A GUIDE TO

Lights, camera, proactive security testing

Crowdsourced security testing for media titans

EBOOK

Table of contents

Introduction

Few industries rival the media sector in terms of public visibility. From the silver screen to the airwaves, from digital platforms to printed pages, the industry offers consumers a window to the world, delivering both news and entertainment on a grand scale.

Correspondingly, cyberattacks on media establishments, regardless of their scale or success rate, garner significant public attention. A poignant example unfolded during February 2023 with the breach attempt targeting Virgin Media TV[1], causing temporary disruptions to programming while the company swiftly implemented mitigation measures.

Some of the top cyber risks threatening entertainment companies are industry-specific. Take, for instance, the allure of media platforms to hacktivists seeking to disseminate messages to broader audiences. Yet, many risks are shared with businesses across various industries. A telling incident occurred in December 2022 when The Guardian, a prominent UK newspaper, fell victim to a ransomware attack[2], resulting in operational disruptions and the compromise of personal data belonging to UK staff members.

Luckily, the media industry does not need to fight this cybersecurity battle alone. Worldwide, thousands of security researchers are using their ethical hacking skills for good through crowdsourced security testing platforms, such as Intigriti.

RESEARCHER
tamaytandiran

[1]go.intigriti.com/virginmediatv
[2]go.intigriti.com/theguardian

If you're reading this eBook, it's fair to assume that you are already facilitating the process for better security testing within your organization. Read on to discover how ethical hacking communities can help security teams:

- → Secure rapidly changing and growing environments
- → Expand cybersecurity skills availability without adding to headcount
- → Keep up with evolving cyber threats
- → Move from periodic to continuous security testing to better suit fast release cycles.

Keep reading as we also put one media industry player in the spotlight to showcase how they're already tackling these challenges.
already tackling these challenges.

RESEARCHER

Pentesterland

The media industry is tackling several cybersecurity pains today

One only has to look back to see evidence of how far the media industry has come regarding its digital and technological advances—think of the 1993 Jurassic Park movie compared to the franchise's most recent release of Jurassic World.

However, the speed at which the industry sophisticates its cybersecurity testing methods is another story. Despite a genuine desire to strengthen cybersecurity, there are some common pain points we hear today from security professionals in the industry.

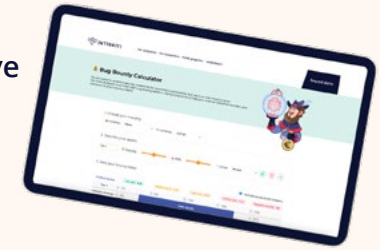
Continuously changing environments

The demands from consumers for new content are at an all-time high. To maintain its competitive edge, the media industry must operate at peak productivity and consistently deliver fresh content to its audiences. However, securing constantly changing environments within rapidly evolving threat landscapes is particularly difficult. This challenge becomes even more complicated when aligning and managing the business risk of new projects or releases.

Calculating the cost of risk

Determining the budget for how much a media organization spends (and how much it intends to spend in the future) on cybersecurity is complex. CISOs in the sector require a straightforward way to demonstrate the cost of specific risks, with a specific focus on the media industry.

Pssst! We have a bug bounty calculator for that!



Poor-fitting security testing solutions for agile environments

The media industry typically works with continuous development lifecycles. However, these don't align well with penetration testing cycles because they are often performed annually. As a result, vulnerabilities mistakenly created during long security testing gaps can remain undiscovered for some time. A more agile and continuous solution is needed.

Cyber threats are evolving

The constant struggle to stay up to date with the latest cyberattack techniques and trends puts media organizations at risk. Yet, hiring specialist skills for every new cyber threat type would be unrealistic and unsustainable.

Rapid growth

The media industry is growing at an impressive rate—but it would be unusual for any fast-growing industry not to experience growing pains. For CISOs in this sector, maintaining visibility of their organization's expanding attack surface is an ongoing battle.

