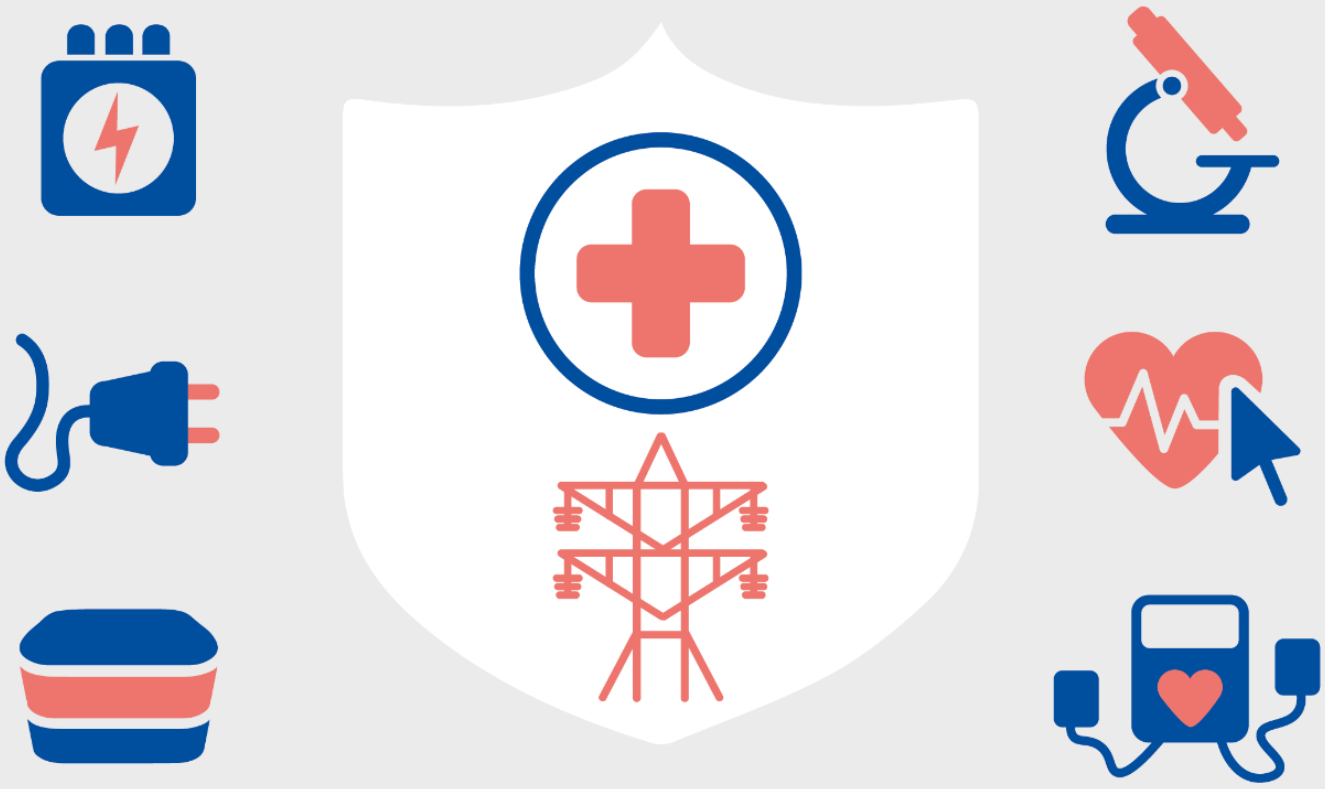
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



PSIRT EXPERTISE AND CAPABILITIES DEVELOPMENT

Health and Energy PSIRT study and recommendations

JUNE 2021

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector, and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For queries in relation to this study, please use resilience@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Peter Biro, European Union Agency for Cybersecurity; Benoît Marion, Wavestone; Xavier Rettel, Wavestone.

ACKNOWLEDGEMENTS

We would like to warmly thank all the teams that took part in our survey and our interviews. Their contributions and inputs were greatly appreciated and were essential to the analysis of the key findings, the formulation of recommendations and the redaction of this report.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-504-3 – DOI: 10.2824/687838

EXECUTIVE SUMMARY

This study focuses on the Sectoral Computer Security Incident Response Team (CSIRT) and Product Security Incident Response Team (PSIRT) capabilities status and development within the energy and healthcare sectors as specified within the NIS directive. This report follows the December 2020 publication of *Sectoral CSIRT Capabilities - Status and Development in the Energy and the Air Transport sectors*.

Desk research has been conducted, followed by a survey which was answered by 7 PSIRTs and 22 CSIRTs from 19 EU Member States. The relatively low number of PSIRTs, especially of those with a scope limited to the energy and healthcare sectors, led us to include more CSIRTs and more sectors in the study. The findings and recommendations still apply to the energy and healthcare sectors, but also offer a wider view of the product vulnerability management landscape.

As a result, 12 key findings were identified, and 9 recommendations have been proposed.

One of the main findings is the lack of visibility of PSIRTs: from an external point of view, it is not always clear what their activities are and who to contact. Even from an internal point of view, the PSIRTs are not sufficiently identified in their role. This report offers recommendations in terms of standardised presentation and increased visibility to improve this issue.

The second main finding is the current difficulties for different stakeholders of the vulnerability ecosystem (PSIRTs, CSIRTs, national/sectoral CSIRTs, end clients, Operators of Essential Services (OES)) in communicating and collaborating efficiently with each other in order to improve product cybersecurity as a whole. The associated recommendations revolve around technical standards to improve interoperability and automation, and processes to streamline the exchange of sensitive information, especially with OES which would greatly benefit from early notification in the case of vulnerability disclosure.

As to the role of ENISA, the respondents to the survey expect the Agency to provide them with guidelines, general security recommendations and, at a more global level, a high-level cooperation framework intended to help develop best practices and improve exchanges among PSIRTs and other incident response (IR) teams within the European Union (EU). NIS 2 should bring improvements in this area, as some of these expectations have already been outlined in the NIS 2 proposal, for instance regarding a vulnerability registry for OES and their suppliers, and regarding the important role of CSIRTs in global coordination.

KEY FINDINGS

The research highlighted the following 12 key findings:

ORGANISATION, PROCESSES & TOOLS

Key Finding #1 Outside their IR Processes, PSIRTs' activities and their involvement in product lifecycle is heterogeneous.

Key Finding #2 The adoption of third-party vulnerability management platforms is uncommon. Those who use one do so because it is easier to manage and improves visibility.

Key Finding #3 Measuring the efficiency of a PSIRT proves to be challenging, as most PSIRTs essentially track efficiency with the number of vulnerabilities reported and mitigated.

Key Finding #4 PSIRT members have both technical skills in product security areas and soft skills which enable smoother exchanges and cooperation between all the stakeholders.

COLLABORATION

Key Finding #5 PSIRTs do not have specific procedures to address vulnerabilities affecting OES and the NIS directive does not seem to have impacted PSIRT activities much.

Key Finding #6 PSIRTs collaborate one with each other, but their collaboration is hindered by the lack of formalised communication and information exchange procedures/standards/framework.

Key Finding #7 Collaboration between PSIRTs and external CSIRTs (sectoral/national) is underdeveloped because of difficulties in establishing contact and sharing sensitive information even though CSIRTs are demanding more regular contact.

Key Finding #8 EU companies that run a PSIRT almost always have a CSIRT, but these are mostly distinct in terms of budget, team members and scope. The collaboration between both entities seems to be strong and efficient when needed.

DEVELOPMENT & VISIBILITY

Key Finding #9 PSIRTs are more common in the industry and digital sectors than in the healthcare and energy sectors.

Key Finding #10 The presentation of PSIRTs' service offering and activities is not standardised. This is a source of difficulty for reporting vulnerabilities as no standard document references who should be addressed, what evidence should be provided, or what communication tools should be used.

Key Finding #11 As PSIRTs emerge, their visibility remains low outside their company. Some of them even lack visibility from internal stakeholders.

Key Finding #12 Most PSIRTs did not ask or look for specific support or guidance from external stakeholders to design and implement their team although they agree on the necessity that ENISA/EU develop best practices, standards, and harmonised certifications.

