce the risk of losses from a cyberattack
- Show a commitment to continuous security testing
- Increase their reputation and trustworthiness as data protectors
- Keep up with ever-evolving cyber threats
- Develop their internal teams based on key learnings and insights.

Why T&L organizations hire ethical hackers

Ethical hackers are highly skilled individuals that can safely simulate the behaviors of malicious hackers to highlight weak links and blind spots in a company's digital environment. By working with ethical hackers, T&L organizations can be alerted to their security vulnerabilities before they're potentially exploited.

Not only does this improve the strength of their IT security posture, but it empowers them to stay one step ahead of cybercriminals. Another reason companies employ ethical hackers is because it helps limit their liability. In the case of a real cyberattack, for example, businesses can demonstrate the steps they've taken to avoid it.

"We need the support of ethical hackers to reinforce our IT Security before non-ethical hackers find a possible vulnerability which, of course, they will not report to us.

JEAN-FRANÇOIS SIMONS
CISO, BRUSSELS AIRLINES

Many in the security industry describe vulnerability disclosure policies as following a

“see something, say something

approach.

Clear vulnerability reporting structures

What is a vulnerability disclosure policy?

Having a vulnerability disclosure policy (VDP) for your website is important because it allows ethical hackers (and good-willed citizens) to assist your business if they come across a security vulnerability.

By having a policy, your business:

- Shows a public commitment to cybersecurity
- Builds trust with customers and other stakeholders
- Reduces the risk of potential exploitations going undetected
- Decreases the risk of losing revenue due to an expensive cyberattack
- Minimizes time-to-remediation
- Streamlines your vulnerability reporting process

Without a VDP, 44% of vulnerability submissions aren’t successfully reported

When an ethical hacker identifies a vulnerability, the majority will look for a way to report it to the concerning business.

Worryingly, 70% of Intigriti’s ethical hacker community have identified vulnerabilities for websites without a VDP. Of that group, 12% didn’t escalate the report. For those that did, 32% of them said the report got lost in the process or they weren’t sure whether it was successfully reported. That’s 44% of the risks that remain potentially undetected.

VDP best practices: What to include

01

Company background

Make sure to provide a brief background on your business within this opening section. For example:

- Who you are
- Business purpose
- Unique selling points
- Customers
- Other relevant stakeholder groups

The reason for providing context around your business is because it helps the researcher know what is important to you from a security standpoint.

02

Commitments

In this section, you can declare your commitments to customers and stakeholders, and explain how you intend to keep their data safe. This is a good opportunity to introduce the reasons why you have the policy, and how it helps your business honor its promises.

03

Scope

The scope is mostly directed at security researchers but is helpful for other stakeholders (such as partners, regulators and the media) to be aware of too.
The essence of this section is to guide researchers on what is acceptable to test for vulnerabilities. However, the scope also defines:

- Types of vulnerabilities that should be reported
- Products, features or assets that your company would especially like researchers to test
- Behavior that is not allowed, such as disruption testing or privacy violations.

A good scope will not only clearly explain what the company perceives to be within the scope but also what they perceive to be on the outside. Doing this helps put everyone on the same page from the offset.

TIP

SCAN
TO SEE MORE VDP TIPS ON OUR BLOG[5]

[5] https://go.intigriti.com/vdp

A good VDP should detail what information the security researcher should report, as well as what they can expect from the disclosure process.

04

Legal safe harbor

You want ethical hackers to disclose bugs in your system responsibly without fear of legal consequences. Therefore, it's important to provide permission to act and to assure that no legal action will be taken against them, provided they remain in scope.

You're actively trying to encourage ethical hackers to report issues to your business. The language you use should be clear, concise but also inviting.

Here is an example of what you could write as part of your safe harbor policy:

> "[Your company name] considers ethical hacking research conducted consistent with this policy to constitute as "authorized" under criminal and civil law. [Your company name] will not pursue civil action or initiate a complaint about accidental, good faith violations.
>
> If legal action is initiated by a third party against you and you have complied with the Terms, [Your company name] will take steps to make it known that your actions were conducted in compliance and with our approval."