Cybersecurity skills shortages

Like all industries, finding the available skillsets for internal cybersecurity teams is still a challenge. As a result, organizations don't have the dexterity to spot and promptly remediate specific security vulnerabilities.

A proven solution to these challenges is to invite ethical hacker (security researcher) communities to help. Businesses can rely on the power of these crowds to assist them in their security testing. Further, they can utilize bug bounty platforms to manage the remediation of new and unknown vulnerabilities.

Bringing security testing into the 21st century

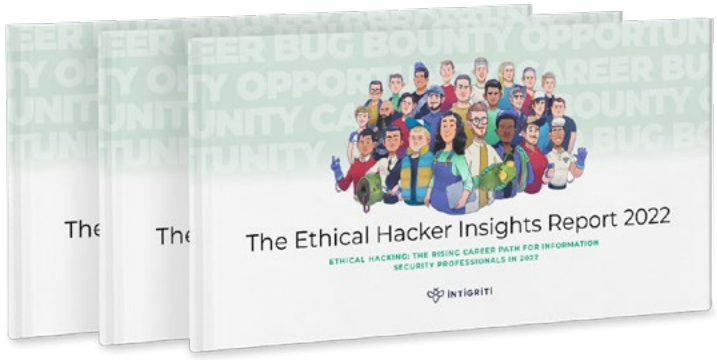
Ethical hackers are highly skilled individuals who can safely simulate malicious hackers' behaviors to highlight weak links and blind spots in a company's attack surface. Security teams, developers, and engineers at a media company can quickly be made aware of vulnerabilities and fix them by working with ethical hackers. Not only does this improve the strength of their organization's overall cybersecurity posture, but it empowers them to stay one step ahead of cybercriminals.

A **vulnerability disclosure policy (VDP)**, **penetration test**, or a **bug bounty program** is the most common way to work with ethical hacker communities.

About 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**[3] found that 70% of our hackers operate on our platform to learn and develop their skills, while 'the challenge' drives 40%. For a fifth of our community, making the internet a safer and more secure environment is their primary goal.

The unique occupation of bug bounty hunting offers a heightened level of freedom and lifestyle that traditional jobs cannot provide but that today's security professionals desire.



Intigriti's Report[4] explored this trend further and found that 96% of ethical hackers would like to dedicate more time to bug bounty hunting in the future, and 66% are considering it as a full-time career.

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%).

[3]https://go.intigriti.com/ethical-hacker-insights-report-2021
[4]https://go.intigriti.com/ethical-hacker-insights-report-2022

The QR code goes to this link
[4]https://go.intigriti.com/ethical-hacker-insights-report-2022

Working with ethical hacker communities

Before we explore how to maximize the success of working with ethical hackers through VDPs and bug bounty programs, let's take a quick look at the similarities and differences between them on Intigriti's platform.

	VDP	BUG BOUNTY
Compliance	**Meets industry standards** | Supports ISO/IEC 29147:2018 and ISO 27001:2013.	
Legal considerations	**Provides a legal framework** | Companies provide ethical hackers with the 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 always to obtain an accurate view of their security posture.	
Communication	**Centralized within the platform** | No need for sharing encrypted mails: the platform will allow secure and reliable communication.	
Search culture	**See something, say something** Allows ethical hackers to report security issues when they notice them without being afraid of legal repercussions.	**Actively search & find something** Security researchers are continuously motivated through bounties without being afraid of legal repercussions.
Reward system	**No promises** There is no promise of a reward, but a thank you is appreciated.	**Rewarded for results** Enables continuous security testing by incentivizing the community through bounties. The size of the reward depends on the impact.
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.	

A step-by-step guide to building a vulnerability disclosure policy

What is a vulnerability disclosure policy?

Having a vulnerability disclosure policy (VDP) for your media company's website is important because it allows ethical hackers (and good-willed citizens) to assist your business if they encounter 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 chance of losing revenue due to an expensive cyberattack
- Minimizes time-to-remediation
- Streamlines your vulnerability reporting process

Some companies choose to keep this process in-house, while others opt to publish a VDP on a bug bounty platform, such as Intigriti. Either way, many in the security industry describe vulnerability disclosure policies as following a "see something, say something" approach.

