State of Vulnerability Disclosure:

Market Insights and Trends by Hackrate

{-} Hackrate

Table of Contents

{-}

In the process of producing this eBook, we conducted an extensive survey that encompassed two main demographics: ethical hackers, penetration testers, and security researchers (Group 1), and individuals responsible for IT security in their organizations, such as Chief Information Security Officers (CISOs), security managers, and heads of application security (Group 2). The survey was designed to gain insights into the perceptions, practices, challenges, and attitudes these groups have towards cybersecurity, vulnerability reporting, and VDPs.

The responses provided offer an invaluable perspective that enhances the understanding of the real-world application of VDPs, and these insights have been interwoven throughout this eBook to provide a balanced, informative, and practical guide to vulnerability disclosure.

1

Introduction

This ebook aims to educate CISOs and security managers about vulnerability disclosure policies (VDP), and highlight the importance of having vulnerability management strategies in place. Furthermore, it evaluates the risks of not having a VDP, and contains an overview of the regulatory environment, best practices, and introduces managed VDP services.

We recommend the ebook to the following organizations:

- Organizations storing sensitive data
- Organizations providing software that is accessible from the internet (incl. Software-as-a-Service providers)
- Any organization that wants to reduce the likelihood of falling prey to a malicious cyberattack
- Organizations aiming to express a conscious and proactive approach to cybersecurity

Vulnerability disclosure policies are essential for receiving actionable feedback on the security aspects of an organization’s web-facing systems, exhibiting a conscious approach to security, and building trust with clients.

2

What is a VDP and why is it important?

”

Vulnerability:
vulnerability refers to a weakness or flaw in a computer system, network, or software that can be exploited through malicious intention to compromise the confidentiality, integrity, or availability of data or system resources.

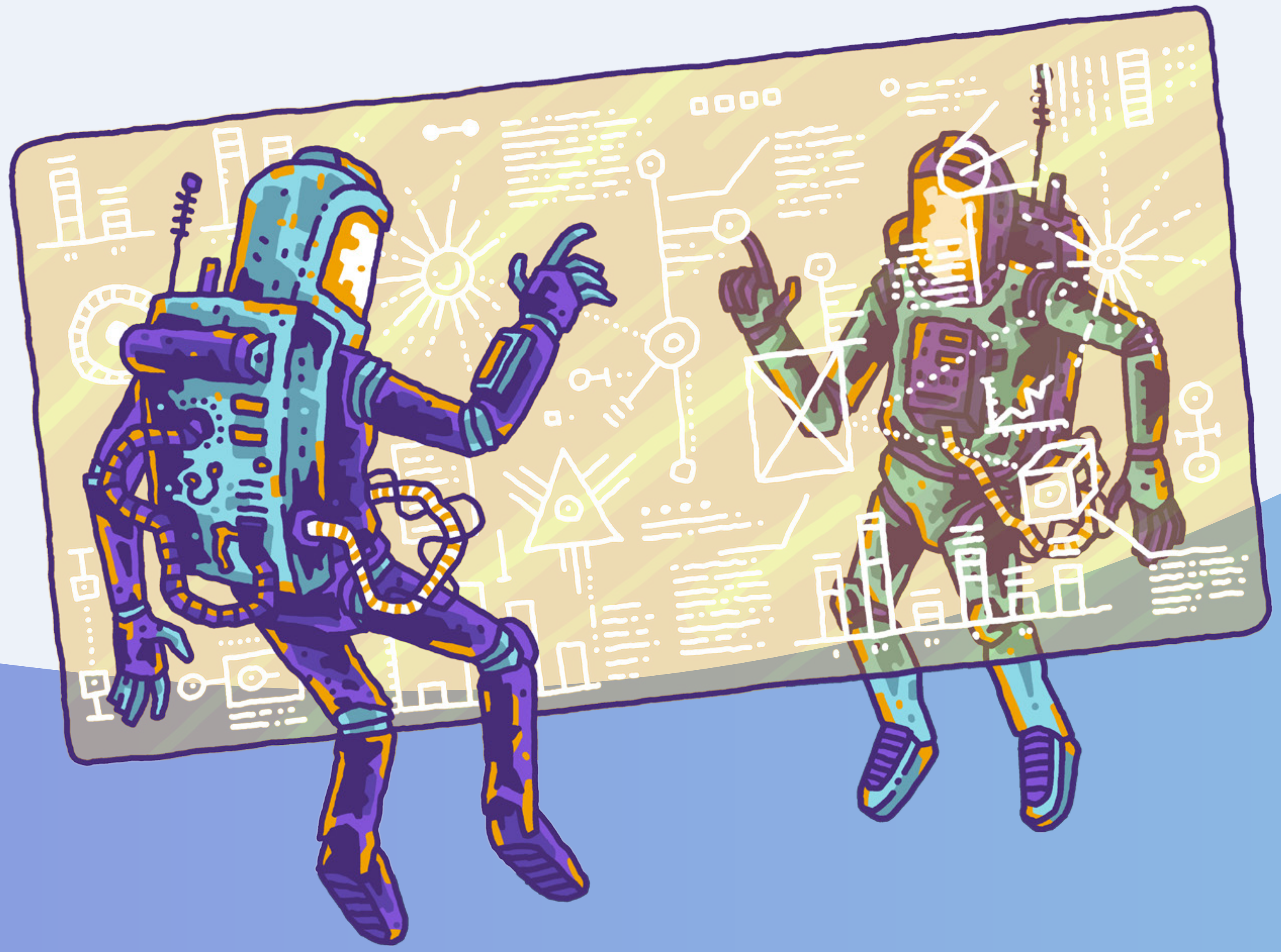
Cybersecurity vulnerabilities exist due to coding errors, changing elements in software, lack of security awareness while scaling up complex computer systems, reliance on third-party components, and unintentional combination of already secure components.

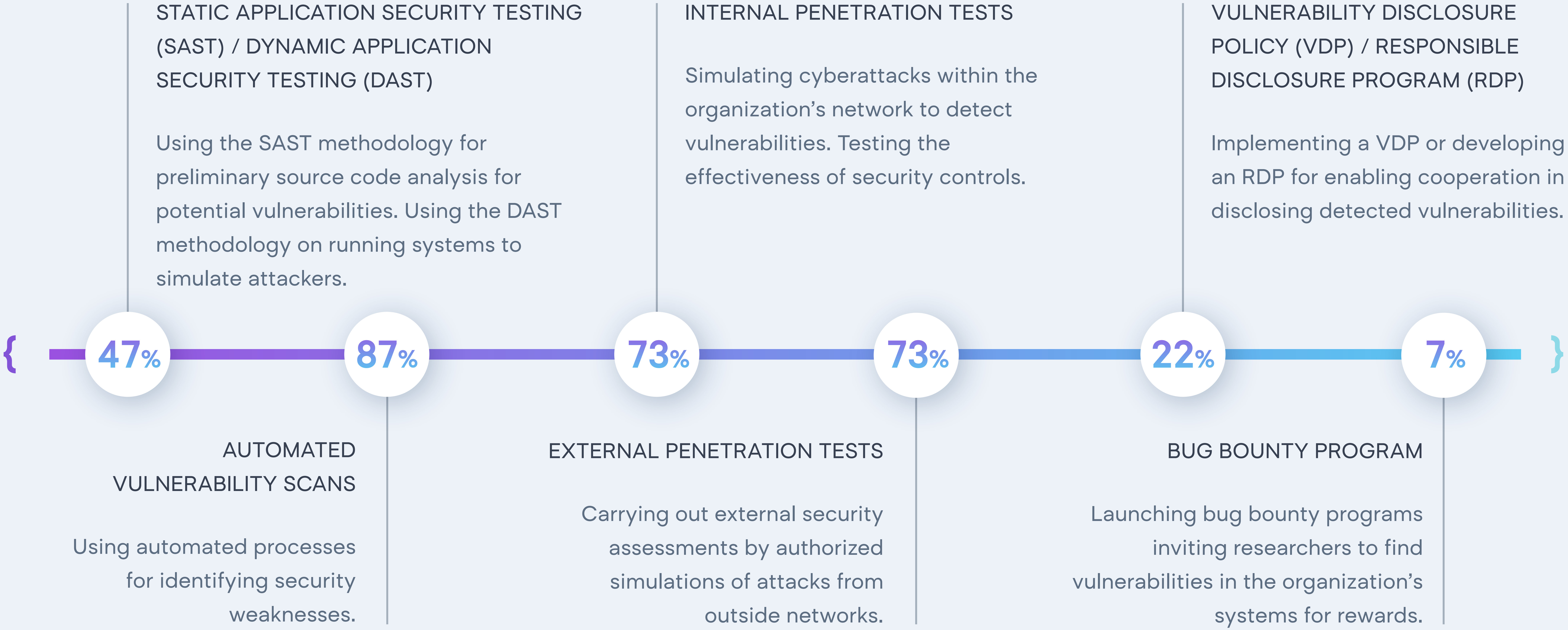
Digital transformation - besides making an organization's life easier and their business more effective - brings risks. Digitalization increases the exposure of organizational and sensitive data through web-facing systems and services. These systems, visible and accessible from the internet, are necessary for every provider to serve their customers and, as a result, are the primary targets for exploitation.

Vulnerability disclosure refers to identifying, reporting, and patching software, hardware, or service weaknesses. You cannot eliminate having vulnerabilities. Reducing risks and demonstrating transparency at the same time by employing a vulnerability disclosure policy, however, demonstrates a conscious approach to security.

In cybersecurity, vulnerability disclosure refers to the process by which information about security vulnerabilities is managed. A VDP or a responsible disclosure program (RDP) enables ethical hackers to report potential vulnerabilities. This process is crucial for improving the defense mechanisms of systems and helping prevent cyber attacks.

Organizations often have vulnerability disclosure policies that outline how they will deal with reported vulnerabilities, including timelines for addressing those vulnerabilities and communication plans for informing the affected parties.





47%

STATIC APPLICATION SECURITY TESTING (SAST) / DYNAMIC APPLICATION SECURITY TESTING (DAST)

Using the SAST methodology for preliminary source code analysis for potential vulnerabilities. Using the DAST methodology on running systems to simulate attackers.

87%

AUTOMATED VULNERABILITY SCANS

Using automated processes for identifying security weaknesses.

73%

INTERNAL PENETRATION TESTS

Simulating cyberattacks within the organization’s network to detect vulnerabilities. Testing the effectiveness of security controls.

73%

EXTERNAL PENETRATION TESTS

Carrying out external security assessments by authorized simulations of attacks from outside networks.

22%

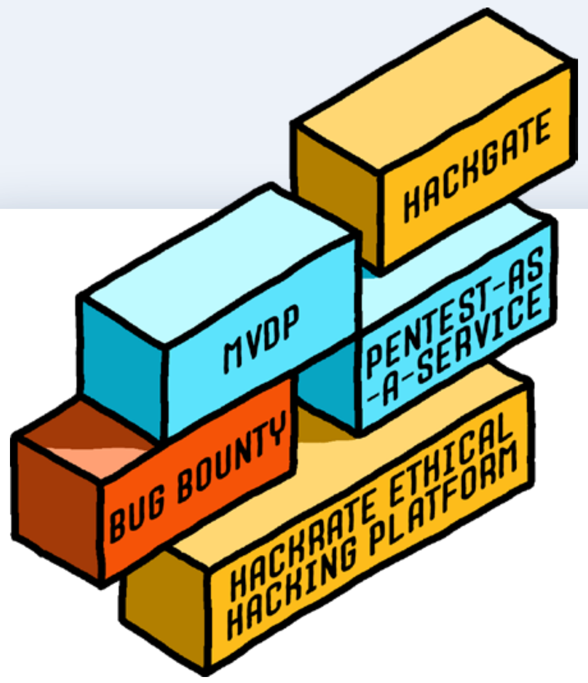
VULNERABILITY DISCLOSURE POLICY (VDP) / RESPONSIBLE DISCLOSURE PROGRAM (RDP)

Implementing a VDP or developing an RDP for enabling cooperation in disclosing detected vulnerabilities.

7%

BUG BOUNTY PROGRAM

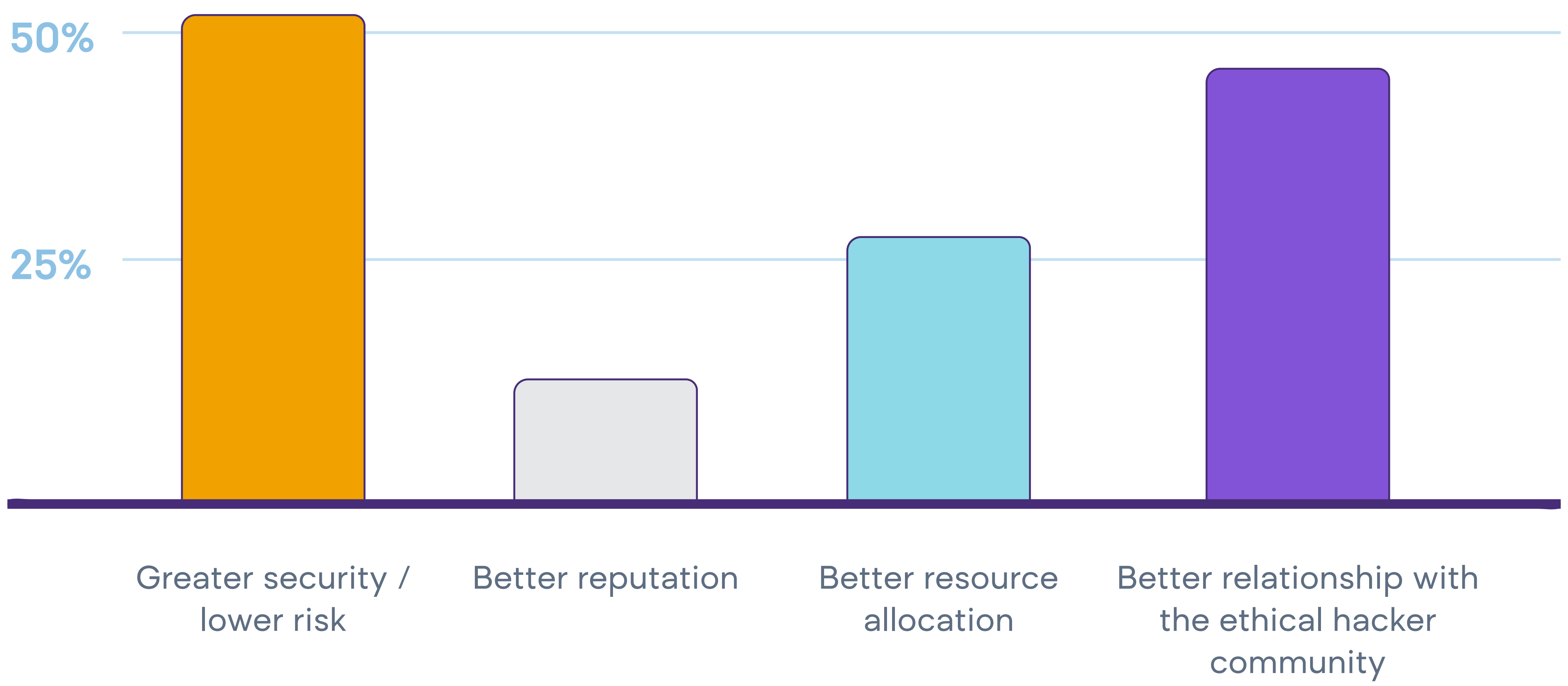
Launching bug bounty programs inviting researchers to find vulnerabilities in the organization’s systems for rewards.



