"Tell Them They Are a Responsible Entity, Not a Customer": Understanding Practitioner Challenges in Sector CSIRTs

Aksel Ethembabaoglu
Delft University of Technology
Delft, Netherlands
a.m.ethembabaoglu@tudelft.nl

Natalia I. Kadenko
National Cyber Security Center (NCSC)
The Hague, Netherlands
Delft University of Technology
Delft, Netherlands
n.i.kadenko@tudelft.nl

Yana Angelova
Delft University of Technology
Delft, Netherlands
y.y.angelova@tudelft.nl

Yury Zhauniarovich
Delft University of Technology
Delft, Netherlands
y.zhauniarovich@tudelft.nl

Rolf van Wegberg
Delft University of Technology
Delft, Netherlands
r.s.vanwegberg@tudelft.nl

Simon Parkin
Delft University of Technology
Delft, Netherlands
s.e.parkin@tudelft.nl

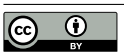
Michel van Eeten
Delft University of Technology
Delft, Netherlands
m.j.g.vaneeten@tudelft.nl

Abstract

In this paper, we study the experiences of practitioners in sectoral Computer Security Incident Response Teams (CSIRTs)—specialized teams that mediate between national cybersecurity authorities and the sector constituency. Through interviews with 18 professionals connected to the Informatiebeveiligingsdienst (IBD-CSIRT) for Dutch local governments, we uncover tensions in how key services are valued. For vulnerability notifications, while the CSIRT staff consider them a core service, many constituents hardly mention them, and systemic gaps in information forwarding mean that crucial alerts often never arrive. We extend these insights with 5 interviews across other sector CSIRTs and a validation workshop with 7 participants, all security officers from sector CSIRTs, revealing shared challenges in balancing technical expertise with sector knowledge, building trust-based relationships, and navigating institutional bottlenecks. Our findings contribute the first systematic account of how sector CSIRT professionals understand and perform their role, highlighting the tensions in providing sector-wide support to professionals with differing security needs.

CCS Concepts

• **Security and privacy** → **Human and societal aspects of security and privacy**; • **General and reference** → *Empirical studies*; • **Social and professional topics** → Management of computing and information systems.



CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/26/04
https://doi.org/10.1145/3772318.3790613

Keywords

CSIRT, CERT, incident response, vulnerability notifications, cybersecurity governance, qualitative study, public sector

ACM Reference Format:
Aksel Ethembabaoglu, Natalia I. Kadenko, Yana Angelova, Yury Zhauniarovich, Rolf van Wegberg, Simon Parkin, and Michel van Eeten. 2026. "Tell Them They Are a Responsible Entity, Not a Customer": Understanding Practitioner Challenges in Sector CSIRTs. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 23 pages. https://doi.org/10.1145/3772318.3790613

1 Introduction

Computer Security Incident Response Teams (CSIRTs) are at the front line in responding to cybersecurity incidents and attacks. They consist of specialized security professionals responsible for handling, responding to, and preventing cybersecurity incidents such as data breaches or malware attacks. Enterprise CSIRTs operate within a specific company to protect its internal systems and data.

In addition, most countries also have a national CSIRT. They deliver a wide range of services, such as issuing advisories, sharing threat intelligence, exchanging information with international partners like other national CSIRTs, and notify responsible parties when scans have detected that their internet-facing systems have vulnerabilities. It is critical that these notifications reach the entities responsible for these systems so that they can remediate the problem.

A national CSIRT is a national coordinating body far removed from individual organizations. Over the last decade, this institutional distance has encouraged the development of more specialised CSIRTs closer to organizations in specific sectors: sector CSIRTs. On paper, they perform similar functions to the national CSIRT,

but for a more targeted set of constituents within a specific sector (e.g., finance, energy, or water). Institutionally, sector CSIRTs are a model that has been copied worldwide[44]. Practitioners in sector CSIRTs are expected to maintain relationships with their constituents so they can channel vulnerability notifications and other information from the national CSIRT to the relevant affected entities, and to support them with incident response, advisories, intelligence sharing, and sector-specific expertise. Doing so relies not only on network-scanning technologies but also on the working relationships and sector knowledge that connect national bodies, sector CSIRTs, and heterogeneous local organizations.

Sector CSIRTs have become critical institutions in their own right. In 2016, the US Presidential Policy Directive 41 (PPD-41) highlighted the importance of sector-specific cybersecurity measures and the collaboration between the Department of Homeland Security (DHS) and sector-specific CSIRTs [46].[1] Around the same time, in the European Union, the Directive on Security of Network and Information Systems (NIS) mandated that certain sectors had to establish incident response capabilities, which included sector-specific CSIRTs [18]. Its 2022 successor in the EU, NIS2, strengthens the role of sector CSIRTs by expanding the number of sectors that are required to set up a sector CSIRT from 7 to 18.

Despite this institutional importance, we know little about how sector CSIRTs actually function as socio-technical arrangements in practice: how practitioners in these teams prioritize between incident response, community education, intelligence sharing, vulnerability notifications, and other services; how constituents experience these services; and how governing bodies and national CSIRTs shape what is expected from sector CSIRTs. These questions are not only about technical capabilities, but about how scarce resources are allocated, how legitimacy is built, and how dependencies between organizations affect the services that are ultimately delivered. Currently, the human factor in sector CSIRT teams is poorly understood. Only by understanding the practitioners and practices on the ground can we establish whether and how security may be advanced [38].

Industry guidance for CSIRTs acknowledges sector CSIRTs but offers little help on these day-to-day challenges. While there is ample guidance for practitioners at 'regular' CSIRTs, for sector CSIRT practitioners, there is only guidance to get started [44], not on how to operate one. Here, by "operate" we mean the practical work of selecting and shaping services within resource constraints, coordinating with national CSIRTs, and engaging a diverse constituency with different levels of security maturity. The current version of the authoritative FIRST (Forum of Incident Response and Security Teams) CSIRT framework recognizes sector CSIRTs as "special types of CSIRTs" and states that it will describe them in future versions of the framework [21].

In academic work, sector CSIRTs remain uncharted territory. Many studies focus on enterprise CSIRTs, e.g., [19, 24, 31, 35, 39, 52]. The few papers that do focus on sector CSIRTs did not study operational sector CSIRTs, but primarily argue that specific sectors would benefit from setting up a sector CSIRT in light of the threats the sector faces [23, 41, 66]. One exception is a case study of the communication channels used by the Norwegian local government sector CSIRT and its members [54]. In sum, we lack empirical insights into how sector CSIRT professionals and their surrounding stakeholders navigate the challenges of operating these organizations and providing services in practice.

In this paper, we address this gap with a mixed-method study of practitioners and stakeholders engaged with sector CSIRTs in the Netherlands. Rather than only interviewing sector CSIRT staff, we deliberately study the ecosystem around a sector CSIRT: its practitioners, its constituents, its governing bodies, and the national CSIRT that depends on it to reach the sector. The first phase of our study is a detailed case study of one specific sector CSIRT, the Informatiebeveiligingsdienst (IBD-CSIRT), which serves the local governments sector in the Netherlands. We conducted interviews with 18 professionals who interact with the IBD-CSIRT: staff of the sector CSIRT itself, representatives from municipalities (constituents), and representatives of governing bodies and the national CSIRT. This design allows us to contrast expectations, perceived value, and tensions across stakeholder groups, rather than foregrounding only the "supply side" of sector CSIRTs.

Across these interviews, participants consistently highlighted incident response, community education and expert insights, and intelligence sharing as key services that make sector CSIRTs valuable to their communities. At the same time, a surprising tension emerged around vulnerability notifications. IBD-CSIRT staff understand notifications as a core preventive service and as an important way for sector CSIRTs to add value on top of national CSIRT scanning, yet many municipal participants hardly mentioned notifications at all. This was notable because, on paper, vulnerability notifications are a canonical example of the mediating role of sector CSIRTs: they depend on up-to-date asset inventories from constituents and on systematic forwarding of scan results from the national CSIRT.

To understand this disconnect, we use vulnerability notifications as an in-depth analytic lens on the institutional dependencies and missing feedback loops that shape sector CSIRT work. In the second phase of our study, we therefore complement the interviews with a historical analysis of the vulnerability notifications that were supposed to be sent to IBD-CSIRT constituents between 2015–2024. Our analysis uncovers a systematic problem in the national notification mechanism: many of the notifications that should have been sent to the IBD-CSIRT, and thus to municipalities, never arrived because the national CSIRT did not forward them. We conducted additional interviews with the professionals involved in the notification program to corroborate this problem and understand its causes. This focus on vulnerability notifications does not imply that they are the only or most important service; instead, they offer a tractable case where we can combine qualitative accounts with log data to reveal how dependencies between organizations can quietly undermine a service that is central in policy documents but nearly invisible to many constituents.

Our in-depth 'vertical' approach around a single sector CSIRT is arguably not scalable across many sectors, let alone different countries. So in the third and final phase, we took a 'horizontal' approach and interviewed professionals of all-but-one other sector CSIRTs in the country ($n = 5$). We also conducted a validation

[1]The nomenclature can differ per country and in the U.S. this role is fulfilled by ISACs (Information Sharing and Analysis Centers).

workshop with most sector CSIRTs in the country ($n = 7$ workshop participants). This allows us to examine to what extent the service portfolio, tensions, and notification challenges identified in the local-government case generalize to other sectors, and to refine our account of cross-cutting practitioner challenges.

We aim to answer the following two research questions: (*i*) What are service-specific challenges and expectations of stakeholders (sector CSIRT staff, governance bodies, and constituents) on the services provided by CSIRT practitioners? (*ii*) What are the strategic challenges for practitioners of a sector CSIRT in providing these services? In sum, we make the following contributions:

- We present the first empirical mixed-methods study on sector CSIRTs. We describe the perspectives of stakeholders and the challenges of practitioners in providing key sector CSIRT services. We find that practitioners' daily practices are shaped by three dynamics: resources, legitimacy, and dependency. For example, we find that the actual provided services often do not align with the expectations of constituents, especially around incident response.
- We identify several strategic challenges for sector CSIRT practitioners: a diverse constituent population in terms of maturity, trust issues, and service-specific organizational dependencies.
- We evaluate the functioning of the national vulnerability notification mechanism – a key service of the sector CSIRT. We find that many notifications are not arriving at constituents. The practitioners did not detect this problem, signalling a missing feedback mechanism – which is missing almost everywhere in vulnerability notification mechanisms.
- We provide an empirical basis and recommendations for the development of guidelines for practitioners operating in sector CSIRTs.

2 Related Work

Frameworks and Industry. The Forum of Incident Response and Security Teams (FIRST) organization provides leading industry guidance on Computer Incident Response Teams (CSIRTs) [20, 21]. The Computer Emergency Response Team (CERT) Division of Carnegie Mellon University developed a framework to establish sector CSIRTs [44] but does not address the challenges of operating one. Other industry efforts have largely focused on non-sectoral CSIRTs [5, 15–17, 56], guiding the establishment and operation of CSIRTs, as exemplified by the continuously updated handbook for CSIRT teams [27, 67].

CSIRTs. Academic research explored various aspects of CSIRTs. Most studies concentrated on enterprise CSIRTs. These studies examined the communication needs, tools, and technical infrastructure required for effective CSIRT functioning [19, 24, 31, 35, 39, 52]. By contrast, limited work has focused on the specific needs and operations of sector CSIRT practitioners. Several studies argue for the benefit of a sector CSIRT in the light of new threats those sectors face [23, 41, 66]. One study described the communication channels used between the Norwegian local government sector CSIRT and its members [54].

Human Factors in incident response. Another line of research explored human factors that play a significant role in the effectiveness of incident response teams. Research has demonstrated that the success of these teams depends not only on technical capabilities but also on the dynamics of individuals working together [10, 50, 51, 55, 58, 63]. Similarly, another line of work studies practitioners at Security Operations Centers (SOCs), how practitioners prioritize, conduct assessments, and set up a SOC [1, 11, 53]. In [6], the authors identified challenges and coping strategies for threathunting practioners. Closely related, there exist additional works that studies security workers [2, 13, 34]. These studies noted that, among other things, for many organizations, recruiting and retaining skilled personnel is a challenge.

Vulnerability Notifications. Finally, there is a large body of work on (vulnerability) notifications and Coordinated Vulnerability Disclosures (CVD) [25, 49]. In [14, 33, 57] the authors find that notifications lead to higher patch rates. This supports the idea of setting up and running a structural notification mechanism. Similarly, in [62], the authors find that security notifications lead to higher fix rates, compared to privacy notifications. They also identify challenges in reaching responsible parties. Similarly, Cetin et al. showed that retrieving contact information at scale was problematic. But once contacted, entities were more likely to remediate [9]. In [71], the authors found that detailed abuse reports increased cleanup rates, but sender reputation was not important. Li et al. found that by addressing owners of resources directly, vulnerability notifications promoted faster remediation than notifications sent to national CERTs [32]. In [65], though, the authors find that many notifications are not acted on, and the sending entity is unaware of this inaction. These studies all highlight the difficulties in effective notification mechanisms without a feedback loop.