05

Reporting methods

This section outlines the process for how ethical hackers should submit vulnerabilities to your business. Be as clear as possible and never assume contributors will know what information you need to process a report. Cover aspects such as:

- Preferred communication channels
- What information they should include
- Whether you require submissions to be written in a specific language

Bear in mind that the researchers have already invested significant time and effort to test your systems so it's important to only ask for information you'll genuinely need. Ask for too much and you may put contributors off entirely.

06

What to expect after a submission

This area of the policy is a good place to outline how reports will be evaluated and what happens when they're accepted or rejected. You should also define a timeline for when they can expect to hear from you.

Including this information helps to manage expectations with regards to what kind of acknowledgements, recognitions and remuneration researchers can expect to receive. You should also indicate when researchers will know (if at all) whether they can publicly disclose a vulnerability they reported to you.

Moving beyond “see something, say something” and **incentivizing action**

Unlike a VDP, which takes a more passive approach to vulnerability reporting, bug bounty platforms allow businesses to work with independent security researchers to report bugs proactively.

Companies will often launch and manage a bug bounty program through a platform, like Intigriti. Organizations with high-security maturity may open their bug bounty program to all ethical hackers in the platform’s community—known as a public program. However, most businesses begin by working with a smaller pool of security talent through a private program.

How bug bounty platforms work

Intigriti defines crowdsourced security through bug bounty platforms as "agile security testing powered by the crowd." Below, we outline how a bug bounty platform is the connecting agent between thousands of ethical hackers and security-driven organizations.

Crowd

A global community of ethical hackers test your systems, software, digital assets, and devices against realistic threats. Ethical hackers look for weaknesses in your security in precisely the same way malicious hackers do, then report their findings.

Bug bounty platform

An interactive platform, usually a cloud service, that facilitates secure communications between ethical hackers and IT security teams, featuring real-time reports of identified vulnerabilities.

Expertise

Tap into the skills, knowledge, and experiences of an entire ethical hacker community. Plus, benefit from client support, continuous hacker engagement, technical expertise, program management, and more.

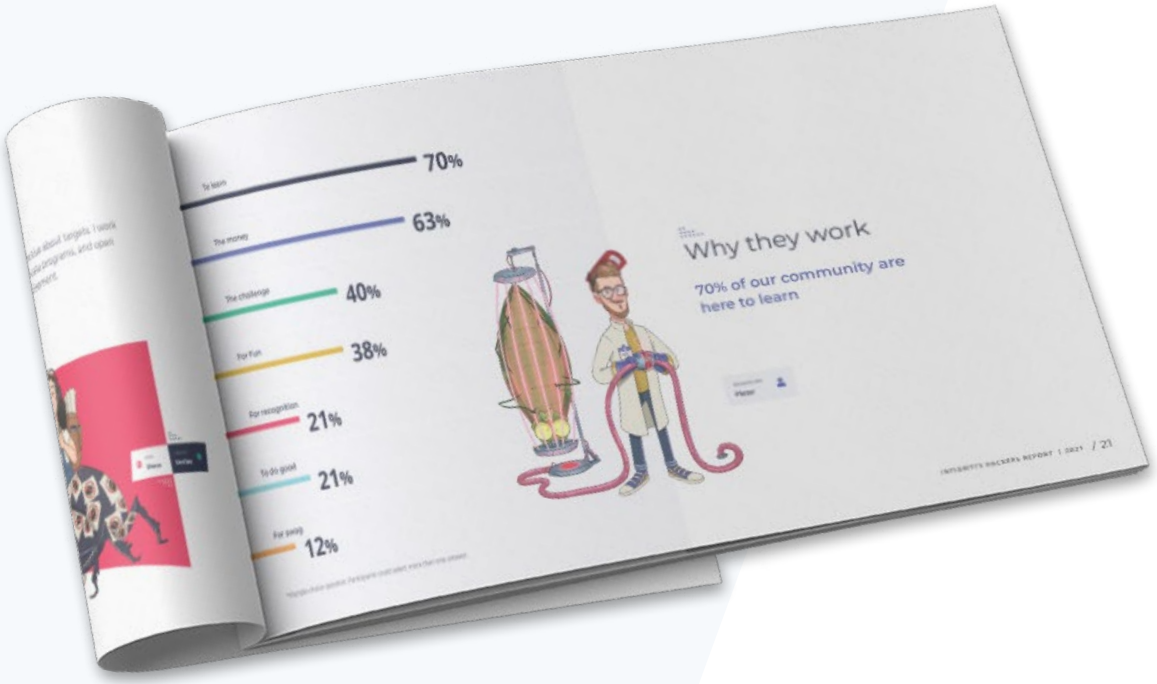
VDP vs bug bounty programs: What's the difference?

