How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study

Received (in revised form): 28th October, 2021

Sharifah Roziah Binti Mohd Kassim

PhD Student, University of Kent, UK

Sharifah Roziah Binti Mohd Kassim is a second year PhD Computer Science student at the School of Computing, University of Kent, UK, focusing research in the area of cyber security. Sharifah is also a Specialist in Malaysia Computer Emergency and Response Team (MyCERT) under the umbrella of CyberSecurity Malaysia, a registered and semi-government entity in Malaysia. Her research interest is primarily in computer security incident response and cyber threat intelligence. Sharifah has authored four papers and co-authored one paper on cyber security topic prior to pursuing her PhD.

Institute of Cyber Security for Society (iCSS) and School of Computing, Keynes College, University of Kent, Canterbury CT2 7NP, UK
Tel: +44 1227 827754; E-mail: sm2212@kent.ac.uk

Shujun Li

Professor of Cyber Security, University of Kent, UK

Shujun Li is a Professor of Cyber Security at the School of Computing, University of Kent in the UK. He is the Director of the Institute of Cyber Security for Society (iCSS), which represents the University of Kent as one of 19 UK government recognised Academic Centres of Excellence in Cyber Security Research (ACEs-CSR). His research interests are mostly around interdisciplinary topics covering cyber security and privacy, human factors, digital forensics and cybercrime, social media analytics, and AI. He has published over 100 research papers at international journals and conferences, and received three Best Paper Awards (at IIEEK IEVC 2012, HAS 2017 and HICSS 2021) and a Honourable Mention (at ICWSM 2020). He published a monograph on cognitive modelling (Springer 2020), and co-edited four books including Handbook of Digital Forensics of Multimedia Data and Devices (John Wiley & Sons, Inc. and IEEE Press 2015). In 2012, he received an ISO/IEC Certificate of Appreciation, for being the lead editor of ISO/IEC 23001-4:2011, the 2nd edition of the MPEG RVC (Reconfigurable Video Coding) standard. He is currently on the editorial boards of a number of international journals, and has been on the organising or technical program committees of over 100 international conferences and workshops. He is a Fellow of BCS, a Senior Member of IEEE, and a Member of ACM. He is a Vice President and Founding Co-Director of the ABCP (Association of British Chinese Professors). More about his research and professional activities can be found at his personal website http://www.hooklee.com/

Institute of Cyber Security for Society (iCSS) & School of Computing, Keynes College, University of Kent, Canterbury CT2 7NP, UK
Tel: +44 1227 823821; E-mail: s.j.li@kent.ac.uk

Budi Arief

Senior Lecturer, University of Kent, UK

Budi Arief is a Senior Lecturer at the School of Computing, and the Innovation Lead at the Institute of Cyber Security for Society (iCSS), both at the University of Kent, UK. His research interests are in cybercrime, the security and dependability of computer-based systems, ransomware, and the Internet of Things, with a strong overarching element of interdisciplinary research. So far, he has published over 50 research papers in the areas of computer security (especially in the topics of ransomware, the Internet of Things, and human factors), dependability, and Intelligent Transport Systems, leading to 1,300+ Google Scholar citations with h-index of 15.

Institute of Cyber Security for Society (iCSS) & School of Computing, Keynes College, University of Kent, Canterbury CT2 7NP, UK
Tel: +44 1227 816797; E-mail: B.Arief@kent.ac.uk

Abstract Computer security incident response teams (CSIRTs) have been established at national and organisational levels to coordinate responses to computer security incidents. It is known that many CSIRTs, including national CSIRTs, routinely use public data, open-source intelligence (OSINT) and free tools in their work. The current literature, however, lacks research on how such data and tools are used and perceived by the staff of national CSIRTs in their operational practices. To fill such a research gap, an online survey and 12 follow-up semi-structured interviews with staff of 13 national CSIRTs from Asia, Europe, Caribbean and North America were carried out. The aim was to gain detailed insights on how such data and tools are used and perceived by staff in national CSIRTs. The study was conducted in two stages: first with MyCERT (Malaysia's national CSIRT) to gain some initial results, and then with 12 other national CSIRTs to expand the results from the first stage. Thirteen participants from MyCERT completed the survey and seven of them took part in a semi-structured interview; 12 participants from 11 other national CSIRTs took the survey and five participants from five national CSIRTs were interviewed. Results from the survey and the interviews led to three main findings. First, the active use of public data, OSINT and free tools by national CSIRT staff was confirmed, eg all 25 participants had used public data for incident investigation. Second, all except two (ie 23 out of 25, 92 per cent) participants perceived public data, OSINT and free tools to be useful in their operational practices. Third, there are a number of operational challenges regarding the use of public data, OSINT and free tools. In particular, there is a lack of standard and systematic approaches on how such data and tools are used across different national CSIRTs. There is also a lack of standard and systematic processes for validating such data and tools. These findings call for further research and development of guidelines to help CSIRTs to use such data and tools more effectively and more efficiently.