Existing work examined enterprise CSIRTs, SOC practitioners, and vulnerability-notification mechanisms, but sector CSIRTs and their role in the broader cyber ecosystem remain largely unstudied. This paper offers the first systematic account of how sector CSIRT professionals understand and enact their role, illuminating tensions inherent in supporting a diverse constituency with uneven security needs. We situate these insights within prior research on practitioner dynamics in SOCs, enterprise CSIRTs, and organizations that consume security services, e.g., the National Vulnerability Ddatabase (NVD). In addition, we empirically analyze the sector's vulnerability-notification pipeline and relate its shortcomings to earlier work on missing feedback loops in critical security mechanisms.

3 Methodology

To answer our research questions, articulated in section 1, we use two approaches for this study. Using a "vertical" approach, we conduct a detailed case-study analysis of the IBD-CSIRT and its relevant stakeholders. Via a "horizontal" approach, we confirm and generalize earlier findings with other Dutch sector CSIRT practitioners. The stakeholders and approaches are presented in Figure 1.

Our study consists of three distinct phases, depicted in Figure 2. First, we analyze stakeholders engaged with the IBD-CSIRT as a case study for a detailed perspective on the provided services, expectations, and challenges.

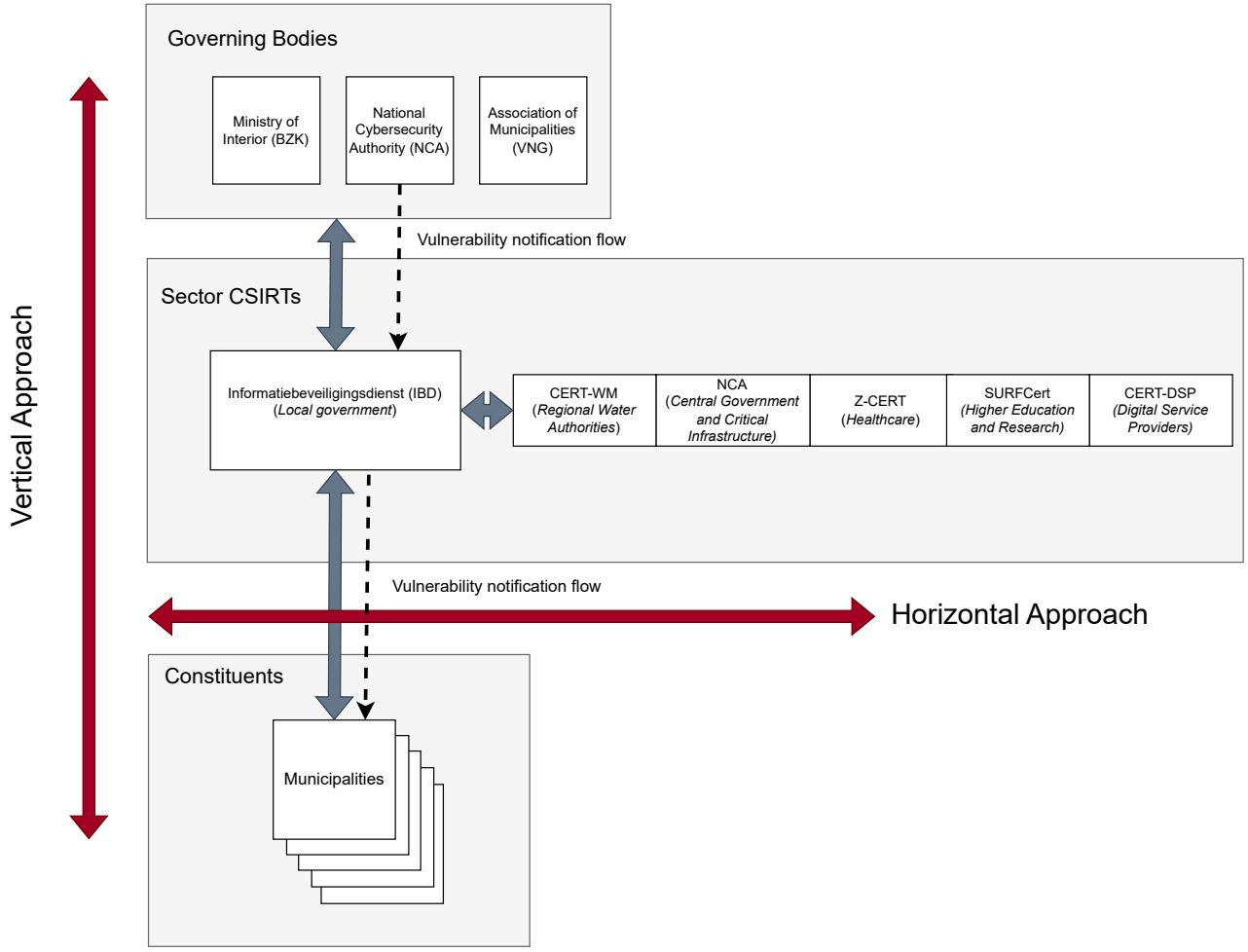


Figure 1: Overview of stakeholder groups engaged with the IBD-CSIRT: Governing Bodies, Sector CSIRTs, and Constituents. Our study adopted a detailed 'vertical' approach via interviews and data analysis. With a 'horizontal' approach, we confirmed findings via interviews and a validation workshop.

In phase 2, we build on the results of phase 1 with an analysis of the vulnerability notification service. After the analysis, we conducted three additional interviews, two with security specialists of the Dutch National Cybersecurity Authority (NCA) notification program, and one with the IBD-CSIRT, to contextualize our findings.

Finally, in phase 3, we first interviewed other Dutch sector CSIRT practitioners. Next, we invited practitioners of all Dutch sector CSIRTs to a workshop session to validate our findings, which we discuss in § 7[2].

[2]The Dutch National Cybersecurity Authority (NCA) acts as both national CSIRT and sector CSIRT for the sector *central government* and the sectors considered *critical infrastructures (CI). Under NIS2, the NCA will act as a sector CSIRT for all sectors that do not already have an established sector CSIRT.*

3.1 Interview Studies

Interview protocol. We developed an interview protocol with minor variations depending on the assigned stakeholder group of the interviewee: *Governance*, *CSIRT*, or *Constituents*, provided in Table 10. Some questions were rephrased depending on the stakeholder group. Furthermore, a minor variation was introduced when referring to either the IBD or to another CSIRT (e.g., Z-CERT), depicted in Table 11. In all variations, we asked participants to articulate a list of CSIRT services. The protocol contains an iteration where we ask the same questions for each articulated service.

To test our protocol, we conducted two pilot interviews, one with a participant of the IBD-CSIRT and one with a participant from a municipality. We made minor changes to the protocol after each interview. The results from the pilot interviews are not included in the final analysis. Additionally, we collected meta-information, e.g., Full-Time Equivalent (FTEs) and budget, about the sector CSIRTs.

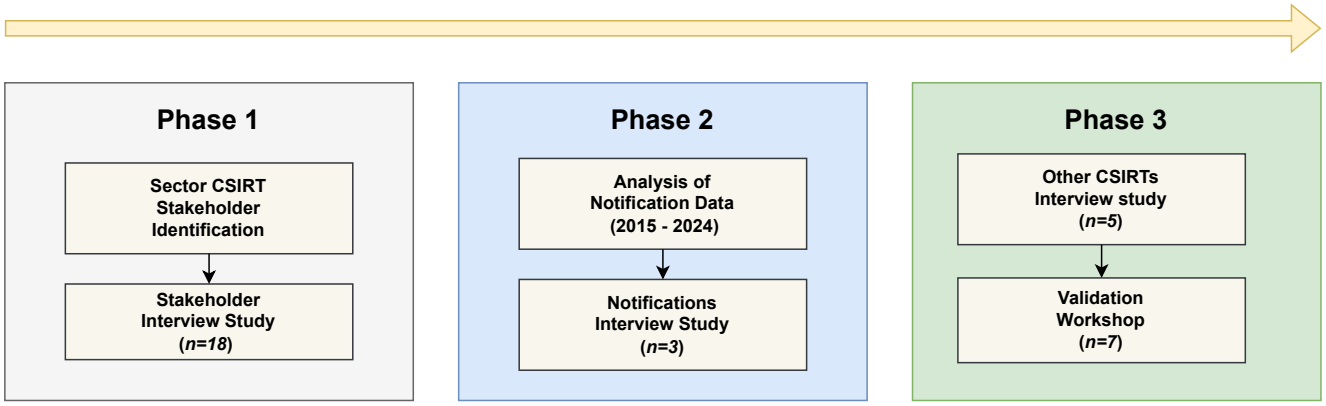


Figure 2: Data collection methodology.

Table 1: Overview of Sector CSIRTs in the Netherlands

ID	Org Name	Sector(s)	Year Founded	Org Structure	FTE 2023	# of Constituents	Budget 2023/2024
1	IBD-CERT	Municipalities	2013	Part of association of municipalities VNG	19	550	2+M
2	Z-CERT	Healthcare sector	2017	Private foundation	37	349	5.2M
3	SURFcert	Education and research	1992	Cooperative association	3.5	200	n/a
4	NCA	National CSIRT *and* sector CSIRT for government and CI	2012	National government body	280	10k+	36M
5	CERT-WM	Regional water authorities	2016	Project at Waterschapshuis	3.5	25	0.5M
6	CSIRT-DSP	Digital Service Providers	2019	National government body of Ministry of Economic Affairs	n/a	n/a	n/a

In doing so, we consulted the interview data and other sources such as organization websites and yearly reports. This information is depicted in Table 1.

In total, we conducted 24 semi-structured interviews with 26 security professionals between October 2024 and May 2025. Nine different municipalities were represented in the ten constituent interviews. In total, for two interviews, two participants were present. One interview with two constituent participants, and one interview with two governance participants. Two interviews were in person, and 22 interviews were conducted remotely. Each interview lasted approximately one hour. During 18 interviews, two researchers were present, while five interviews were conducted by the lead researcher alone.

Participant selection. For phase 1, we identified three groups of stakeholders with whom participants interact with sector CSIRT practitioners: (1) governing bodies, (2) sector CSIRT staff, and (3) constituents. To be considered for the study, participants had to interact with the IBD-CSIRT. For CSIRT staff, we focused on practitioners handling incidents and engaged with constituents. At the IBD-CSIRT, five practitioners fitted our criteria, of which we interviewed the majority ($n = 3$).

We pitched the study at a webinar for municipalities where people could opt in to be contacted. Through snowballing, we gathered additional constituent participants. Via contacts at the Dutch National Cybersecurity Authority (NCA), personal relations within our research group, and conferences, we recruited respondents from the sector CSIRT and governance bodies. In doing so, we tried to maintain a balance in the number of participants per stakeholder group. Table 2 describes the number of participants per group for phase 1. Note that each group has a different ID letter identifier.

For phase 2, we reached out to the NCA for participants who were involved in the vulnerability notification program. For phase 3, the NCA helped us set up a workshop session with relevant sector CSIRT practitioners. Via our network, we reached out to practitioners from other sector CSIRTs. We reached out to CSIRT-DSP for an interview, but they declined to participate because the organization is merging with the national CSIRT.

Ethics. A user study is our primary data source for this study. We received approval from our Institutional Review Board (IRB) for conducting this human-subjects research. We obtained informed consent from participants before conducting the interviews and the workshop. Participants were informed about the study and use of

Table 2: IBD-CSIRT Stakeholder Respondents (n = 18)

ID	Organization	Role	Group
P-G1	Ministry of Interior (BZK)	Policymaker	governance
P-G2	National Cybersecurity Authority	Manager	governance
P-G3	National Cybersecurity Authority	Technical Manager	governance
P-G4	National Cybersecurity Authority	Threat Data Expert	governance
P-G5	Association of Municipalities (VNG)	Manager	governance
P-S2	IBD-CSIRT (municipalities)	Security Expert	csirt
P-S3	IBD-CSIRT (municipalities)	Security Expert	csirt
P-S4	IBD-CSIRT (municipalities)	Security Expert	csirt
P-C1	Municipality	Technical Security	constituent
P-C2	Municipality	Information Security	constituent
P-C3	Municipality	CISO	constituent
P-C4	Municipality	CISO	constituent
P-C5	Municipality	Information Security	constituent
P-C6	Municipality	Information Security	constituent
P-C7	Municipality	Information Security	constituent
P-C8	Municipality	CISO	constituent
P-C9	Municipality	Security Expert	constituent
P-C10	Municipality	Security Expert	constituent

Table 3: Vulnerability Notifications Respondents (n = 3)

ID	Organization	Role	Group
P-N1	National Cybersecurity Authority	Security Expert	governance (notifications)
P-N2	National Cybersecurity Authority	Security Expert	governance (notifications)
P-N3	IBD-CSIRT (municipalities)	Security Expert	csirt (notifications)

Table 4: Other (Non-IBD) Sector CSIRT Respondents (n = 5)

ID	Organization	Role	Group
P-S1	National Cybersecurity Authority	Sector CSIRTs Expert	csirt
P-S5	CERT-WM (water)	Security Expert	csirt
P-S6	Z-CERT (healthcare)	Security Expert	csirt
P-S7	Z-CERT (healthcare)	Manager	csirt
P-S8	SURFcert (higher education)	Security Expert	csirt

information for which they provided informed consent beforehand. We assured participants that their data was handled confidentially and would only be presented in an aggregated and anonymized form. The CSIRT community is small, but the organizations remain large enough to protect participant anonymity. No participant identities or municipality names would be mentioned in the paper. However, we do provide the participant ID with their role and organization type as context to quotes. Before publication, we presented a draft of the paper to the participants to check and correct quotes attributed to them, and to ensure no statements or data could lead to attribution.

