INTIGRITI

A GUIDE TO

Reducing Risk For The Retail Industry

Security testing powered by crowd knowledge

EBOOK

Table of contents

3 The state of cybersecurity in retail

4 Introduction

5 How hackers can help retailers

6 Clear vulnerability reporting structures

7 VDP best practices: What to include

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

11 VDP vs bug bounty programs: What’s the difference?

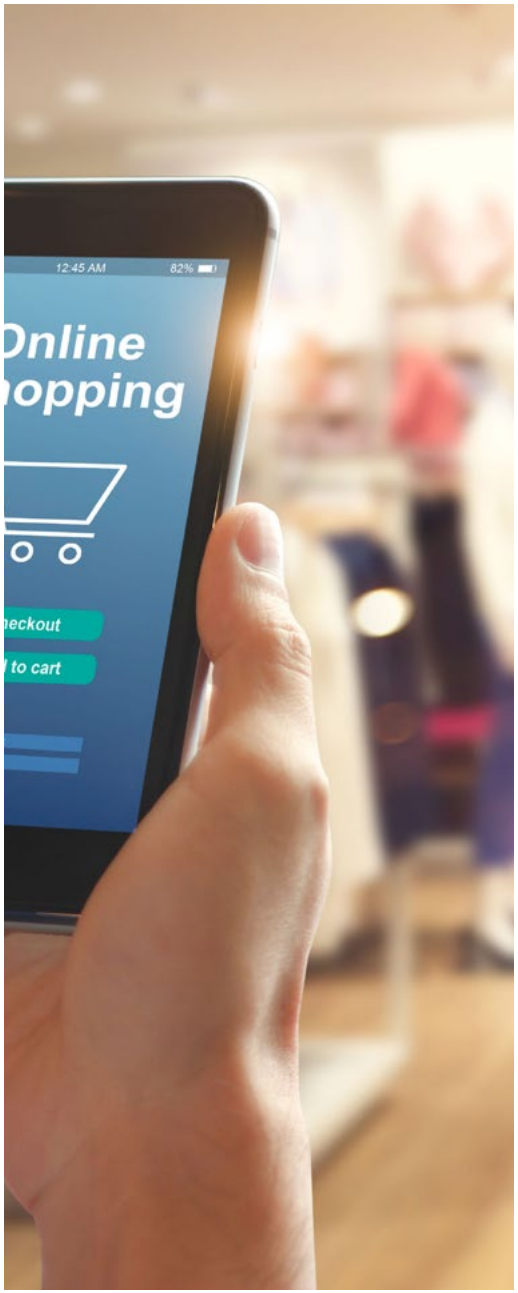
13 Ethical hacker communities

15 How vulnerability management works on Intigriti

17 Customer spotlight - Torfs

19 Glossary

20 About Intigriti



The state of cybersecurity in retail

24% of cyberattacks target retailers[1]

Online retailers have access to a wealth of payment information. Even a relatively small retailer could have many credit cards or bank accounts kept in their digital data files. With varying levels of security in place, it's no surprise that 24% of all cyberattacks are aimed at retailers.

Data breaches are a particular pain point for retailers[2]

The retail sector faces the usual cybercrime attacks such as ransomware, but also has to deal with the additional threat of cybercriminals targeting payment card data, with 70% of breaches in 2023 stemming from web applications.

[1] https://go.intigriti.com/fortinet
[2] https://go.intigriti.com/verizon
[3] https://go.intigriti.com/clearsale
[4] https://go.intigriti.com/security-intelligence

83% of consumers won't return to unprotected online stores[3]

According to report by ClearSale, 83% of consumers will never return to an online store that failed to protect them from fraud and 86% prefer fraud protection over easy checkout.

Cybersecurity is becoming an increasing priority in retail[4]

In a survey focusing on digital transformation in retail, more than half (57%) of respondents say bolstering cybersecurity was among their top three short-term business goals. Two in five (40%) said the same about their long-term goals, demonstrating a gradual shift towards better security in the retail industry.

Introduction

Global retail eCommerce sales are projected to surpass 8 trillion dollars by 2027. **However, a rise in eCommerce sales and activity also presents more cybersecurity opportunity for criminals.**

Retailers are, and always have been, attractive targets for cybercriminals. As the industry rapidly evolves its digital landscape and its metrics stay firmly focused on maximising revenue, platforms and applications are often left with weak spots in their defences.

One only has to perform a quick online search of data breaches to know that customer data is increasingly subject to theft for online stores. But business owners in this industry are quickly waking up to these issues and increasing their security measures. The VMWare Carbon Black 2020 Cybersecurity Outlook Report[6] found that more than three quarters (77%) of the eCommerce brands surveyed had purchased new security products in the last year and 69% had increased their security staff headcount.