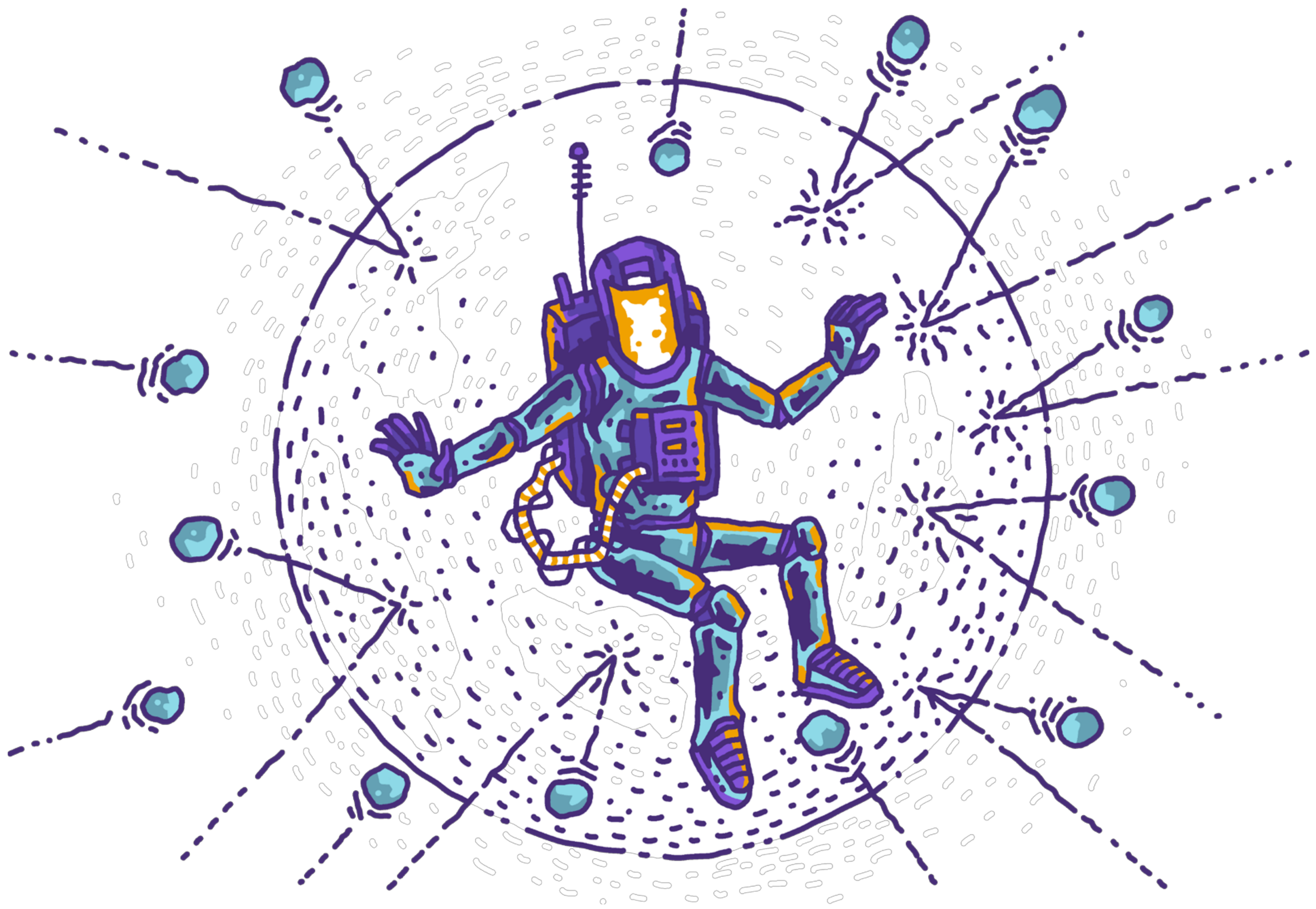
More than 90% of surveyed CISOs have implemented one or multiple cybersecurity testing solutions, with automated vulnerability scans being the most popular.

Why is having a VDP vital?

What do you think is the main benefit of your VDP policy?



Around half of those surveyed think that their VDP policy provides greater security, lowers the risk, and helps to build a better relationship with the ethical hacker community.

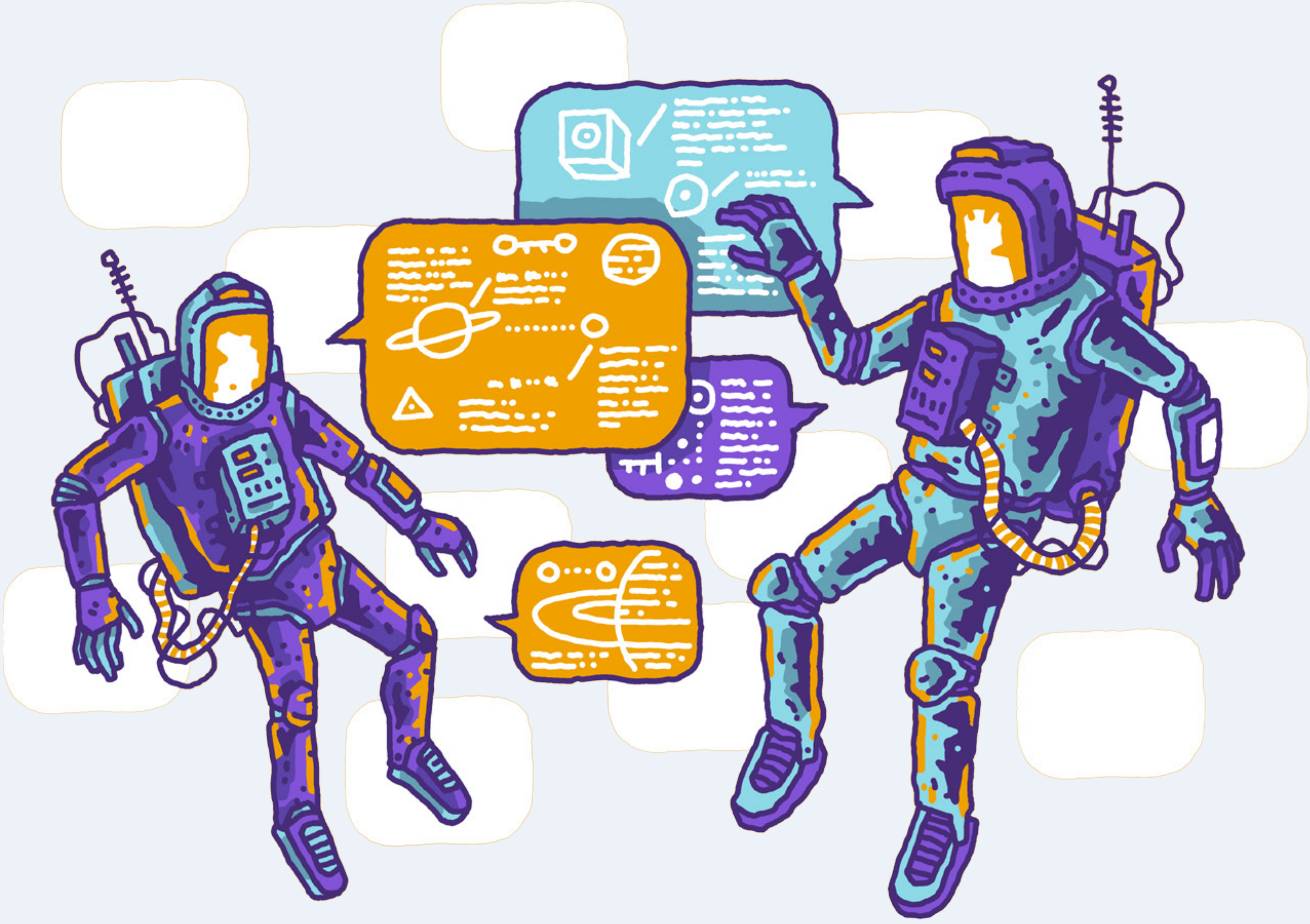


The cybersecurity threat landscape is evolving dynamically and continues to expand both in scope and complexity every quarter. Additionally, many vulnerabilities can persist for months or even years before being discovered. Even when detected, most vulnerabilities are not found by the system's owner but by third parties, who may have various reasons for not reporting their findings to the affected organization.

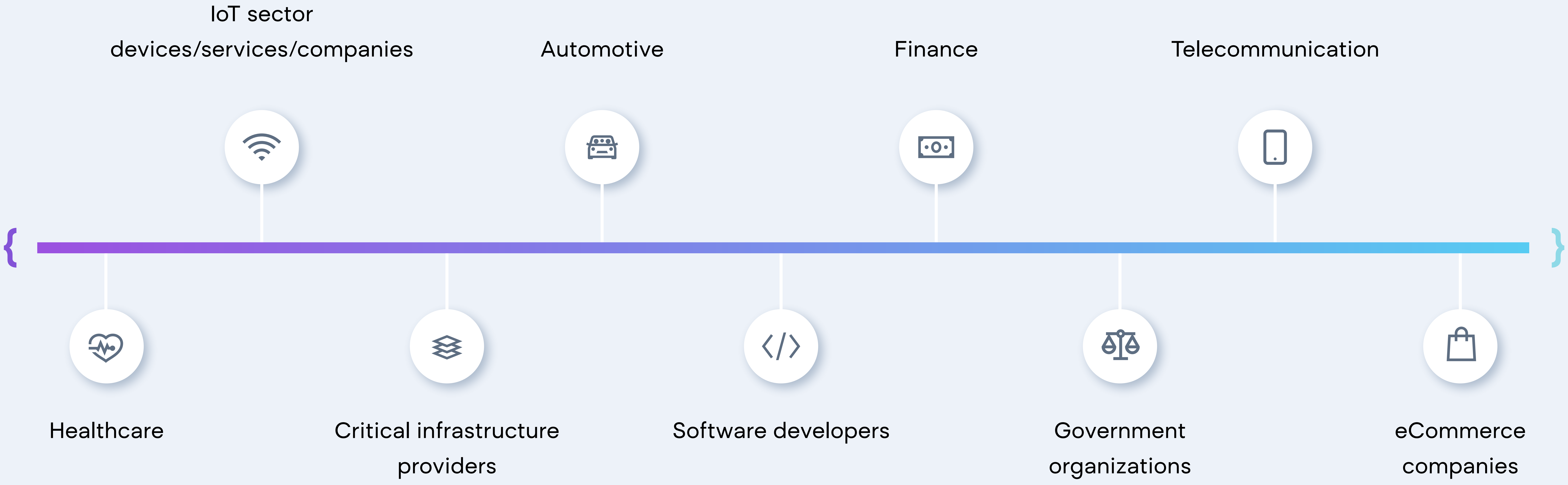
Responsible disclosure programs (RDPs) are important to any organization's security strategy. Employing a vulnerability disclosure policy (VDP) enables your company to **receive reports of potential security vulnerabilities** in a responsible and coordinated manner. A well-crafted and implemented VDP can provide several benefits:

- **Improves security** by establishing a systematic process for fixing security problems.
- **Reduces legal risk** by adhering to specific security directives and guidelines.
- **Helps build trust** between the company and its customers.
- Demonstrates that the company **takes security seriously** and is willing to collaborate with ethical hackers to **protect customer data**.

By having a VDP, organizations can ensure the security of their IT systems and data. By establishing a program, companies can encourage researchers and other security professionals to report any potential vulnerabilities they find without fear of legal action. Published on companies' websites, VDP allows them to identify and address issues before they become significant problems.