RECOMMENDATIONS

The research highlighted the following 9 recommendations, along with the targeted population:

ORGANISATION, PROCESSES & TOOLS

Recommendation #1
Security teams | PSIRT

The adoption of an agile approach by product teams could be an opportunity for PSIRTs and security teams to tackle security issues, whether by introducing new tools in the DevOps pipelines or more globally by providing an internal catalogue of product security related services.

Recommendation #2
PSIRT

PSIRTs should strive to build a multidisciplinary team composed of application and software development experts with security training, and security experts with application and software development training. The members of a PSIRT should have a good technical understanding of the security and applicative issues at hand but also good soft skills to communicate effectively with all stakeholders, whether internally or externally, and ensure smooth IR processing.

COLLABORATION

Recommendation #3
CSIRT | PSIRT

To facilitate the sharing of disclosed vulnerability information among IR teams, and considering the ever-increasing volume of vulnerabilities, a machine-readable standard should be promoted to automate this process. These exchanges should rely on a secure communication channel.

Recommendation #4
OES | PSIRT

There needs to be a stronger link between OES and PSIRTs in terms of information exchange quality, fluidity, and transparency. On the matter that PSIRTs may not know whether their products are used by OES, it could be more efficient to build and implement a legal and technical framework that would allow OES to receive vulnerability information from vendor PSIRTs, possibly in advance of their official disclosure, to mitigate their impact.

Recommendation #5
ENISA | PSIRT

To foster links between PSIRTs and develop the overarching community, regular events dedicated to PSIRTs could be developed either through a centralised initiative, or at the initiative of a small group of PSIRTs, at the national or the EU level. Such events could also be encouraged worldwide to develop a wider community and to account for increasingly global information security issues.

DEVELOPMENT & VISIBILITY

Recommendation #6
ENISA

PSIRTs, both emerging and well-established, are eager to have more guidance and support from ENISA. These could come in the form of guidelines, general security recommendations, and at a more global level, a high-level cooperation framework intended to help develop best practices and improve exchanges among PSIRTs and other IR teams within the Union Members.

Recommendation #7
PSIRT

The use of a presentation standard, like the one defined in RFC 2350, may help improve the understandability of the offer, the visibility of the PSIRT team and facilitate the vulnerability reporting process. This document could be largely based on the template defined in RFC 2350.

Recommendation #8
PSIRT

To facilitate communication and collaboration with external stakeholders, be they reporters or other IR teams, PSIRTs should be encouraged to register their team and contact information on a specialised directory.

Recommendation #9
PSIRT

IR teams should strive to improve their external visibility to facilitate and develop their vulnerability reporting process. This could be achieved through communication with clients or a stronger involvement in the IR community (conferences, working groups, etc.).

TABLE OF CONTENTS

1. INTRODUCTION

1.1 CONTEXT

The EU Cybersecurity Act states that ENISA shall support Member States in developing national strategies on the security of network and information systems, and promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices.

As part of its effort to support EU Member States in their IR development, ENISA would like to further develop and apply ENISA recommendations for the CSIRT capability development following the update of the state-of-the-art view of the CSIRT landscape and development in Europe. ENISA would like to conduct a study on Sectoral CSIRT/PSIRT capabilities status and development within energy and healthcare sectors as specified within the NIS directive.

1.2 OBJECTIVE OF THE STUDY

The project aims at building an overview of current capabilities of CSIRTs and PSIRTs from both a strategic and operational perspective within the energy and healthcare sectors. This report should help to identify standard operating models, activities, and tools of IR teams within both sectors.

This study is based on structured data that was gathered via desktop and field research and has been consolidated in this report.

An overview of the methodology and an assessment and presentation of the collected data can be found in Chapter 2.

1.3 SCOPE OF THE STUDY

This study provides data and an analysis of IR capabilities (IRC) within the energy and healthcare sectors in Member States. Though the IR ecosystem necessarily goes beyond the border of the EU, this study focuses on the EU scope for which ENISA has leverage.

This study examines:

- Capabilities of PSIRTs and sectoral CSIRTs
- Current levels of maturity
- IR services
- IR processes and procedures
- IR tools
- Cooperation mechanisms with internal and external stakeholders
- NIS impact
- Examples and/or lessons learnt

1.4 DEFINITIONS

Key concepts of the research were defined as follows:

CSIRT: A Computer Security Incidence Response Team is an entity which, at its core, responds to computer security or cybersecurity incidents.

Incident response (IR): The protection of an organisation's information by developing and implementing an IR process (e.g. plans, defined roles, training, communications, management oversight) in order to quickly discover an attack and effectively contain the damage, eradicate the attacker's presence, and restore the integrity of the network and systems.

Incident response capabilities (IRC): The processes (e.g. plans, defined roles, training, communications, management oversight), procedures and tools (log analysis, Intrusion Detection Systems, Vulnerability scanners, Data Capture & Incident Response Forensics Tools, Patch management systems, etc.) used to identify, respond to and mitigate the impact of an attack, and to restore continuity of service.

National/Government (N/g) CSIRTs: Teams that serve a country's government by helping to protect its critical information infrastructure. N/g CSIRTs play a key role in coordinating incident management with relevant stakeholders at the national level. They also bear responsibility for cooperation with other countries' national and governmental teams.

National Sectoral (N/s) CSIRTs: Entities responding to computer security or cybersecurity incidents affecting a specific sector at national level. N/s CSIRTs are usually established in NISD sectors such as the healthcare, energy, and transport sector. Unlike N/g CSIRTs which serve the public sector, N/s CSIRTs provide services to constituents from a single sector in one country (in the context of this study, the N/s CSIRTs and sectors mentioned are mainly the air transport and energy sectors).

NIS Directive: The Directive on Security of Network and Information Systems (NISD) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. The NISD provides legal measures to boost the overall level of cybersecurity in the EU.

NIS Directive sectors: Critical sectors for the EU's society and economy are heavily dependent on ICT. Member States have been requested to identify OES for the seven sectors listed in the NIS Directive (NISD sectors). These seven sectors – and related subsectors – listed in the Directive are:

- Energy (electricity, oil, gas)
- Transport (air, rail, water, road)
- Banking
- Financial market infrastructures
- Healthcare sector
- Drinking water supply and distribution
- Digital Infrastructures

Operators of Essential Services (OES): OES are private or public sector entities who play an important role in providing healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure, and water supply. According to the NIS Directive, Member States should be responsible for determining which entities meet the criteria of the definition of OES.

OES CSIRT/IRTs: Entities or teams responding to computer security or cybersecurity incidents affecting an OES within a sector.

PSIRT: A Product Security Incident Response Team is an entity which, at its core, responds to cybersecurity vulnerability reports within the products and services provided by an organisation.

PSIRT organisational structure:

- **Distributed**: The Distributed model utilizes a small core PSIRT that works with representatives from the product teams to address security vulnerabilities in products.

- **Centralised**: The Centralised model has a larger PSIRT staff drawn from multiple departments that report into one or more senior executives responsible for the organisation's product security.
- **Hybrid**: The Hybrid model is a variation that includes characteristics of both the Distributed and Centralised model.

Sectoral CSIRT of international organisation: Entities or teams within an international organisation or company responding to computer security or cybersecurity incidents affecting the organisation and providing services to constituents from a single sector at regional (EU) or international level.

2. METHODOLOGY AND DATA COLLECTION

2.1 OVERVIEW OF THE METHODOLOGY

Our methodology to identify, collect and analyse data on IR set-up and capabilities with a focus on PSIRTs within the healthcare and energy sectors is illustrated below. The methodology consists of five main steps and is presented in this chapter.

Figure 1: Overview of the methodology

2.2 A FIVE-STEP APPROACH

2.2.1 Step 1 – Collect comprehensive data on IR setup

The objective of this task was to collect data on IR setup within the healthcare and energy sectors with a focus on PSIRTs through desktop research.

This data collection method implied collecting data from third parties, mostly through the internet. The main sources of information were official statistics, academic research, external studies, and official documents as well as reports, white papers, legislation, policies, strategies, initiatives, and other research projects.

This research focussed on the scope of EU Member States and was extended to international non-European organisations to broaden our understanding of the subject.