Interview coding. Interviews were transcribed and coded using ATLAS.ti [4]. The interviews were coded inductively by two researchers using codebook-style Thematic Analysis (TA) [8]. During the entire coding process, the themes and codes were discussed periodically with the full author team to settle on central themes to ensure the reliability of findings [37].

Both researchers coded the first interview separately in the same coding session, discussing the coding afterwards to build an initial codebook. Next, the lead researcher coded nine interviews, and the other researcher coded two other interviews. Both researchers coded those interviews separately, while discussing them in periodic coding meetings. The interview coding work split was decided on the participant planning schedule and the researcher's availability. After this coding process, the researchers reviewed each other's work, discussed the results, and refined the codes. There was no major disagreement on the meaning of individual codes, but rather, codes were grouped or split for refinement. The coded interviews were then recoded with the refined codebook by the lead researcher. The lead researcher then coded the remaining ten

interviews. As a quality check, the other researcher coded one of these ten interviews in isolation. Afterwards, the two researchers compared the coding of the interview. No major disagreements surfaced during the discussion. This led to another minor refinement of the codes. The coded interviews were then recoded with the updated codebook by the lead researcher. Finally, minor code refinements, i.e., code renaming, were made by both researchers during the analysis phase.

We did not calculate Inter-Rater Reliability (IRR), but did monitor the form and reasoning underpinning disagreements (as noted above); this is in line with Braun & Clarke, and others, who note that IRR is not usually a measure of quality for codebook-based TA [8, 37]. The final codebook is available in § 8.

3.2 Data and Methodology for Vulnerability Notification Analysis

In phase 2 of our study, we investigate the vulnerability notification mechanism. Most vulnerability data that reaches constituents is based on data from a security non-profit called Shadowserver Foundation [60]. Shadowserver runs global scans daily and then sends reports for detected vulnerable machines to national CSIRTs worldwide. The latter are then meant to send it onwards to sector CSIRTs and other stakeholders.

We examine the notification delivery mechanism by investigating IP addresses in Shadowserver reports and comparing them to IBD-CSIRT ticketing data that captures all outgoing notifications to constituents. The IBD-CSIRT generously gave the lead researcher access to their ticketing data. These tickets do not include general security advisories but, instead, include notifications about vulnerable and compromised assets that the IBD-CSIRT receives from the national CSIRT and responsible disclosures. The lead researcher had on-premise access to the data via a VPN connection. We collected a total of 3,065 tickets, created between 17 July 2015 and 16 September 2024.

Additionally, the IBD-CSIRT gave the researchers a database with 'last-updated' changes to the asset inventories, as registered by the constituents. The asset inventory comes in two types. The first type ('ICT photo') describes the constituents' software infrastructure. The second type ("IP ranges and domains") contains the IPs and domains of the constituent.

Furthermore, the research team had access to the full Shadowserver reports for the Netherlands from 2018 to 2024. Shadowserver reports contain all IP addresses for that country for a specific vulnerability. The vulnerability, and hence report, is also typically assigned a severity level. The number of reports per severity per year is depicted in Table 7. Reports from Shadowserver are not static, over time, they get merged or discontinued. Since we do not consider IPv6 addresses within this study, we marked the reports associated with these addresses as "n/a".

We received the set of IP addresses (IPv4) for Dutch municipalities from the IBD-CSIRT for 2022 and 2024. The list for 2022 contained 251,851 IP addresses for 278 unique constituents. The list for 2024 contained a total of 191,643 IP addresses for 295 unique constituents. IP lists are continuously maintained, and these are two ad-hoc snapshots that the CSIRT could share.

We matched IPs in Shadowserver reports with the IPs of municipal IPs for 2018 up to, and including, 2024. For the years 2018-2022, we used the 2022 IP list to find matches. For 2023 and 2024, we used the 2024 IP list. There is, however, a risk that IPs are outdated because IPs can be updated throughout the year. We use the asset-update database to remove results when the assets may have been updated. We checked the organization of a hit against the 'last update' field for IPs in the update database. If a hit occurred before or in the last update year for that organization, we removed it from the results. With this approach, we tried to mitigate the risk of false positives. We go into details of the findings in § 5.

3.3 Validation Workshop

To test the generalizability of our findings we organized a 90-minute focus-group session for security practitioners of all Dutch sector CSIRTs. The session included seven participants from all the Dutch sector CSIRTs we previously interviewed (Table 1). The lead researcher acted as the session moderator, a co-author acted as the assistant moderator. Responses were recorded via note-taking by the assistant moderator for note-based analysis [47]. Participants were asked to indicate their stance on each finding by a show of hands: (a) agreement, (b) disagreement, or (c) abstention. Following the vote, we invited participants to elaborate on their views through open-ended discussion. This approach is a form of mixed analysis [59].

4 Results: Challenges and Stakeholder Experiences with Sector CSIRT Services

Here we address our first research question (RQ1): *What are service-specific challenges and expectations of stakeholders on the services provided by CSIRT practitioners?* We asked participants about their experiences with sector CSIRT services. We first asked what services are provided or used, resulting in a set of services articulated by participants, depicted in Table 5. According to practitioners, these are the valuable services that sector CSIRT practitioners provide.

Next, for each service, we asked, how is it used and what obstacles do you run into in practice? We coded the interviews and identified sub-codes for each service. Below, we iterate over the articulated services, describe how participants used them, and describe the challenges participants ran into.

We interviewed participants from three types of stakeholder groups: *governance*, *csirt*, and *constituent*, as seen in Table 2. The participant identifiers, e.g., P-G2, P-S5, or P-C3, reflect which stakeholder group they belong to. The notification participants have the N identifier (e.g., P-N1).

4.1 Incident Response: Clashing Expectations

All participants indicated that incident response (IR) is the most important service a sector CSIRT provides. This is in parallel to how governing bodies for local government acted on global efforts to boost cybersecurity for these sectors (P-G4). How this service functions in practice, and what constituents need, is harder to determine. While this service is deemed important by all participants, constituents were somewhat disappointed by the incident response capability that the IBD-CSIRT provided, noting that they hoped the

Table 5: Sector CSIRT services derived from the interviews

Name	Description
Incident Response	Detecting and addressing security incidents to limit impact. A CSIRT may support triage, provide playbooks, assist with stakeholder management, and advise on communication.
Advisories	Non-asset-specific vulnerability information, typically including steps to patch or mitigate issues.
Expert Insights	Guidance on specific security topics, including *knowledge products* such as templates for organizational processes.
Vulnerability Notifications	Asset-specific alerts about vulnerabilities or abuse affecting constituent-reported assets.
Intelligence Sharing	Ad-hoc warnings and updates (e.g., new phishing trends), along with tips, experiences, and relevant best practices.
Outreach and Community	Activities to build relationships, foster trust, present services, and learn about constituent challenges.

sector CSIRT would provide off-the-shelf, ready-to-go solutions to manage and (technically) remediate the incident.

Where some constituents had not yet experienced an incident, the image they had was instead informed by a notorious case where an organization called the IBD-CSIRT for help during an incident, and the IBD-CSIRT responded to clarify that it does not send first responders on-site. P-S2 noted that constituents wrongly believed that the IBD-CSIRT has digital forensic specialists on standby during an incident. This signalled to constituents that the IBD-CSIRT, despite being perceived as an incident response party, did not come to aid during an incident in the way constituents expected. This undermined the credibility of the sector CSIRT as a trusted organization that assists constituents during an incident.

These misaligned expectations led to disappointment or angry phone calls within the constituency when help was needed. CSIRT participants noted that the reasoning was that municipalities are themselves responsible for their information security, and the CSIRT only offers additional help. The incident response capability, therefore, is not viewed the same by the CSIRT and the constituency. Different perceptions of services or issues by different groups are not uncommon in the security domain [28, 30], nor in other domains such as healthcare [48]. While the specifics of earlier work differ, what they share is that by making perceptions and assumptions explicit, practitioners are able to overcome the challenge of misaligned expectations.

For example, CSIRT practitioners noted that they did learn from the experience, and they nowadays more explicitly communicate to their constituents (e.g., on their website, via fact sheets, during webinars, etc.) what to expect from them during an incident, i.e., triage, playbooks, advice, stakeholder support, and/or coordination efforts. This effort seems to better align the expectations, as P-C1 to P-C10 all described the IR capability in those terms. What we see here also highlights the impact expectations can have on how defenders seek to coordinate in critical situations– none of the constituent participants indicated that they expected the IBD-CSIRT to send incident responders, but this had already been informed by shared stories ahead of the CSIRT's clarification efforts.

The IBD-CSIRT is gradually being considered to instead be more of a "trusted broker" for Digital Forensics and Incident Response (DFIR) services. As P-C6 noted, *"...I expect them to refer me to a forensics company [as] they don't have the capacity for that"*, with the Sector CSIRT seemingly then learning where they can play a role in the defender community that is within their capabilities while being shaped by the needs of constituents. This is in contrast to other sector CSIRTs, where P-S5 and P-S8 indicated that their sector CSIRT *does* have the capability to send technical incident responders on-site to their constituency (due to having more advanced technical capabilities).

P-G1, P-G4, and P-S2 felt that the title "CSIRT" did not automatically require technical incident response capabilities (despite P-G2 indicating this). Their views highlight that the resources required to meet the specific needs of every constituent would be problematic, noting that the capability should be provided efficiently, meaning it can also be provided by a sector CSIRT with the help of a DFIR provider with which the organization has a contract.

4.2 Advisories: Contested Value

Similar to the incident response service, according to P-G4, historically, advisories were a primary task of a sector CSIRT, and served as an important measure to prevent, rather than mitigate, incidents. P-G1 and P-G5 noted the importance of this service, and its acknowledgement on a regulatory level: under the NIS2 directive, paragraph 3b [12], CSIRTs must disseminate information relevant to their constituency about vulnerabilities. According to paragraph 3a, the *national* CSIRT must monitor and analyze vulnerabilities. The sector CSIRTs, therefore, only need to forward those advisories to their constituents. From a governing perspective, P-G1 and P-G5 suggested that they view the distribution of advisories via CSIRTs as an important service to comply with the NIS2 directive. However, they also noted, that the legislation for the actual implementation is still under development and they are having talks with practitioners from governing bodies and CSIRTs to determine the details.

IBD-CSIRT participants noted that they are very dependent on the national CSIRT in providing advisories. They do not spend any resources on expanding on that service, such as parsing the

advisory or providing new advisories. By contrast, P-S5, P-S6 from other sector CSIRTs noted that they developed their own additional advisories. These advisories are about software products that are popular or specific to their constituency. Unsurprisingly, P-S5 and P-S6 highlighted the value of the advisories to their constituency. By contrast, P-S2 questioned the value of the advisories of the national CSIRT, stating *"...we don't want this service to be a day job on our end, nor send too much information to the constituents...we want to provide value... it's a waste of our time if they can't act on the advisory or if they get the information already from elsewhere."* Similarly, P-S8 stated that much of the information from CSIRT advisories can be found elsewhere, and therefore, his sector CSIRT stopped sending advisories altogether.

The contested value of advisories is observed among municipal constituents, too. Some constituents perceived the advisories as one of the critical services of the sector CSIRT, as it helps them learn about potentially vulnerable systems in their network. Other constituents mentioned that they get the same information, sometimes sooner, from other sources. Particularly, participants of larger municipalities considered this a flaw of the service, or even of the sector CSIRT itself. They would rather receive advisories directly from the national CSIRT than from the sector CSIRT because they would get it faster.

According to constituent participants, several other factors influence the perceived value of advisories. First, P-C1, P-C3, and P-C6 reported that there is a process in the organization set up to directly turn advisories into tickets. These tickets are used for reporting and to allocate staff to act on the advisory. P-C6 noted *"...we use them for our internal processes. When a notification comes in, a ticket is created. We can act on those tickets, and I can report on them by the end of the month."* While this benefit may seem mundane, getting such patching processes in place is challenging for many constituents, according to P-C1.

Second, because the advisory is sent from an authoritative organization, it helps convince internal stakeholders, even when the issues have already been flagged by the internal team. For example, P-C2 noted, *"sometimes they don't take our word for it, and then the authority of the CSIRT is very useful."* Advisories sent from CSIRTs thus carry authoritative value for their constituency. The value of institutional authority does not appear to be a Dutch phenomenon, as it was also observed in [3], where CERT-SE was widely regarded as a trusted source of intelligence. Furthermore, it appears that the advisories have a utility beyond the actual contents of the advisory: practitioners acknowledge the advisory as a valuable tool to convince internal stakeholders. At the constituency, the advisory serves as a common ground between technical practitioners and management. A similar dynamic was found in [69], where the authors found that the National Vulnerability Database (NVD) worked best as a boundary object for a dialogue between the security team and others within the organization.