KEYWORDS: CSIRT, computer security incident response team, national CSIRT, CERT, computer emergency response team, staff, perception, cyber incident, public data, OSINT, open-source intelligence, free tool

INTRODUCTION

Nowadays, computer and network security incidents are happening frequently on a large scale, affecting organisations, citizens and critical information infrastructures. While preventive measures — such as applying security updates, performing backups and regular network security inspection — are important, it is not sufficient to rely solely on them. Instead, efficient handling of computer security incidents is equally important.[1] This means that it is necessary to create and maintain dedicated teams of professional cyber security analysts to detect, mitigate and help organisations recover from computer security incidents.[2]

To this end, computer security incident response teams (CSIRTs) have been widely established. They are formed within different types of organisation, such as those in governmental, military, critical infrastructure, academic and business sectors.[3] Their services include reactive services,[4] incident management,[5,6] proactive services such as monitoring, vulnerability handling[7–9] and information sharing within the team.[10] Among all CSIRTs, national CSIRTs play a critical role in protecting a nation's infrastructure from cyberattacks[11–13] through computer security incident handling,[14] similar to the role of fire brigade emergency services.[15,16] National CSIRTs were highlighted by the Pan-European Cooperation Commission in 2009, which requested its member states and concerned stakeholders to ensure that national CSIRTs

act as the key component of national capability for preparedness, information sharing, coordination and response, and that they may be tasked to lead national contingency planning and exercises.[17]

In 2016, the European Parliament and the European Council passed the EU NIS Directive,[18] which requires EU member states to have well-functioning CSIRTs 'complying with essential requirements to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level'. In addition, Article 12 of the EU NIS Directive also mandates cross-border collaboration between EU member states, including the pan-EU CSIRTs Network.[19] Worldwide, as more and more countries and regions have created their national CSIRTs, the UN body International Telecommunication Union (ITU) is actively helping countries to establish national CSIRTs.[20,21] In this paper, the term 'nation' is used to refer to an administrative region with its own dedicated 'national' CSIRT, which may be a nation, a state or a province of a nation, a self-governing region (eg Hong Kong) or an inter-governmental union (eg European Union).

In supporting their operations, CSIRTs normally have access to data and investigative tools from various closed-source origins. This includes self-reported incident data or evidence from victims (including organisations and citizens), law enforcement agencies (LEAs), as well as from trusted partners such as collaborating CSIRTs; however, these closed-source data and tools are often insufficient for staff of CSIRTs to conduct their investigations effectively. For instance, the first author of this paper — a member of staff within the Malaysia CSIRT (MyCERT) — observed that the availability of closed-sourced data and commercial investigative tools in national CSIRTs is limited. Therefore, CSIRTs often need to resort to public data, open-source intelligence (OSINT) and free tools available on the Internet for additional intelligence to support incident responses. Some CSIRTs also actively develop their own tools to support incident response, or even advocating their use and sharing them for free on the Internet.[22–25]

Nonetheless, a systematic open discussion with regard to how public data, OSINT and free tools are being used in national CSIRTs' operations is lacking in the current research literature. Additionally, the first author's observation within MyCERT indicates that public data, OSINT and free tools are not utilised systematically in the operations. Therefore, the present study aims to investigate this identified research gap by exploring how public data, OSINT and free tools are used and perceived by staff in national CSIRTs' operations.

Terminology

Throughout this paper, the following terms are used to define the scope of the study more precisely:

- 'Public data': Data that is available to the general public for free[26] on the Internet;
- 'Closed-source data': Non-public (ie private or confidential) data that belongs to victims and organisations who report cyber incidents or provide information to CSIRTs;
- 'OSINT tools': Software tools and online services that are used specifically to facilitate and extract cyber threat intelligence (CTI) from open-source (ie public) data;
- 'Free tools': Software tools and online services that are available for free (freeware or open-source software) to help investigate cyber incidents;
- 'CSIRT staff': Employees of national CSIRTs who are involved in daily handling of incidents in the operations, involving analysts, team leaders and executives who have knowledge of how incidents are responded in their operations;

- 'Cyber incidents': 'Any event having an actual adverse effect on the security of network and information systems' (definition in Article 4 of the EU NIS Directive[27]).

Research questions (RQs)

Two main research questions for this study are:

- RQ1: What are the current operational practices in national CSIRTs regarding the use of public data, OSINT and free tools?;
- RQ2: How do staff of national CSIRTs perceive the usefulness of public data, OSINT and free tools in their operational practices?

Contributions

The main contributions of the study are:

1. Detailed insights on how public data, OSINT and free tools are used in operational practices across different national CSIRTs;
2. Empirical evidence confirming that national CSIRT staff perceive that public data, OSINT and free tools are useful to facilitate investigations of incidents;
3. A number of identified operational challenges faced by national CSIRTs, the knowledge of which can help guide future research and development in this area.

The rest of this paper is organised as follows. The second section provides an overview of previous work on the use of public data, OSINT and free tools in CSIRTs' operations. The subsequent section explains the methodology used in the study, which includes an online survey and a number of semi-structured interviews. This is followed by the results and findings from the study, and a discussion of the overall study findings. The study concludes with some suggestions for future research.