Given that data regarding the healthcare and energy sectors was scarce in relation to our focus on PSIRTs, we extended our scope to include entities outside the healthcare and energy sectors in order to have sufficient data available for analysis.

The data collected during this phase was structured in a grid following the main Service Areas details in FIRST's PSIRT Framework (FIRST, 2020A). The data was then consolidated and analysed in order to help prepare a questionnaire.

2.2.2 Step 2 – Prepare questionnaire for assessing IR setup

As anticipated, publicly available information on IR setup within sectoral CSIRTs with a focus on PSIRTs was not detailed enough to provide truly insightful inputs.

This step was thus focussed on the preparation of a questionnaire, the primary goal of which was to enrich and to validate the accuracy of the data collected during step 1.

Once the survey was defined, two main recipient categories were identified to participate:

- **22 PSIRTs**
- **39 National or Sectoral CSIRTs**

Further information on the data collected can be found in Appendix A: Presentation of the raw data.

Together with ENISA, the project team drafted the survey to be sent to both audiences considering aspects such as collaboration with internal and external stakeholders, participation in the Software Development Life Cycle (SDLC), the impact of the NIS Directive, etc.

The final version of the survey validated by ENISA is available in Appendix B: survey – questionnaire.

2.2.3 Step 3 – Conducting the survey and complementary interviews

The survey was sent by ENISA to the PSIRTs and CSIRTs that were previously identified. The survey included a presentation of the study and its context.

Targeted emails were sent to relevant contacts and were followed up on to maximize participation.

Following the survey, additional interviews took place to complement and further enrich the data collected from the survey and the desktop research.

An overview of the raw data collected through the survey is detailed in Appendix A: Presentation of the raw data.

2.2.4 Step 4 – Analysis of the collected data and identification of key findings

The project team started by producing a draft version of the report using inputs from steps 1 and 3. This report presented the results identified during the analysis of desktop research data and the answers to the survey and the interviews conducted during step 3.

Once the draft report was formalised, it was presented to ENISA and iteratively refined during collaborative workshops.

2.2.5 Step 5 – Final report preparation

This final version of the report was then prepared, presented, and validated by ENISA.

2.3 OVERALL ASSESSMENT OF THE DATA & INFORMATION AVAILABILITY

The identification of reliable and qualitative data was crucial throughout the study. For each activity conducted during this study, namely the desktop research phase, the survey and the complementary interviews, an overall assessment of the data and information availability was conducted, and several assumptions were made.

During the desktop research and survey data collection phases, a large number of PSIRTs both in the healthcare and energy sectors and outside of these sectors, and both in the Member States and outside of them were identified so as to provide a wider understanding of the IR ecosystem.

All national CSIRTs within the Member States were targeted, along with sectoral CSIRTs (both within and outside the healthcare and energy sectors). Focus was also directed to a few national sectoral CSIRTs when they could be identified.

Further information is presented in Appendix A: Presentation of the raw data.

2.3.1 Desktop research – Data collection assessment

During the desktop research phase, data was collected mainly based on publicly available information on CSIRT and PSIRT teams and activity presentation webpages, along with information from third-party vulnerability management vendors' presentations and a few other literature sources.

- The data collected during this phase was structured in a grid following the main Service Areas details in FIRST's PSIRT Framework (FIRST, 2020A).
- The clarity and level of information available for each CSIRT or PSIRT was uneven from one to another.
- As anticipated, information on internal activities, structure, tools, and maturity was not publicly available.
- Information on procedures and processes followed by IR teams was rarely fully detailed in publicly available documents.

2.3.2 Survey – Data collection assessment

29 respondents answered the survey:

- 22 CSIRTS/CERTs
- 7 PSIRTs

2.3.3 Interviews – Data collection assessment

Two additional interviews were conducted with sectoral PSIRTs that operate within or in close connection with the healthcare and energy sectors. These PSIRTs were selected from among those that had answered the survey.

3. KEY FINDINGS

3.1 ORGANISATION, PROCESSES & TOOLS

3.1.1 Key finding #1 – PSIRT activities

Outside their IR Processes, PSIRTs' activities and their involvement in product lifecycle is heterogeneous.

Aside from their core IR responsibilities, PSIRTs may have other security related activities, such as participation in the Software Development Life Cycle (SDLC) for their company's products, or providing security training for developers, for instance.

The survey and the interviews that we conducted highlighted differences in PSIRTs' involvement in such activities related to company and team organisation, but also to the mandate given to the PSIRT.

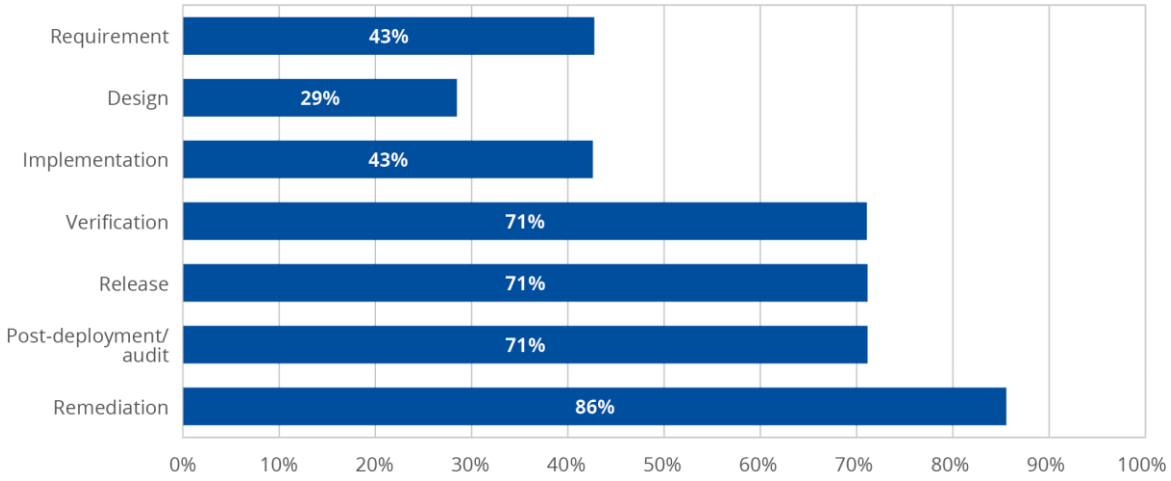
The Software Development Life Cycle (SDLC) outlines and divides the traditional software development process into a few main phases.

Our survey included a focus on the PSIRTs' involvement in the SDLC. In the survey, participants were asked about their participation in the following phases:

- Requirements
- Design
- Development
- Testing
- Release

PSIRTs appear to be globally involved in their company product's SDLC, albeit unevenly. Setting aside two respondents that declared that they do not take part in the SDLC, participation in the testing and release phase is frequent, while participation in the earlier requirement, design and implementation phases is less so.

Figure 2: PSIRT involvement in each phase of software life cycle according to our survey



The PSIRTs that reported not being involved in the SDLC in the survey gave details regarding their answers during interviews:

- In one case, though the PSIRT is sponsored by a product development team, as their company products are strongly diversified, it would be impossible for the PSIRT team members to be sufficiently knowledgeable about all product specifics in order to be able to participate in the SDLC efficiently. Thus, they rely on security delegates (Product Security Officers) within each product team.
- In the other case, the PSIRT does not directly take part in the SDLC but is part of a security competence centre that does.

3.1.2 Key finding #2 – Third-party vulnerability management platforms

The adoption of third-party vulnerability management platforms is uncommon. Those who use one do so because it is easier to manage and improves visibility.

In recent years, a few commercial or non-commercial third-party vulnerability management platforms have appeared on the market: *Hacker One, Bug Crowd, Yes We Hack, BugHeist, OpenBugBounty*, etc.

These platforms generally offer various security related services such as penetration testing, bug bounties and vulnerability disclosure programmes.

These services can be complementary to traditional PSIRT activities, especially regarding their penetration testing offerings, but also as specific tools that can outsource part of the vulnerability reporting process. In this case, vulnerability reports can be created by reporters directly on these platforms which then relay the information to the PSIRT.

According to our desk research and survey, the adoption of these third-party platforms, at least regarding their vulnerability disclosure programme services, is uncommon among European PSIRTs.