4.3 Expert Insights: One-Size-Fits-None

Participants from governing bodies and the CSIRTs noted that they have deep expertise in both security and the constituency. They offer this security expertise to their constituency in the form of topical briefs, webinars, policy documents, templates and advice, threat assessments, and quarterly news updates. Within this domain, practitioners often also use the term "knowledge products". Contrary to the incident response and advisory services, this service is not part of a regulatory framework but grew organically. According to P-S2, this service originates from the CSIRT observing low levels of security knowledge among constituents, a relatively high turnover rate of municipal staff, and municipalities with many more responsibilities than resources. P-S3 also noted that the CSIRT wanted to grow professionally and in its service offerings, reason from the perspective of the needs of its customers. In doing so, they ran customer satisfaction surveys to determine what customers (i.e., their constituency) needed. A need for these "knowledge products" was one of the findings from those surveys, and therefore got allocated more resources by the CSIRT.

However, CSIRT participants explained that there are operational challenges for the sector CSIRT in providing knowledge products to its constituency. P-S2 and P-S3 stated that their sector CSIRT offers a lot of value to their constituents with "templates" for policy and internal processes, such as a standardized supplier agreement or the outline of a security process. However, they need to provide these templates to many constituents, with many maturity levels. This makes it problematic to provide specific, actionable templates that anyone can use. The result is that, according to constituents, the templates are often generic and impractical. For example, P-C5 stated, *"...the information could be very useful but...it's almost impossible to provide this 'golden glove' for all organizations..."*. Producing these types of products has another inherent drawback for sector CSIRTs, it burdens them with the maintenance of the documents. These one-size-fits-all solutions are not uncommon in the security world. In [36], the authors found that one-size-fits-all solutions to provide more security are not realistic, because it places burdens on their users, which leads to great variations among participants' security approaches and implementations. This also has parallels to policymakers' views of consumer advice around the security of smart devices [64], in wanting to be seen to provide advice, yet it does not match the needs of all the people who need it.

4.4 Vulnerability Notifications: The Unseen Service

CSIRT participants and constituents mentioned that the sector CSIRT sends asset-specific vulnerability and abuse notifications to its constituents. P-S2, P-N1, and P-N2 explained how this process works. This process, i.e., "notification flow", is visualized in Figure 3 and further detailed in section 5.

Interestingly, constituents rarely mentioned this service during the interviews, suggesting that they do not see this as a valuable sector CSIRT service, whereas CSIRT participants highlighted it as a service to prevent incidents. When the service did come up, participants indicated that they "probably signed up" for the service but had not received any notifications. Some constituents assumed that because they did not receive notifications, things were probably okay.

Constituents may receive vulnerability notifications from other sources (e.g., vulnerability scanners), reducing the perceived value of CSIRT notifications. Although we did not ask participants directly about alternatives, some noted that they conduct their own

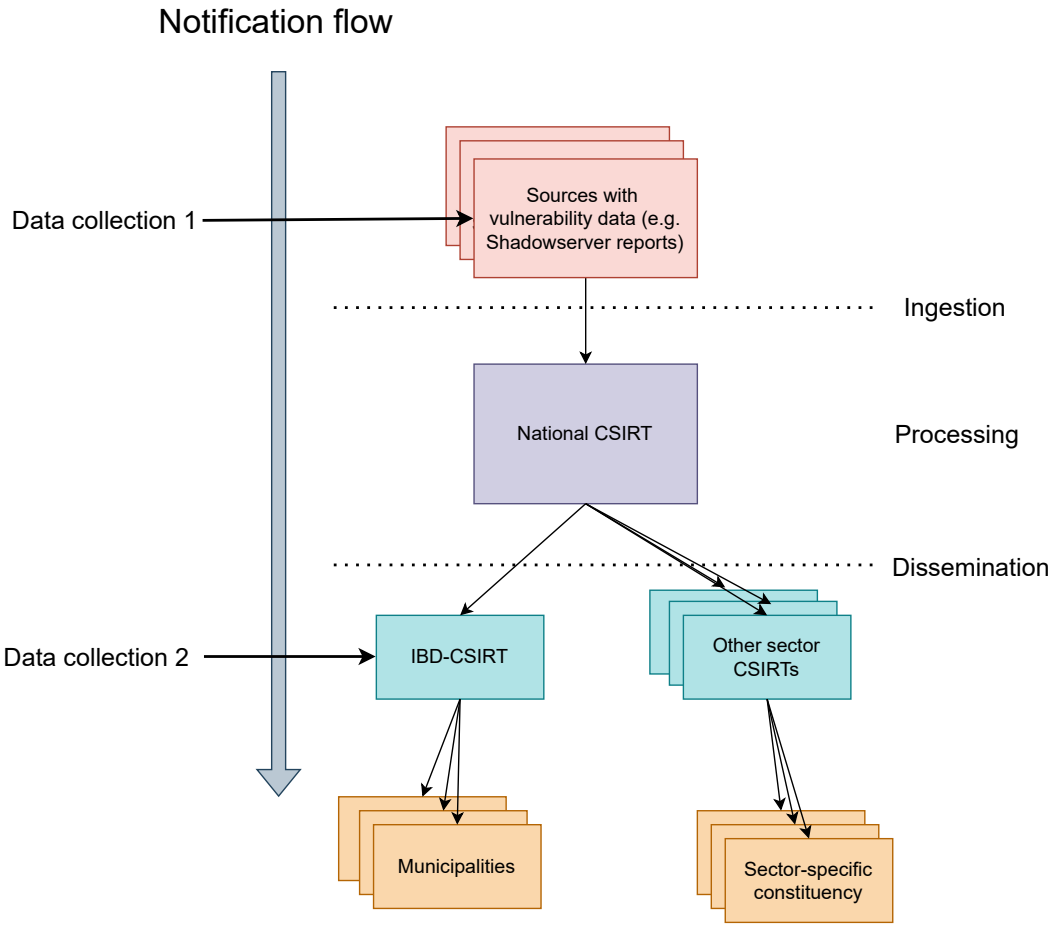


Figure 3: Overview of automated vulnerability notification flow

vulnerability scanning, which could lessen their reliance on the CSIRT. Still, none described the CSIRT's notifications as redundant. Instead, three constituents (P-C1, P-C2, P-C7) viewed them as a useful "second opinion" or as complementary to their external attack-surface management. This suggests that, when executed well, CSIRT vulnerability notifications retain clear value for constituents. This also suggests that CSIRT notifications have value for highly resourced countries, or sectors, e.g., banks, which could be explored in future work.

For most constituents, the service did not really seem to be on their radar. Somewhat related, P-S2 noted that there were times when the sector CSIRT rarely received notifications from the national CSIRT, which made them wonder if everything was ok.

To send notifications, CSIRTs need an up-to-date asset inventory of constituents. We hypothesized that if constituents valued the service, they would maintain a recent asset inventory. Therefore, we asked participants of the IBD-CSIRT for any data about constituent asset registrations. They maintained a list of the last asset change per constituent in Excel, as described in section 3. We found that this data shows that constituents rarely update their IPs and domains with the sector CSIRT, depicted in Figure 4. There are approximately 350 municipalities, Figure 4 shows that more than 100 municipalities last updated their IPs at the sector CSIRT in 2014. Another explanation is that constituents lack the resources to track all their assets. This is indeed the case—many reported limited capacity for various security tasks. In [6], it was also observed that defensive security efforts were hindered by budget constraints. However, all constituent participants maintained an asset inventory, even if it was potentially incomplete or inaccurate, which was not updated at the CSIRT.

This data suggests there might be a bootstrapping problem on the notification service: if the constituents do not keep their asset registrations current, then they might not get the relevant vulnerability and abuse notifications; yet, in the absence of getting relevant notifications, they are not incentivized to keep the registration current. At the same time, though, it's also the constituents that have the least (technical) knowledge and capacity and may need help.

Lastly, CSIRT participants explained that vulnerability notifications can also come in via responsible disclosures, as opposed to notifications from the national CSIRT. Several CSIRT participants mentioned the value of their responsible disclosure service, protecting their constituency from the hassle of managing responsible

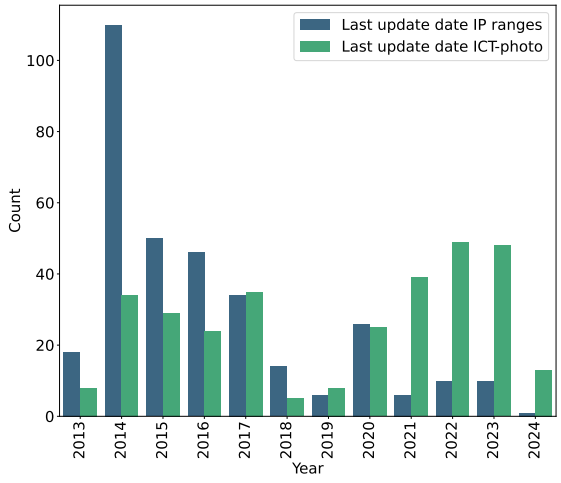


Figure 4: Constituency last-update value for asset registration per year. To illustrate, in 2014 more than 100 municipalities (out of approximately 350 total) last updated their IP ranges at the IBD-CSIRT.

disclosures themselves. They described the sector CSIRT process as follows. The sector CSIRT receives responsible disclosures from researchers who think the issue is related to some municipal asset – e.g., it relates to a domain name with the name of a municipality. The sector CSIRT then verifies the claim and assesses the severity. It then sends an actionable report to the constituent. Several CSIRT participants noted how much time and energy this service costs the sector CSIRT. The cost resides mainly in verifying the vulnerability and discussing the severity with the reporter. P-S6 noted that 90% of the received vulnerabilities were not taken into consideration after verification.

While CSIRT participants took pride in the handling of responsible disclosures, the service was not mentioned by constituents. This underlines that the perceived value of a sector CSIRT service, at least partly, depends on the visibility of the service by the constituent – i.e., most constituents have not received a responsible disclosure notification in recent years.

4.5 Intelligence Sharing: Visibility Equals Authority

CSIRT participants explained that advisories focus on vulnerabilities that are not asset-specific. Vulnerability notifications are asset-specific warnings. Expertise insights are often strategic and technical organizational products. By contrast, they noted that *intelligence sharing* revolves around the sector CSIRT sending out ad-hoc warnings for an issue (e.g., a new type of phishing attack), tips, experiences, best practices, or other relevant information.

A majority of constituent participants noted that they frequently received such intelligence and considered this sector CSIRT service very valuable, helping them tune their defenses, share expertise, or get help. P-S4 noted that, despite the service being valued, it was sometimes hard to get information back from the community. He suspected that constituents are afraid that they might do things wrong and that their information and ways of working are judged. In fact, he stated, the CSIRT lauds any efforts from constituents that give back to the community. In [70], it was observed that malware analysts also tended not to share information. However, in their case, they refrained from sharing because they felt it was only one-way or that it did not help others.

This service is highly visible—constituents frequently receive intelligence—which may explain its perceived value. An alternative explanation is that utility, rather than visibility, drives value perception. Indeed, utility is likely to be a factor. However, as discussed in subsection 4.4, responsible disclosure handling was considered useful by CSIRT practitioners but was not visible to constituents and therefore not perceived as valuable. This supports the hypothesis that visibility is also a factor in how constituents value a service. According to participants from the CSIRT and governing bodies, sharing intelligence has another benefit for the sector CSIRT: the sector CSIRT continues to maintain its reputation as an expert or authority within its domain or sector.

4.6 Outreach and Community: Bringing Constituents Together

CSIRT participants stressed the importance of knowing their constituency. They mentioned that they travel across the country to attend meetings, join regional initiatives, meet people from constituent organizations, and talk to suppliers. P-S3 and P-S4 noted that underpinning these efforts is a desire of the sector CSIRT to foster trust with and among constituents, showcase services, and learn what issues constituents are dealing with. These efforts are part of the 'constituent expertise' that participants from governing bodies value so highly of sector CSIRTs.

Constituents considered sector CSIRT outreach and community-building efforts more practically, focusing on how the sector CSIRT has a facilitating role in bringing constituents together who face similar challenges. Some constituents stated that regional initiatives failed without the sector CSIRT involved, and noted that the sector CSIRT should have a facilitating role. P-S4 noted that the sector CSIRT would like to personally know all constituents, but that simply is not possible with the size of the constituency and their geographic distribution over the country. Regional initiatives, like a CISO platform where local CISOs get together, help the sector CSIRT scale their networking efforts as well as bring constituents together.

Another CSIRT participant highlighted the value of these efforts to manage expectations among constituents. With the NIS2 directive coming into effect, many more organizations will fall under a critical sector. These organizations, generally, do not have experience with cybersecurity legislation and obligations. However, those organizations will have obligations. P-S1 noted that *"...we want to make ourselves as clear as possible and show what services we provide...I want that clearly on the website...I want to manage those expectations, and clearly communicate what we do. Tell them that they are a [responsible] 'entity', not a customer."* This illustrates the underlying relation between sector CSIRT practitioners and constituents: CSIRT practitioners are there to support constituents

as best as they can but ultimately, constituents have their own responsibilities, and they are not CSIRT customers who can demand whatever they like.

5 Results: Evaluating the Vulnerability Notification Service

In subsection 4.4, we found that CSIRTs and constituents did not appreciate the vulnerability notification service equally: CSIRTs considered it important, in stark contrast to constituents who were mostly unaware of it. To understand this dichotomy, we investigate how this service functioned in practice. We do so by measuring notifications at each stage of the flow (Figure 3) to quantify throughput and identify obstacles. We cover the period 2015 to 2024. In late 2024, the system was revamped. Our methods were: (1) a longitudinal empirical analysis to assess whether notifications reached IBD-CSIRT constituents and which factors impeded delivery; and (2) three follow-up interviews to contextualize findings: two with national-CSIRT program leads and one with a sector-CSIRT practitioner operating the service.