RELATED WORK

Jaatun *et al.*[28] conducted a survey and semi-structured interviews, in the context of the Norwegian petroleum CSIRT, to study capacity issues in responding to security incidents within the petroleum industry. Their study found that participants were relatively satisfied with their own CSIRT capacity, but they believed it could be improved through better communication among CSIRT staff and other key people in the industry, as well as through having dedicated information-sharing platforms.

Werlinger *et al.*[29] investigated incident response practices in the academic, governmental and private sectors using semi-structured interviews. They found that incident response is a highly collaborative work, which very often requires practitioners to develop in-house tools for diagnostics and detection of incidents tasks. Furthermore, detection of incidents is complicated, requiring expertise on the part of the staff, as well as effective support from usable and reliable security tools. Even though the study was not precisely about national CSIRT operations, it provides some insights into general incident response practices and the common problems that might be encountered.

Mana and Friligkos[30] investigated the incident handling practices of Eurocontrol Air Traffic Management's computer emergency response team (EUROCONTROL/EATM-CERT). They found that threat data and other threat information needed for incident response are actively shared among internal CSIRTs within the EATM-CERT and with several national CSIRTs in Europe, benefiting from using an automated tool such as Malware Information Sharing Platform (MISP).[31]

Grispos *et al.*[32] conducted an empirical study on the practices of CSIRTs within a Global Fortune 500 organisation with a focus on incident learning. The study focused on the data quality that is needed for post-incident learning but did not delve into

the types of data that would be needed for effective investigation, which might implicate the learning process from incidents as well.

A study by Line *et al*.[33] looked into the incident response teams of several industrial control system organisations and found that documented plans, policies and procedures required to support effective incident management process did not exist in the organisations participated in the study. Participants mainly relied on their tacit knowledge to respond to incidents; they felt this to be sufficient, as long as the staff responsible for incident handling are available during an incident.

Kijewski and Kozakiewicz[34] emphasised the importance of threat detection tools, honeynets, classified and closed-source data for CSIRTs to handle and detect cyber threats more efficiently and timely. They did not, however, highlight how public data, OSINT or free tools have been or can be used to improve detection and response in CSIRT operations.

Tøndel *et al*.[35] conducted a systematic literature review of incident response practices of various organisations and found that the incident response processes identified from the literature are in accordance with the incident management phases defined in the ISO/IEC 27035:2011 standard. (Note that ISO/IEC 27035:2011[36] has been revised by ISO/IEC 27035-1:2016[37]and ISO/IEC 27035-2:2016.[38]) They highlighted the importance of tools support for investigations and the need for automation in the practices but did not elaborate further on how incident response staff perceived the usefulness of such tools.

Public data has long been used to enrich closed-source data in many applications, eg to facilitate crime investigation by LEAs to obtain timely, reliable and actionable intelligence,[39,40] for efficient business decision making to increase product sales,[41] and to monitor the spread of viruses in medical situations.[42,43] Digital forensic intelligence uses public data to obtain intelligence because it is 'fast, flexible, dynamic, communicable, shareable and partner forming'.[44] In a similar way, OSINT tools, free tools and online services have a great potential to make a positive contribution to incident investigation — for example, to collect information about possible cyber threats and breach of other sensitive data due to cyberattacks. They can even be used to inspect threats against critical infrastructures,[45] to simulate how cybercriminals would conduct cyberattacks — an understanding of which would help in mitigating such threats,[46] to improve cyber security posture in organisations,[47] to improve search for novel information when combined with Google search,[48] for background checks during job hire and to verify authenticity of students' assignment,[49] and to track cybercriminals' activities at their early stage.[50]

The main argument here is that most of the studies in the current literature focused on CSIRT practices of *organisational* rather than *national* CSIRTs. Furthermore, these studies were mainly published before 2017, and as such, they do not reflect the state-of-art of the present threat landscape and operational challenges. More than half of these studies are about information sharing, coordinating cyber incidents and management practices of CSIRTs. Very little work was done on how incidents are investigated with the use of public data, OSINT and free tools. Other researchers have also observed that the topic of CSIRTs is still under-represented in the academic research, due to the novelty of the topic itself,[51] suggesting the need for more empirical studies in this field to gain more insights[52] and to explore the many areas within this topic for a more comprehensive understanding of the computer security incident response practices.[53] Therefore, the lack of studies focusing on public data, OSINT, free tools used in national CSIRTs calls for more research into the real-world practices of national CSIRTs and operational

challenges they are facing, particularly on how public data, OSINT and free tools can help address such challenges.

METHODOLOGY

A mixed method was used for this study, including an online survey and a number of semi-structured interviews, similar to some other previous studies.[54–56] The data was analysed following a mix of quantitative and qualitative approaches. This study received a favourable opinion from the ethics board of the authors' institution, under reference number 0621920. Participants gave their consent to include their direct quotations in research publications and reports as long as their personal information is not disclosed.