Only one respondent to our survey declared using a third-party platform for their vulnerability disclosure programme. They mention the ease of setup, the fact that there is no need to administer the service and the external visibility induced by the presence on the platform as motivation to do so.

During our interviews, when asked why they had not chosen to use a third-party platform, PSIRTs declared that they were reluctant to have vulnerability information stored on external platforms and preferred this information to stay within internal systems. Another factor mentioned was the overall low number of vulnerabilities handled each year, meaning there is little or no demand for the use of third-party platforms.

However, we note that the development of these platforms is still relatively new. As most PSIRTs among our survey respondents were found to be 5+ years old, this might be a factor in the relatively low adoption rate among our panel. This was confirmed during one of our interviews: the PSIRT in question was created over 10 years ago, and these services were either not available then or not as popular as they are nowadays.

3.1.3 Key finding #3 – KPIs

Measuring the efficiency of a PSIRT proves to be challenging, as most PSIRTs essentially track it with the number of vulnerabilities reported and mitigated.

When it comes to measuring the efficiency of a PSIRT, the most common KPI seems to be the number of vulnerabilities reported or remediated. Although these indicators seem suitable

considering the main mission of the PSIRT, the PSIRT does not have any influence on them. Indeed, if no vulnerability is discovered or if a lot of them are reported to the team, in both cases, we cannot assume that the PSIRT is efficient or not.

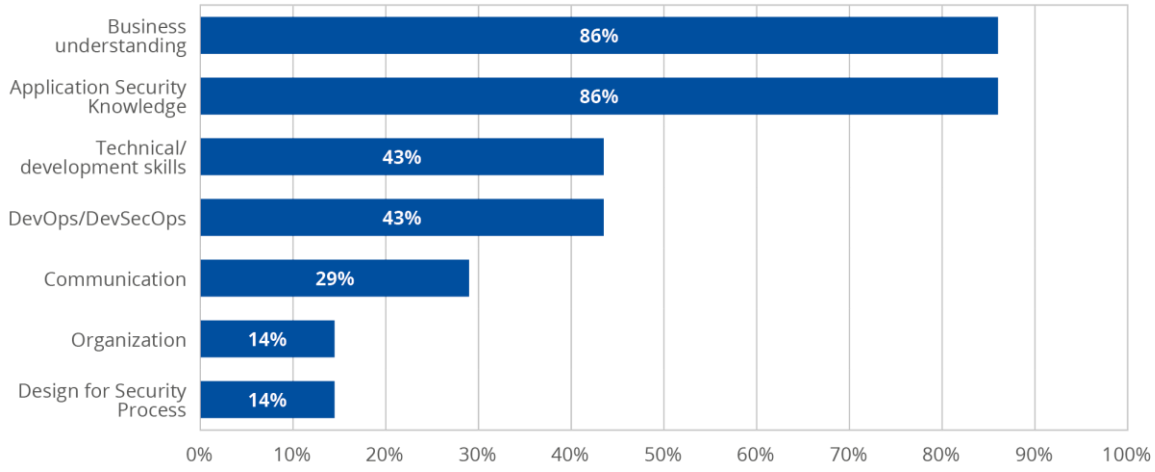
Additionally, few KPIs are taking IR time, the time to onboard stakeholders or the diversity of stakeholders into account.

3.1.4 Key finding #4 – Skills

PSIRT members have both technical skills in product security areas and soft skills that enable smoother exchanges and cooperation between all the stakeholders.

The scope covered by PSIRTs includes both technical and business aspects.

Figure 3: Specific desired skills in order to fulfil PSIRT functions



All PSIRTs interviewed reckon that good technical knowledge is a requirement, especially in application security. It enables an accurate evaluation of reported vulnerabilities and a better understanding of addressed topics. A good understanding of business is also needed as one responsibility of their mission is to prioritise reported vulnerabilities. This would be especially true in the context of an exponential surge in the number of reported vulnerabilities.

"PSIRT members require technical skills to judge whether a reported vulnerability can be real and to judge whether the response of the business side makes sense"

With the emergence of agility in product teams, some PSIRTs stated that DevOps and DevSecOps are desired skills to fulfil their functions. It seems to be unrelated to the involvement of PSIRT teams in the remediation of the incident as this skill is mentioned both by PSIRTs that are directly involved in such processes and those who are not.

On the other hand, we observe a strong desire for business understanding. Given that PSIRTs oversee the vulnerability remediation progress, they should be able to understand business processes and matters in order to be efficient.

They also should be able to exchange with internal and external stakeholders. Beyond product teams and developers, these stakeholders can be security researchers, legal teams, or communication teams. In this case, communication skills at technical and business levels are also necessary to understand and be understood by all these actors.

3.2 COLLABORATION

3.2.1 Key finding #5 – Impact of NIS Directive

PSIRTs do not have specific procedures to address vulnerabilities affecting OES and the NIS directive does not seem to have affected PSIRT activities much.

The Directive on Security of Network and Information Systems (NISD) was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016 (European Commission, 2016). This Directive provides legal measures to boost the overall level of cybersecurity in the EU.

It defines OES as private or public sector entities that play an important role in providing healthcare, transport, energy, banking and financial market infrastructure, digital infrastructure, and water supply.

As part of the general IR landscape, PSIRTs may establish contact with OES either because their parent company itself is an OES, or because the product they sell or the service their company offers is provided to an OES.

None of the respondents to our survey say they have currently implemented specific procedures to address vulnerabilities affecting OES, though two say they are still evaluating the impact of the NIS Directive.

One of our interviewees declared not having specific OES procedures as they handle all vulnerabilities on a case by case basis and thus did not feel that this would be needed.

Another interviewee raised concern regarding the impact of NIS on their activities. They belong to an industrial company that makes parts for other vendors and though they do not have direct OES clients, their products end up being used in other companies' products and may thus be used by OES. However, the PSIRT does not know how its products are used. Therefore, the PSIRT cannot determine whether a vulnerability would affect an OES or not.

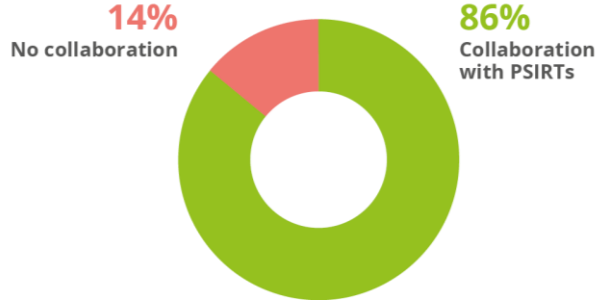
3.2.2 Key finding #6 – Collaboration between PSIRTs

PSIRTs collaborate one with each other, but their collaboration is hindered by the lack of formalised communication and information exchange procedures/standards/framework.

Collaboration amongst IR teams is essential for the IR process efficacy and efficiency. It is also important for them to communicate to forge a community of experts, thus enabling smooth information exchange, knowledge-sharing and trust.

Regarding the collaboration between PSIRTs, our survey highlights the overall will from PSIRTs to collaborate with each other.

Figure 4: Division of answers regarding the collaboration of PSIRTs with other PSIRTs



To establish contact, PSIRTs rely on existing security communities and sometimes attend events hosted by organisations such as FIRST, or by coordinating through the CERT Coordination Centre or the Industrial Control Systems Joint Working Group, for instance. However, PSIRTs may find that these events are perhaps not specific enough to their activities, as one of our interviewees declared.

PSIRTs may also establish informal contacts directly with a few other selected PSIRTs. Once contact is established, PSIRTs cited sharing information about:

- Best practices
- Tips and tricks
- Tools
- Process improvement ideas

It appears that the exchange of information regarding vulnerabilities is a more complex issue. Indeed, two main matters were brought to our attention.

Firstly, the lack of commonly established standard procedures and protocols to securely exchange information about vulnerabilities hinders collaboration, especially now that the sheer volume of vulnerabilities makes manual and traditional sharing almost impossible:

"Some of our clients urged us to make our reports machine readable because they do not have time to process that much data manually"

Secondly, sharing vulnerability information with competitors may only work if there is a strong trust relationship that ensures that *"sharing vulnerabilities won´t be used against us",* as one PSIRT declared in our survey. During our interviews, this issue did not seem to be much of an issue however and the security of both the product and users was put above these concerns.