The key difference between a VDP and a bug bounty program is that a VDP follows a passive approach whereas a bug bounty program incentivizes action. Go to the next page to understand the similarities and differences between them on Intigriti's platform.

	VDP	BUG BOUNTY
Compliance	**Meets industry standards** | Supports ISO/IEC 29147:2018	
Legal considerations	**Provides a legal framework** | Companies provide contributors with assurance that no legal action will be taken against them provided reports are made in good faith.	
Vulnerability management	**Track submissions in real-time** | Companies can streamline the vulnerability disclosure process and keep track of submission security statuses in real-time, allowing them to obtain an accurate view of their security posture at all times.	
Communication	**Centralised within the platform** | No need for sharing encrypted mails, the platform will allow communication in a safe and reliable way.	
Search culture	**Say something, see something** Allows people to report security issues when they notice them, without being afraid of legal repercussions.	**Actively search & find something** Security researchers are continuously activated through bounties, without being afraid of legal repercussions.
Reward system	**No promises** There is no promise for a reward, but a thank you is appreciated.	**Rewarded for results** Enables continuous security testing by incentivising the community through bounties. The size of the reward depends on impact (severity).
Researcher quality	**A diverse community of security enthusiasts** | In our experience, beginner to intermediate security researchers tend to focus on VDPs, whereas bug bounties attract more experienced hacking talent.	
Quality assurance	**Handled by Intigriti** | Intigriti's triage team provides a layer of quality assurance before escalating vulnerabilities to businesses. This means your security team only receives reports that are valid, unique, and in scope.	

Ethical hacker communities

Ethical hackers are highly inquisitive, curious, and investigative people. They're eager to develop their knowledge of the fast-moving and ever-changing security landscape.



The Ethical Hacker Insights Report[6] found that 70% of our hackers operate on our platform to learn and develop their skills, and 40% are driven by the challenge.

For a fifth of our community, making the internet a safer and more secure environment is their primary goal.

[6] https://go.intigriti.com/ethical-hacker-insights-report

Earning potential is also an attractive aspect for security researchers. **Just over three-quarters (76%) of our community hack with a financial motive.** For example, 20% search for low-hanging fruit by choosing what they describe as 'easy targets.' 23% seek out bounties that offer fast payments, and a third (33%) look for vulnerability programs that offer a large maximum or minimum payment.

Reasons for picking a bug bounty target according to The Ethical Hacker Insights Report[6]

68%
says lots of scope

42%
says responsive team

80% of our community work within the IT industry and use Intigriti as a secondary source of income.

Where do the rest come from?