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 business concerned.

Worryingly, 70% of Intigriti's ethical hacker community has identified vulnerabilities for websites without a VDP. Of that group, 12% didn't escalate the report due to a lack of a transparent reporting process. For those that did, 32% said the report got lost in the process or weren't sure whether it was successfully reported. That's 44% of discovered risks that remain potentially undetected for businesses.

Considering that cyberattacks against film and media industries are escalating[5], 44% of undetected risks is a concerning statistic.

RESEARCHER
Alicanact60

[5]https://www.forbes.com/sites/davidbalaban/2021/06/11/why-cyber-attacks-against-film-and-media-industries-are-escalating/?sh=602f441a6896

VDP best practices: What to include

A good VDP should detail what information the security researcher should report and what they can expect from the disclosure process. We suggest including the below six components:

01

Company background

Ensure you provide a brief background on your business within this opening section. For example:

- Who you are
- Media business sector & purpose
- Unique selling points
- Customers - B2B and/or B2C
- Other relevant stakeholder groups

The reason for providing context around your media 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 area is an excellent opportunity to introduce why you have the policy and how it helps your business honor its promises.

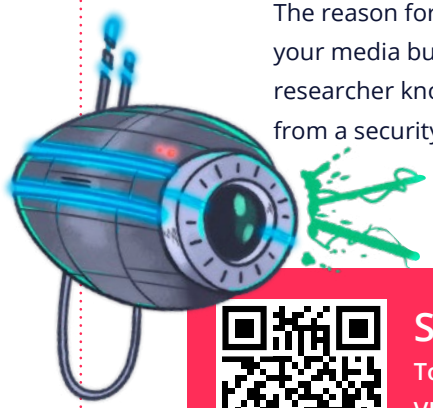
03

Scope

The scope is mostly directed at security researchers but is also helpful to other stakeholders such as partners, regulators, and the media. 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 clearly explain what the company perceives to be within the scope and what they perceive to be outside. Doing this helps put everyone on the same page from the offset.



SCAN[6]
To see more VDP tips on our blog

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

04

Legal safe harbor

You want ethical hackers to disclose bugs in your system responsibly without fear of legal consequences. Therefore, it's essential 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 encouraging ethical hackers to report issues to your business. The language you use should be clear, and 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 a third-party initiates legal action 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 establishes 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.