3.2.3 Key finding #7 – Collaboration between PSIRTs and CSIRTs

Collaboration between PSIRTs and external CSIRTs (sectoral/national) is underdeveloped because of difficulties in establishing contact and sharing sensitive information even though CSIRTs are demanding more regular contact.

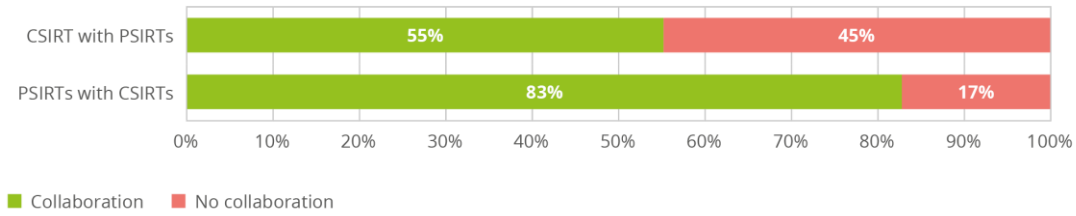
Similar to the collaboration between PSIRTs, collaboration between PSIRTs and external CSIRTs is essential for the IR process efficacy and efficiency.

According to our survey, when PSIRTs and CSIRTs collaborate, they mostly exchange hot topics, recently disclosed vulnerabilities, or the latest development ideas.

However, collaboration does not appear to be a completely widespread practice. Indeed, among the PSIRTs and CSIRTs that answered our survey:

- 83% of the PSIRTs declared having contacts with CSIRTs
- 55% of the CSIRTs declared having contacts with PSIRTs

Figure 5: Division of answers regarding the collaboration between PSIRTs and CSIRTs



It appears that few CSIRTs, and especially national ones, had the opportunity to collaborate with a PSIRT on IR. Those who did described their relationship as functional, but with room for improvement.

This lower figure among CSIRTs may be nuanced by some of the answers that either mention the complete absence or the relatively low number of PSIRTs in their country.

Similar to the previous Key Finding about the communication among PSIRTs, collaboration between PSIRTs and CSIRTs is hindered by the lack of commonly established standard procedures and protocols to securely exchange information. The ever-increasing volume of information regarding vulnerabilities is becoming impossible to process with traditional manual processes.

One of the PSIRTs we interviewed voiced their concern that, from their experience, CSIRTs do not seem to fully consider hardware specifics during IR collaboration. Indeed, if a vulnerability affecting a product's hardware components is reported, it may take longer to find a fix and then deploy it than for purely software related products, considering all the supply chain issues associated with it (development, certification, production, delivery, physical access for patching, etc.). This longer remediation period can possibly span multiple months and may require a considerable effort (physically dispatching engineers to apply a patch, for instance), that may not yet be quite considered by the traditional CSIRT IR processes.

3.2.4 Key finding #8 – PSIRT/CSIRT complementarity within a company

EU companies that run a PSIRT almost always have a CSIRT, but these are mostly distinct in terms of budget, team members and scope. The collaboration between both entities seems to be strong and efficient when needed.

PSIRT and CSIRT are two complementary yet distinct IR teams. They have specific approaches and expertise, which is why, for the most part, they have different team members, tools, and different sponsorship.

On the one hand, a CSIRT typically has a mandate for protecting the company's internal information system against threats. On the other hand, a PSIRT is typically more focused on the security of the product developed in the structure. Its objective is to address vulnerabilities affecting them and to ensure they are remediated in time. Some PSIRTs are directly involved in the implementation of remediation, but it varies among structures as there is no clear definition of the scope of PSIRTs' missions.

The lack of a clear perimeter of the responsibilities has another consequence: it makes it difficult for external stakeholders to get in contact with the right person. For example, a national CSIRT reported that it is sometimes unclear if reports should be addressed to the support team, the product team or the PSIRT.

"It might be confusing for external parties though, if there is no clear publication of their respective missions"

Although the teams have a different scope, if a company has a PSIRT and a CSIRT, both entities naturally share their knowledge and exchange information. They exchange reports mostly about threat intelligence but may sometimes also organise joint conferences.

Regarding operational cooperation on incidents, they have very few occasions to work together because their areas of expertise are different. A product vulnerability does seldom affect a company's internal security, and vice-versa. However, when such an incident occurs, interviewed teams describe their relationship as strong and efficient.

3.3 DEVELOPMENT & VISIBILITY

3.3.1 Key finding #9 – Sectoral distribution

PSIRTs are more common in the industry and digital sectors than in the healthcare and energy sectors.

The initial focus of our desktop research was put on PSIRTs in the health and energy sectors. Once it became evident that there was not a sufficiently significant number of PSIRTs in these sectors, our research scope was broadened to include all sectors.

The lack of PSIRTs in the health and energy sectors could be explained by the fact that IT companies are more exposed to security vulnerabilities due to the nature of their product, and are consequently more likely to develop a dedicated structure and solution to handle these incidents than health and energy ones, which tend to be users of these solutions.

Table 1: PSIRT sector repartition in our desktop research

Source attached to the European Union	PSIRT sector	Source count
YES	Industry	9
	Digital	4
	Health	1
NO	Digital	37
	Industry	7
	Health	2
	Energy	2

Note that in some cases where the PSIRT's company was operating in multiple sectors, we selected the sector that appeared to be the most prevalent.

Most of the PSIRTs we found, especially outside the EU, were attached to a company either in the digital sector (software vendors in particular) or the industry sector (equipment manufacturers, for instance). We also identified a few CSIRTs that operate transversally in the industry, healthcare, or energy sectors.

The relatively limited number of specific healthcare and energy PSIRTs in place can thus perhaps be nuanced by the existence of PSIRTs in their industrial supplier companies.

3.3.2 Key finding #10 – PSIRT activities presentation

The presentation of PSIRTs' service offering and activities is not standardised. This is a source of difficulty for reporting vulnerabilities as no standard document references who should be addressed, what evidence should be provided, or what communication tools should be used.

Through the desktop research, we found that PSIRTs' service offering is mainly presented through a dedicated page on the website of their company. This presentation most commonly includes information regarding:

- The PSIRT charter containing a short description of the PSIRT mission, purpose, roles, responsibilities, and services.
- The channels available for the intake of vulnerabilities (a dedicated email address, a specific web form, a dedicated tool, etc.).
- A high-level overview of the vulnerability reporting process.
- The type of vulnerability disclosure agreement that is followed.
- Some form of hall of fame or acknowledgment for past vulnerability reporters.

We noticed a few of the PSIRTs that were analysed during the desktop research phase seemed to follow or at least to have based their offer presentation on publicly available and open source examples.

The presentation and the amount of information available about each PSIRT varies greatly, however. For instance, we found that information regarding these key topics is rarely available:

- General Service Level Agreement information (report acknowledgment delay, for instance)
- The amount of details expected to be included in a vulnerability report (description of the vulnerability, reproduction steps, proofs, etc.)

If we look at CSIRTs, RFC 2350 (Brownlee & Guttman, 1998) provides guidelines on how to present the IR activities of a CSIRT, along with a template that can be used for this purpose. This document is structured in seven parts:

- Document information
- Contact information
- Charter
- Policies
- Services
- Incident reporting forms
- Disclaimers

Our desk research did not highlight any PSIRTs that provided such a document.

As the vulnerability reporting process can differ from one PSIRT to another, the lack of a formal and standardised document that presents the PSIRT's activity could hinder the efficiency of the reporting process and the overall visibility of a PSIRT.

3.3.3 Key finding #11 – PSIRT visibility

As PSIRTs emerge, their visibility remains low outside their company. Some of them even lack visibility from internal stakeholders.

PSIRT are relatively new in the security vista and collaboration between them will be essential for their development. Then, improving their visibility is necessary to create a relationship among actors, resulting in a strong community and smoother exchanges.