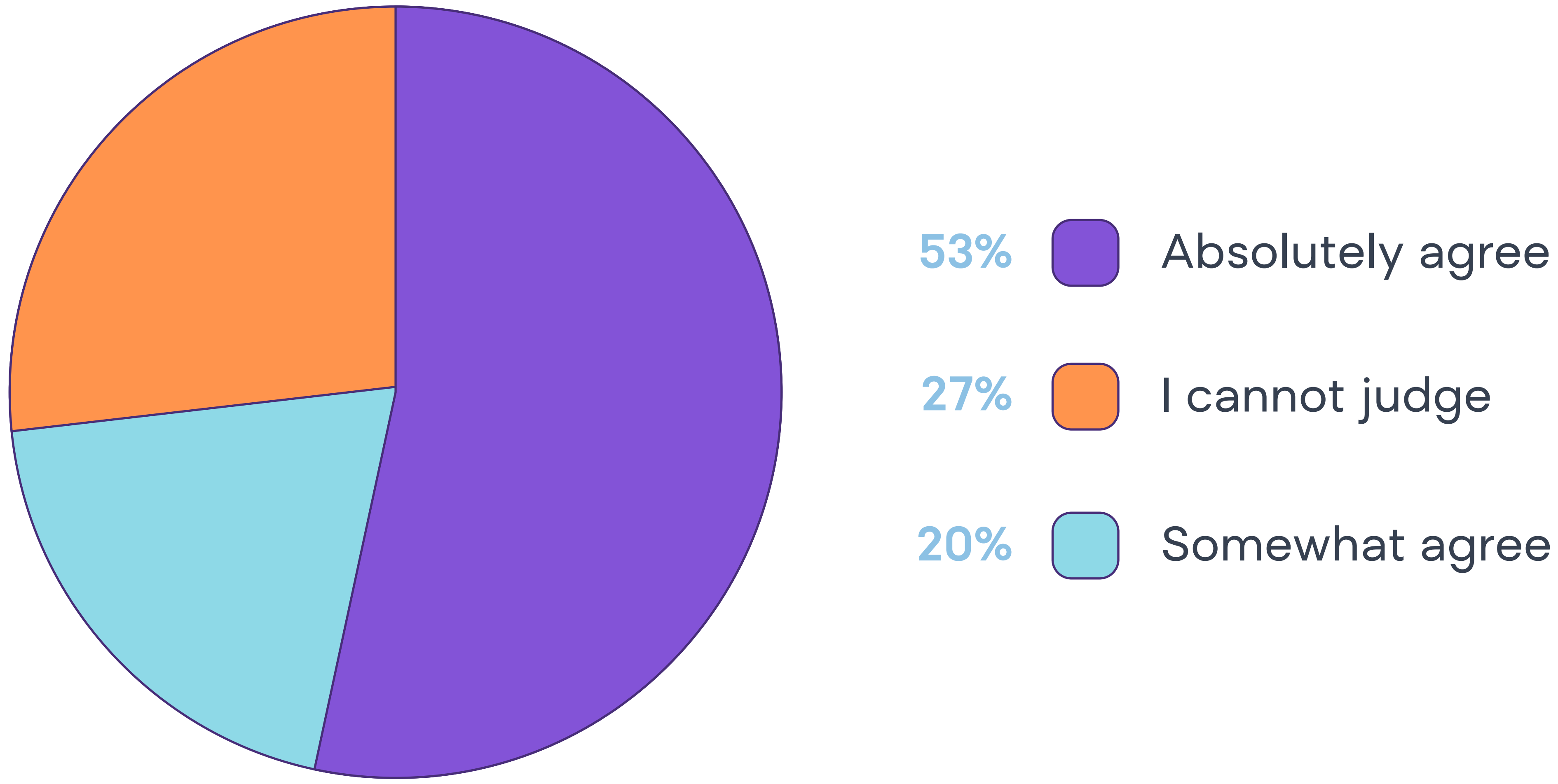


In today’s digitized environment, a proper VDP is essential to the vulnerability management strategy for all security-conscious organizations. However, there are sectors where a VDP implementation is especially critical, such as:



- Healthcare
- IoT sector devices/services/companies
- Critical infrastructure providers
- Automotive
- Software developers
- Finance
- Government organizations
- Telecommunication
- eCommerce companies

How much do you agree that companies in your industry should have a VDP policy?



More than half of the surveyed agree that companies in their industry should have a VDP policy.

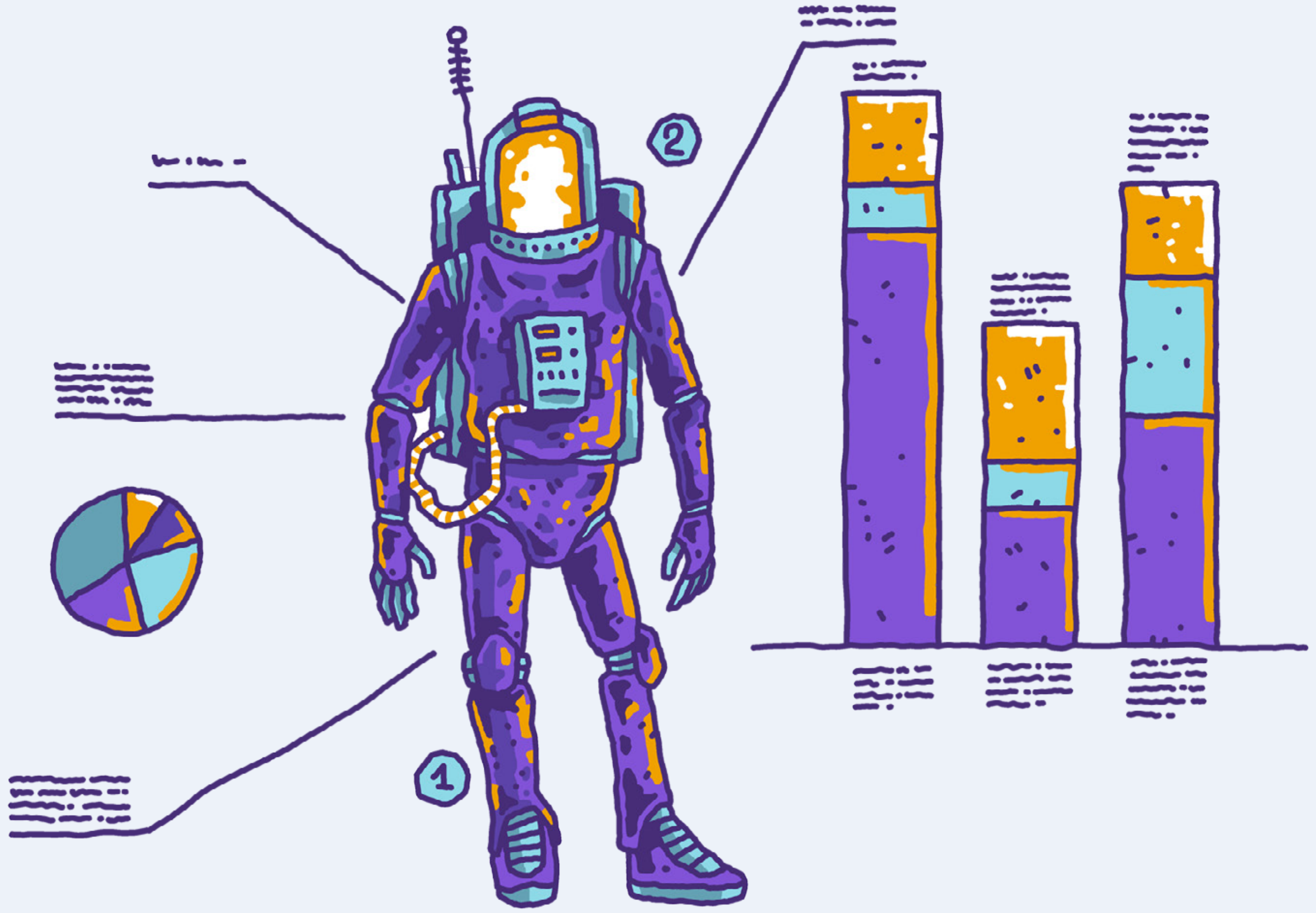
VDP as a third-party requirement

> A VDP can be really useful to have in your own best interest, but it is also becoming a requirement in many areas of business life.

VDP is often required by external entities, such as regulatory bodies, industry standards, or agreements. For example, sectors like telecommunications, healthcare or financial services may have specific compliance requirements that mandate the implementation of VDPs. Additionally, business partners or clients may require organizations to have a VDP as part of their contractual agreements, ensuring a transparent and responsible approach to handling vulnerabilities.

VDPs and Bug Bounty Programs

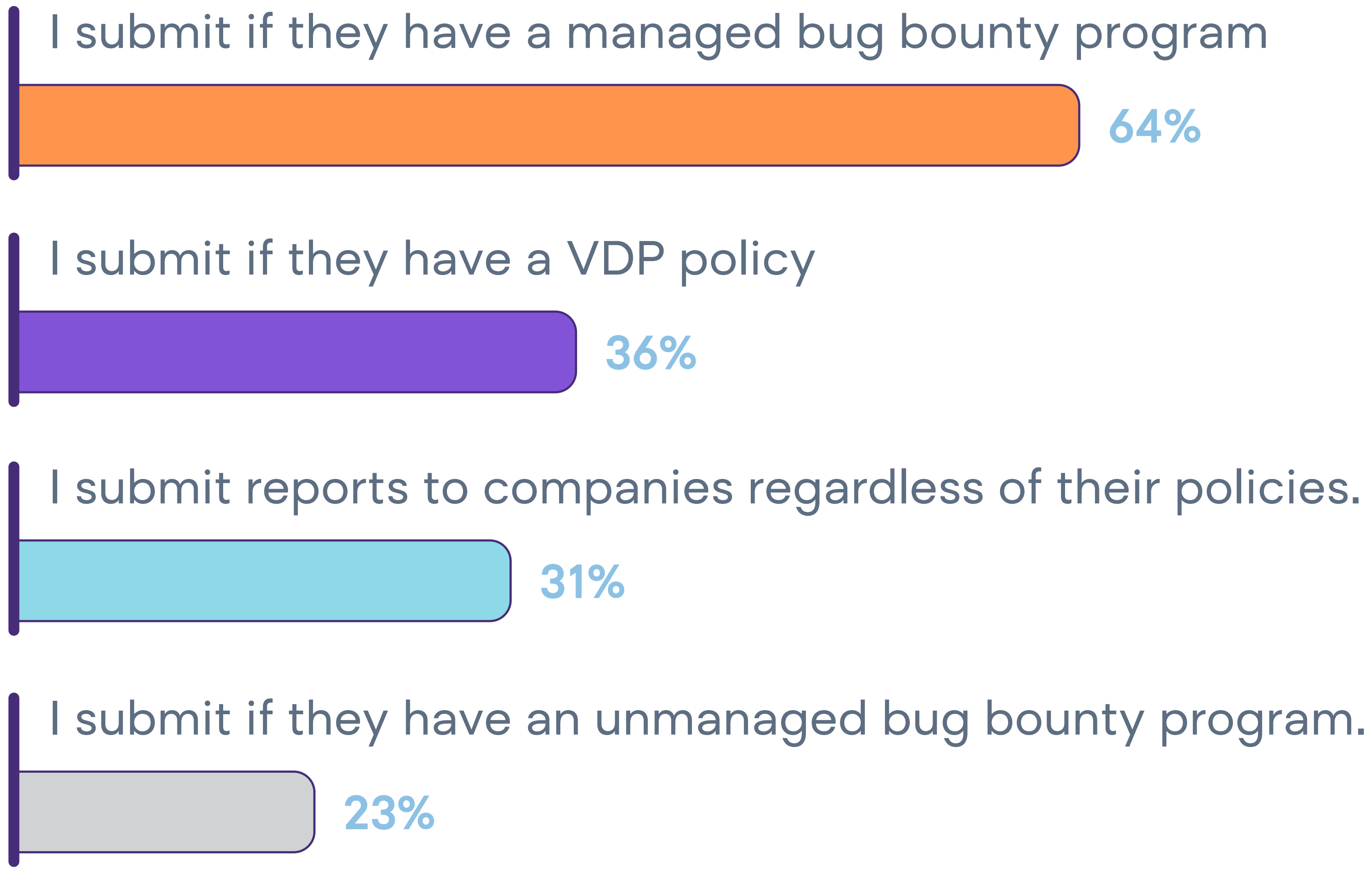
VDP does not encourage researchers to look for vulnerabilities in the organization’s systems but provides a secure channel to report such vulnerabilities to the owner. It ensures that if a detected vulnerability is ethically reported, it will not involve legal actions from the owner toward the reporter.



Bug bounty programs, however, encourage researchers to actively look for vulnerabilities and offer prizes for detecting previously unknown bugs and security gaps. In bug bounty programs, test users are provided for accessing the test systems, and most importantly, the hacker has to prove that their findings are indeed errors. Bug bounty programs can be regarded as crowdsourcing certain parts of security testing.

Such programs leverage the collective intelligence, skills, and diversity of a large number of independent security researchers to identify and address vulnerabilities in the target systems.
This concept is centered on the idea that a crowd’s combined efforts and varied expertise over a long time can surpass what a small dedicated team can achieve during a regular penetration test.

What type of vulnerability reporting process do you prefer at companies you submit vulnerabilities to?



Near two-third of the surveyed ethical hackers / pentesters / security researchers prefer a managed bug bounty program while one third prefer a VDP policy as the vulnerability reporting process.

By combining a VDP with a bug bounty program, organizations can significantly improve the security of their products and services. A bug bounty program can be seen as an extension of a VDP. While a VDP lays the foundation for reporting vulnerabilities, a bug bounty program adds an incentive layer to promote and reward active participation.