5.1 Measuring Notification Flow

The dissemination of vulnerability notifications from the sector CSIRT to constituents happens via a ticketing system at the IBD-CSIRT. We assess the functioning of this flow by comparing the notifications that constituents *should* have received to what they *actually* received.

The methodological details of this analysis are discussed in § 3.2. We analyse ticketing data from IBD-CSIRT. The system creates a ticket for all vulnerability notifications received from the national CSIRT. It then automatically notifies the associated municipality of the ticket. We analyzed 2,826 tickets ranging from 17 July 2015 to 16 September 2024.

Most vulnerability data received from the national CSIRT came from Shadowserver. For our evaluation, we had access to full Shadowserver vulnerability reports that the national CSIRT receives, the asset inventory list of constituents, and the IBD-CISRT ticketing data. This allows us to check if IP addresses that show up in Shadowserver reports (data collection point 1) are seen in tickets of the IBD-CSIRT to their constituents (data collection point 2 in Figure 3).

First, we analyzed the vulnerability data from Shadowserver. It consists of reports that contain IP addresses that are vulnerable or compromised [60]. Table 7 depicts the total number of reports by year and severity. The national CSIRT receives all Shadowserver reports for the Netherlands. The researchers had access to the same Shadowserver data. According to P-N3, the IBD-CSIRT does *not* have access and relies on the national CSIRT.

Using the IPs in the Shadowserver reports, we determine the set of 'hits': municipal IP addresses that show up in the Shadowserver reports. These hits make up the set of notifications that IBD-CSIRT should have received.

According to the national CSIRT participants P-N1 and P-N2, a ticket is created once per day per report type. When a vulnerability notification ticket is created, it contains an abuse attachment that may contain multiple IPs. This leads to only one ticket per day. Therefore, we take tickets per day as the unit of analysis. We analyzed 2,826 tickets; of these, 378 describe notifications pertaining to the Shadowserver data.

We matched all Shadowserver reports on municipal IPs and found hits in 67 unique reports. However, IBD-CSIRT received notifications for only 6 different reports. Thus, our first important finding is that many Shadowserver reports do not lead at all to notifications to the constituents.

For the six report types that do show up in the tickets, we observe that there are hits with municipal IPs that do *not* lead to ticket creation. From 2018 to 2024, we observed 378 tickets, i.e., 378 days where a ticket was made that references one or more hits on municipal IPs in the Shadowserver data. In the raw Shadowserver data, for the same period, we observed 1,365 days for which Shadowserver registered a hit on one or more municipal IPs in the six reports. Thus, only 27% of days with Shadowserver hits led to ticket creation. Figure 5 depicts the number of days per year that a hit was present in the Shadowserver data, but no ticket was created. This observation is most salient in 2022, when 353 days with one or more hits did not lead to any ticket creation. Figure 5 depicts the number of notifications that should have been sent versus the number of notifications in the ticketing data.

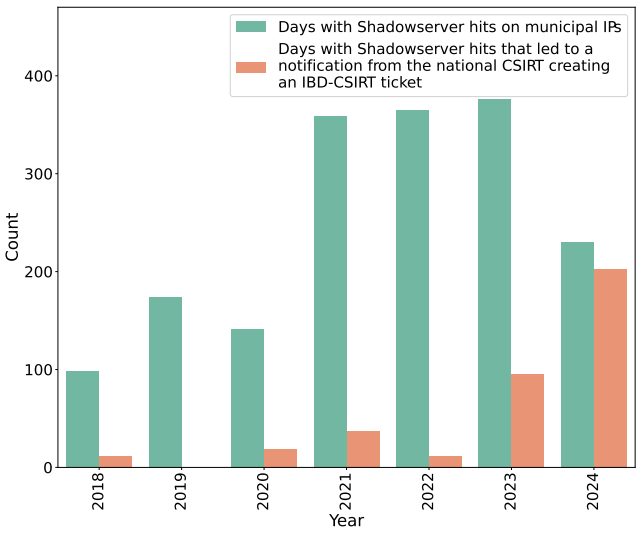


Figure 5: All days with Shadowserver hits on municipal IPs vs. the days with Shadowserver hits on municipal hits that led to an IBD-CSIRT ticket.

These findings suggest that the vulnerability notification service was not functioning as intended: most vulnerability data is not reaching the respective constituents. This may explain why constituents rarely mentioned the service during the interviews: they probably never received notifications. Surprisingly, though, this mechanism was in place for many years during which the missing notifications were not detected.

Table 6: Overview of the Value and Challenges for Articulated CSIRT Services

Service	Value	Challenges
Incident Response	Assistance during an incident CSIRT acts as trusted (DFIR) broker	Misaligned expectations over service implementation Role of CSIRT during incident unclear Lack of resources
Advisories	Incident prevention NIS2 compliance Advisories facilitate constituent internal processes	Dependency on national CSIRT Advisories not timely Custom advisories cost scarce resources Constituents cannot always act on advisory Advisory information available elsewhere
Expert Insights	Sector-specific expertise available Provide and perserve cybersecurity expertise	Uniform knowledge products not actionable Service maintenance costs resources
Vulnerability Notifications	Incident prevention Asset-specific notifications	Dependency on national CSIRT Constituents do not update assets Service not valued by constituents Responsible disclosures efforts not visible and valued
Intelligence Sharing	Sector-specific actionable intelligence Establishes CSIRT as an authority	Intelligence collection from constituency
Outreach and Community	Foster personal relations between CSIRT, constituency and suppliers Develop expertise among constituency	CSIRTs role in regional initiatives unclear Constituency too big and dispersed CSIRT can only facilitate

Table 7: Number of Shadowserver Reports

Severity	Year						
	2018	2019	2020	2021	2022	2023	2024
info	2	2	3	6	9	9	10
low	5	5	6	4	4	6	6
medium	12	14	16	19	24	24	23
high	22	24	24	28	40	41	43
critical	9	9	9	22	19	18	22
special	0	0	0	1	4	1	0
n/a	4	4	2	11	24	36	35
total	**54**	**58**	**60**	**93**	**124**	**135**	**139**

5.2 Reflections Evaluating the Notification Program

We found that a lot of vulnerability notifications were not reaching constituents, contrary to the prescribed notification flow depicted in Figure 3. We presented these findings to P-N1 and P-N2 of the national CSIRT, who operated the program. We also presented the findings to P-N3 of the sector CSIRT. We wanted to confirm we correctly understood the notification mechanism and identify the root causes for the missing notifications.

P-N1 and P-N2 talked openly about the challenges in the setup and running of the notification service. P-N1 indicated that, contrary to other domains, the cyberdomain was new at the time, and nothing in terms of regulation or best practices was in place. They were tasked to do something new and had to figure out what worked along the way.

For our first finding, that only a fraction of the Shadowserver reports were sent, they noted that, depending on the type of organization to which they send the notifications, the system may decide to include more or fewer reports. This system was put in place to not overburden recipient organizations like IBD-CSIRT by sending too many notifications that they could not act on. N3 was not aware of this filtering process, let alone consented to it.

For our second finding, not all vulnerable IPs led to a ticket, P-N1 and P-N2 stated that they did not directly have an explanation for the numbers. They speculated that their notification tooling used e-mail to send the Shadowserver reports to IBD-CSIRT. Perhaps some tickets were not created due to delivery failures. They also noted that their internal tooling sometimes has issues and may temporarily be offline. It could well be that a "queue" of messages could have been deleted. Additionally, they mentioned that their internal notification tooling was set up to process hits without automatically sending actual notifications, as a safety precaution.

When discussing the total lack of notifications in 2019, the participants speculated that for a certain period, an IBD-CSIRT

recipient address to send notifications to may have been missing or "unchecked" in the tooling. They could verify this checking/unchecking mechanism in the tooling but could not verify whether this had taken place. They also noted that one of the six Shadowserver reports was only "turned on" in 2023, explaining some of the discrepancies. To verify, we removed this report from our analysis for the years 2018-2022 and observed that some missing notifications in 2021 and 2022 indeed decreased. However, many missing notifications remain, in those and in other years.

Finally, P-N1 and P-N2 noted the lack of quality assurance processes to test and evaluate their notification pipeline. While they voiced a desire for such processes, a lack of resources and more pressing priorities prevented their implementation. The absence of a feedback loop is therefore problematic.

The absence of a feedback loop in the critical mechanism of vulnerability notifications has been a fundamental problem that has been observed across many countries. Earlier studies on such mechanisms [9, 32, 65, 71] found that recipients almost never respond to notifications, so it is very difficult for the sender to observe if the notifications were correctly delivered, let alone acted upon. The lack of a feedback loop has also been observed as a problem in government efforts. When CISA evaluated its Ransomware Vulnerability Warning Pilot (RVWP), it observed that its personnel relies on subsequent internet scans to infer that the vulnerability was mitigated, confirming the absence of a feedback loop from the notified entity [61].

In sum, the practitioners who run a national notification service are faced with internal decision-making processes (i.e., filtering hits from reports by making assumptions about the recipients), source selection and processing (what reports are trustworthy), and tooling issues. These are factors that impede notification delivery. Practitioners are faced with limited resources and diverging priorities. The lack of feedback caused the missing notifications to go undetected for years. Even if the sector CSIRT and its constituents have strong bonds, they do not know they are not receiving the information meant for them, so they can't correct the problem.

6 Results: Strategic Challenges for Sector CSIRT Practitioners

In this section, we address our second research question (RQ2): *What are the strategic challenges for practitioners of a sector CSIRT in providing services?* We interview practitioners and determine the challenges that transcend specific CSIRT services.

Two groups of organizational challenges emerged from grouping subcodes from the interviews, available in Table 12: (*i*) governance structure and external stakeholders; and (*ii*) infrastructure and capability management.

6.1 Governance Structure and Stakeholders

We observe that most sector CSIRTs originated from practitioners' best-effort bottom-up (i.e., unregulated) initiatives with limited resources, providing many services. Additionally, P-G4 noted that the sector CSIRTs have a minimal top-down structure and rely heavily on personal relations. Consequently, existing sector CSIRTs have different governance structures, depicted in Table 1. By contrast, the NCA did not originate as a bottom-up organization.

The sector CSIRTs' governance structure can be problematic. For example, Z-CERT (CSIRT for healthcare), under NIS2, will be entitled to government funding. However, because of its legal structure, a foundation, the organization may not be eligible to receive the funding. It may also not recommend certain commercial parties to constituents, which is considered 'disrupting the market'. This highlights the importance of considering the risks and benefits of various governance structures when establishing the sector CSIRT because it may limit the specific things a sector CSIRT may undertake down the line.

For certain services, the sector CSIRT is highly dependent on other stakeholders, e.g., for advisories described in § 4.2. Constituents depend on those advisories as a mitigation measure to manage their attack surface. For some constituents, according to P-C5 and P-C6, those advisories are the primary source of vulnerability information. A similar dependency exists between the sector CSIRT and the national CSIRT in providing vulnerability notifications. Finally, constituents rely on commercial parties for the IT infrastructure. This creates a situation wherein a constituent may receive advisories, but is incapable of acting on them because they do not directly control the infrastructure. This process is problematic in practice, as the IT service provider does not always act as fast as the organization wants. For example, P-S2 reported that organizations sometimes have to wait up to a month before their ticket on a patch is resolved.

Next, we observed trust as an important component during an ongoing incident. Previous academic work also identified the essential role of trust among CSIRTs [2, 5, 22, 31, 40, 68], and in industry [45]. CSIRT participants noted that if an organization is hit by an attack, the sector CSIRT is supposed to be invited to a triage meeting. However, CSIRT participants noted that this does not always happen for a variety of reasons. For example, an organization may be scared because the sector CSIRT acts as an independent party, and victim organizations fear that they might be blamed for not having security measures in place.

Closely related, CSIRT participants noted that they want to be a *trusted partner* for their constituents. *Liaisons* were mentioned as a way to build trust. Additionally, sector CSIRTs engage in various outreach and community efforts, described in § 4.6. Participants from sector CSIRTs fear that they are viewed as an authoritative organization that tells constituents what to do. Therefore, CSIRT participants note that they take great care to protect trust among stakeholders. Yet, constituents did not indicate that they feel the sector CSIRT is telling them what to do too much. Instead, some constituents indicated the sector CSIRT may be *more* authoritative to get basic security measures in order at certain lagging constituents.

Regarding its constituent population, a sector CSIRT faces challenges in serving many constituents with mixed maturity levels. All CSIRT participants acknowledged this, even those with fewer constituents, see Table 1. The value of CSIRT services can suffer because organizations have varying needs—knowledge, tools, or infrastructure. For example, P-C4 and P-C5 noted that the IBD-CSIRT uses "one-size-fits-all" knowledge products. This approach fails both immature organizations, which lack the expertise to use them, and mature ones, for whom the products are too basic. P-C8 observed that the products may work for smaller organizations but not for larger ones. Or, as P-C4 stated, *"one size fits none"*.

Finally, P-G1 emphasized that the diversity of constituents is where a sector CSIRT adds value: acting as a glue, building trust, and facilitating collaboration—a view shared by all CSIRT participants.