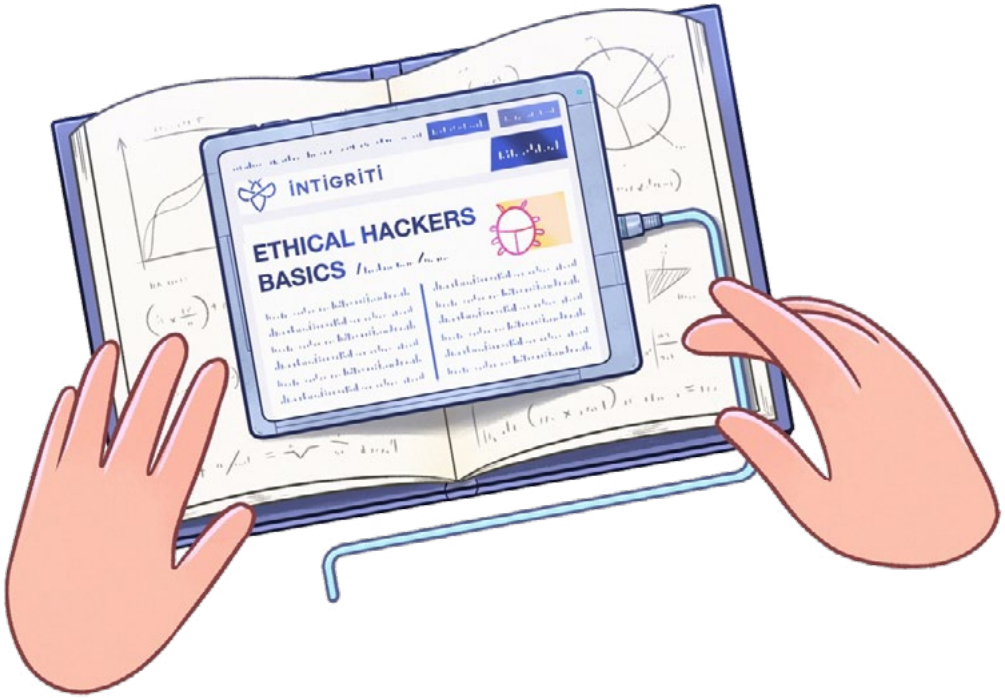
- Engineering or manufacturing
- Business, consultancy, or management
- Healthcare
- Teacher training or education
- Accountancy, banking or finance
- Energy and utilities
- Media
- Retail
- Law
- Public services or administration

Most of Intigriti's researchers are young adults — but don't let that dupe you into thinking they're lacking experience. **More than half (55%) of our community have completed a bachelor's degree and a further 15% have a master's degree.** The majority are working within cybersecurity-related jobs and 40% hold an official information security certificate.

The majority (80%) of our community work within the IT industry and use Intigriti as a secondary source of income. However, 79% still devote up to 20 hours a week to bug bounty hunting. **For their day-job, popular professions include Penetration Tester (43%), Security Analyst (27%), and Software Developer (6%).**

How bug bounty programs work with Intigriti

- Researcher **searches** for a **vulnerability**
- Researcher **submits** a **report** via Intigriti
- Intigriti's **triage** begins **communication** with researcher
- Intigriti's **triage** team applies **quality assurance** steps
- In-scope, unique and well-written **reports** are **submitted** to client
- **Client accepts** report, and **payment** is **automatically** processed



REQUEST A DEMO[7]

[7] https://www.intigriti.com/demo

Port of Antwerp's bug bounty program strengthens its world-class security defenses

About Port of Antwerp

As Europe's second-largest port, the Port of Antwerp is a major lifeline for the Belgian economy. The Port of Antwerp handles around 231 million tons of international maritime freight annually and is home to Europe's largest integrated chemical cluster. The Port of Antwerp accounts, directly and indirectly, for a total of 143,000 jobs and more than €19 billion added value.

The challenge

Limitations of traditional security testing methods

True to its mission; a ‘home port as a lever for a sustainable future,’ Antwerp’s Port Authority aims to flexibly respond to a rapidly evolving maritime market. As the Cyber Resilience Manager & CISO of Port of Antwerp, Yannick Herrebaut is responsible for building world-class security defenses.

To test the port’s cybersecurity strength, Yannick employed the help of an agency to carry out an annual penetration test (also known as a pentest). Whilst there were some findings, the test didn’t meet all his needs and expectations.

Due to this time constraint, Yannick set out to explore alternatives that would enable him and his team to implement scalable, continuous security testing cost-effectively and sustainably.