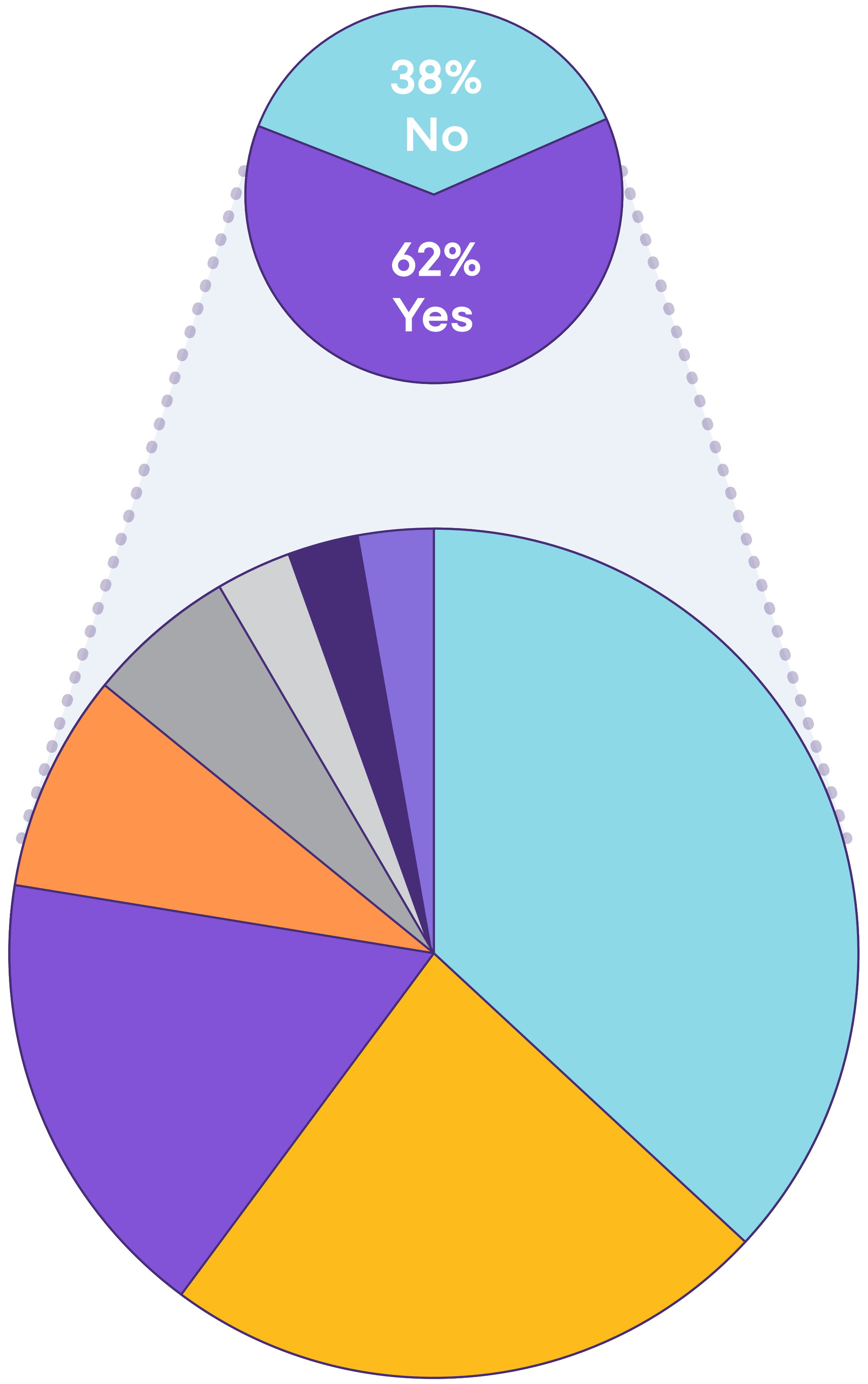
The combination not only helps in identifying and patching vulnerabilities but also serves as a deterrent for malicious actors who might seek to exploit these vulnerabilities.

Find Hackrate's managed Bug Bounty Program here.

3

Risks of neglecting VDP

Developing a vulnerability disclosure policy, and managing the incoming reports along with the identified vulnerabilities involves a great amount of dedicated work, but it should not be disregarded. All online systems are susceptible to vulnerabilities, and you can count on some of those to be found by third parties first, not your organization.



Have you ever neglected to report a vulnerability you discovered?

If yes, why?

37%	🟦	No reward offered
23%	🟨	The company had previously been unresponsive
17%	🟪	No channel to report the vulnerability
8%	🟧	I forgot about it
6%	⬜	Disagreed with the company’s disclosure terms
3%	⬜	The company had previously been challenging to work with
3%	⬛	The company had threatening language on its website
3%	🟪	Other

More than half of the surveyed ethical hackers / pentesters / security researchers have neglected to report a vulnerability, unresponsiveness and missing communication channels being in the top reasons.

Neglecting to prepare for such scenarios by not implementing a proper VDP means risks and challenges for your organization at different levels.

1

The initial difficulty for organizations neglecting VDPs is the **inability to efficiently receive and manage vulnerability reports** from security researchers. This stems from a lack of a coordinated and responsible process for reporting and fixing security vulnerabilities. Without a dedicated channel, incoming **reports will be scattered**. With no appropriate channels for this purpose, hackers will send messages about their findings to random email addresses such as support@ or info@. It is also not uncommon to contact the CISO of an organization through LinkedIn with such information.

2

Receiving out-of-scope reports and findings by automated vulnerability scans will result in a **high noise level** in the incoming information. This makes it **hard to discern critical issues**, and handling **invalid reports costs precious time and resources for the organization**. This unorganized approach can also lead to **blackmailing** attempts, as the absence of a proper reporting system entices exploitation. Moreover, companies **miss out on invaluable insights** as the best reports are usually received through well-structured VDP forms.

3

In the long run, not identifying and patching a vulnerability leaves the company’s **systems and data perilously exposed**. Consequently, the likelihood of a **severe data breach** escalates, compromising both company and customer data.

4

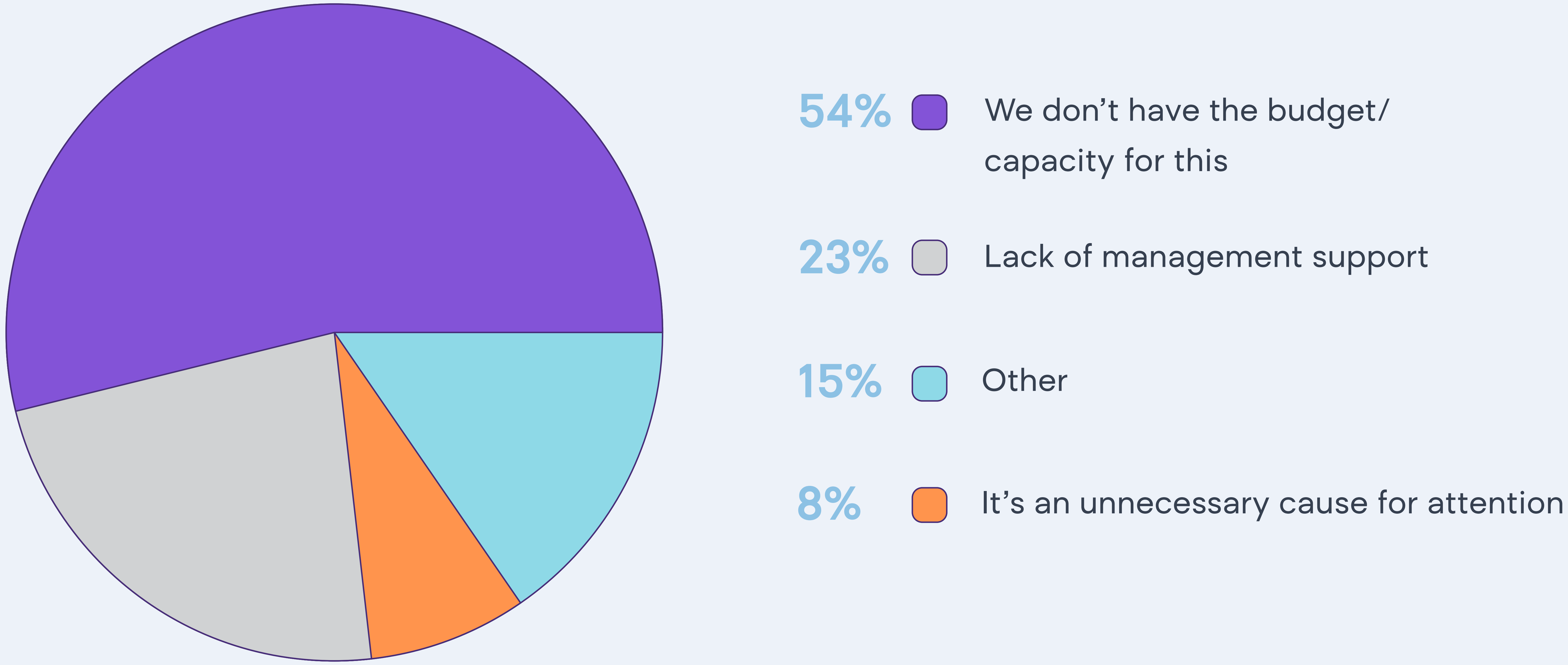
Furthermore, without a VDP, it is **hard to demonstrate commitment to information security and data protection** to stakeholders and customers. This has a ripple effect of **eroding trust** among third parties in the market. It also **hampers** the organization’s ability **to meet regulatory and standardization requirements**, practically mandatory for companies beyond a certain scale.

5

In addition, neglecting VDP exposes the organization to **greater legal risk**. Without a well-structured legal framework or clear legal statements, the company stands vulnerable to legal challenges and unforeseen complications.

Less customer trust directly impacts the company’s reputation and stakeholders’ confidence in the brand. This loss of trust and reputation can have long-lasting effects, potentially hindering the growth and success of the organization.

If your company doesn’t have VDP policy, what are your reasons for it?



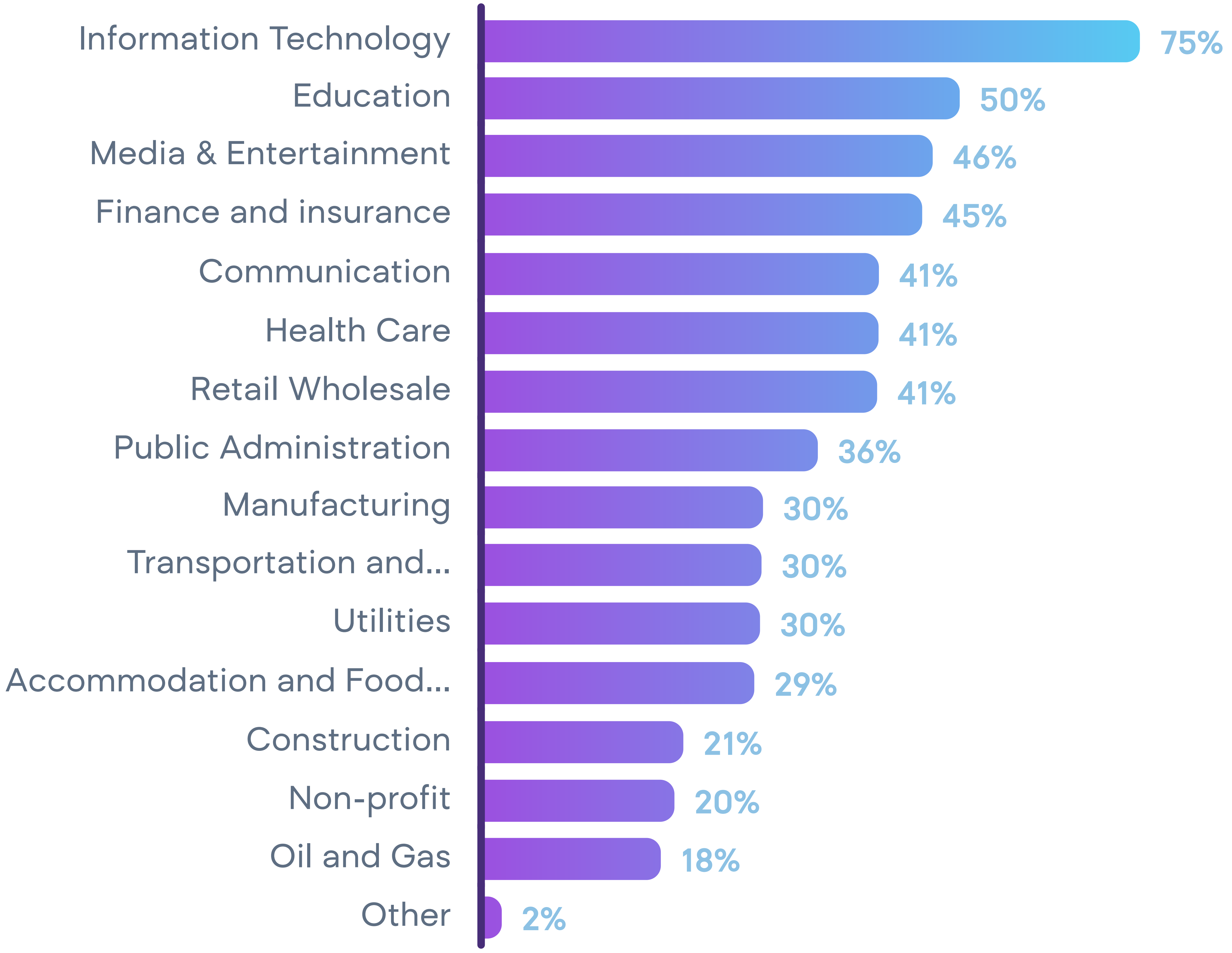
The primary reasons given by security managers for not having a VDP policy are the lack of budget/capacity, and management support.

4

Regulatory environment

Recently, regulatory bodies have started encouraging or even mandating VDPs in specific sectors. For example, in the U.S., the Cybersecurity and Infrastructure Security Agency (CISA) has issued a directive requiring federal agencies to establish VDPs.

What verticals do you most frequently test for vulnerabilities?