6.2 Infrastructure and Capability Management

Participants state that infrastructure and asset management is challenging. Maintaining a complete, up-to-date asset inventory is difficult. While internal IP ranges are stable and monitored, SaaS services frequently change, and inventories rely on departments reporting assets. These unreported systems weaken security and hinder sector CSIRTs. Without accurate inventories, CSIRTs cannot deliver or receive vulnerability notifications from the national CSIRT. Many services are outsourced or moved to the cloud, and constituents rely on external security services. P-S8 warned that this reduces organizational control and visibility, making it hard to act on alerts. P-G5 noted that during incident triage, debates arise over control, outsourcing, and responsibility for security measures.

Table 8: Overview of CSIRT Strategic Challenges

CSIRT Strategic Organizational Challenges
Mandate and legal structure may impact service provision and resource allocation
Limited resources for many services
CSIRT is dependent on other organizations
Lack of trust may impede service provision
Diverse constituency with mixed-maturity levels
Outsourcing parts of constituent infrastructure makes incident triage complex

7 Results: Findings Validation Workshop

To more rigorously test the generalizability of our findings and further deepen them, we validated findings with practitioners from multiple sector CSIRTs via a workshop session. The practitioners were all security officers. In light of the time constraints, we selected a subset of seven findings of § 4 and § 6, which we paraphrased for brevity and easy comprehension. We used the approach detailed in subsection 3.3.

An overview of the results is depicted in Table 9. In many cases, some participants voted "abstained" because they felt the agree / disagree vote was too simple. Instead, they preferred to elaborate on their situation.

1. Practitioners of sector CSIRTs are dependent on other stakeholders for the delivery of services. Two participants noted that this finding depends on the specific service, mentioning their red-team services as an example where they are not dependent. Sector CSIRT practitioners may thus vary in their level of dependency on others depending on the specific service. As a "coordinating" body [21], however, by its very nature, many services (e.g., notifications or advisories) introduce these dependencies.

2. The diversity of constituents is a big challenge in the development and offering of services. Those who agreed raised their hands instantly and vocally agreed with this statement. The participant who disagreed claimed that his organization simply offered several "flavors" of its services, depending on the maturity of the constituent. Some of the participants who agreed responded that providing such "flavors"of services took additional resources that are rarely available.

3. Trust between stakeholders is essential for practitioners of sector CSIRTs to provide services. The participant who disagreed argued that practitioners from his organization can *always* deliver services, but without trust, the quality of those services would be degraded. However, he did not elaborate on how.

All participants agreed that trust in the security domain is important because much information is shared via personal connections for information sharing. Furthermore, sector CSIRT practitioners put great value in trust with their constituency, so they are contacted by them when needed, so that the CSIRT can be 'found' by constituents, as noted in sector CSIRT industry guidelines [44].

Thus, personal relations are important for unhindered information exchange between stakeholders. For those relations, trust is essential, and it acts as a catalyst in providing information-dependent services.

4. Many constituents rarely update their asset list at the sector CSIRT which undermines the effectiveness of sector CSIRT services. A discussion occurred over what constitutes an asset. Some participants considered 'contact details' assets, and they had trouble with outdated details and could not reach constituents. Others noted that they invest time in managing those contacts, and they did not recognize the problem. A participant who disagreed indicated that their organization controls the network infrastructure of its constituents, so IP registrations were not much of a problem.

If we expand the term 'assets' to include contact details, then asset registration is widely seen by participants as problematic because they are not frequently updated. Inaccurate contact information in the notification process, which prevents contacting an entity, was also observed by [9]. Keeping asset registrations up to date was difficult for everyone, except for the sector CSIRT practitioners who operate network infrastructure for its constituents.

5. Constituents expect technical assistance on location with the Incident Response service, but practitioners of the sector CSIRT are not equipped to do so. One participant noted that they are equipped for IR, but it depends on the magnitude of the incident. Another participant mentioned that their documentation on how much support constituents could expect from the sector CSIRT during an incident was the biggest source of confusion among constituents [43]. The discussion focused on constituent incident response expectations of the CSIRT. This was largely seen as problematic because the practitioners could not deliver the expected support.

6. Practitioners of sector CSIRTs had concerns about not receiving all vulnerability notifications of the national CSIRT. Two participants noted that their organization had their own Shadowserver feed and do not rely on the national CSIRT for vulnerability data. Another participant noted that his sector CSIRT, up to now, has had no reason to doubt that they are not receiving all vulnerability notifications. This finding seemed specific to IBD-CSIRT practitioners, as only they observed anomalies in their ticketing data in 2019. However, without some kind of feedback mechanism,

Table 9: Validation Workshop Voting Results per Finding

Finding	Section	Agree	Disagree	Abstained
Practitioners of sector CSIRTs are dependent on other stakeholders for the delivery of services.	6.2	4	0	3
The diversity of constituents is a big challenge in the development and offering of services.	6.2	5	1	1
Trust between stakeholders is essential for practitioners of sector CSIRTs to provide services.	6.2	3	1	3
Many constituents rarely update their asset list at the sector CSIRT which undermines the effectiveness of sector CSIRT services.	6.3	2	2	3
Constituents expect technical assistance on location with the Incident Response service, but practitioners of the sector CSIRT are not equipped to do so.	4.1	3	1	3
Practitioners of sector CSIRTs had concerns about not receiving all vulnerability notifications of the national CSIRT.	4.4	1	2	4
Services are often shallow because scarce resources are distributed among many services.	6.2	5	0	2

it is very difficult for practitioners to actually know that they are not receiving all notifications, unless there are glaring anomalies.
7. Services are often shallow because scarce resources are distributed among many services. Participants vocally agreed to recognizing this finding. The two participants who abstained may also have nodded agreement, but the researchers are not sure. Nonetheless, this issue was widely agreed upon.

8 Discussion

In this study, we try to lift the veil on how the professionals in and around sector CSIRTs experienced their functioning. For our first research question, we analyzed the experiences and challenges tied to six specific services that sector CSIRTs provide. The results are summarized in Table 6. For our second research question, we identified strategic challenges that transcended the specific services, summarized in Table 8. Here, we want to make sense of the underlying dynamics that shape these experiences and challenges. We organize these dynamics around three concepts: resources, legitimacy, and dependency.

First, we found misaligned expectations and challenges in providing the services that are associated with the label 'CSIRT.' Sector CSIRTs are small, much smaller than a 'normal' CSIRT, because they were formed bottom-up and are funded primarily by organizations in the sector pooling some resources. This puts persistent constraints on their capabilities. While they provide various services, many of them are rather shallow in their implementation. The clearest example is that constituents expected "boots on the ground" during incident response. The sector CSIRT was not able to provide this.

A seemingly straightforward strategy to better align the expectations with the available resources would be to make it more explicit to constituents what the sector CSIRT can and cannot do. To some extent, this is what happened for the "boots on the ground" issue. Over time, constituents learned not to expect this from their sector CSIRT. Such a strategy, however, would overlook the other dynamics at work, which help to understand why the misalignments not only arise, but are sustained over time.

A second dynamic is the sector CSIRT's pursuit of legitimacy. Telling their constituents to expect less also makes the sector CSIRT less relevant. So the professionals operate in a tension: promise too much and risk disappointment, versus promise too little and risk being irrelevant. This tension makes an easy alignment of expectations with capabilities difficult. There will always be pressure to do more for their constituents, stretching the limited resources.

Yet, it is not all about servicing the constituents. As one sector CSIRT professional phrased it: *"I want to manage those expectations, and clearly communicate what we do. Tell them that they are a [responsible] 'entity', not a customer."* If the constituents are not customers, then what are they? The term 'entities' is a nod to the regulatory frameworks, most notably NIS2, which applies to 'essential' and 'important entities.' To call the constituents responsible entities is to say that it is their responsibility to meet certain security requirements. The sector CSIRT is meant to support them in bringing about this outcome. In other words, it is not just about meeting the needs of the constituents, but also about getting them to change their practices; paternalistically nudging them in the 'right' direction.

This is the reason why governments in many countries have encouraged setting up sector CSIRTs. In the EU, under NIS2, this is now even mandated. The organizations are seen as instruments to improve security in the sector. And yet, when we consider this as a community of practitioners, it aligns with commentary on community-owned interventions [7], that community-level transformation would fare better if the people within that community can own the change themselves, rather than have it forced upon them by outside experts. The sector CSIRT must understand them, show them, and act alongside them.

This dual mandate – helping constituents while also getting them to change their behavior – means that the legitimacy of the

sector CSIRT comes from the top as much as from the bottom. It helps us understand why the sector CSIRT sees the vulnerability notification service as very important, yet it was barely mentioned by the constituents as something they expect from the sector CSIRT. This service is not driven by demand from the constituents, but by demand from the government. So the sector CSIRT professionals are managing two legitimacy relationships at the same time. This is also why misalignments are not easy to resolve, because alignment with one side might cause misalignment with the other. As noted by Kocksch et al. [29] in the discussion of care in IT security, "IT security, as an organizational achievement, relies on an intricate entanglement of care and organizational authority"; we get the sense that the sector CSIRT cannot walk away from their remit, this being that constituents must be protected.

Finally, we observed dynamics around dependencies. The malfunctioning vulnerability notification service clearly shows a dependency on the national CSIRT. It did not forward the relevant notifications to the sector CSIRT, which in turn sent fewer notifications to constituents. This contributed to the latter not really seeing the value of the service. It also eroded the incentives for the constituents to update the asset registrations that they have submitted to the sector CSIRT.

These dependencies interact to create a bootstrapping problem: without relevant vulnerability notifications, the constituents are less likely to correctly register their assets, and the absence of up-to-date asset registration makes it less likely that they will get relevant vulnerability notifications. The more general version of this bootstrapping problem is: the sector CSIRT can provide value for the constituents if the constituents invest time and effort into working with it, yet as long as they do not see the value, they are unlikely to make those investments.

This assumes that constituents actually know their assets to begin with. Our participants noted that constituents' users may spin up assets without telling anyone. In examining UNICEF logistics, Jack & Jackson [26] refer to the reality of 'messy infrastructures' rather than something neater. To force neatness into asset management would be to force a change to the way whole organizations operate, undoing their naturally messy nature.

In the end, the sector CSIRTs can only offer different types of carrots, they lack any kind of stick. Within the EU, the NIS2 legislation might help overcome the bootstrapping problem as it requires constituents to take certain actions – e.g., by reporting incidents to the sector CSIRTs. It remains to be seen if these obligations are enough, as some constituents simply lack the knowledge or resources to engage more fully, or to impose their own mandate upon the rest of their organization.

Recommendations. Our recommendations are organized around the concepts of resources, legitimacy, and dependency.

- *Focus on least-capable.* CSIRTs have limited resources, yet face a diverse constituency in terms of maturity. Given that their goal is to augment the capabilities of the constituents, it makes sense to spend the limited resources on the least-capable, rather than trying to support everyone. Such an approach leads to "one-size-fits-none" solutions. At the same time, realistic baselines should be established for those constituents to avoid raising expectations that the sector CSIRT cannot live up to.
- *Include challenges in guidelines.* Second, we recommend to extend industry guidelines by flagging the issues that our empirical data has surfaced around resources, legitimacy and dependencies, which might help new CSIRTs to better diagnose the issues they are facing. The current support is very sparse and limited to a single SEI report about how to set up a sector CSIRT, not how to operate one [44]. The FIRST framework has yet to release guidelines specifically for sector CSIRTS [20]. The SEI report anticipates challenges and suggests that sector CSIRTs should focus on offering a small set of services and doing those well. We found that, in reality, due to legitimacy tensions, CSIRTs might over-expand their provided services, undermining the trust of constituents. Such lessons learned may help other organizations to navigate difficult issues, rather than having to reinvent the wheel.
- *Build feedback loops.* We found that practitioners could not easily detect the missing vulnerability notifications: there was no feedback mechanism. In our case, this allowed a malfunctioning pipeline from the national CSIRT to the sector CSIRT to persist for years. The absence of a feedback loop has also been observed in notification research [9, 32, 65, 71]. This work found that the final recipients often do not act on vulnerability notifications. Both problems undermine the effectiveness of this important sector CSIRT service.
  This lack of a feedback loop likely applies to numerous other provided services. By introducing a feedback mechanism, stakeholders will a) know that services are operating correctly (e.g., all vulnerability notifications are arriving), and b) know if the service is either useful or being acted on (e.g., CSIRT will know if constituents are doing something with advisories and vulnerability notifications).
- *Mix top-down with bottom-up incentives.* Fourth, CSIRTs face a bootstrapping problem. This issue can be addressed via a mix of top-down and bottom-up incentives. One top-down incentive is to make updated asset registrations a stronger norm. The Dutch national CSIRT is working towards a constituent registration platform for all sector CSIRTs and constituents [42]. This national platform is inspired by NIS2 and will replace the ad-hoc efforts of single-sector CSIRTs, which, at least for IBD-CSIRT, were not very successful. A stronger incentive is the option to impose regulatory requirements on constituents to engage with the sector and national CSIRT, as is the case under NIS2, where constituents are required to report incidents. Bottom-up, as a community of practitioners, sector CSIRTs may continue to invest time in helping constituents develop their capabilities that will allow them to see the value of the services and encourage them to invest in engaging more with the sector CSIRT.