Recruitment of participants

The intended participants for the study are staff who respond to incidents and staff who have knowledge of how incidents are responded to in national CSIRTs. In the first stage, 16 participants from MyCERT were recruited via e-mails through a gatekeeper to focus the study on the operations in a single national CSIRT only. MyCERT was chosen since the first author of the paper is an employee of MyCERT so has direct access to staff, thus making the recruitment easier. Thirteen participants agreed to participate in the survey, while seven of them agreed to participate in a semi-structured interview. In the second stage, participants from other national CSIRTs were recruited through the first author's contact with CERT/CC of Carnegie Mellon University, USA. The purpose was to expand and validate findings from the first stage. In total, 12 employees of 11 other national CSIRTs participated in the online survey and one each from five other national CSIRTs participated in a follow-up interview. This second stage allowed the collection of viewpoints and perspectives from a more diverse set of national CSIRTs to avoid biases observed from a single CSIRT (MyCERT). The numbers of participants in the two stages and the two data collection methods, and the national CSIRT they belong to, are listed in Table 1.

Table 1: The numbers of participants from different national CSIRTs and their breakdown into the two stages and two data collection methods

Stage	National CSIRT	Website	No. of participants	
			Survey	Interviews
1	MyCERT (Malaysia)	https://www.mycert.org.my/	13	7
2	CERT.at (Austria)	https://www.cert.at/	1	1
	BGD e-GOV CIRT (Bangladesh)	https://www.cirt.gov.bd/	1	0
	CSIRT-RD (Dominican Republic)	https://cncs.gob.do/	1	0
	CERT-FR (France)	https://www.cert.ssi.gouv.fr/	0	1
	JPCERT/CC (Japan)	https://www.jpcert.or.jp/	1	0
	CERT-PH (Philippines)	https://www.ncert.gov.ph/	1	1
	Sri Lanka CERT/CC (Sri Lanka)	https://www.cert.gov.lk/	1	1
	INCIBE-CERT (Spain)	https://www.incibe-cert.es/	1	0
	SWITCH-CERT (Switzerland)	https://www.switch.ch/	1	1
	TwCERT/CC (Taiwan)	https://www.twcert.org.tw/	1	0
	US-CERT (USA)	https://us-cert.cisa.gov/	1	0
	One anonymised national CSIRT		2	0
Total			25	12

Online survey

The survey was conducted using Typeform,[57] a subscription-based online survey platform. The survey questionnaire consists of 23 questions in three sections:

- Section A asks information about participants' work experience and job scope to help contextualise their answers to other questions and what they said in the follow-up interview;
- Section B is about the type of data and OSINT tools used in the operational practices and how useful they are, as perceived by staff;
- Section C tries to capture information on operational challenges at national CSIRTs, on the use of public data and OSINT tools.

Some questions have multiple choices, but often with an 'other' option and an open-ended text box for participants to provide further details. Some other questions are completely open-ended so participants can fill in what they see fit. The questions used in the survey are listed in Appendix A.

Semi-structured interviews

Semi-structured interviews were used in the study to draw out more detailed insights from CSIRT staff through interactive discussions.[58] The interview schedule consisted of 25 general questions about participants' basic information, how public data, OSINT and free tools are used by CSIRT staff and challenges faced by the participants in their work (see Appendix B). Each interview took about an hour to complete. The order of the interview questions and the topics were flexible, whereby interviewees were allowed to highlight any other relevant new topics. All interviews took place virtually on an online video meeting platform chosen by the participants: six on WhatsApp, four on Zoom, one on Google Meet and one on Microsoft Teams. All interviews were audio-recorded with permission from participants, and the interviewer (the first author) also took notes of key points during the interviews.

Data analysis

The survey data was analysed mainly using a quantitative approach, based on descriptive-statistics analysis that summarises and categorises the data into numeric form of figures and percentages. Some qualitative analysis was also done by synthesising the overall responses from all participants.

The results from the online survey were used to inform the qualitative analysis of the interview data, from which the main findings were drawn.

In the semi-structured interview, the 12 interview recordings were transcribed manually, with each transcript labelled with the corresponding CSIRT's name (not the participant's name), in order to respect their privacy. The credibility and accuracy of the transcripts were validated using member checking with the interviewees. The transcripts were loaded into a qualitative analysis software system called Atlas.Ti[59] for subsequent software-aided encoding. A bottom-up qualitative approach[60] with thematic analysis was used to capture important themes or patterns that emerge from the interview data.[61] It involved an iterative process by constantly moving back and forth between the whole interview data set and the code extracts.

A descriptive-focused encoding scheme[62] was used for the whole coding process. This began with highlighting important quotations or excerpts from the interview data using Atlas.Ti, followed by extracting significant codes from the quotations. The codes describe the data by capturing the interviewees' views or opinions without the interviewer (the first author) putting her view on them, while keeping the research questions in mind.[63,64] The codes were then categorised into smaller code groups based

on their semantic similarities, which were finally used to determine significant themes.