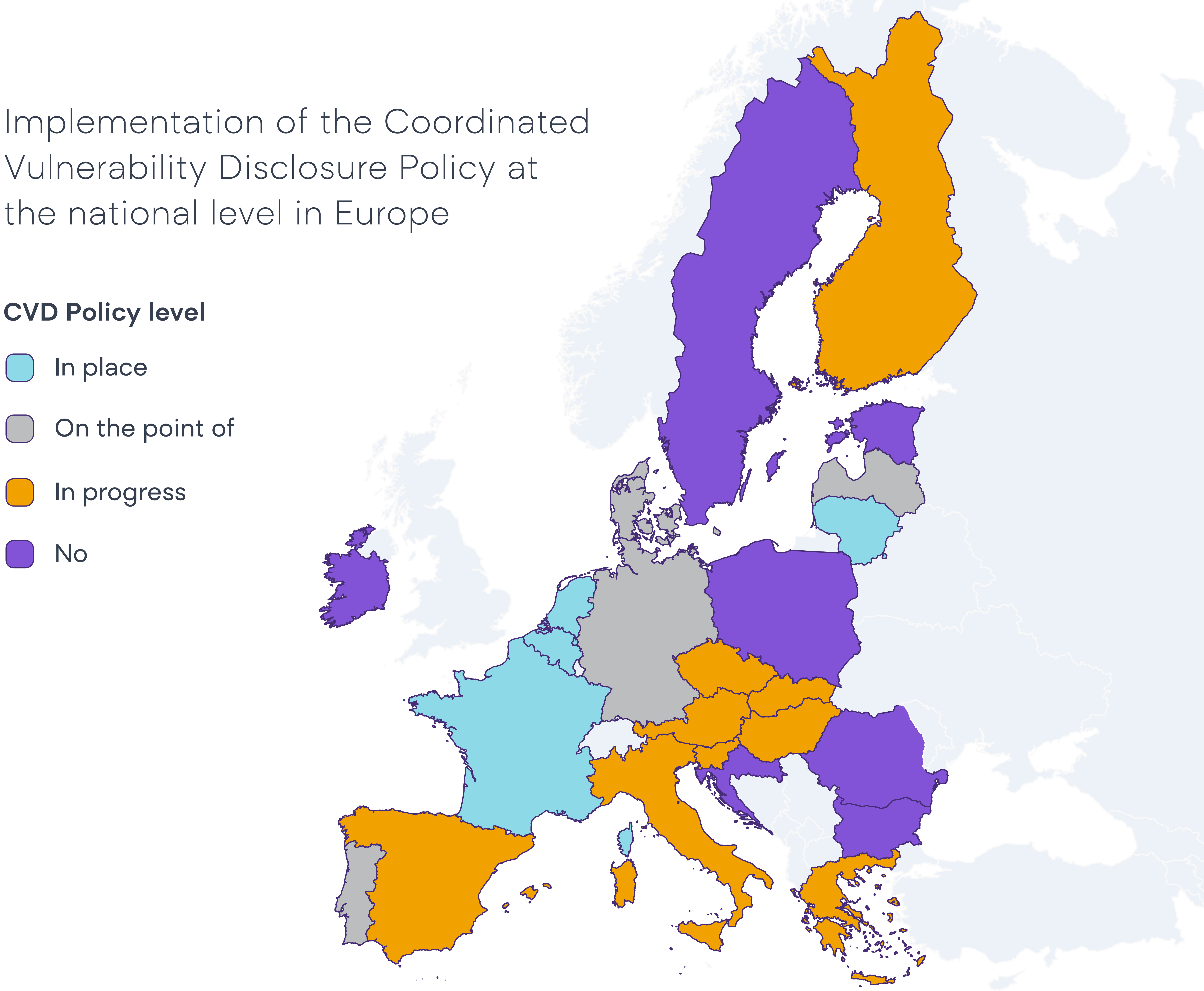


According to the surveyed ethical hackers / pentesters / security researchers the most frequently tested sectors are IT, Education and Media & Entertainment

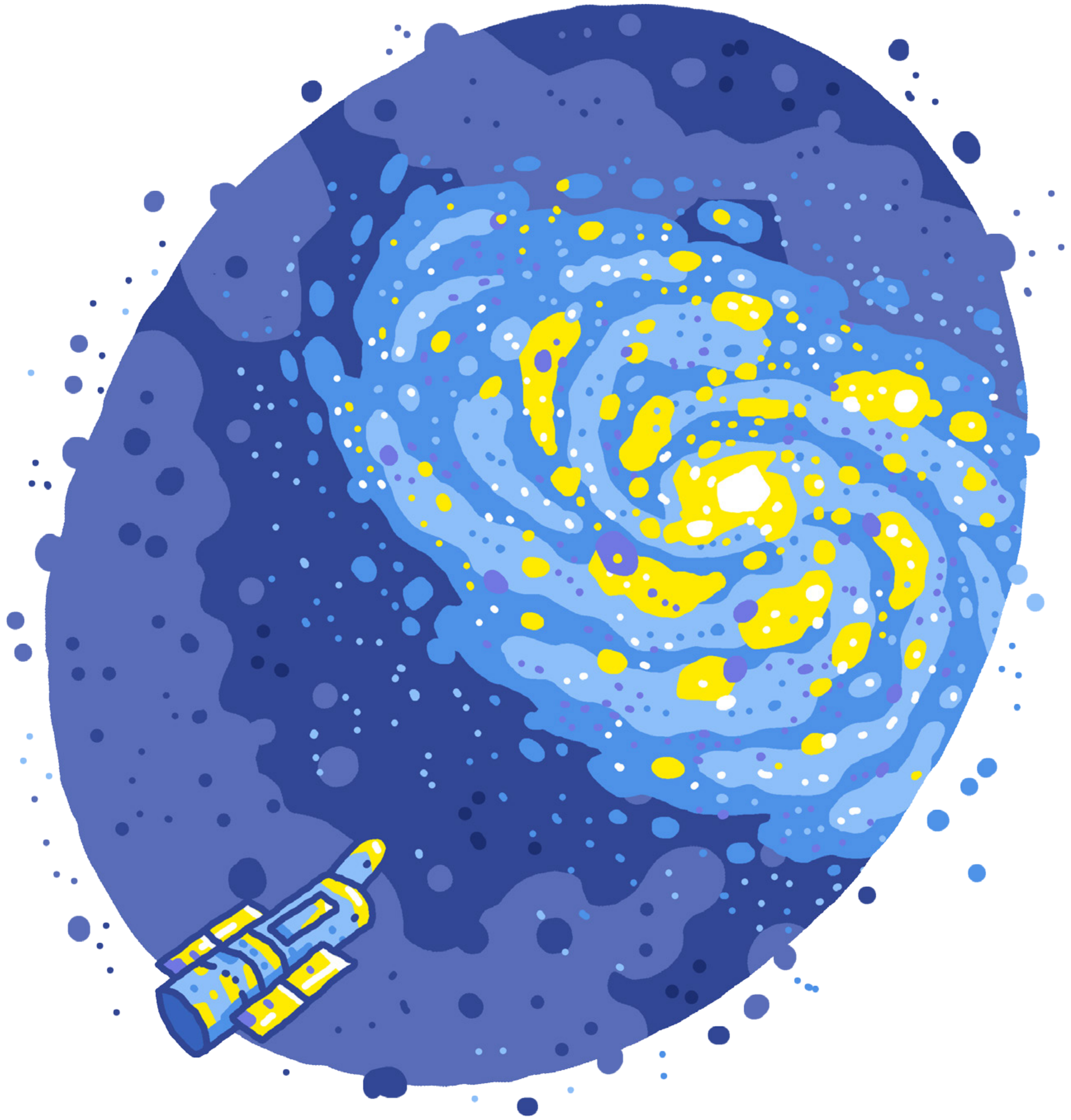
At a legislative level, the EU promotes adopting a preventive and conscious mindset in cybersecurity through its directives, such as NIS, NIS2, and the European Cyber Resilience Act. Some countries have also launched national initiatives promoting VDPs.
For instance, the Netherlands' National Cyber Security Centre has established a Guideline for Responsible Disclosure, which many Dutch organizations have adopted.

The European Union Agency for Cybersecurity (ENISA) also provides guidelines to help organizations develop and manage VDPs. ENISA strongly advocates for responsible vulnerability disclosure and offers resources to help organizations manage the process.

Implementation of the Coordinated Vulnerability Disclosure Policy at the national level in Europe



Source: Coordinated Vulnerability Disclosure Policies in the EU
European Union Agency for Cybersecurity, April 2022



The NIS and NIS2 Directives

In December 2020, the European Commission proposed a revision to the NIS Directive, also referred to as the ”NIS2 Directive,” as an update and expansion of the initial piece. As its predecessor, it further widens the scope and framework for cyber threat management, and paves the way for a more conscious security mindset for the whole of the EU.

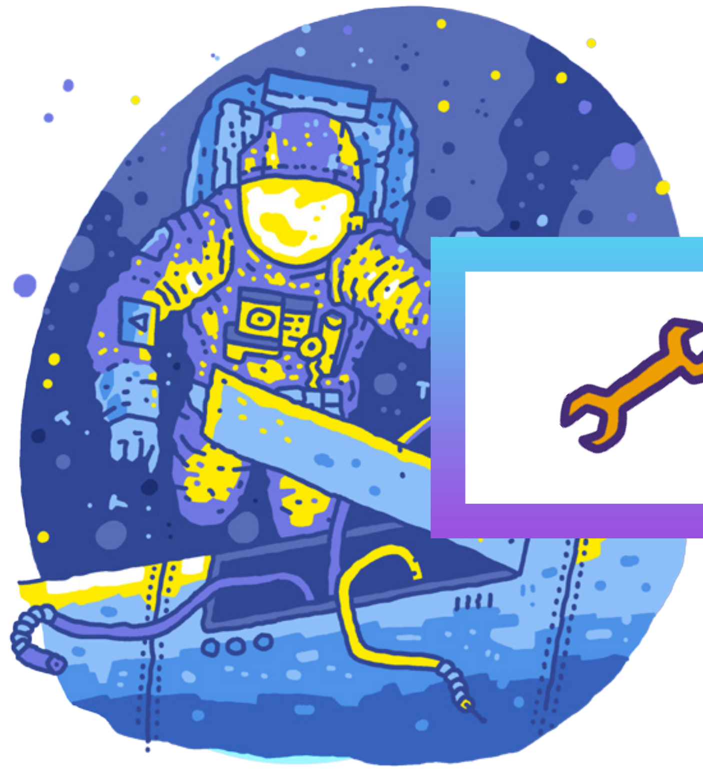
NIS2 places great emphasis on risk management. The directive highlights the importance of establishing security measures (such as vulnerability disclosure policies) to mitigate network and information systems risks. All medium and large organizations operating in these sectors fall under the scope of NIS2.

For more information on the NIS2 Directive, follow this link.

ENISA Coordinated Vulnerability Disclosure (CVD)

Coordinated Vulnerability Disclosure (CVD) gathers information from discovering the vulnerability to public disclosure. It involves crucial steps to ensure that each stakeholder does their part to protect users from harm. The purpose is to learn about a vulnerability, mitigate it, and disclose the information to advance system security rather than exploit it.

The ENISA (European Union Agency for Cybersecurity) has provided guidelines and recommendations for setting up a CVD process.



🔧 The detailed ENISA guidelines can be found here.

These recommendations include:

1. **Preparation:** Establishing a dedicated CVD team, creating a clear CVD policy, and preparing infrastructure for disclosures.
2. **Reception:** Receiving vulnerability reports, establishing a secure communication channel with the reporter, and ensuring reporters' anonymity if desired.
3. **Assessment & Fixing:** Assessing the validity and severity of a reported vulnerability, identifying affected products, and developing fixes or mitigations.
4. **Disclosure:** Coordinating with relevant stakeholders for a simultaneous release of disclosure information, and recognizing the reporter's contribution unless they prefer to stay anonymous.
5. **Post-Disclosure Activities:** Updating affected users about the availability of patches or mitigations and conducting a post-mortem analysis.

The Cyber Resilience Act

The European Cyber Resilience Act, issued in 2022, introduces essential requirements for hardware manufacturers, software developers, distributors, and importers of digital products and services on the EU market.

The following obligations and requirements have to be fulfilled at every stage of the value chain:

1. An appropriate level of cybersecurity
2. Prohibition of selling products with known vulnerabilities
3. Security by default configuration
4. Protection against unauthorized access
5. Limitation of attack surfaces
6. Minimizing incident impact

Manufacturers are expected to conduct regular vulnerability tests, and are obligated to provide duty of care for the entire lifecycle of such products. Non-compliance with these regulations can result in severe penalties.

More on the Cyber Resilience Act.

Product Security and Telecommunications Infrastructure Act 2022

The Product Security and Telecommunications Infrastructure Act 2022 in the UK introduces mandatory security requirements for consumer connectable products, and updates the existing rules for telecommunication infrastructure.

The act explicitly contains a guideline on requiring products to have a vulnerability disclosure policy whereby any security weakness in a product is identified and notified.

It will come into effect from April 29, 2024, and this is one of the criteria that IoT manufacturers must meet if they want to sell their products in the UK. US and EU regulations are on the horizon as well.

The Product Security and Telecommunications Infrastructure Bill.

ISO Standards

{ ISO 27001 }

ISO 27001 is an international standard that provides a framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).

Organizations using ISO 27001 should have mechanisms for employees and other relevant stakeholders to report perceived weaknesses in systems or processes. These reporting mechanisms can be part of a vulnerability disclosure program, which aims to identify, report, and address vulnerabilities in a system.

Although ISO 27001 doesn’t prescribe a specific approach to vulnerability disclosure, it encourages a culture of continuous improvement and proactive risk management, which aligns with best practices in vulnerability disclosure.

For specific procedures and policy guidance for vulnerability disclosure, organizations might refer to other standards or frameworks such as ISO 29147 (vulnerability disclosure) and ISO 30111 (vulnerability handling processes).

{ ISO 29147 }

ISO/IEC 29147:2018 is an international standard that provides guidelines for disclosing potential vulnerabilities in products and online services.

The goal of ISO 29147 is to establish best practices for this process, promoting better cooperation between vendors and vulnerability reporters, such as security researchers or users who identify potential security issues.