Limitations. Our research design faces several limitations, most notably regarding external and internal validity. First, our main focus was on one sector CSIRT in one country, with its constituency

and governance bodies. Generalizability to other sectors in the country is supported by our cross-sector validation workshop, where practitioners from other domains reported similar dependencies, asset-inventory pain points, and expectation gaps.

We did not research sector CSIRTs in other countries. While this limits the generalizability of our findings, we would argue that the findings have wider relevance. Institutional contexts for sector CSIRTs differ across countries, yet there are strong similarities. The sector CSIRT model is literally a model, one that has been copied worldwide – first under the name sector CERT (Computer Emergency Response Team), but after the name CERT was trademarked, the label sector CSIRT was adopted. The U.S. Department of State commissioned a report by SEI to support this dissemination by developing a general framework for the founding of new sector CSIRTs [44]. Within FIRST, there is a vibrant community that supports setting up new instances of the model in different countries and sectors. Of course, all implementations will be adapted to local conditions, but we would argue that the triad we surfaced —- resources, legitimacy, and dependencies —- offers a transferable analytic frame that supports the work of sector CSIRT professionals elsewhere.

In terms of internal validity, our sample size was limited. We were able, however, to recruit representatives of all selected stakeholders. including all sector CSIRTs except one. Our participants only reflect a part of the perspectives within their respective organizations. We addressed this limitation by recruiting several people from an organization whenever possible. In the first phase, we interviewed three IBD-CSIRT practitioners. While a small number, it reflects the team's limited size: only five practitioners handle incidents and interact directly with constituents, with the remainder in support or administrative roles. Thus, our sample covers a substantial share of the relevant professionals. Furthermore, given the challenge of recruiting participants, limited resources, and the saturation of themes, we believe the sample size to be adequate to support our findings.

Future work. We presented exploratory work on practitioner challenges in operating a sector CSIRT. We propose several areas for future work. First, this study could be replicated in other countries or sectors to corroborate our findings or determine factors that affect our observed challenges. Second, we investigated the vulnerability notification service in detail. Yet, for the other services, an in-depth study remains. Third, for the small set of Shadowserver reports that *were* used to send notifications, the program did improve in 2024. Consequently, this may impact service perceptions by constituents, which may be analyzed further.

Conclusions. We investigated challenges of practitioners at sector CSIRTs by asking what stakeholders expected. In doing so, we identified challenges practitioners face in providing services. Sector CSIRT practitioners need to deal with a diverse constituent population, trust issues, and organizational dependencies. For the vulnerability notification service, this dependency turned out to be problematic, as not all notifications arrived at constituents. We highlighted factors that undermine the national notification mechanism. While regulatory frameworks increasingly rely on sector CSIRTs, there is a need to better understand these organizations as institutional structures to mitigate cyber threats.

Acknowledgments

We are grateful for our collaboration with the IDB-CSIRT and other participating organizations. We thank the anonymous reviewers for their constructive feedback that improved the paper. This work was supported by the Ministry of the Interior and Kingdom Relations of the Netherlands and Delft University of Technology under Grant M75B07 and partially by NWO-project "THESEUS" (NWA.1215.18.006).

References

[1] Maziana Abd Majid and Khairul Akram Zainol Ariffin. 2021. Model for successful development and implementation of Cyber Security Operations Centre (SOC). *PloS One* 16, 11 (2021), e0260157. doi:10.1371/journal.pone.0260157

[2] Noura Alomar, Primal Wijesekera, Edward Qiu, and Serge Egelman. 2020. "You've Got Your Nice List of Bugs, Now What?" Vulnerability Discovery and Management Processes in the Wild. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, USA, 319–339. https://www.usenix.org/conference/soups2020/presentation/alomar

[3] Annika Andreasson, Henrik Artman, Joel Brynielsson, and Ulrik Franke. 2024. Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval. *Cognition, Technology & Work* 26, 4 (2024), 709–731.

[4] Atlas.Ti. 2023. ATLAS.ti | The #1 Software for Qualitative Data Analysis. https://atlasti.com

[5] M Bada, S Creese, M Goldsmith, C Mitchell, and E Phillips. 2014. Improving the Effectiveness of CSIRTs Global Cyber Security Capacity Centre.

[6] Priyanka Badva, Kopo M. Ramokapane, Eleonora Pantano, and Awais Rashid. 2024. Unveiling the Hunter-Gatherers: Exploring Threat Hunting Practices and Challenges in Cyber Defense. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA, 3313–3330. https://www.usenix.org/conference/usenixsecurity24/presentation/badva

[7] Peter Block. 2018. *Community: The structure of belonging*. Berrett-Koehler Publishers, Oakland, CA, USA.

[8] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology* 18, 3 (2021), 328–352. arXiv:https://doi.org/10.1080/14780887.2020.1769238 doi:10.1080/14780887.2020.1769238

[9] F. Cetin, C. Gañán, Maciej Korczyński, and M. van Eeten. 2017. Make Notifications Great Again: Learning How to Notify in the Age of Large-Scale Vulnerability Scanning. Workshop on the Economics of Information Security (WEIS). https://www.semanticscholar.org/paper/Make-notifications-great-again%3A-learning-how-to-in-Cetin-Ga%C3%B1%C3%A1n/ed24ca9d63385392bbd6ac52288933b93444c43d Paper.

[10] Tiffani R. Chen, Daniel B. Shore, Stephen J. Zaccaro, Reeshad S. Dalal, Lois E. Tetrick, and Aiva K. Gorab. 2014. An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams. *IEEE Security & Privacy* 12, 5 (Sept. 2014), 61–67. doi:10.1109/MSP.2014.85 Conference Name: IEEE Security & Privacy.

[11] Justin Novak Christopher Rodman, Breanna Kraus. 2024. SOC Service Areas: Identification, Prioritization, and Implementation. https://www.ndss-symposium.org/ndss-paper/auto-draft-521/

[12] European Commission. 2025. NIS2 Directive: new rules on cybersecurity of network and information systems | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[13] A. D'Amico and K. Whitley. 2008. The Real Work of Computer Network Defense Analysts. In *VizSEC 2007: Proceedings of the Workshop on Visualization for Computer Security*, John R. Goodall, Gregory Conti, and Kwan-Liu Ma (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 19–37. doi:10.1007/978-3-540-78243-8_2

[14] Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, and J. Alex Halderman. 2014. The Matter of Heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference* (Vancouver, BC, Canada) *(IMC '14)*. Association for Computing Machinery, New York, NY, USA, 475–488. doi:10.1145/2663716.2663755

[15] ENISA. 2019. Study on CSIRT landscape and IR capabilities in Europe 2025. https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025

[16] ENISA. 2022. CSIRT Maturity Framework. https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity. Accessed December 18, 2024.

[17] ENISA. 2024. How to set up CSIRT and SOC | ENISA. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

[18] ENISA. 2024. NIS Directive and national CSIRTs | ENISA. https://www.enisa.europa.eu/publications/nis-directive-and-national-csirts

[19] O. I. Falowo, K. Koshoedo, and M. Ozer. 2023. An Assessment of Capabilities Required for Effective Cybersecurity Incident Management: A Systematic Literature Review. In *Proceedings of the 2023 IEEE International Conference on Digital Security and Privacy (DSPP)*. IEEE, Piscataway, NJ, USA, 1–11. doi:10.1109/DSPP58763.2023.10404318

[20] FIRST.ORG. 2019. FIRST CSIRT Services Framework. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_bugfix1.pdf Accessed: 2024-Nov-23.

[21] FIRST.ORG. 2019. Team Types Within the Context of Services Frameworks. https://www.first.org/standards/frameworks/csirts/team-type_1-0 Accessed: 2024-Nov-23.

[22] Konstantinos Fysarakis, Vasileios Mavroeidis, Manos Athanatos, George Spanoudakis, and Sotiris Ioannidis. 2022. A Blueprint for Collaborative Cybersecurity Operations Centres with Capacity for Shared Situational Awareness, Coordinated Response, and Joint Preparedness. In *Proceedings of the 2022 IEEE International Conference on Big Data (Big Data)*. IEEE, Piscataway, NJ, USA, 2601–2609. doi:10.1109/BigData55660.2022.10020736

[23] Muhammad Haidar, Yudho Giri Sucahyo, Teddy Sukardi, and Arfive Gandhi. 2021. Analysis of CSIRT Services in Facing Cyber Security Challenges in Indonesia. In *Proceedings of the 4th International Conference on Information and Communications Technology (ICOIACT 2021)*. IEEE, Piscataway, NJ, USA, 154–159. doi:10.1109/ICOIACT53268.2021.9563925

[24] Otto Hellwig, Gerald Quirchmayr, Edith Huber, Gernot Goluch, Franz Vock, and Bettina Pospisil. 2016. Major Challenges in Structuring and Institutionalizing CERT-Communication. In *Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES 2016)*. IEEE, Piscataway, NJ, USA, 661–667. doi:10.1109/ARES.2016.57

[25] Allen Householder and Jonathan Spring. 2022. *A State-Based Model for Multi-Party Coordinated Vulnerability Disclosure (MPCVD)*. Technical Report. Carnegie Mellon University. doi:10.1184/R1/16416771.v1

[26] Margaret Jack and Steven J. Jackson. 2016. Logistics as Care and Control: An Investigation into the UNICEF Supply Division. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 2209–2219.

[27] Georgia Killcrece, Klaus-Peter Kossakowski, Robin M. Ruefle, and Mark Zajicek. 2018. Organizational Models for Computer Security Incident Response Teams (CSIRTs). doi:10.1184/R1/6575921.v1

[28] Iacovos Kirlappos, Simon Parkin, and Martina Angela Sasse. 2014. Learning from "Shadow Security": Why Understanding Non-Compliance Provides the Basis for Effective Security. In *Workshop on Usable Security (USEC 2014)*. Internet Society, Reston, VA, USA, 1–8. doi:10.14722/usec.2014.23007

[29] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT security: Accountabilities, moralities, and oscillations in IT security practices. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.

[30] Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. 2019. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, New York, NY, USA, 1955–1970.

[31] Olaf Kruidhof. 2014. Evolution of National and Corporate CERTs – Trust, the Key Factor. In *Best Practices in Computer Network Defense: Incident Detection and Response*. IOS Press, Amsterdam, The Netherlands, 81–96. doi:10.3233/978-1-61499-372-8-81

[32] Frank Li, Zakir Durumeric, Jakub Czyz, Mohammad Karami, Michael Bailey, Damon McCoy, Stefan Savage, and Vern Paxson. 2016. You've Got Vulnerability: Exploring Effective Vulnerability Notifications. In *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, Austin, TX, 1033–1050. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/li

[33] Frank Li, Grant Ho, Eric Kuan, Yuan Niu, Lucas Ballard, Kurt Thomas, Elie Bursztein, and Vern Paxson. 2016. Remedying Web Hijacking: Notification Effectiveness and Webmaster Comprehension. In *Proceedings of the 25th International World Wide Web Conference (WWW 2016)*. ACM, New York, NY, USA, 1007–1016.

[34] Chanel Macabante, Sherry Wei, and David Schuster. 2019. Elements of Cyber-Cognitive Situation Awareness in Organizations. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 63, 1 (2019), 1624–1628. arXiv:https://doi.org/10.1177/1071181319631483 doi:10.1177/1071181319631483

[35] Stuart Madnick, Xitong Li, and Nazli Choucri. 2009. Experiences and Challenges with Using CERT Data to Analyze International Cyber Security. doi:10.2139/ssrn.1478206

[36] Shrirang Mare, Mary Baker, and Jeremy Gummeson. 2016. A Study of Authentication in Daily Life. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 189–206. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/mare

[37] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 1–23. doi:10.1145/3359174

[38] Ola Aleksandra Michalec, Dirk van der Linden, Sveta Milyaeva, and Awais Rashid. 2020. Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding Policy Implementation Practices across Critical Infrastructures. In *Proceedings of the Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Berkeley, CA, USA, 301–317. https://www.usenix.org/conference/soups2020/presentation/michalec

[39] S. R. B. Mohd Kassim, S. Li, and B. Arief. 2023. Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions. *Digital Threats: Research and Practice* 4, 3 (2023), 18 pages. doi:10.1145/3609230

[40] Stuart Murdoch and Nick Leaver. 2015. Anonymity vs. Trust in Cyber-Security Collaboration. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security* (Denver, Colorado, USA) *(WISCS '15)*. Association for Computing Machinery, New York, NY, USA, 27–29. doi:10.1145/2808128.2808134

[41] Ali Naseri and Omid Azmoon. 2012. Proposition of model for CSIRT: Case study of telecommunication company in a province of Iran. *International Journal of Computer Science Issues (IJCSI)* 9, 1 (2012), 156.

[42] Nationaal Cyber Security Centrum (NCSC-NL). n.d.. Over MijnNCSC. https://www.ncsc.nl/aansluiten-en-samenwerken/mijnncsc/over-mijnncsc. Accessed September 11, 2025.

[43] Nationaal Cybersecurity Centrum (NCSC). 2025. Ondersteuning bij cyberincidenten – Als sectoraal CSIRT. https://www.ncsc.nl/documenten/factsheets/2025/februari/11/ondersteuning-bij-cyberincidenten---voor-nis2-organisaties. Accessed April 22, 2025.