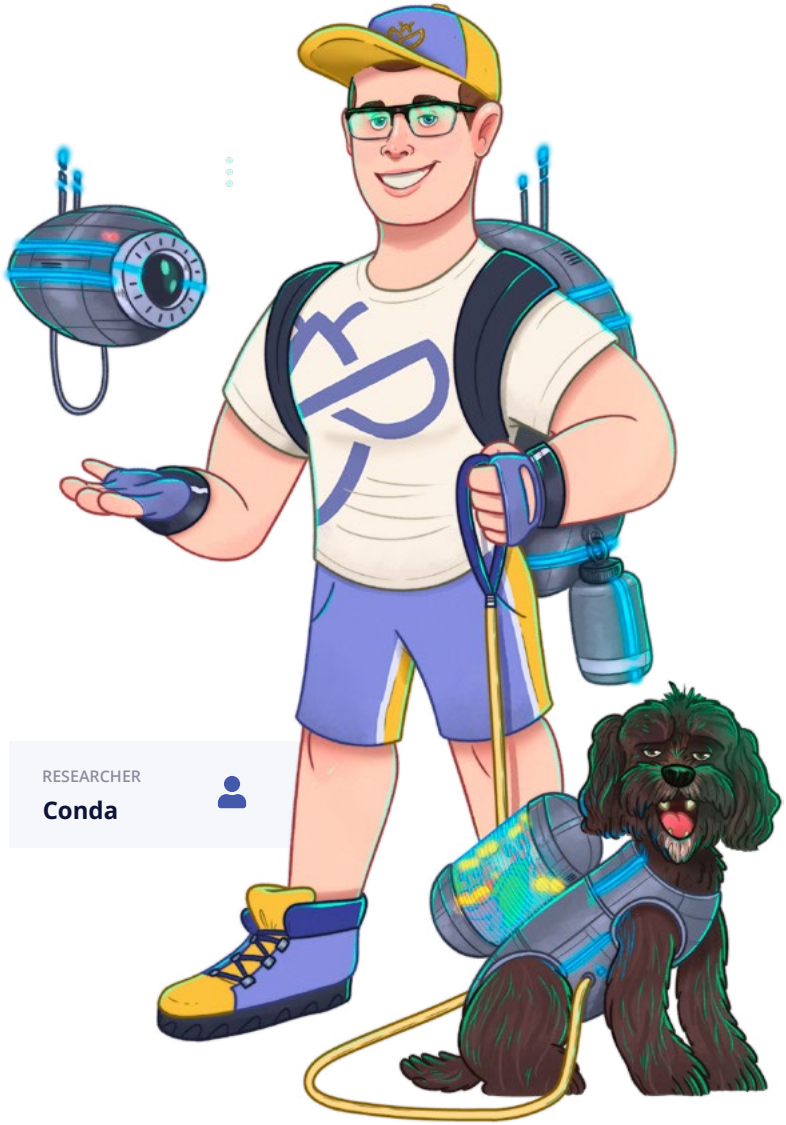
Remember that the researchers have already invested significant time and effort in testing your systems, so it's crucial to only ask for information you'll genuinely need. Ask for too much, and you may put contributors off entirely.

06

What to expect after a submission

This policy area is a good place to outline how your company (and bug bounty platform, if relevant) will evaluate reports 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 regarding what kind of acknowledgments, 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 platforms allow businesses to work with independent security researchers to report bugs proactively.

Media 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.

The impact of bug bounty programs on cybersecurity

By launching a bug bounty program, **organizations** experience:

More robust protection

Company data, media assets, brand, and reputation have additional protection through continuous security testing.

Enabled business goals

An improved security posture leads to a more secure platform for innovation and growth.

Improved productivity

Increased workflow with fewer disruptions to the availability of services. More strategic IT projects that executives have prioritized, with fewer security "fires" to put out.

Increased skills availability

Internal security team's time is freed by using a community for security testing and triage.

Clearer budget justification

Ability to provide more significant insights into the organization's security posture to justify and motivate for an adequate security budget.

For **CISOs, CIOs, and security leaders**, the personal benefits of a successfully run bug bounty program are also impactful:

Peace of mind

Knowing that the organization's infrastructure, applications, and media assets have an additional layer of security testing.

High morale

Team spirit improves by reducing manual tasks, resulting in other departments increasingly seeing the CIO or CISO as a good leader.

Confidence

The organization's security policy is progressive and more mature. The team and security leaders can hit personal and company cybersecurity KPIs.

Improved relationships

Project delays significantly decrease without the reliance on traditional pentests. The CIO or CISO comes to be seen as a project enabler rather than a roadblock by project managers, engineers, and other teams, resulting in a better reputation.

DPG Media uses bug bounty programs as the final step in its security process

About DPG Media

DPG Media[7] is an international digital media network. It has more than 90 un brands within its portfolio across The Netherlands, Belgium, and Denmark. The media production conglomerate provides its 15 million viewers, listeners, visitors, and mobile phone users with premium content and technologies that cover the full spectrum of interests of the modern consumer. In addition, DPG Media offers advertising opportunities to strategic business partners.