Luckily, retailers do not need to fight this cybersecurity battle alone. Worldwide, thousands of security researchers are using their ethical hacking skills for good. They're helping to build a safer digital shopping experience for consumers by researching, identifying, and alerting eCommerce brands to weak links in their security systems before they're taken advantage of.

[5] https://go.intigriti.com/global-retail
[6] https://go.intigriti.com/vmware

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
- **How** eCommerce stores work with ethical hackers to strengthen their cybersecurity defences
- **VDP's** — Vulnerability disclosure policies
- **Bug bounty programs** — Incentivised vulnerability disclosure.

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

Hiring ethical hackers enables businesses to:

- **Show a commitment** to continuous security testing
- **Reduce the risk of losses** from a cyberattack
- **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.

How hackers can help retailers

Ethical hackers are highly skilled individuals that can safely simulate the behaviours of malicious hackers to highlight weak links and blind spots in a company's attack surface. By working with ethical hackers, retailers can become aware of and fix their vulnerabilities.

Not only does this improve the strength of their cybersecurity 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.

"Through Intigriti's bug bounty program, we discovered some serious issues. If a malicious hacker would have found them, they would have cost us a lot of money and would have done a lot of damage to our brand.

RAF DE LEU
IT MANAGER, TORFS

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.

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 without a VDP.

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.

TIP

SCAN

TO SEE MORE VDP TIPS ON OUR BLOG

This link goes to https://go.intigriti.com/ebook-retail-vdp

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.

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.

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 VDP, which takes a more passive approach to vulnerability reporting, bug bounty programs present businesses with an opportunity to proactively work with independent security researchers to report bugs. By continuously working with ethical hackers through a bug bounty program, organizations become aware of and fix their vulnerabilities. Not only does this improve the strength of their cybersecurity posture, but it empowers them to stay one step ahead of cybercriminals.

How bug bounty platforms work

Crowd

Thousands of ethical hackers security test your systems, digital assets and devices against realistic threats — ethical hackers test in precisely the same way malicious hackers do.

Bug bounty platform

An interactive platform that facilitates communications between ethical hackers and IT security teams, and features real-time reports of identified vulnerabilities.

Expertise

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

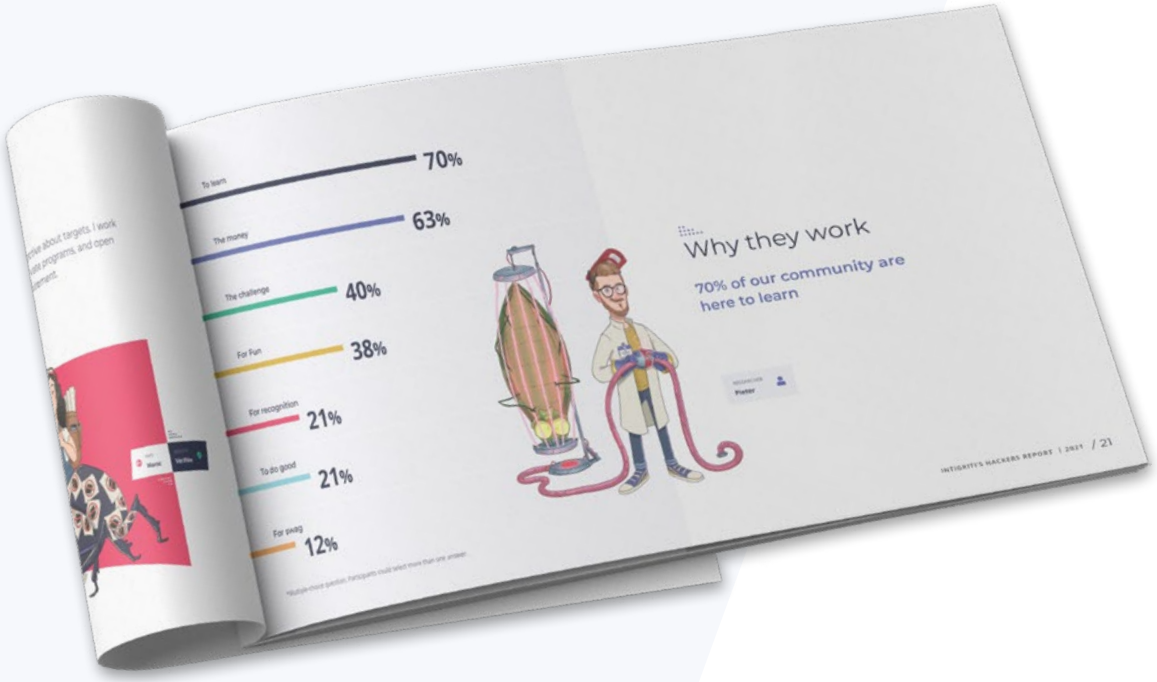
VDP vs bug bounty programs: What's the difference?