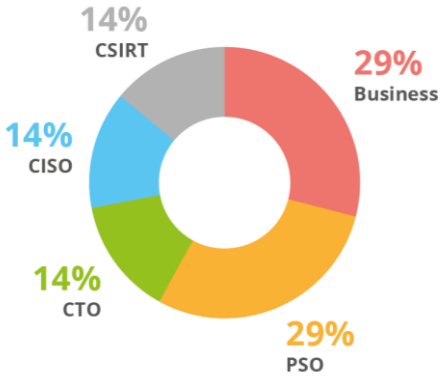
As PSIRTs are more recent than CSIRTs, they do not have a community as wide as CSIRTs do. To gain visibility in the IR domain, PSIRT teams often attend events hosted by other communities, such as CSIRTs. However, such events are considered too big and not specific enough by the teams we interviewed.

Nonetheless, from an external point of view, it is sometimes unclear whether a company runs a PSIRT, and how to contact it. If some of them have a dedicated website with clear contact details, others are never mentioned in a company's documents. Furthermore, it appears that

some PSIRTs do not want to contact nor to be contacted by other PSIRTs or CSIRTs under the belief that they do not need cooperation yet.

This issue of visibility is not just limited to external actors. It also exists within companies. When there is no clear sponsorship for PSIRTs, other departments are sometimes unaware of the existence of a PSIRT. Indeed, PSIRTs can report to their company's Chief Technical Officer (CTO), Chief Information Security Officer (CISO), Product Security Officer (PSO), CSIRT Manager or other Business functions depending on the company.

Figure 6: Sponsorship of PSIRTs



In one case, the CISO did not know of the existence of a PSIRT in their company even though it was created some years ago, thus highlighting a flaw in the communication channel.

This is a real concern because, as one of the respondents notes:

> *"It is important for all parts of a company to know that a PSIRT exists."*

3.3.4 Key finding #12 – External guidance and support

Most PSIRTs did not ask or look for specific support or guidance from external stakeholders to design and implement their team although they agree on the necessity that ENISA/EU develop best practices, standards and harmonised certifications.

PSIRTs are relatively new in the cybersecurity vista. Most of the PSIRTs that responded to our survey were 5+ years old and reckoned that, at the time they were created, there was no guidance for this new kind of IR team. As a result, PSIRTs developed heterogeneously and each company defined their own scope, procedures, and organisation.

As of today, there are few documents describing what is a PSIRT and how to build one. The most known is the recently published PSIRT Service Framework published by the FIRST organisation. It was first released as a draft in 2017 and the final version was published in 2020.

Most recent PSIRTs have relied on this framework to build themselves. They also got support from the existing CSIRT and PSIRTs communities, professional associations, and industry players.

Though few PSIRTs benefited from guidance, most of them wish for more guidance and a move toward standardised communication and protocols to enhance information sharing and exchanges.

Moreover, as some PSIRTs suggested, national entities could support teams to step into international IR communities to benefit the community experience.

4. RECOMMENDATIONS

PSIRTs and CSIRTs are essential players in the global IR ecosystem. Our recommendations thus address PSIRT specifics but also wider security community considerations.

4.1 ORGANISATION, PROCESSES & TOOLS

4.1.1 Recommendation #1 – Security and Agility

More and more product teams are shifting to an agile approach for application development, which reduces the duration of development cycles. They are mostly implementing DevOps, which brings development and operational teams closer together.

This shift is a concern for security teams whose processes are not yet compatible with this new organisation at scale. Traditional integration of security in projects does not fit these new development methods easily, especially in a context of continuous delivery. As a result, security teams can be quickly overloaded, and the number of vulnerabilities may increase.

Yet, from a security perspective, DevOps, and more specifically the automated pipelines, can also be an opportunity to perform automatic security assessments. Security tools such as Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) or Secret Detection can detect most of the common vulnerabilities and flaws in developed applications. Therefore, the security teams, including PSIRTs, should also be involved in these new processes to promote the adoption of such security tools and to ensure processes are controlled. This would reduce the number of reported vulnerabilities by “shifting security left”, i.e. upstream in the development processes.

A long-term objective would be the integration of an Agile security Target Operating Model (TOM) at scale, with the development of autonomous product teams fully aware of security matters.

In the meantime, to improve application security, security teams could provide tools and consumable services to support product teams and foster application security maturity. These accelerators could be framed in a dedicated catalogue tailored for product teams and could relieve overloaded security teams by raising developers’ awareness regarding application security.

The content of the catalogue itself should mostly depend on the organisation stack and available skills, but it may contain the following types of accelerators:

- Support services, such as detaching a security expert in product teams. Their objectives would be to raise developers’ awareness about application security and ensure security issues are properly handled. It could be enriched with security audits, training sessions, or penetration testing.
- A list of security tools (SAST, DAST, Secret manager) which can be integrated in pipelines, along with guidance and secure configuration templates to avoid security flaws due to misuse.

To be relevant, the catalogue should take the current maturity level and team’s objectives into account. It should be built upon an AppSec Maturity Model, for example the Software Assurance Maturity Model (OWASP, 2009), and adapted to the specificities of each company.

4.1.2 Recommendation #2 – Multidisciplinary team

PSIRTs should strive to build a multidisciplinary team composed of application and software development experts with security training, and security experts with an application and software development training.

The members of PSIRTs should have a good technical understanding of the security and applicative issues at hand but also good soft skills to communicate effectively with all stakeholders, whether internally or externally, and ensure smooth IR processing.

This would enable teams to be practical about the addressed vulnerabilities and avoid common misunderstandings by having a broad vision of the issue. For example, due to the limited computing power of some products, the security teams may not suggest strong encryption as remediation given that it cannot be implemented.

4.2 COLLABORATION

4.2.1 Recommendation #3 – Standard vulnerability information exchanges

Collaboration between IR teams is currently hindered by the lack of standardised procedures and protocols to exchange information securely and automatically about vulnerabilities.

To facilitate the sharing of disclosed vulnerability information, and considering the ever-increasing volume of vulnerabilities, a machine-readable standard should be promoted to automate this process.

Some companies are already working on such a standard. It would enable security teams to automatically filter relevant vulnerabilities that could affect their products or information systems.

Naturally, given the sensitive nature of the information, these exchanges should rely on a secure communication channel.

Besides, ENISA agrees with the NIS 2 proposal to “establish a vulnerability registry where, OES and their suppliers […] may, on a voluntary basis, disclose vulnerabilities and provide the vulnerability information that allows users to take appropriate mitigating measures” (European Commission, 2020). Although such databases already exist, ENISA recalls that they are hosted and maintained by entities that are not established in the EU. This registry would be a centralised source of information and help users to take appropriate mitigating measures.

4.2.2 Recommendation #4 – Communication between PSIRTs and OES

The NIS Directive does not appear to have had an impact on PSIRT activities yet. However, there needs to be a stronger link between OES and PSIRTs in terms of information exchange quality, fluidity, and transparency.

On the matter that PSIRTs may not know whether their products are used by OES, it could be more efficient to build and implement a legal and technical framework that would allow OES to receive vulnerability information from vendor PSIRTs, possibly in advance of their official disclosure, so as to mitigate their impact.

For better coordination between actors, especially on vulnerability disclosure, the NIS 2 directive stipulates that Member States should designate a CSIRT to take the role of a coordinator. When vulnerabilities affect multiple organisations, it should identify and contact concerned entities (including PSIRTs), support reporting entities and negotiate disclosure timelines.

Finally, given the prevalence of incidents where entities have fallen victim to cyber-attacks by exploiting vulnerabilities affecting third party products and services, they should therefore assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers. A supplementary recommendation would be to check whether actors in the supply chain have a PSIRT and, in this case, to cooperate with them on a regular basis.

4.2.3 Recommendation #5 – PSIRT community events

Collaboration and communication among PSIRTs, between PSIRTs and CSIRTs and more generally in the global IR ecosystem are essential to IR efficacy and efficiency.

To foster links between PSIRTs and develop the overarching community, regular events dedicated to PSIRTs could be hosted either through a centralised initiative, or at the initiative of a small group a PSIRTs, at the national or the EU level. These events could even have a sectorial focus if appropriate.

Such events could also be encouraged worldwide to develop a wider community and to account for the increasingly global information security issues.

4.3 DEVELOPMENT & VISIBILITY

4.3.1 Recommendation #6 – ENISA guidance

The PSIRT ecosystem is growing in the EU and worldwide. PSIRTs, both emerging and well-established, are eager to have more guidance and support from ENISA.