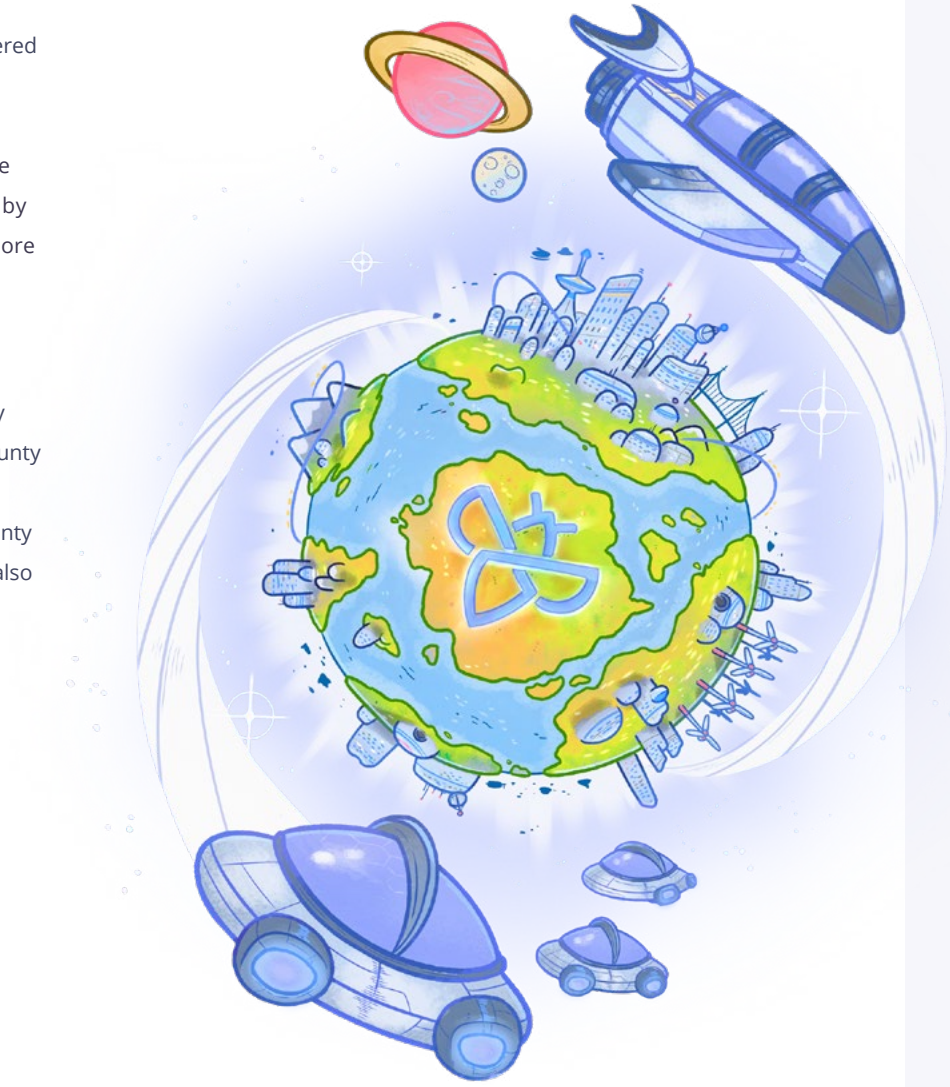
The solution

Host a responsible disclosure policy and bug bounty program on Intigriti

Soon into this research, Yannick's team discovered crowd security testing:

> "We encountered Intigriti after doing some market research. I was instantly intrigued by the concept and requested budget to explore responsible disclosure and bug bounty programs."

Port of Antwerp's security maturity was already advanced and so it began with a public bug bounty program alongside a responsible disclosure program. To assess the success of the bug bounty program fairly and accurately, Yannick's team also ran a penetration test for the port in parallel.



"

The most important result of working with Intigriti is that it offers you tangible and actionable results that significantly increase your security maturity.