[7]https://www.dpgmediagroup.com/en

RESEARCHER
Rekter

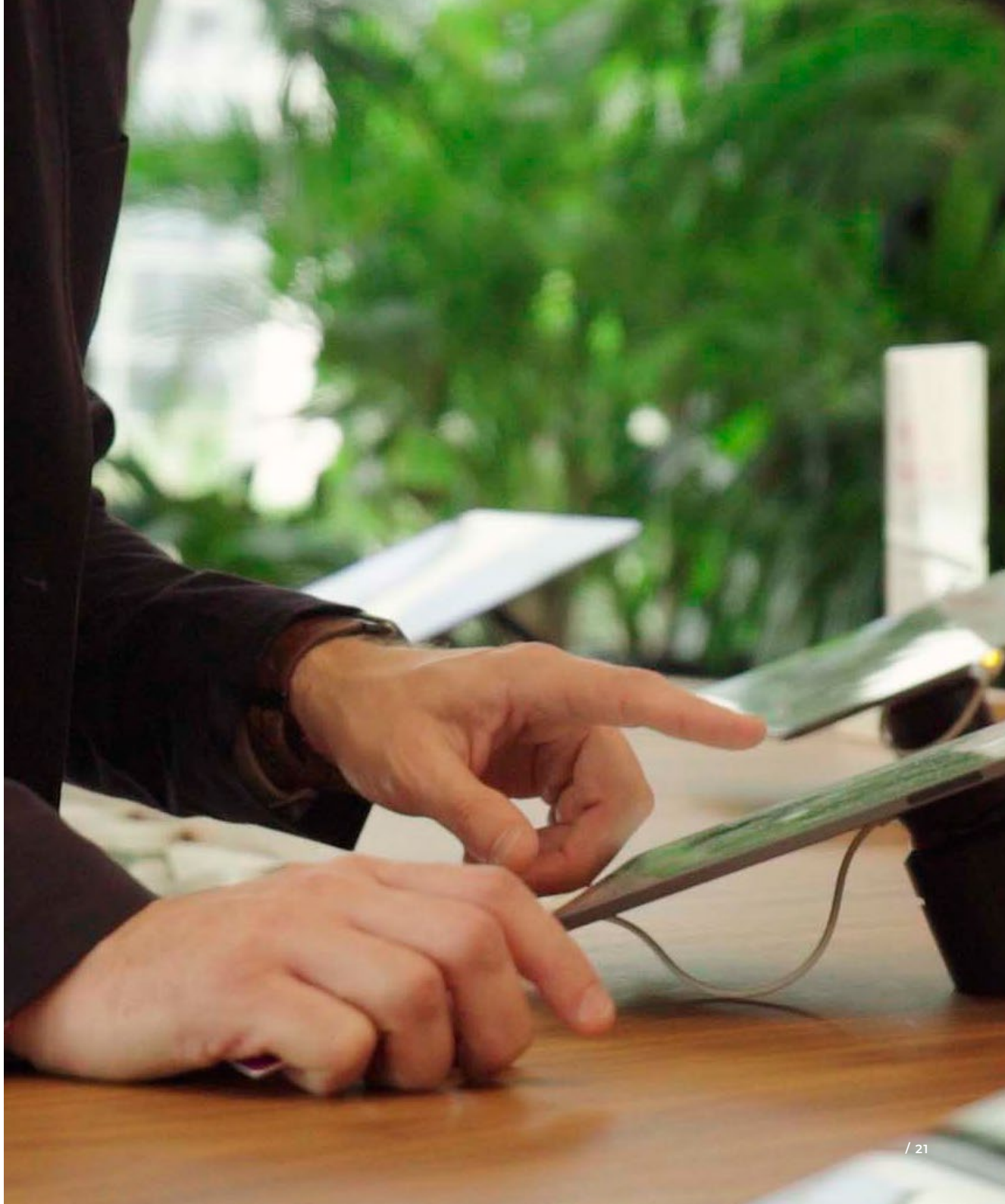
The challenge

Defend an extensive attack surface

DPG Media has more than 14,000 customer-facing domains and applications. Despite having a highly-skilled cybersecurity department, defending the network's enormous attack surface alone was challenging.

Thomas Colyn, an **award-nominated**[8] security specialist and CISO of DPG Media, is responsible for the IT security and information management of all assets of the DGP Media Group (The Netherlands, Belgium, and Denmark). He created a process whereby each product, domain, or application within the network undergoes a series of security testing steps, including penetration testing. To finalize this process, Colyn needed a solution that would apply continuous security testing thereafter.