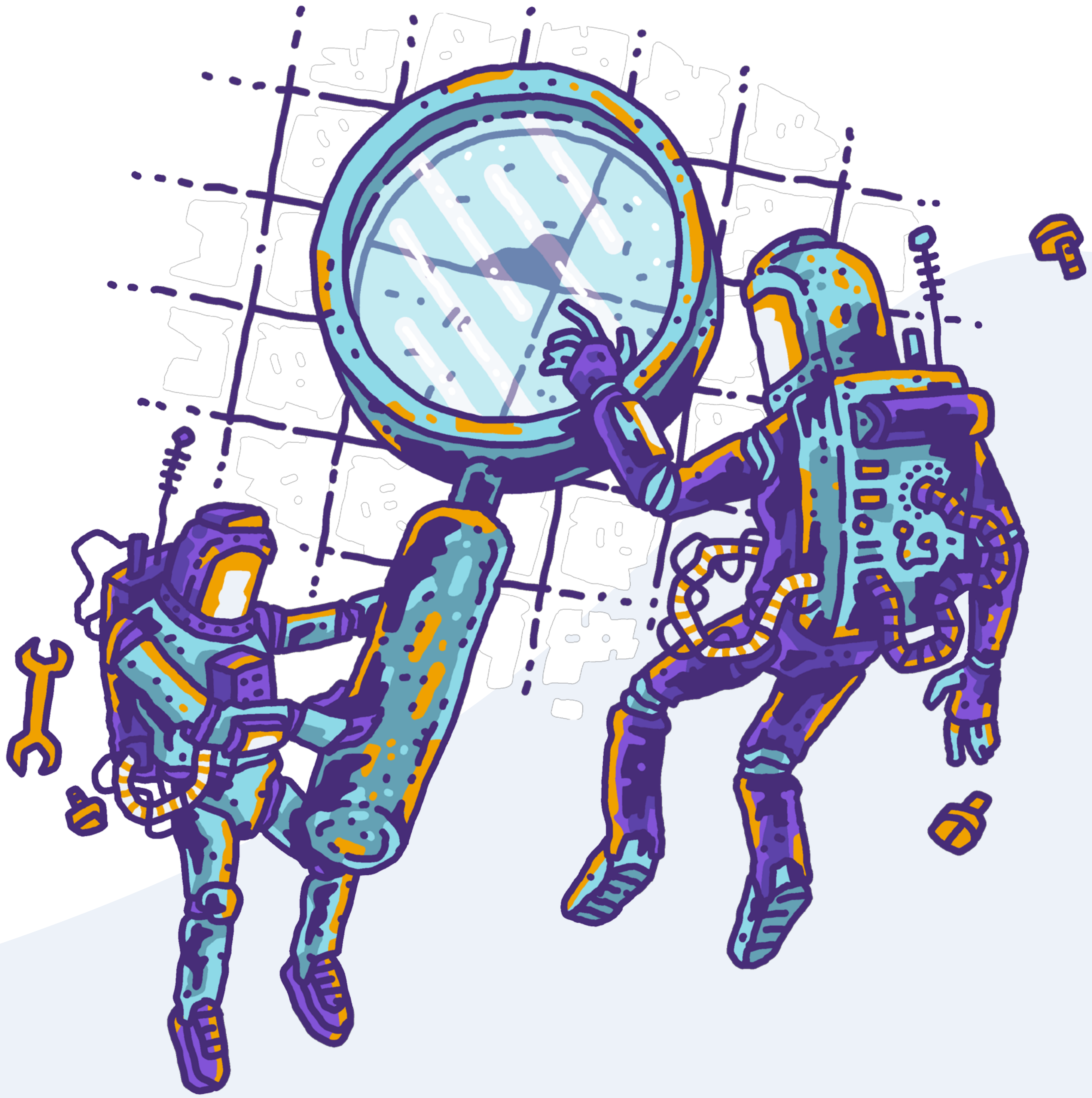
The key elements of this standard include guidelines for vendors, guidelines for researchers discovering vulnerabilities and the information elements of vulnerability disclosure.

{ ISO 30111 }

The ISO 30111 international standard focuses on managing cybersecurity risks for road vehicles. Concerning vulnerability disclosure, it provides guidelines for automotive organizations on handling and responding to vulnerabilities discovered in their vehicles or automotive systems.

The standard underlines the importance of establishing an effective vulnerability disclosure process that encourages external parties, such as researchers and the general public, to report identified vulnerabilities responsibly.

The most important points discussed by ISO 30111 are developing a disclosure policy for vulnerabilities, maintaining appropriate channels for reporting, and ensuring timely acknowledgment, assessment and response. It also promotes coordinated disclosure and remediation through communication between the reporter and the organization, maintaining confidentiality, while sharing the relevant details with affected stakeholders.



Why do IT security managers think that VDP is an important topic today?

“Performing structured internal PT activities together with ”unstructured ’’ ones conducted by external experts (playing with defined rules) fosters an increased completeness of vision, an enrichment of perspective and an extension of the hacking approaches put in contact with the targets. With the mindblowing increase of the attack rate, this could be beneficial in helping a faster remediation.”

“As our dependence on digital systems grows, so do the threats. Data breaches, hacks, and other cyber threats are becoming more sophisticated and frequent. VDPs allow organizations to learn about vulnerabilities in their systems that they may not have been aware of and to fix them before they can be exploited.”

“Cybersecurity is a shared responsibility. Hackers, security researchers, and even users can discover vulnerabilities. A formal VDP provides a clear channel for these individuals to share their findings responsibly and safely.”

“When organizations embrace VDPs, they are committed to security and transparency. This can help build trust with users, customers, partners, and regulators.”

5

VDP in the IoT industry

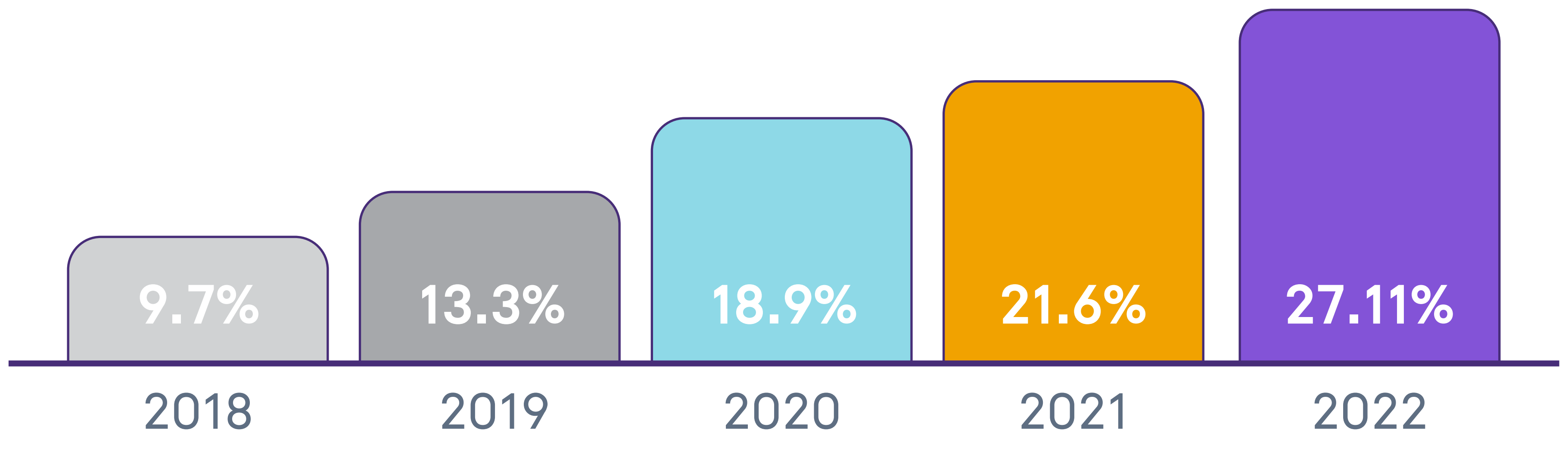
If you work in web application security or web bug bounty hunting, you'd typically expect well-established companies to have a clear and easily accessible VDP. But things look pretty different regarding the IoT (Internet of Things) sector.

In the 2010s, the number of VDPs in the IoT industry was almost non-existent. However, there has been some progress since then, and we're hopeful that things will continue to improve.

The graph below is from the survey conducted by the Internet of Things Security Foundation (IoTSF) in 2023 involving 300+ manufacturers: only 27% of the companies surveyed had a VDP on their website - the majority still didn't.

Vulnerability Disclosure in Practice Trend

Percentage of dataset



BUGPROVE

"The VDP requires the company to create new procedures and invite external input, establishing a structured connection between reporters and the company. While it's currently not mandatory, upcoming regulations seek to alter that." - Gergő Hosszú, Security researcher, Co-Founder of BugProve.

Every legislator agrees that having a Vulnerability Disclosure Program is a first and crucial step for every IoT vendor to improve its security. One example is the Product Security and Telecommunications Infrastructure Act 2022 in the UK listed above in the "Regulatory environment" section.

6

How to start your VDP journey?

A responsible disclosure policy outlines the process for reporting security vulnerabilities and guides how to handle them. Here are the recommended steps for creating a responsible disclosure program.

1. **Establish clear guidelines for reporting security vulnerabilities**

   a. Define the scope of the program

   b. Specify accepted vulnerability types

   c. Outline the reporting process

   d. Determine eligibility criteria

   e. Include information required in the report

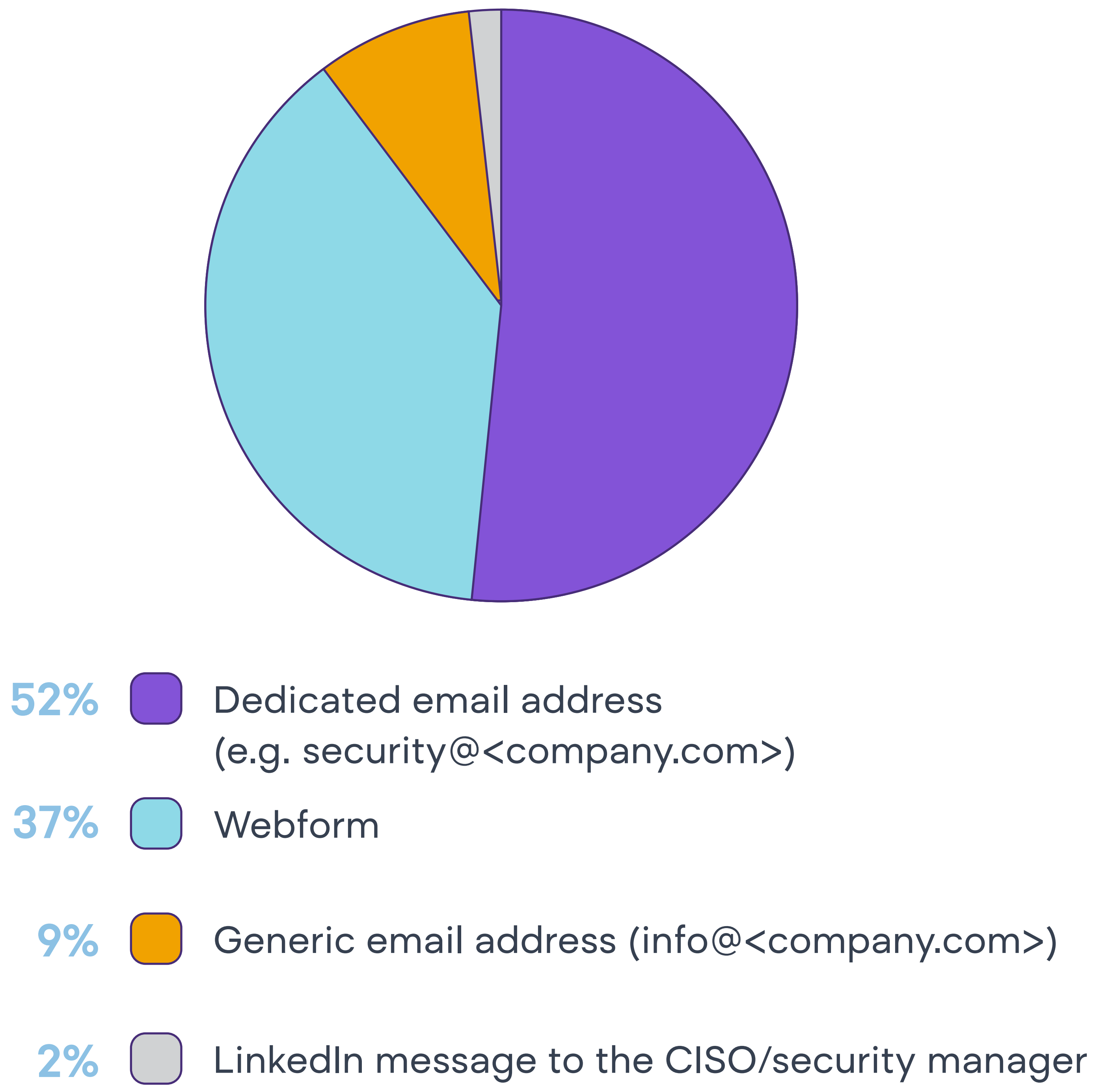
   f. Implement safe harbor practices

2. **Create a communication plan**

   a. Establish a secure channel for vulnerability reports

   b. Develop a system for communication with researchers

What is your preferred channel for submitting vulnerability reports?



More than half of the surveyed ethical hackers / pentesters / security researchers prefer a dedicated email address as the main communication channel for submiting vulnerability reports.