These could come in the form of guidelines, general security recommendations, and more globally a high-level cooperation framework intended to help develop best practices and improve exchanges among PSIRTs and other IR teams within the EU Member States.

4.3.2 Recommendation #7 – PSIRT presentation standardisation

PSIRTs' service offering and activities presentation for external stakeholders is not standardised. This is a source of difficulty when reporting vulnerabilities as no standard document references who should be addressed, what evidence should be provided, or what communication tools should be used.

The use of a presentation standard, like the one defined in RFC 2350, may help improve the understandability of the offer, the visibility of the PSIRT team and facilitate the vulnerability reporting process. This document could be largely based on the template defined in RFC 2350, and should be regularly maintained to ensure it is up to date.

4.3.3 Recommendation #8 – PSIRT directory

Team visibility is a prerequisite to receiving vulnerability reports from external stakeholders, but also an enabler for communication with other teams. To facilitate communication and collaboration with external stakeholders, be they reporters or other IR teams, PSIRTs should be encouraged to register their team and contact information on a specialised directory.

4.3.4 Recommendation #9 – Reputation & recognition

Reputation and recognition from both internal and external stakeholders are key success factors for IR teams.

IR teams should strive to improve their external visibility to facilitate and develop their vulnerability reporting process. This could be achieved through communication with clients or a stronger involvement in the IR community.

IR teams' internal visibility should also be a main objective, as it allows for better cooperation with internal stakeholders (Product teams, Legal, Communication, Customer Support, etc.) and ensures a smooth response to vulnerability reports and incidents. One way of achieving better visibility could be for PSIRTs to develop stronger links with their company's PSO and CISO, through sponsorship or day-to-day cooperation.

5. BIBLIOGRAPHY

Brownlee N., and Guttman E., *Expectations for Computer Security Incident Response*, RFC 2350, June 1998, Retrieved from URL https://tools.ietf.org/html/rfc2350

FIRST, *PSIRT Services Framework*, 2020, Version 1.1, Retrieved from URL https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

FIRST, *CSIRT Services Framework*, 2020, Version 2.1, Retrieved from URL https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

International Organization for Standardization, *Information technology - Security techniques - Vulnerability handling processes*, ISO/IEC 30111:2019

International Organization for Standardization, *Information technology - Security techniques - Vulnerability disclosure*, ISO/IEC 29147:2018

Open Web Application Security Project*, Software Assurance Maturity Model,* v1.5, 2020, Retrieved from URL https://owaspsamm.org/v1-5/

European Commission*, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, July 2016, *OJ L 194, 19.7.2016, p. 1–30,* Retrieved from URL *https://eur-lex.europa.eu/eli/dir/2016/1148/oj*

European Commission, *Proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*, December 2020, Retrieved from URL https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166

A APPENDIX: PRESENTATION OF THE RAW DATA

A.1 DESKTOP RESEARCH

The objective of the desktop research was to collect data on the IR setup within the health and energy sectors with a focus on PSIRTs.

Table 2: Overview of the desktop research data

Source attached to the European Union	Type	Sector	Count
YES	CERT	National	31
		Energy	4
		Europe	1
		Health	1
	PSIRT	Industry	9
		Digital	4
		Health	1
	Literature	N/A	1
refe	CERT	National	2
		Energy	1
		Health	1
	PSIRT	Digital	37
		Industry	7
		Health	2
		Energy	2
	Platform	N/A	2
	Literature	N/A	1
Total			**107**

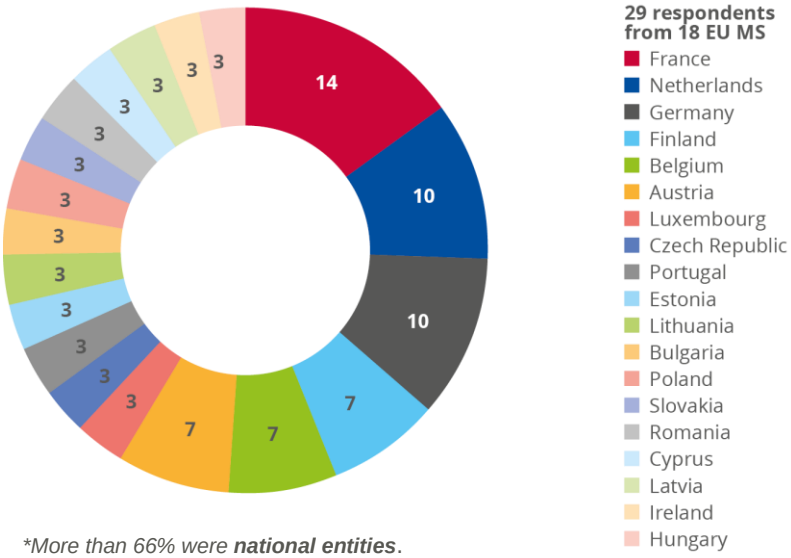
A.2 SURVEY

The raw data gathered from the survey was consolidated in an Excel table.

The table was structured around the answers of each respondent according to the questions of the survey available in Appendix B.

The data collection relies on **7 responses from PSIRTs and 22 from CSIRTs from 19 EU Member States**.

Figure 7: Survey respondent by country



*More than 66% were ***national entities***.

Figure 8: Survey respondents by sector

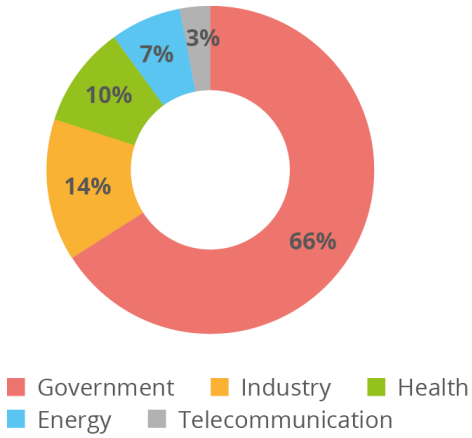
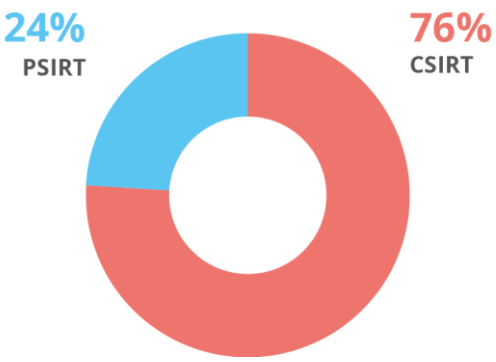


Figure 9: Survey respondents by type



A.3 COMPLEMENTARY INTERVIEWS – RATIONALE AND KEY FIGURES

The main objective of the interviews was to collect additional information and insights into IR set-ups, gather qualitative assessments of recent changes and account for the impact of the NISD. After reviewing initial survey results, complementary interviews took place with healthcare, energy, and industry PSIRT teams.

B APPENDIX: SURVEY – QUESTIONNAIRE

B.1 PSIRT VERSION

GENERAL

1 What is your company's activity area?

- Healthcare
- Energy
- Industry
- IT
- Other (please specify)

2 How long has your team been in place?

- 0-1 year
- 1-5 years
- 5+ years

SPONSORSHIP, ORIGIN & PURPOSE

3 What key factors led you to implement a Product Security Incident Response Team?

- Regulatory / Legal issue
- Lessons learnt from past incidents
- The large panel of products sold
- The large number of vulnerability reports received on products sold
- The need to improve vulnerability management process
- The need to facilitate product vulnerability cooperation with external stakeholders
- Other (please specify)

4 Who is the sponsor of your PSIRT?

- Board or Executive Committee
- Business function in charge of products development
- CISO Chief information security officer
- PSO Product Security Officer
- Other (please specify)
- No specific sponsor

5 What statistics do you collect to measure your team's efficiency?

- Number of vulnerability reports processed
- Number of vulnerabilities remediated
- Response time upon vulnerability identification
- Number of finders
- Number of vulnerabilities found by internal teams
- Other (please specify)