[8]https://www.computable.nl/artikel/informatie/awards-nieuws/7206208/1853296/thomas-colyn-dpg-media-scoort-nominatie.html



The solution

Crowdsourced security testing as a final step in the process

To meet DPG Media's business goals, Colyn chose to lean on Intigriti's bug bounty platform for support. The platform meant he could tap into a network of security researchers (ethical hackers). At the same time, he could leverage Intigriti's customer support and triage teams.

The role of a triage team is to review and screen incoming vulnerability reports. This important step means the client only receives relevant, valid, and in-scope vulnerability reports. A triage team also replicates the reported findings to evaluate their impact and severity.

Intertwining bug bounty programs into DPG Media's security testing process

When a project launches within DPG Media, the first layer of cybersecurity checks includes testing within a quality and assurance environment, followed by a penetration test. These steps bring the project to a level of maturity whereby Coly team is satisfied to launch it as a bug boun program.

> "The bug bounty programs provide me with more assurance that even the most difficult to find vulnerabilities are discoverable. We can then mitigate the quickly. In return, we provide more assurance to our customers, our reade and our listeners."

THOMAS COLYN, CISO
DPG MEDIA

DPG Media has already launched public bug bounty programs for 14 of its brands, including **VTM Go**[9], **HLN**[10], **De Volkskrant**[11] and **Algemeen Dagblad**[12].

[9]https://app.intigriti.com/programs/dpgm/vtmgo/detail
[10]https://app.intigriti.com/programs/dpgm/hetlaatstenieuws/detail
[11]https://app.intigriti.com/programs/dpgm/devolkskrant/detail
[12]https://app.intigriti.com/programs/dpgm/algemeendagblad/detail

Continuous dedication toward defending against cyber threats

Within one year of launching bug bounty programs on the Intigriti platform, DPG Media received more than 1,900 vulnerability submissions across 14 brands. The severity of vulnerabilities reported ranged from low to exceptional.

Increased visibility of hard-to-find security vulnerabilities

Since DPG Media's bug bounty programs are continuous, Colyn has peace of mind that an additional layer of security testing and validation has been applied to the organization's applications.

Effective time allocation

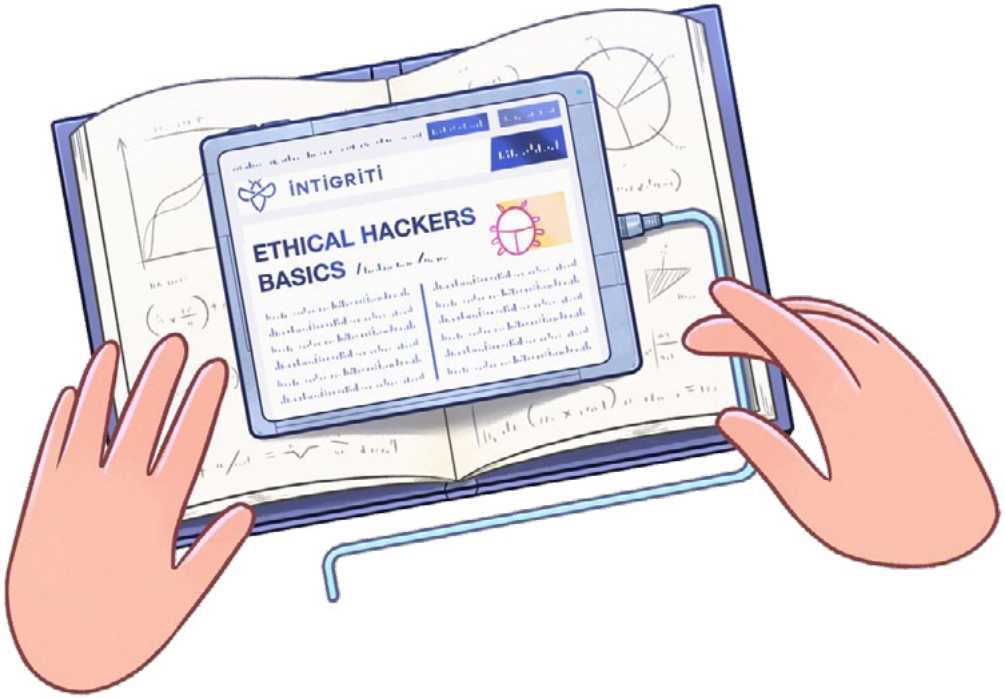
Duplicates, out-of-scope, and invalid vulnerability reports were rejected from the vulnerability management process by Intigriti's triage team. This meant the network's cybersecurity team only paid attention to genuine security risks needing a patch.