[44] Justin Novak, Brittany Manley, David McIntire, Sharon Mudd, Angel Hueca, and Tracy Bills. 2021. The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities. Carnegie Mellon University, Software Engineering Institute's Digital Library. https://doi.org/10.1184/R1/13624148 Accessed: 2024-Sep-23.

[45] Justin Novak, Brittany Manley, David Mcintire, Sharon Mudd, Angel Hueca, and Tracy Bills. 2021. The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities.

[46] The White House Office of the Press Secretary. 2016. Presidential Policy Directive – United States Cyber Incident Coordination. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[47] Anthony J. Onwuegbuzie, Wendy B. Dickinson, Nancy L. Leech, and Annmarie G. Zoran. 2009. A Qualitative Framework for Collecting and Analyzing Data in Focus Group Research. *International Journal of Qualitative Methods* 8, 3 (2009), 1–21. arXiv:https://doi.org/10.1177/160940690900800301 doi:10.1177/160940690900800301

[48] Andreas Oster, Eivor Wiking, Gunnar H. Nilsson, and Christina B. Olsson. 2024. Patients' expectations of primary health care from both patients' and physicians' perspectives: a questionnaire study with a qualitative approach. *BMC Primary Care* 25, 1 (April 2024), 128. doi:10.1186/s12875-024-02389-2

[49] Eric Pauley, Paul Barford, and Patrick McDaniel. 2023. The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits against Two Years of Zero-Days. In *Proceedings of the 2023 ACM on Internet Measurement Conference* (Montreal QC, Canada) *(IMC '23)*. Association for Computing Machinery, New York, NY, USA, 236–252. doi:10.1145/3618257.3624810

[50] Prashanth Rajivan and Nancy Cooke. 2017. *Impact of team collaboration on cybersecurity situational awareness*. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10030. Springer Verlag, Germany, 203–226. doi:10.1007/978-3-319-61152-5_8

[51] Kristin Repchick, Stephen Zaccaro, Lois Tetrick, Julie Steinke, Daniel Shore, Carolyn Winslow, Amber reecho, Hargrove, Balca Alaybek, Jennifer Green, Tracy McCausland, and Alan Tomassetti. 2016. Improving social maturity of cybersecurity incident response teams.

[52] Thea Riebe, Marc-André Kaufhold, and Christian Reuter. 2021. The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 478 (Oct. 2021), 30 pages. doi:10.1145/3479865

[53] Mario Saraiva and Nuno Mateus-Coelho. 2022. CyberSoc Framework a Systematic Review of the State-of-Art. *Procedia Computer Science* 204 (2022), 961–972. doi:10.1016/j.procs.2022.08.117 Publisher Copyright: © 2022 Elsevier B.V.. All rights reserved.; 2022 International Conference on Industry Sciences and Computer Science Innovation, iSCSi 2022 ; Conference date: 09-03-2022 Through 11-03-2022.

[54] Vilja Steffensen and Vahiny Gnanasekaran. 2024. Information Sharing between the Computer Security Incident Response Team and its Members: An Empirical Study. *Norsk IKT-konferanse for forskning og utdanning* 3, 3 (Nov. 2024), n/a pages. https://www.ntnu.no/ojs/index.php/nikt/article/view/6250

[55] Julie Steinke, Balca Bolunmez, Laura Fletcher, Vicki Wang, Alan J. Tomassetti, Kristin M. Repchick, Stephen J. Zaccaro, Reeshad S. Dalal, and Lois E. Tetrick. 2015. Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. *IEEE Security and Privacy* 13, 4 (jul 2015), 20–29. doi:10.1109/MSP.2015.71

[56] Don Stikvoort. 2015. SIM3: Security Incident Management Maturity Model. https://cybilportal.org/publications/sim3-security-incident-management-

maturity-model/ Accessed: 2024-09-23.
[57] Ben Stock, Giancarlo Pellegrino, Christian Rossow, Martin Johns, and Michael Backes. 2016. Hey, you have a problem: on the feasibility of large-scaleweb vulnerability notification. In *Proceedings of the 25th USENIX Conference on Security Symposium* (Austin, TX, USA) *(SEC'16)*. USENIX Association, USA, 1015–1032.
[58] Sathya Chandran Sundaramurthy, John McHugh, Xinming Simon Ou, S. Raj Rajagopalan, and Michael Wesch. 2014. An Anthropological Approach to Studying CSIRTs . *IEEE Security & Privacy* 12, 05 (Sept. 2014), 52–60. doi:10.1109/MSP.2014.84
[59] Abbas Tashakkori and Charles Teddlie. 2003. *Handbook of Mixed Methods in Social & Behavioral Research*. SAGE Publications, Thousand Oaks, CA, USA. https://books.google.nl/books?id=F8BFOM8DCKoC
[60] The Shadowserver Foundation. n.d.. The Shadowserver Foundation. https://www.shadowserver.org/. Accessed April 28, 2025.
[61] U.S. Department of Homeland Security. 2024. *FY 2024 Annual Performance Report, Appendix D: Measure Descriptions, Data Collection Methodologies, and Completeness and Reliability Information.* Annual Performance Report. U.S. Department of Homeland Security. https://www.dhs.gov/sites/default/files/2025-01/2025_0117_dhs_annual_performance_report_fy2024_appendixd.pdf Appendix D, p. 25.
[62] Christine Utz, Matthias Michels, Martin Degeling, Ninja Marnau, and Ben Stock. 2023. Comparing Large-Scale Privacy and Security Notifications. In *Proceedings on Privacy Enhancing Technologies*. Sciendo, Warsaw, Poland, 1–25. https://publications.cispa.saarland/3918/ ISSN: 2299-0984.
[63] Rick van der Kleij, Geert Kleinhuis, and Heather Young. 2017. Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Frontiers in Psychology* 8 (2017), 194. https://www.frontiersin.org/articles/10.3389/fpsyg.2017.00194
[64] Veerle van Harten, Carlos Hernandez Ganan, Michel van Eeten, and Simon Parkin. 2025. "All Sorts of Other Reasons to Do It": Explaining the Persistence of Suboptimal IoT Security Advice. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 387, 19 pages. doi:10.1145/3706598.3713719
[65] Koen van Hove, Jeroen van der Ham-de Vos, and Roland van Rijswijk-Deij. 2023. Your Vulnerability Disclosure Is Important To Us: An Analysis of Coordinated Vulnerability Disclosure Responses Using a Real Security Issue. arXiv:2312.07284 [cs.NI] https://arxiv.org/abs/2312.07284
[66] YM Wara and D Singh. 2015. A guide to establishing computer security incident response team (CSIRT) for national research and education network (NREN). *African Journal of Computing & ICT* 8, 2 (2015), 1–8.
[67] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. 1998. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, USA.
[68] Johannes Wiik, Jose Gonzalez, and Klaus-Peter Kossakowski. 2006. Effectiveness of Proactive CSIRT Services. In *Proceedings of the TF-CSIRT Meeting 2006*. TERENA, Innsbruck, Austria, 67–81.
[69] Julia Wunder, Alan Corona, Andreas Hammer, and Zinaida Benenson. 2024. On NVD Users' Attitudes, Experiences, Hopes, and Hurdles. *Digital Threats* 5, 3, Article 33 (Oct. 2024), 19 pages. doi:10.1145/3688806
[70] Rei Yamagishi, Shota Fujii, Shingo Yasuda, Takayuki Sato, and Ayako A. Hasegawa. 2025. Collaborative Work in Malware Analysis: Understanding the Roles and Challenges of Malware Analysts. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 865, 15 pages. doi:10.1145/3706598.3713652
[71] Orçun Çetin, Mohammad Hanif Jhaveri, Carlos Gañán, Michel van Eeten, and Tyler Moore. 2016. Understanding the role of sender reputation in abuse reporting and cleanup. *Journal of Cybersecurity* 2, 1 (12 2016), 83–98. arXiv:https://academic.oup.com/cybersecurity/article-pdf/2/1/83/10833175/tyw005.pdf doi:10.1093/cybsec/tyw005

Interview Protocol

The interview protocol in Table 10 followed a general structure across all interviews. Note that we asked participants to articulate a list of CSIRT services. The section "Experiences per Service X", was repeated for each articulated service.

Minor variations in which questions were asked were introduced depending on the stakeholder group: governance, CSIRT staff, and constituents. It also presents the generic protocol and indicates which stakeholder groups received each question. A value of "Yes" means the question was asked of that group. "No" means the question was not asked. Some questions were slightly rephrased depending on the stakeholder group.

The interview protocol for other sector CSIRT practitioners, depicted in Table 11, is almost identical, except for the organization name reference.

Codes

Table 10: Interview protocol with stakeholder-specific variations

Section	Question	Const.	CSIRT	Gov.
Introduction	Can you tell me about yourself and your role?	✓	✓	✓
	What does a typical day look like?	✓	✓	✓
Expectations of IBD	In what capacity are you dealing with the IBD?	✓	✗	✓
	How would you describe that interaction?	✓	✗	✓
	What are your/the expectations of the services provided by the IBD?	✓	✓	✓
	What services are you using/providing, and has that changed over time?	✓	✓	✓
Experiences per Service X	For service X, how is it used?	✓	✓	✗
	For service X, what challenges are you facing?	✓	✓	✓
	For service X, has that changed over time?	✓	✓	✗
Missing Services	What services are you missing?	✓	✗	✗
Outro	What didn't we ask that we should have asked?	✓	✓	✓

"Gov." = governance stakeholders; "Const." = constituents; "CSIRT" = IBD staff.

Table 11: Interview protocol for practitioners at other sector CSIRTs

Section	Question
Introduction	Can you tell me about yourself and your role?
	What does a typical day look like?
Expectations of {ORG}	What do you think are the expectations of the services provided by {ORG}?
	What services are you providing, and has that changed over time?
Experiences per Service X	For service X, how is it used?
	For service X, what challenges are you facing?
	For service X, has that changed over time?
Outro	What didn't we ask that we should have asked?

{ORG} denotes the specific CSIRT organization, depending on interviewee context.

Table 12: Full Codebook (Services — Incident Response and Advisories)

Group	Theme	Subcode	Description
Services	Incident Response	Incidents	Participants explaining incidents they did or did not encounter and the value of the CSIRT during
		Boots-on-the-ground	Participants explaining their expectations of the CSIRT during an incident
		Responsibilities	Participants explaining who does what during an incident
		Communication	Participants explaining how they communicate about this service
		Technical Capabilities and Resources	Participants explaining the expected and actual available technical capabilities and resources to handle incidents
		Incident Reporting and Regulation	Participants explaining if and how they report incidents to the CSIRT, and the regulatory context (NIS2 and BIO) for these processes
	Advisories	Acting on Advisories	Participants describing the value of advisories and how they are acted upon
		Software Inventory and Reporting	Participants explaining how the inventories of their software are managed and reported to the CSIRT.
		Timeliness	Participants describing the timeliness of advisories
		Frequency	Participants describing how often they receive advisories
		False Positives	Participants describing the problem of false positives in whether or not they are running vulnerable software
		Internal Decision-making	Participants describing the role of advisories in internal decision-making processes

Table 13: Full Codebook (Services — Expert Insights and Vulnerability Notifications)

Group	Theme	Subcode	Description
Services	Expert Insights	Operationalization Issues	Participants describing their difficulties in providing and maintaining templates of knowledge products
		Recipient Diversity	Participants describing the difficulties of tailoring the level of detail of products for mixed maturity levels of constituents
		Quality	Participants describing the value and quality of the service
		Legal Issues	Participants explaining legal issues in offering templates for certain processes
		Implementation Issues	Participants describing the difficulties in implementing the templates into actual processes within their organization
	Vulnerability Notifications	Asset Inventory	Participants describing the state of their current asset inventory
		Reporting Assets	Participants explaining the reporting process of their asset inventory to the CSIRT
		Frequency	Participants describing the value and frequency of vulnerability notifications
		Process	Participants describing their process to collect and update their asset inventory
		Responsible Disclosures	Participants describing the value, difficulties, and process of handling incoming responsible disclosures

Table 14: Full Codebook (Services — Intelligence Sharing and Outreach)

Group	Theme	Subcode	Description
Services	Intelligence Sharing	Types	Participants describing the value of different kinds of intelligence
		Frequency	Participants describing that they often received shared intelligence
		Visibility	Participants describing that intelligence puts the CSIRT on their radar as a supportive organization
		Reputation	Participants describing the reputation of the CSIRT or fearing their own reputation in sharing back
	Outreach and Community	Knowing Constituents	Participants describing the value of personal relations and the importance of knowing the constituency and the CSIRT staff
		Building Trust	Participants describing the role of this service to increase trust with the CSIRT and among constituents
		Community Facilitation	Participants describing efforts and initiatives to bring constituents together

Table 15: Full Codebook (Practitioner Organizational Challenges)

Group	Theme	Subcode	Description
Practitioner Organizational Challenges	Governance structure and stakeholders	Mandate and structure	Practitioners describing the CSIRT mandate and/or their organizational structure
		Organizational dependencies	Practitioners describing their interactions and/or dependencies on other organizations in providing their services
		Trust	Participants describing the value and necessity of trust to share information
		Constituent population	Participants describing their constituent population
	Infrastructure and capability management	Infrastructure and asset management	Participants describing their infrastructure and related (management) processes.
		Internal and external security services	Participants describing their security services and related processes