YANNICK HERREBAUT
CYBER RESILIENCE MANAGER & CISO – PORT OF ANTWERP

The result

Increased discovery of vulnerabilities and faster remediation

Port of Antwerp received 135 vulnerability submissions from security researchers from Intigriti within a few months of launching. This was an encouraging result for Yannick and his team — particularly as the pentest yielded only a handful of vulnerabilities. Yannick explains:

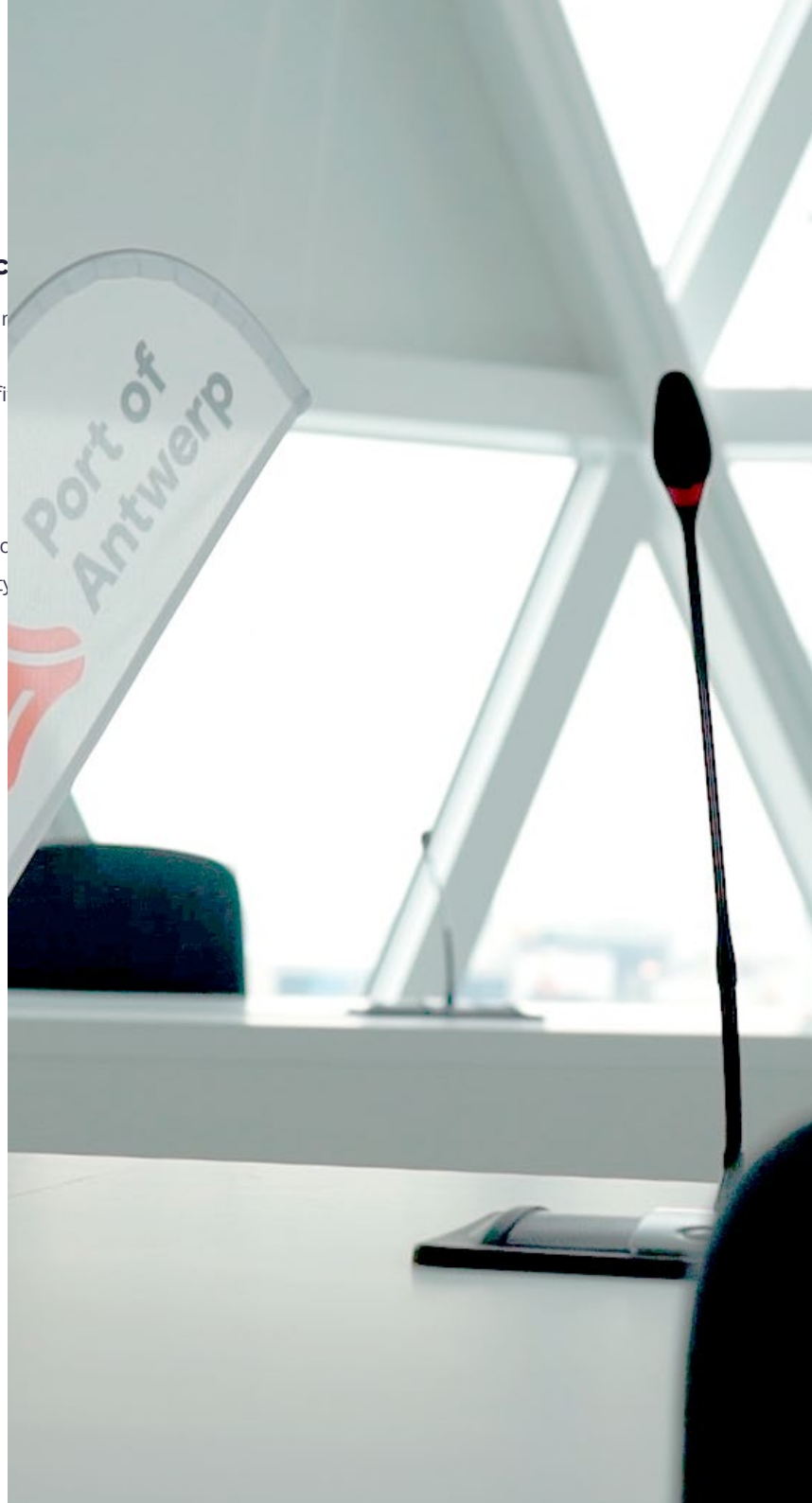
> "The amount and the quality of reports from the responsible disclosure program were a lot higher than what was discovered during the pentest, and at a fraction of the cost."