> “The most impact we have experienced from working with Intigriti is the extra time my security team gets back from not triaging reports. What I also appreciate about Intigriti is the feeling that the customer comes first. It is an open and collaborative relationship where we share a common goal to mitigate found vulnerabilities.”

THOMAS COLYN, CISO
DPG MEDIA

How bug bounty programs work with Intigriti

- The security researcher **searches** for a **vulnerability**
- The 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 the client
- **The client accepts** the report, and **payment** is **automatically** processed



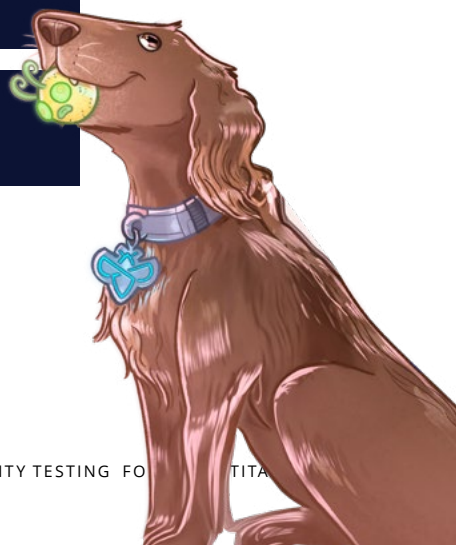
REQUEST A DEMO

Penetration testing vs. bug bounty programs

There are some alternatives to bug bounty programs, such as penetration tests (pentests.) Bug bounty programs and pentests both aim to identify vulnerabilities that hackers could exploit. However, there are some key differences:

While your media company will receive a certificate to say it's 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 to pentests.

	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[13]
To learn more about Hybrid Pentesting

[13]https://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 media 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 media companies to better calculate the bounty budget on their new scope item.

BUSINESS NEED

New to bug bounty programs

Media 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 media 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

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.

Security researchers

Also known as bug bounty hunters, white hat hackers, and ethical hackers. Security researchers are cybersecurity experts who use their skills and expertise to hack for good. Some of Intigriti's researchers are full-time bug bounty hunters, while others are employed in full-time jobs and hack during their leisure time.

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 organization accepts the submission, the researcher receives a reward or compensation, better known as a 'bounty.'

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.

Hybrid pentesting

The hybrid pentest enables our clients to request dedicated security testing time from a selected researcher within a fixed time window. However, it comes with the reward model, motivation, reporting, and triage of bug bounty programs.

About Intigriti

Intigriti is the leading European-based 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 test their digital assets for vulnerabilities continuously.

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

Information from Q2/2024. We are constantly growing, so please contact our sales department or see our website for an accurate number.

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—all submissions are rigorously assessed by our dedicated triage team before we transmit them to the client. This enables your team to stay focused on business-critical tasks. Our offering includes triage, account management, customer success, knowledge base, technical support, and more.

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 organizations to identify and remediate risks quickly.

04 Customized pricing

We provide a scalable model that aligns with customer aspirations and program expansion. Clients of all sizes and from various business sectors, including large media companies, use our services.

Intigriti hackwithintigriti @intigriti Intigriti Intigriti

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

Illustrations by Zwoltopia