In total, 344 quotations were extracted from the interview data, and 44 codes were derived from the quotations. The 44 codes were sorted into 18 code groups and four themes. In addition, all interviewees were asked to give general background information about their national CSIRT. Such information was not encoded due to its simplicity but summarised from the interview scripts directly. The four themes and the general background of the participating national CSIRTs are described in detail in 'memoing' — a useful step during encoding in qualitative data analysis — which was also used in the analysis stage.[65] Eleven memos with the first author's own observation and reflection about the interview data were produced.

RESULTS AND FINDINGS

In this section, the analysis results of the online survey and the interviews are presented. The results based on data from MyCERT are presented first, followed by results based on data from other national CSIRTs.

Results of online survey

As mentioned before, the survey data was analysed based on descriptive statistics and some qualitative synthesis. The results are shown in different aspects below.

Participant demographics

Thirteen participants from MyCERT and 12 participants from other national CSIRTs participated in the online survey. The 25 participants also included four team leaders and two executives. Note that team leaders are also analysts, but normally with richer experience. The executives are not analysts but people who support analysts. The detailed distribution is shown in Figure 1. All participants had sufficient experience working at national CSIRTs, as shown in Figure 2.

Methods for incident investigation

One survey question asked participants how incidents were investigated at their national CSIRT. This could be manual, semi-automated, automated or the different combinations of the three basic methods. As shown in Figure 3, semi-automated approaches were the most popular, and most participants relied on such approaches partly or fully. No participants reported that they used (fully) automated approaches alone, so this option is not shown in Figure 3. The results from MyCERT participants are largely aligned with those from participants of other national CSIRTs.

Participants' experience with public data

The survey results showed that all 25 participants of the survey had used public data for incident investigations. This indicates

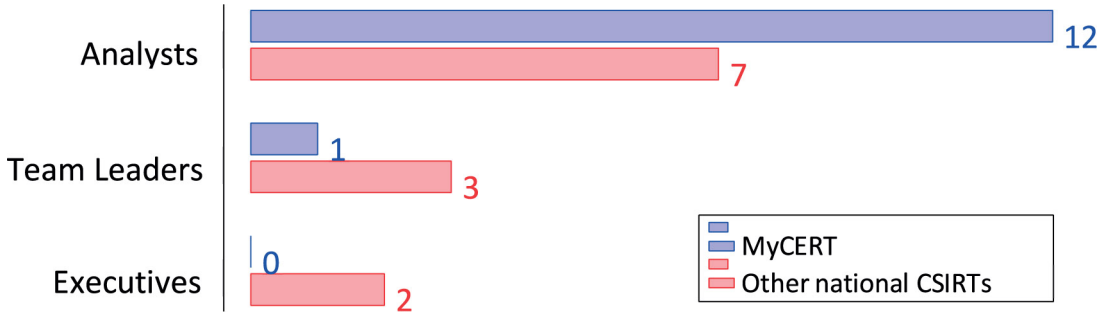

Figure 1: Distribution of survey participants' roles within their national CSIRTs

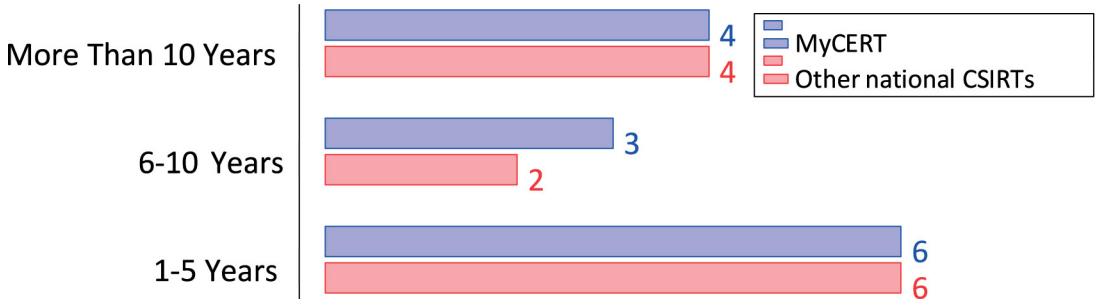

Figure 2: Distribution of survey participants' working experience within national CSIRTs