STRUCTURE AND ACTIVITIES

6 How is your PSIRT structured?

- Distributed model: this model utilizes a small core PSIRT that works with representatives from the product teams to address security vulnerabilities in products.
- Centralized model: this model has a larger PSIRT Staff drawn from multiple departments that reports to one or more senior executives responsible for the organisation's product security
- Hybrid model: this model is a variation that includes characteristics of both the Distributed and Centralized model
- Other (please specify)

7 What are the specific desired skills in order to fulfil your PSIRT functions?

- Development team understanding (DevOps, DevSecOps)
- Application security knowledge
- Code analysis skills
- Business understanding
- Other (please specify)

8 Which specific tools and associated procedures does your organisation rely on to operate the following services:

Service Area	Function	Tools & procedures
1. Vulnerability discovery	Intake of vulnerability reports	
	Identify new or unreported vulnerabilities	
	Monitoring for product component vulnerabilities	
2. Vulnerability triage and analysis	Vulnerability qualification	
	Vulnerability reproduction	
3. Vulnerability Remediation	Vulnerability remediation	
	Incident handling	
4. Vulnerability Disclosure	Disclosure	
	Coordination	
5. Training and Education	PSIRT Training	
	Others stakeholders training	
	Feedback	

9 Do you use third-party vulnerability management platforms (such as HackerOne, BugCrowd, etc)? If yes, what are the reasons?

- Yes, we do (please specify which one)
  - Easy to set up
  - Free of charges
  - Better customer experience
  - No need to manage the service
  - Visibility
  - Other (please specify)
- No, we don't use one

10 Who is usually involved in your vulnerability remediation process, in addition to PSIRT members?

- Development team members
- CSIRT members
- Legal team
- Support team
- Communication team
- External stakeholders (please specify)
- Other (please specify)

11 In which phases of your products' SDL is the PSIRT involved?

SDL Phases	PSIRT involvement	Comment
Requirements phase		
Design phase		
Development phase		
Test phase		
Release phase		

12 Does your company have a CERT/CSIRT?

- Yes
- No

13 If you have a CSIRT, what are the relations between the PSIRT and the CSIRT? Do you share means, staff, tools, procedures, etc?

Topic	Answer
Staffed members	
Funding	
Incident handling	
Vulnerability handling	
External communication	
Internal communication	
Others (please specify)	

14 Based on your experience, what are the benefits of implementing a PSIRT while already having a CSIRT?

- <Free answer>

COLLABORATION BETWEEN PSIRTS, CSIRTS AND END-USER ORGANISATIONS

15 Do you have regular contacts with other PSIRTs? With other CSIRTs/CERTs? To what purpose? What main benefits do you get/expect by developing cooperation procedures between Response Teams (CSIRTs and PSIRTs)?

- <Free answer>

16 What main barriers or difficulties do you face when developing cooperation procedures between Response Teams (CSIRTs and PSIRTs)?

- No desire to cooperate from other teams
- Lack of communication procedures

- Lack of communication tools
- Difficulty to establish contact
- Disclosure policy restrictions
- Lack of time due to work overload
- Other (please specify)

17 Do you have specific procedures to handle vulnerability issues that directly affect end-users of critical importance (such as Operators of Essential Services or governmental institutions), especially in Energy and Healthcare sectors?

- Yes (if yes, please specify the procedure)
- No, we don't have specific procedures
- We don't have such customers

18 In case of a security incident related to a product vulnerability affecting OES end-users (especially in Energy and Healthcare sectors), how would you describe the collaboration between the different teams of your company, other external stakeholders and the OES end-users?

- <Free answer>

19 What are the main challenges faced when collaborating with OES in the Energy/Healthcare sectors?

- Confidentiality issues
- Commercial issues
- GDPR-related issues
- No 24/7 coverage / capabilities
- Lack of security culture among OES
- The management (and the security) of OES IT infrastructure is often outsourced
- Cross-sector interdependencies and cooperation
- Cross-border issues
- Regulatory issues
- Resources or expertise issues
- Supply chain management
- Other (please specify)

FEEDBACK

20 Based on your experience, what are the key factors facilitating the development of a PSIRT?

- The contact with existing PSIRTs sharing their experience
- Product-specific regulations clarifying the security requirements and responsibilities
- Request or requirement from clients
- Cooperation agreements between PSIRTs, CSIRTs, and product end-user organisations
- Access to funding and support of PSIRT development through the Connecting European Facility (CEF) program or other funding sources
- The dissemination of threat intelligence, exchange of good practices and lessons learnt
- Other (please specify)

21 Do you need / have you asked or looked for any specific support or guidance from external stakeholders to design and implement your PSIRT?

- Yes (If Yes, please specify)
  - European Union entities
  - International authorities
  - National authorities
  - Professional associations or industry players
  - CSIRT/PSIRT communities/peers
  - Other
- No

22 What specific resources and tools are in place to support the development of PSIRTs in your sector?

- Training and Education activities
- A network of PSIRTs at a national or sectoral level to exchange good practices about information exchange, capabilities, cooperation etc.
- Methodological baselines and tools to support vulnerability handling (e.g.: specific software tools, risk assessment methodologies, best practices, frameworks)
- Shared framework for vulnerability classification and criticality
- Other (please specify)

23 Can you tell us about one time where the vulnerability handling process proved to be particularly efficient?

- <Free answer>

24 Can you tell us about one time where the vulnerability handling process showed flaws that potentially resulted in a product vulnerability incident, and what were the causes and consequences?

- <Free answer>

25 What measures could be implemented that would further improve the security regarding the use of products by OES?

- <Free answer>

26 What possible measures undertaken by European Union entities, ENISA, international or national authorities or bodies would help improve the overall effectiveness of PSIRT services?

- <Free answer>

27 What is the impact of NIS Directive on your activities, and what are your expectations about it?

- <Free answer>

28 What specific processes or tools in place in your organisation would you recommend to other PSIRT?

- <Free answer>

29 Do you have any other input about your work you would like to share with us?

- <Free answer>

B.2 CSIRT VERSION

GENERAL

1 What type of CSIRT best matches your entity?

- Company CSIRT
- Sectoral CSIRT (Healthcare)
- Sectoral CSIRT (Energy)
- National CSIRT
- European CSIRT
- Other (please specify)

2 How long has your team been in place?

- 0-1 year
- 1-5 years
- 5+ years

STRUCTURE AND ACTIVITIES

3 Does your company have a PSIRT?

- Yes
- No
- Not applicable

4 If you have a PSIRT, what are your relations with the PSIRT? Do you share means, staff, tools, procedures, etc?

Topic	Answer
Staffed members	
Funding	
Incident handling	
Vulnerability handling	
External communication	
Internal communication	
Others (please specify)	

5 Based on your experience, what are the benefits of implementing a PSIRT while already having a CSIRT?

- <Free answer>

COLLABORATION BETWEEN PSIRTS, CSIRTS AND END-USER ORGANISATIONS

6 Do you have regular contacts with PSIRTs? To what purpose? What main benefits do you get/expect by developing cooperation procedures with PSIRTs?

- <Free answer>

7 What main barriers or difficulties do you face when developing cooperation procedures with PSIRTs?

- No desire to cooperate from other teams
- Lack of communication procedures
- Lack of communication tools
- Difficulty to establish contact
- Disclosure policy restrictions
- Lack of time due to work overload
- Other (please specify)

8 In case of a security incident related to a product vulnerability affecting OES end-users (especially in Energy and Healthcare sectors), how would you describe the collaboration between your team and the involved PSIRTs?

- <Free answer>

FEEDBACK

9 **Can you tell us about one time where the vulnerability handling process proved to be particularly efficient?**

- <Free answer>

10 **Can you tell us about one time where the vulnerability handling process showed flaws that potentially resulted in a product vulnerability incident, and what were the causes and consequences?**

- <Free answer>

11 **What measures could be implemented that would further improve the security regarding the use of products by OES?**

- <Free answer>

12 **What possible measures undertaken by European Union entities, ENISA, international or national authorities or bodies would help improve the overall effectiveness of PSIRT services?**

- <Free answer>

13 **Do you have any other input about your work you would like to share with us?**

- <Free answer>

C APPENDIX: FIGURES AND TABLES

TP-09-21-128-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-504-3
DOI: 10.2824/687838