3. **Issue a public statement acknowledging responsible disclosure and expressing gratitude to participants**

4. **Develop a process for assessing and addressing reported vulnerabilities**

   a. Verify the validity of the reported vulnerabilities

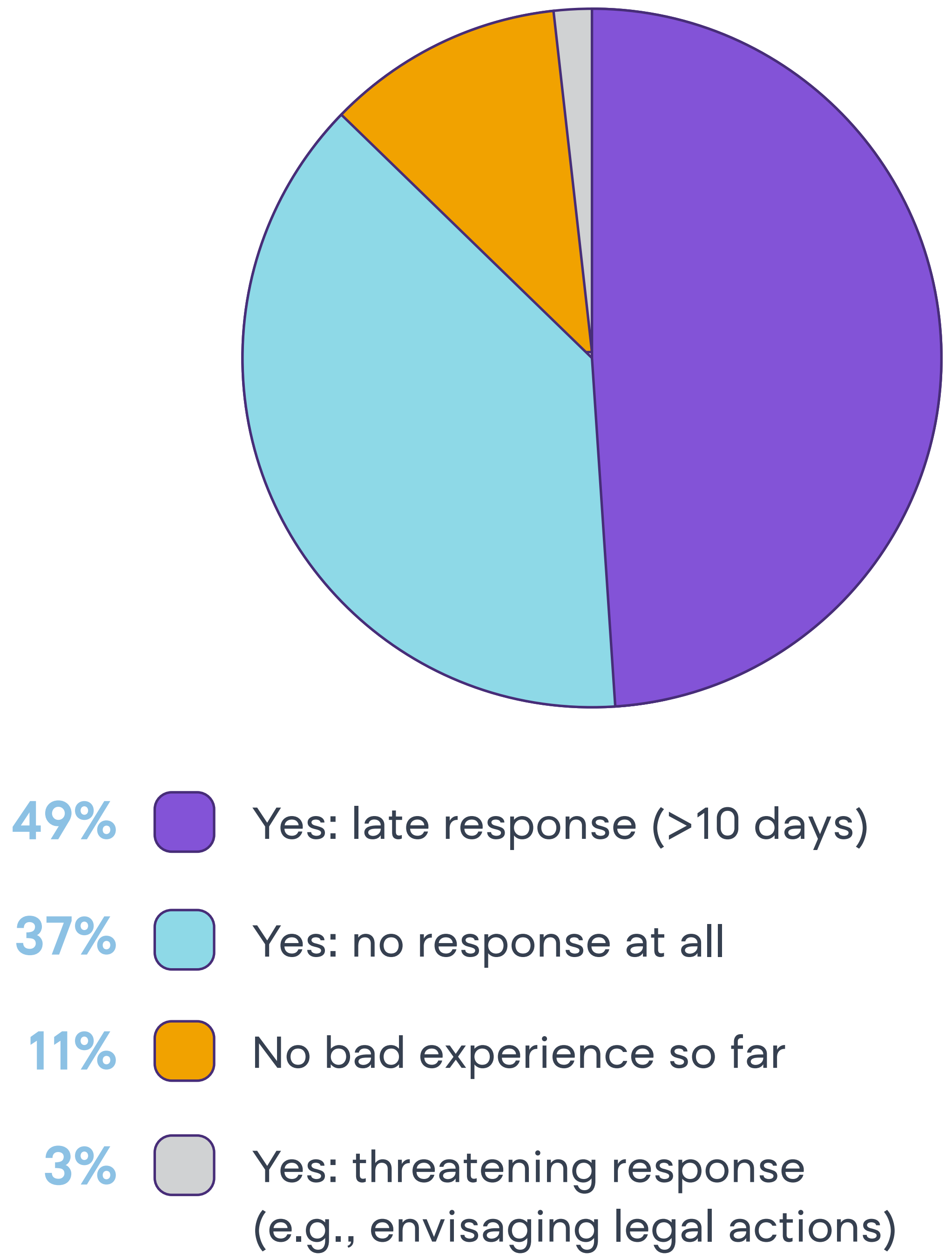
   b. Evaluate the severity of each vulnerability

   c. Implement necessary fixes or patches

   d. Set a timeline for response and resolution

5. **Consider implementing an incentive structure, such as a bug bounty program, to reward researchers who report valid security vulnerabilities in your products or services**

Have you ever had a bad experience following your report submission to an organization?



More than 80% of the surveyed ethical hackers / pentesters / security researchers already had a bad experience after reporting a vulnerability due to late or non existing responses.

Following these steps, you can create a responsible disclosure program that helps protect your company from potential cyber-attacks. We recommend following the two ISO standards for vulnerability management as guidance (ISO/IEC 29147: Vulnerability disclosure and ISO/IEC 30111: Vulnerability handling processes).

With these elements in place, organizations can create an effective, responsible disclosure program that encourages collaboration between security researchers and IT teams while promoting security best practices.

Elements of a well-rounded VDP program:

Statement of intentions (what parties can expect from each other)

Scope (products, systems covered, types of vulnerabilities, types of testing allowed)

The process of reporting detected vulnerabilities

Preferences and aspects of evaluating reports

The OWASP approach

The Open Web Application Security Project (OWASP), one of the most advanced and up-to-date projects in the field, developed comprehensive best practices for vulnerability disclosure based on extensive research. Responsibilities and recommended behavior collaboration in vulnerability disclosure according to OWASP:

Researchers should:

- Ensure that any testing is legal and authorized
- Respect the privacy of others
- Make reasonable efforts to contact the security team of the organization
- Provide sufficient details to allow the vulnerabilities to be verified and reproduced
- Not demand payment or rewards for reporting vulnerabilities outside of an established bug bounty program

Organizations should:

- Provide a clear method for researchers to securely report vulnerabilities
- Establish the scope and terms of any bug bounty programs
- Respond to reports in a reasonable timeline
- Communicate only with researchers
- Not threaten legal action against researchers
- Request CVEs where appropriate
- Publish clear security advisories and changelogs
- Offer rewards and credits

Refer to the Vulnerability Disclosure Cheat Sheet on OWASP's website for a helpful guide on the vulnerability disclosure process.

7

Introduction of mVDP

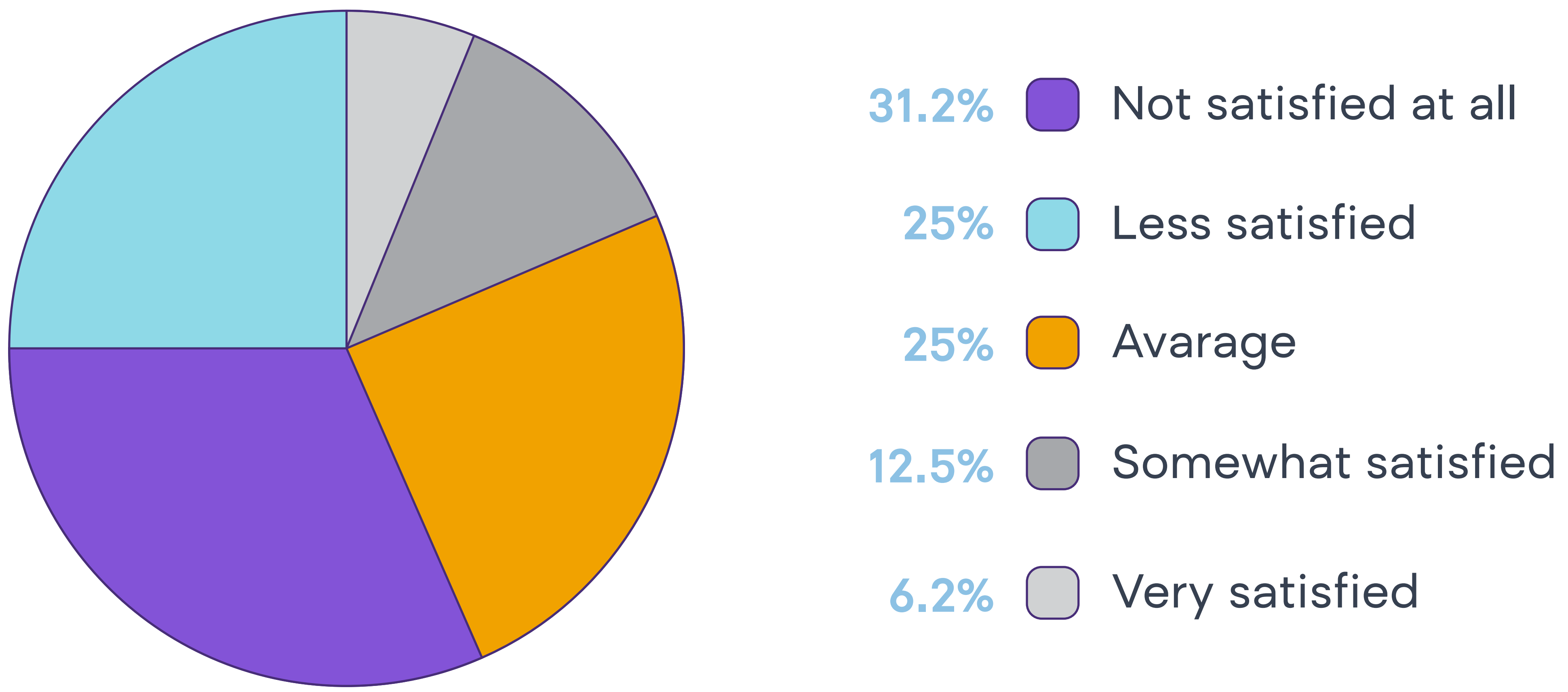
A Managed Service to Establish Your VDP Process

More than half of the surveyed security managers are not or less satisfied with their current vulnerability management practice.

VDPs require substantial internal resources, including staff time for creating policies, handling communications, validating reports, and fixing vulnerabilities.

The initial setup is not expensive, but maintaining their own team and resources over time can add up. Organizations need to have in-house expertise in security to effectively manage disclosures and assess the severity of vulnerabilities. Responsiveness to reports is crucial and might be slower, especially for organizations with limited security staff.

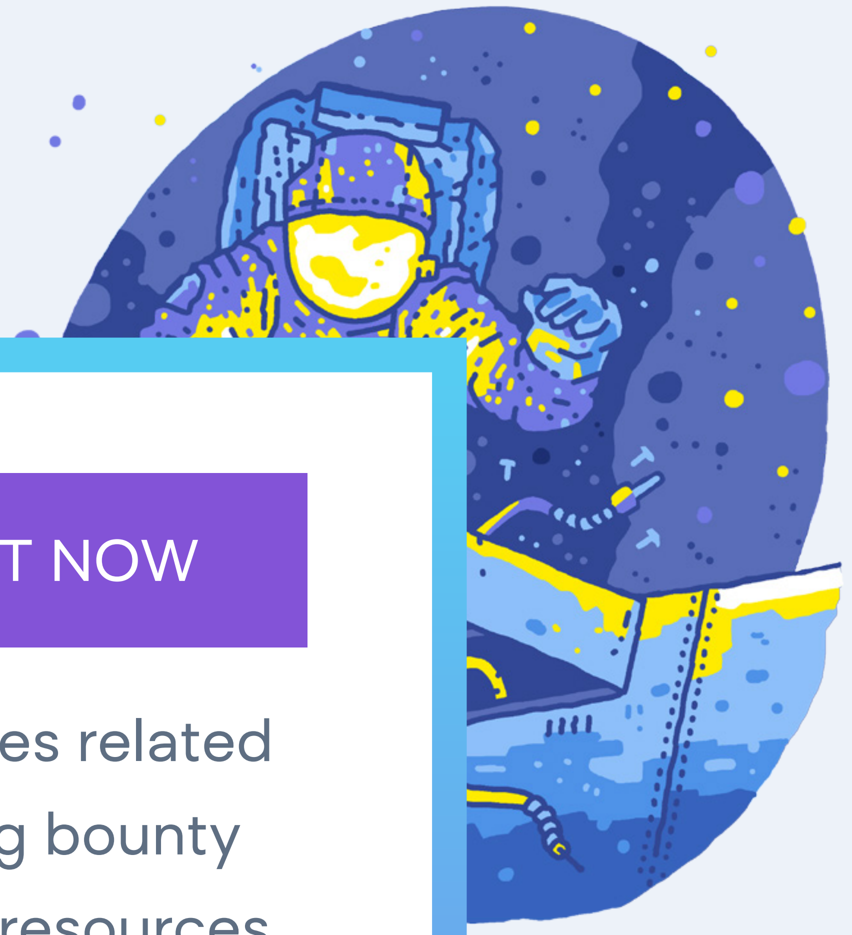
How satisfied are you with your company’s current vulnerability management practice?



With VDP management as a service, providers typically have **teams of experts** who can assist in evaluating and triaging the reported vulnerabilities. They oversee the implementation process, providing templates, communication channels, and a platform for managing the disclosures.

Service providers can generally **scale quickly** to handle an increasing volume of reports, **maintaining responsiveness** with dedicated teams to manage communications.
VDP management as a service usually involves an ongoing fee, but becomes significantly **more cost-effective** in the long run, especially for organizations that don't have the capacity to manage VDPs in-house.

Self-managed VDPs offer greater control but require more resources and expertise, making them suitable for larger organizations with well-established security teams.
On the other hand, vulnerability Disclosure Policy Management as a service is particularly beneficial for organizations lacking the internal resources or expertise to manage a VDP effectively.



{-} Hackrate

TRY IT NOW

Hackrate is a cybersecurity company that provides services related to vulnerability management, penetration testing, and bug bounty programs. Hackrate can help you reduce implementation resources and operational tasks of your VDP, with a VDP-as-a-Service, called managed vulnerability disclosure policy (mVDP).

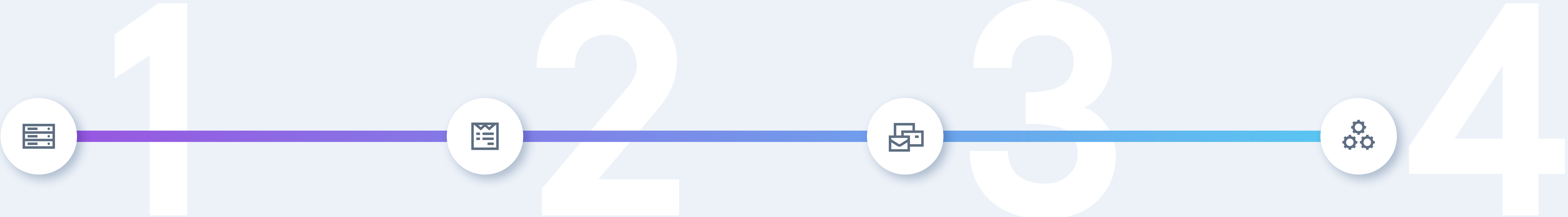
Hackrate's managed VDP solution alleviates the burden of dealing with the high number of reports. Elevates the quality of work by letting professionals manage reports and handle vulnerabilities. Significantly lowers costs by eliminating the need for having the appropriate number of skilled employees dedicated to the task.

- Predefined replies to automated reports.
- Hackrate can handle 99.9% of incoming vulnerability reports. Only a few disputed ones are forwarded to the client for assessment.
- Tries to reproduce the error based on the error description and reports the successfully reproduced error to the client.
- No need to have access to the client's systems.