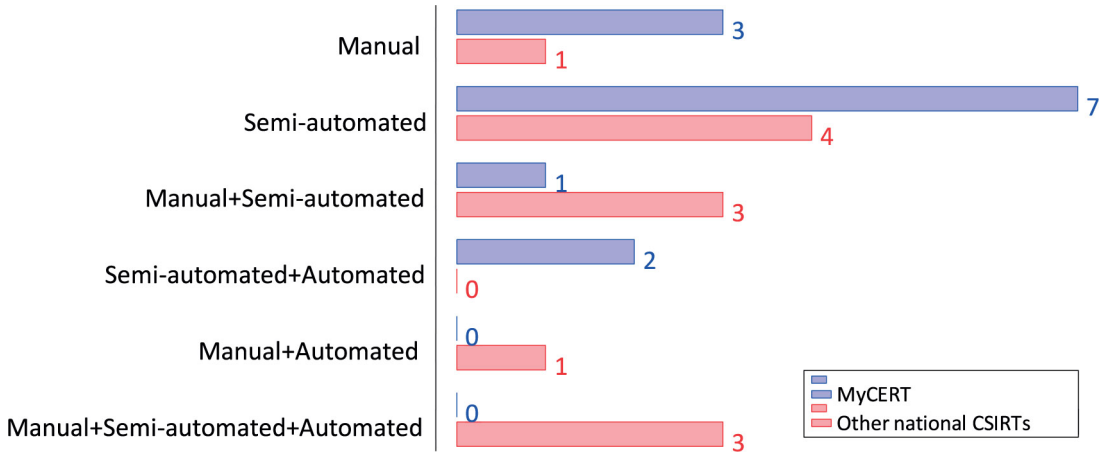

Figure 3: Method for investigating incidents, as reported by participants of the online survey

that public data plays a very important role in the operational practices of national CSIRTs.[66]

Many different types of public data were used by participants. Examples include publicly shared malware samples such as those from Virus Total,[67] publicly disclosed malicious Internet protocol (IP) addresses and uniform resource locators (URLs) of phishing websites, public domain name service (DNS) records, data from search engines such as Google Search, public information from other national CSIRTs, public data from honeypots, ad hoc public data feeds and datasets such as Shodan,[68] Google Hacking Database[69] and Censys,[70] publicly released threat reports by many different organisations, public data on online social media (eg Twitter) and news reports. Some participants also mentioned public application programming interfaces (APIs), sensors deployed in multiple network gateways and domain registry databases, and dark web, without explaining what they referred to exactly.

Notably, all 25 participants reported that they had always validated public data before using them for cyber incident investigation at their national CSIRT.[71] They reported the use of a range of tools and methods for this purpose, including running validation experiments,[72] cross-checking the data with trusted external organisations (eg other national CSIRTs) and people (eg independent cyber security experts and researchers), using third-party validation tools to check the data, and cross-checking the data with other data collected from different platforms.

Participants' experience in using closed-source data

In order to put the use of public data into the right context, the survey also had a question about the use of closed-source data within national CSIRTs. All participants except one from a non-MyCERT national CSIRT reported that they had used closed-source data. This data is from victims and organisations who report incidents and share information with national CSIRTs. The closed-source data used include different types of artefacts from compromised systems, such as system logs, malware samples, digital forensic images, e-mail headers, URLs of phishing websites, malicious IP addresses and domain names, defaced web pages and closed-source intelligence about threats.

All participants from MyCERT and other national CSIRTs reported challenges in analysing closed-source data. According to them, these challenges include a lack of detail about attacks under investigation, a lack of the full context such as the complete history of an incident, incompatible data formats and unstructured data that require bespoke parsing tools,[73] and too much information that requires human experts to interpret the data. Some of the reported challenges have been reported in the literature; eg Grispos *et al*.[74] pointed out that system logs often lack sufficient information for investigation.

Participants' experience with software tools

The survey also asked participants about different types of software tools (including online services) they had used for incident investigation. Participants mentioned both OSINT and non-OSINT tools. They mentioned that the choice of these tools depends on the incident type, the participant's role and expertise. Most OSINT tools used by participants are free, while some are commercial tools for very specific areas of investigation such as digital forensics. Free tools mentioned by participants are listed in Table 2. Some participants did not want to disclose the tools they had used, especially commercial tools, due to the worry of over-disclosing operational practices at their national CSIRTs, so the list is an incomplete list of tools used by national CSIRT staff. Note that some tools were also considered public data sources since their functionalities include or are about providing public data (eg Google Hacking Database).

How participants perceived usefulness of public data and OSINT tools

The survey asked participants how they perceived the usefulness of public data and OSINT tools, on a five-point Likert scale. All except one participant from MyCERT agreed or strongly agreed that public data and OSINT tools are useful in CSIRT operations. The same was observed for participants from other national CSIRTs: 11 out of 12 participants agreed or strongly agreed on the usefulness of public data and OSINT tools. The detailed breakdown statistics are shown in Figure 4.

For another question regarding combining public and closed-source data, a majority (eight out of 13, 62 per cent) participants from MyCERT agreed or strongly agreed that they could often get better results in their analysis by combining public data with closed-source data. A similar trend was observed among participants from other national CSIRTs: nine out of 12 participants (75 per cent) agreed or strongly agreed on the same perception.

Results of semi-structured interviews

The results of the online survey led to some interesting findings, eg all participants used public data, and most participants considered OSINT tools useful. Such findings were further consolidated and extended by the semi-structured interviews. As shown in Table 1, 12 interviewees from six national CSIRTs participated in an interview,

including seven from MyCERT and one from each of five other national CSIRTs. Following the thematic analysis method described later in the paper, the results of the interviews will be discussed around four identified themes:

- *Theme 1*: How national CSIRTs use public data, OSINT and free tools;
- *Theme 2*: How CSIRT staff perceive public data, OSINT and free tools;
- *Theme 3*: Reporting and sharing of information about cyber incidents;
- *Theme 4*: Operational challenges faced by national CSIRTs.