As well as a cost-benefit, Port of Antwerp experienced:

Increased vulnerability researc

Through the platform, Yannick and his team car interact directly with the security researcher community. Commenting further on this benefi Yannick says:

> "I think the biggest value of working with Intigriti is they have found a fantastic way to combine the security researcher community with the businesses through an extremely user-friendly platform."



Exceptional time-saving through Intigriti's triage service

Intigriti's triage process ensures its customers only receive genuine vulnerabilities so that they can decide whether to accept (or reject) the report and start working on a resolution. This security validation process is executed by Intigriti's in-house Security Analysts. Explaining how this step enables Yannick's team to work faster and smarter, Yannick shares:

> "I cannot understate the importance and the value that the triage team offers to us. The researcher sees or notices something, documents it, and publishes it on the platform. It then goes through the triage team as a quality check before we receive it. Our developers know that any vulnerability that makes it through this step is important and in need of remediation. The value is immense for us. Thanks to the recent integration between Intigriti and our in-house ticketing system, we've been able to streamline the remediation process even further."

Scalable security testing

The Port of Antwerp's next steps in terms of responsible disclosure and bug bounty is to extend the program to encompass its entire application portfolio. Talking more on the future of Port of Antwerp's bug bounty program, Yannick says:

> "Early on into the program's launch, we could already see it was a success. For that reason, we decided to go ahead with the program next year, and the years after that!"

Port of Antwerp

INDUSTRY
Maritime

EMPLOYEES
1,000 – 5,000

FOUNDED
1997

Penetration testing vs bug bounty programs

Bug bounty programs and penetration tests (pentests) both aim to identify vulnerabilities that could be exploited by hackers. However, there are some key differences. Pentests focus on one moment in time, whereas bug bounty programs are continuous.

Whilst you'll receive a certificate to say you're secure at the end of a penetration test, it won't necessarily mean that's still the case the next time you make an update. This is where bug bounty programs work well as a follow-up.

Another big difference between pentests and bug bounty programs is the pricing model. With a bug bounty platform, the security researcher gets a fee if they discover and report a previously undetected bug. What you pay also depends on how critical the vulnerability is — you pay according to impact. Pentesting, on the other hand, pays for the service delivered by the ethical hacker.

Unlike pentesting, a bug bounty program doesn't follow a specific methodology. Businesses that opt into Intigriti's ethical hacking platform, for example, will pay a subscription fee to **list their program**[8] in a controlled environment. This allows a community of ethical hackers to assess the security of their digital assets by taking a more creative approach.

Programs can be open to the entire community or they can be set to private. A private program means security researchers may only contribute to a company's program if they're invited.

[8] https://go.intigriti.com/bug-bounty-programs

	PENTESTING	BUG BOUNTY
TEAM SIZE	Smaller teams or individuals	Thousands of security reseachers
BRIEF	Methodology-driven	Creative approach
DEADLINE	Time-bound	Continuous
INVOICING	Pay for testing time	Pay for results
SCOPE	Narrow scope	Broad scope
RESOURCE	Expertise & skillsets of specific individuals	Expertise & skillset of a crowd

Hybrid pentesting: Combining the best of bug bounty with pentesting

As an alternative to bug bounty programs and pentests, Intigriti defined a new approach. Hybrid pentests utilize aspects of both testing solutions to create a new and additional solution to what's currently available on the security testing market.

SCAN[9]
To learn more about Hybrid Pentesting

[9] go.intigriti.com/hybrid-pentesting

What is hybrid pentesting?

Intigriti's hybrid pentest is a program type specifically developed to support clients who need more control over their bug bounty security testing.

Ideally suited to the fast pace of change in the logistics and tranport industry, this new solution can assist and augment a continuous testing strategy, depending on the organization's business needs:

BUSINESS NEED

Expanding the scope of a bug bounty program

Security teams can get a first glimpse of the security posture of a new asset before adding it to the scope of an existing bug bounty program. The hybrid pentest allows companies to better calculate the bounty budget on their new scope item.