How to set up your mVDP?

{ the Hackrate approach }

If you want to know more about managed VDP solutions, visit Hackrate.



Set up your VDP

Hackrate helps you specify the content of your VDP.

Publish the reporting form on your website

Embed the Hackrate submission form on your website to use Hackrate's platform for receiving vulnerability reports.

Receive validated reports

Hackrate's team validates all incoming submissions before you receive them. The structured vulnerability report form improves the quality of the reports.

Fix the vulnerabilities

Hackrate manages the entire process, including mitigation efforts, and assisting in communication with ethical hackers.

8

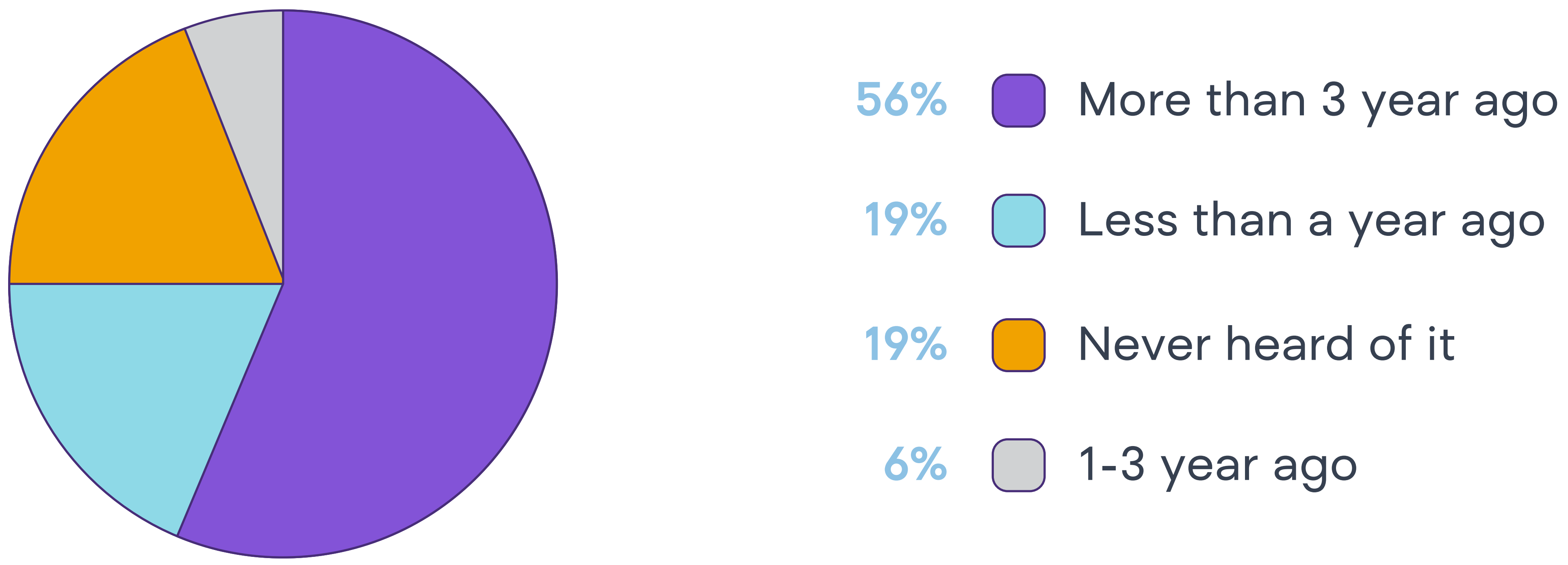
VDP Overview in Europe

Vulnerability Disclosure Programs (VDPs) have increasingly become an important aspect of cybersecurity within European organizations. Many European organizations, especially those in technology, finance, and critical infrastructure, have adopted VDPs.

Despite the progress, challenges remain. Some organizations still hesitate to invite unknown security researchers to test their systems.

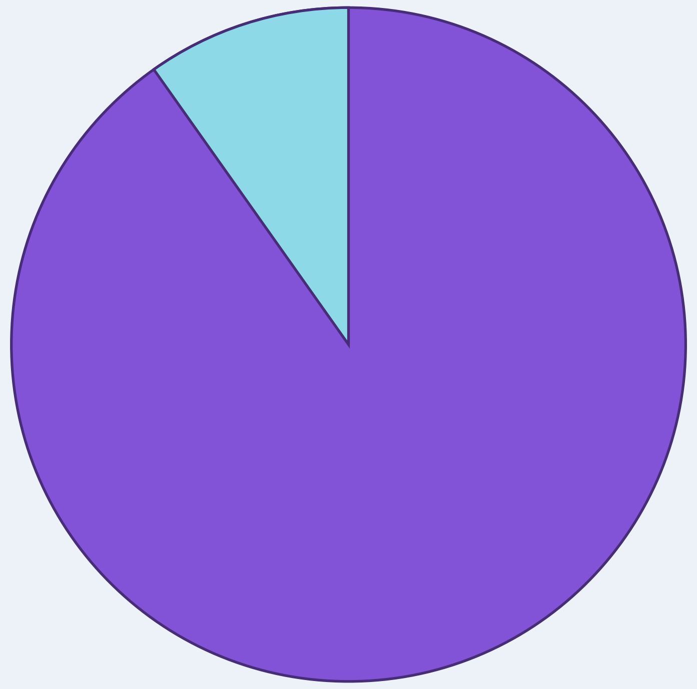
The future of VDPs in Europe seems promising, as organizations continue to embrace the benefits of crowd-sourced security testing and the regulatory environment continues to evolve in favor of more proactive and comprehensive cybersecurity practices.

When did you first hear about Vulnerability Disclosure Policy?



Most of the surveyed security managers heard about VDP more than 3 years ago.

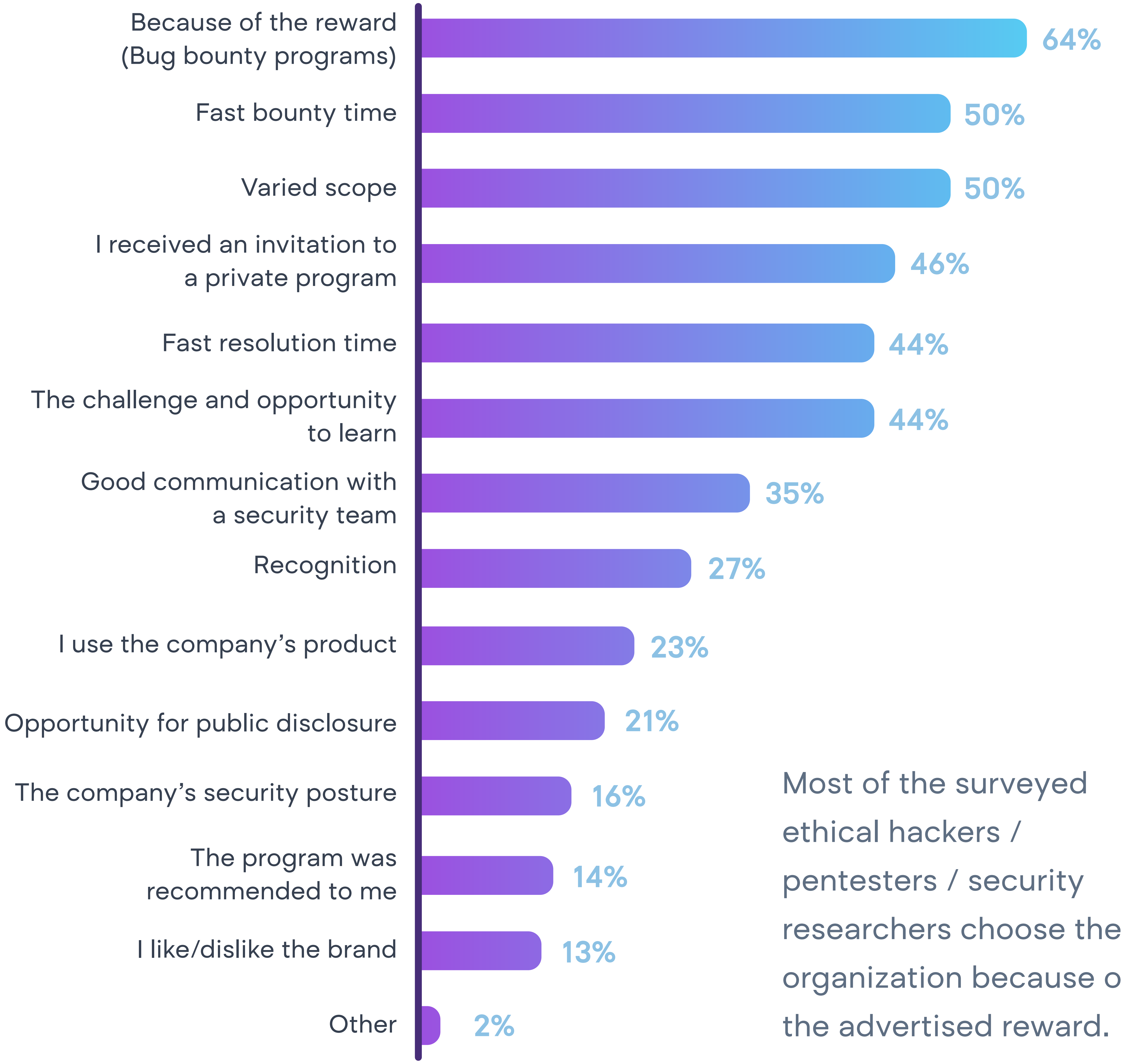
Have you ever submitted a vulnerability report or participated in a bug bounty program of an Organization?



89% 🟪 Yes 11% 🟦 No

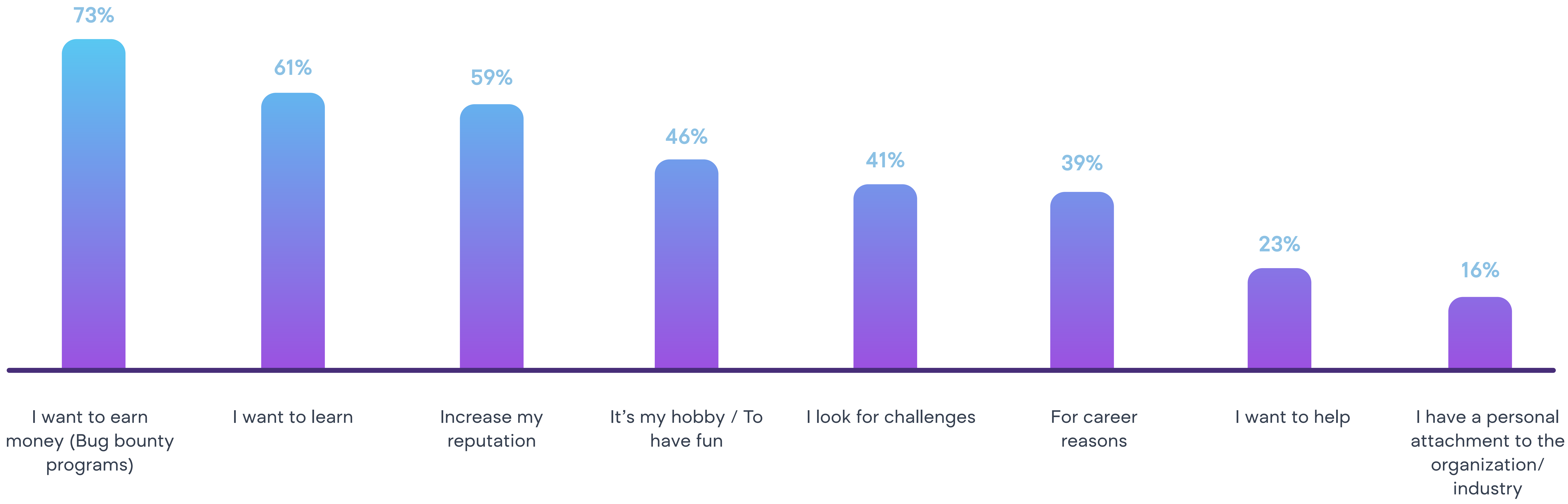
Most of the surveyed ethical hackers / pentesters / security researchers have already participated in a bug bounty program.

How do you choose the organization to test?



Most of the surveyed ethical hackers / pentesters / security researchers choose the organization because of the advertised reward.

What is your key motivation behind submitting vulnerability reports to organizations?



Most of the surveyed ethical hackers / pentesters / security researchers are motivated by the reward and learning.

9

Conclusion

Today, VDPs are becoming a best practice in corporate cybersecurity. Organizations, from small startups to large corporations, have established VDPs, often with the help of platforms that manage the process.

We can expect to see even wider adoption of VDPs and the continued evolution of these policies to address new challenges and threats. This may include greater emphasis on managing supply chain risks, increased cooperation between different organizations, and further integration of VDPs into broader risk management and cybersecurity frameworks.

Learn more about Hackrate's managed VDP service.

List of references

Common Vulnerabilities & Exposures Program - CVE
https://www.cve.org/About/Overview

Coordinated Vulnerability Disclosure policies in the EU - ENISA
https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

Economics of Vulnerability Disclosure - ENISA
https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

Coordinated Vulnerability Disclosure Policy - CISA
https://www.cisa.gov/coordinated-vulnerability-disclosure-process

Federal Information Security Moderniztation Act - FISMA
https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act

Cybersecurity Framework - NIST
https://www.nist.gov/cyberframework

EU Cyber Resilience Act
https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Vulnerability Reporting - National Cybersecurity Centre
https://www.ncsc.gov.uk/information/vulnerability-reporting

Directive on Measures for a High Common Level of Cybersecurity Across the Union - NIS2 Directive
https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT in 2022 - A report prepared by Copper Horse Ltd., 2023
IoTSF-Release-The-State-of-Vulnerability-Disclosure-Usage-in-Global-Consumer-IoT-in-2022.pdf (iotsecurityfoundation.org)

Vulnerability Disclosure Cheat Sheet - OWASP
https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html