Before the results of the above four themes are presented, the general background (which stemmed from the early discussions with the interviewees) is given to provide the context.

General background of national CSIRTs

At the beginning of all interviews, interviewees were asked to introduce their national CSIRT and their general understanding of operational practices at national CSIRTs.

Most national CSIRTs largely manage and deal with security incidents by using a help desk or a ticketing system. Cyber incidents are responded based on a procedure defined in the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide[75] and the SANS Institute's Six Steps of Incident Handling.[76] Interviewees from MyCERT explained that MyCERT manages incident responses following a three-level tier process, whereby incidents are handled according to three levels of complexity. Similar levels were reported by one interviewee from SWITCH-CERT, one of the two Switzerland's national CSIRTs, where a dedicated team handles complex malware incidents. A participant from CERT-FR (France's national CSIRT) reported that CERT-FR has a dedicated team that focuses on data acquisition and analysis. Interviewees from other national CSIRTs stated that their CSIRTs do not have a similar hierarchy, but plans are in place to develop such levels in their operations.

Interviewees were asked to talk about how their CSIRT classify incidents. This was discussed because CSIRTs often use a predefined incident classification scheme,[77–79] which normally splits cyber incidents into two types: *technical incidents* (such as malicious codes, spams, vulnerability handling, intrusions and intrusion attempts and denial of service attacks) and *non-technical incidents* (such as harassment, content-related and fraud). Interviewees' responses revealed that there is not a single incident classification scheme used by all national CSIRTs. Among the six national CSIRTs, three handle technical incidents only, while the other three handle both technical and non-technical incidents.

Theme 1: How national CSIRTS use public data, OSINT and free tools

This theme focuses on the discussions about the use of public data, OSINT and free tools within national CSIRTs. These interviews are different from the online survey, where questions about free tools were not explicitly asked to avoid any unnecessary confusion. In the interviews, the subtle relationships between OSINT tools and free tools were covered.

Considering the results of the online survey, it is not surprising to see that all seven interviewees from MyCERT reconfirmed the use of public data in their daily incident response work. All participants from MyCERT stated that public data is mainly used to obtain richer (contextual) information and more insights about a particular incident. Apart from facilitating investigations, interviewees said that public data is also used as inputs for the production of security advisories and alerts regarding

new threats (as part of their security awareness activities for the general public).

Similarly, regarding the use of OSINT tools, just over half of the interviewees from MyCERT (four out of seven) used OSINT tools in their incident investigation work, while all the interviewees used free tools (OSINT and non-OSINT tools).

The findings from MyCERT interviewees were confirmed by interviewees from other national CSIRTs. All the five interviewees used public data, OSINT and free tools in their work. Additionally, they used them for very similar reasons and purposes.

Most tools mentioned by other national CSIRTs survey participants were further confirmed in the interviews, eg IntelMQ listed in Table 2 was mentioned by interviewees from CERT.at, SWITCH-CERT and CERT-FR. Some interviewees also mentioned a number of additional free tools, which are listed in Table 3. One interviewee also referred to tools developed by CERT.at, the Austria's national CSIRT, whose GitHub portal[80] lists many tools such as IntelMQ.

Although both the online survey and the semi-structured interviews showed that public data and OSINT and free tools are largely used in the operations, it was observed that such data and tools are often used on an ad hoc basis, without a systematic approach. This problem can be seen from the following quotations from two interviewees:

> 'No, it's done on ad hoc basis.' (Interviewee, CERT.at)

> 'Unfortunately, we don't have a procedure. Not yet. Actually, we're slowly building the procedure, this one, we don't have yet.' (Interviewee, CERT-PH)

These above remarks indicate a gap in the current approach. Therefore, further studies are recommended to look into how the current practices within national CSIRTs can be improved with more systematic approaches.

Theme 2: How CSIRT staff perceive public data, OSINT and free tools

This theme focuses on the interviewees' perception of public data, OSINT and free tools, including the advantages (especially whether they are considered to be useful in CSIRT operations or not) and some disadvantages (including issues with validity, authenticity and usability). Overall, all interviewees from MyCERT and other national CSIRTs perceived public data, OSINT and free tools to be useful.

Interviewees perceived public data to be useful for viewing cyber incidents from different perspectives and they can serve as a pivot point to other useful information, as mentioned by one interviewee from MyCERT:

> 'We can get different view of the data given to us, get different point of view from different angle, different additional view, either new information from other data or correlation.' (Interviewee, MyCERT)

Some interviewees also mentioned that they favoured public data because it is often more up to date (which is much needed for timely responses to incidents). One interviewee stated that public data can help save time because useful findings such as analysis of new types of malware are often readily available in public data. This can be consumed directly to augment an investigation. Echoing the results from the online survey, all interviewees from MyCERT and other national CSIRTs reconfirmed that public data can often lead to better investigation results when they are used together with closed-source data.