BUSINESS NEED

New to bug bounty programs

Companies can run a hybrid pentest to kick off their community-powered testing journey. They'll start with a single security researcher to get comfortable with Intigriti's platform, while at the same time ruling out low-hanging fruit.

BUSINESS NEED

Compliance requirements call for a penetration test

Fulfill testing and compliance requirements that come with a dedicated deadline. Intigriti's hybrid pentests provide a letter of attestation that companies can share with customers to prove the security maturity of their products.

Intigriti in numbers

53

is the **average number of vulnerabilities** submitted within the first week **after a program launches.**

37

is the **average number of submissions** that are accepted within the first week **of a program's launch.**

24h

is how long it takes on average for Intigriti's triage team to **review, and accept or reject a report.**

48h

is how long it takes on average for customers to **accept or reject the report (if escalated).**

23%

of our registered ethical hackers submit **at least one report every month.**

71%

of companies get a **high to critical submission within the first 48 hours** of their program launching on Intigriti.

Glossary

Security researchers

Security researchers are **cybersecurity experts who use their skills and expertise to hack for good**. They're also known as bug bounty hunters, white hat hackers and ethical hackers.

Some of Intigriti's researchers are dedicated to bug bounty hunting full-time, whilst others are employed in full-time jobs and hack at their leisure.

Bugs

'Bugs' are **security exploits and vulnerabilities**. If deemed new and valuable, which depends on the scope provided within the program, the security researcher will report these via a submission.

Bounty

If the submission is accepted by the organization it relates to, the researcher is paid a **reward or compensation** which is better known as a 'bounty'.

The reward or compensation is typically monetary, but it can also be in the form of gifts like goodies and swag.

VDP

A vulnerability disclosure policy (VDP) is also known as a responsible disclosure policy. It provides ethical hackers with an **outline for submitting vulnerabilities to an organization**.

It's also an opportunity for organizations to demonstrate their willingness to work with external actors working in good faith.

Bug bounty program

A bug bounty program allows independent security researchers **to report bugs** to an organization in a legally compliant matter.

Bug bounty platform

A bug bounty platform provides a trustworthy infrastructure for security researchers to **engage and communicate** with companies **in a structured, safe, and reliable way**.

Most security researchers choose to report vulnerabilities through a bug bounty platform, like Intigriti.

About Intigriti

Intigriti is a rapidly growing cybersecurity company that specializes in crowdsourced security services to help organizations protect themselves from cybercrime.

Founded in 2016, Intigriti now has a global team of 100+ employees spread across Belgium, the United Kingdom, the Netherlands, and South Africa. And with the backing of our recent Series B Funding, we're planning on taking our growth to the next level.

Agile security testing powered by the crowd

What to expect as an Intigriti customer

01 Conquer the limitations of traditional security testing

Continuously test your digital assets for vulnerabilities by leveraging the expertise of Intigriti's 90,000 registered security researchers.

02 Industry-leading support

Only receive unknown, unique, valid, and in-scope vulnerability reports to enable your team to focus on business-critical tasks. Our offering also includes Account Management, Customer Success, Knowledge Base and Technical Support as standard.

03 Reduced risk

On average, Intigriti clients receive 53 vulnerability reports within one week of launching a bug bounty program through our platform. Intigriti's support empowers organisations to identify and remediate risks quickly.

04 Customized pricing

We provide a scalable model that is aligned to customer aspiration and program expansion. Clients of all sizes and from a wide array of business sectors utilize our services.

Information from Q1 2024. We are constantly growing, so please check our website for an accurate number.

Contact us

Need some help getting started with ethical hackers?
Our experts can help you maximise the success of your bug bounty program. Get in touch today to connect with the brightest and most experienced researchers on the globe.

www.intigriti.com

hello@intigriti.com

Intigriti hackwithintigriti @intigriti Intigriti Intigriti

Illustrations by Zwoltopia