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. Turn 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 2022[7] found that 74% of our hackers operate on our platform to learn and develop their skills and 35% got better at bug bounty hunting.

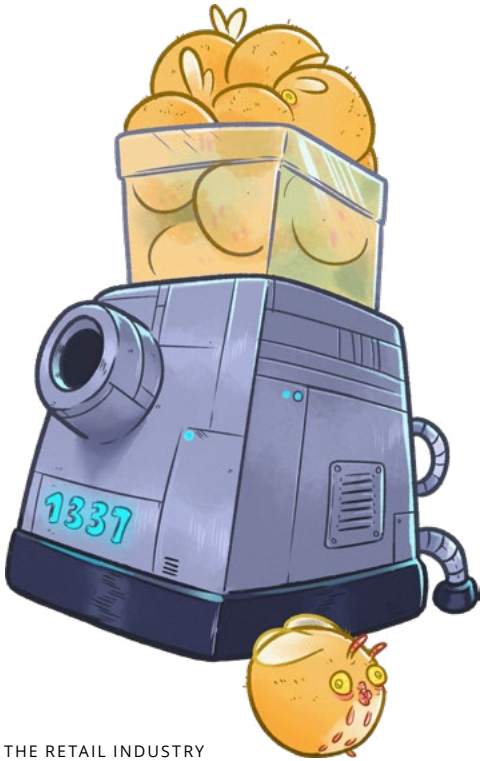
For 36% of our community, helping companies to be more secure was a primary motivator.

[7] https://go.intigriti.com/ethical-hacker-report-22

Earning potential is also an attractive aspect for security researchers. Just over half (53%) of our community had a financial motive.

What is the total cybercrime cost savings of Intigriti's bug bounty platform and services?

Some would say $71.7 million, as this is the total cybercrime cost we have saved our customers since launch. Based on the average cost of a data breach ($4.24 million, according to IBM) and total number of triaged reports by Intigriti.



23%

of vulnerability reports submitted via the Intigriti platform in 2022 were deemed high impact

1,600

average vulnerability submissions per month (up 44% from the year before)

$71.7M

total cybercrime costs saved since Intigriti's bug bounty platform launch

How vulnerability management works on 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

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.

Torfs found major vulnerabilities within two hours of launching on Intigriti's platform

We've continued to discover some serious security issues through Intigriti. It would have cost us a lot of money and brand damage if a malicious hacker would have found them.

RAF DE LEU
IT-MANAGER TORFS

The challenge
Website vulnerability

"Security has always played a major role in our eCommerce story," says Torfs' IT manager Raf De Leu. "Until 2018 we ran a custom-built website. It was a beautiful website, but under the hood, it was a patchwork of custom code combined with various frameworks. The website was vulnerable, and we struggled with security issues."

The solution

Inviting ethical hackers to find and disclose security issues

Torfs was already working with two ethical hackers who would carry out security tests for the brand every few months. However, the retailer was aware that they were reliant on the knowledge of just two people, despite them being highly-skilled professionals. For this reason, Torfs launched a bug bounty program on Intigriti's platform.

The result

An immediate increase in visibility over the attack surface

Once Torfs was on the platform, De Leu immediately saw **the benefits**:

> "We had only been live with the program for two hours before some major vulnerabilities were reported."

Other benefits included:

- Leveraging the expertise of an entire crowd of security researchers
- Exceptional customer support throughout the setup process and post-launch
- Intigriti's triaging service meant Torfs' security team could focus on unique, genuine, and in-scope vulnerabilities that truly required their attention
- The ethical hackers would retest the issue once it had been fixed
- Torfs' internal security team gained new cybersecurity skills and knowledge from Intigriti's ethical hackers.

As a result of the initial bug bounty program's success, Torfs expanded the scope to also include its microsites. De Leu summarised:

> "Through the bug bounty program, we continued to discover some serious issues. If a malicious hacker would have found them, they would have cost us a lot of money and damaged our brand."

TORFS

INDUSTRY

Ecommerce - retail

ECOMMERCE REVENUE

28 million EUR

COMPANY TYPE

Enterprise

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 the European leading platform for bug bounty and ethical hacking. The platform enables organizations to reduce the risk of a cyberattack by allowing Intigriti's network of security researchers to continuously test their digital assets for vulnerabilities.

Founded in 2016, Intigriti set out to conquer the limitations of traditional security testing. The interactive platform features real-time reports of current vulnerabilities, enabling organizations to obtain greater visibility over their attack surface and remediate issues faster.

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.

Crowdstrike is currently growing, so please contact our sales department or see our website for an accurate number.

Intigriti hackwithintigriti @intigriti intigriti

Contact us

Need some help getting started with ethical hackers? Our experts can help you maximize 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

Illustrations by Zwoltopia