Regarding free tools, five interviewees from several national CSIRTs talked about their usefulness. For instance, one interviewee from MyCERT asserted that free

Table 2: Tools mentioned by survey participants

Tool	URL	Brief description
VirusTotal	https://www.virustotal.com/	OSINT, FOS, malware intelligence and analysis
Google Hacking Database	https://www.exploit-db.com/google-hacking-database	OSINT, FOS, online intelligence shared by Google
AlienVault OTX	https://otx.alienvault.com/	OSINT, FOS, online threat indicators
MISP	https://www.misp-project.org/	OSINT, OS, for obtaining, sharing and co-relating indicators of compromises
Maltego Community Edition	https://www.maltego.com/	OSINT, FW, for profiling threat actors
Shodan	https://www.shodan.io/	OSINT, FOS, for searching into the IoT
OSINT Framework	https://osintframework.com/	OSINT, OS, FOS, online collector of information from free tools and resources
IntelMQ	https://intelmq.readthedocs.io/	OSINT, OS, for collecting and processing security feeds
Taranis	https://github.com/NCSC-NL/taranis3	OSINT, OS, for monitoring and analysing news items and writing security advisories
Censys Search	https://search.censys.io/	OSINT, FOS, for discovering, monitoring, and analysing Internet-connected devices
Hybrid-Analysis	https://www.hybrid-analysis.com/	FOS, malware analysis
REMnux	https://remnux.org/	FW, malware analysis
Windows Process Monitor	https://docs.microsoft.com/en-us/sysinternals/downloads/procmon	FW, for monitoring running processes on Windows
MobSF	https://github.com/MobSF/Mobile-Security-Framework-MobSF	OS, for mobile device pentesting and malware analysis
Wireshark	https://www.wireshark.org/	OS, network protocol analyser
Security Onion	https://securityonionsolutions.com/	OS, network protocol analyser
Windows Sysinternal Suite	https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite	FW, a Windows toolset for troubleshooting
Joe Sandbox	https://www.joesandbox.com/	OS, FOS, malware analysis
PeiD (PE iDentifier)	https://www.aldeid.com/wiki/PEiD	FW, PE file analysis for detecting packers, cryptors and compilers used
Hxd	https://mh-nexus.de/	FW+OS, hex editor
SiLK (System for Internet-Level Knowledge)	https://tools.netsa.cert.org/silk/	OS, network flow collection and storage infrastructure
nfdump	https://github.com/phaag/nfdump	OS, for collecting and processing netflow and sflow data
Nfsen	http://nfsen.sourceforge.net/	OS, graphical frontend of nfdump
DomainTools WHOIS	https://whois.domaintools.com/	FOS, domain name and IP address lookup
Cuckoo Sandbox	https://cuckoosandbox.org/	OS, malware analysis sandbox
Apache Pulsar	https://pulsar.apache.org/	OS, for netflow analysis
Apache Flink	https://flink.apache.org/	OS, for netflow analysis

(OS = fully open-source, FW = freeware without open-source, FW+OS = freeware with partial open-source, FOS = free online service)

Table 3: Additional tools mentioned by interviewees

Tool	URL	Brief description
IDA Pro Free Version	https://hex-rays.com/ida-free/	FW, malware analysis
Splunk Free Version[81]	https://www.splunk.com/en_us/ download.html	FW, for log analysis
Notepad++	https://notepad-plus-plus.org/	OS, universal file editor for log analysis
Kali Linux	https://www.kali.org/	FW+OS, security-enhanced Linux distribution with many useful tools
Nmap	https://nmap.org/	OS, for network discovery and security auditing
OpenCTI	https://www.opencti.io/	OS, for storing, organising, visualising and sharing knowledge on cyber threats
Tiny Tiny RSS	https://tt-rss.org/	OS, web-based news feed reader and aggregator

(OS = fully open-source, FW = freeware without open-source, FW+OS = freeware with partial open-source, FOS = free online service)

tools can produce results comparable to those from commercial tools:

> 'We use IDA Pro, the free version, to check the network behaviour of the binary and to see what the malicious binary is doing towards the operating system (OS). We still can get result of the static analysis even if it is free, maybe some features are limited. Other people use [ANONYMISED] (commercial tools). The result is [the] same, just that it is in different format.' (Interviewee, MyCERT)

Another interviewee from Sri Lanka CERT/CC mentioned how a free tool had helped them to successfully identify a command and control (C&C) server involved in an incident, which allowed them to inform the relevant LEA for taking down the server.

A third interviewee from SWITCH-CERT considered the main advantage of free tools to be their availability. They also mentioned that open-source tools have advantages in terms of customisation and an active community around them:

> 'The benefits are, free tools are free and if you have open-source tools, you add or modify the source codes, as you like, as intended. If you have open-source in the community, the community develop further for the community.' (Interviewee, SWITCH-CERT)

Nevertheless, interviewees also reported problems about using public data, OSINT and free tools, in terms of reliability and authenticity of public data, usability and lack of validated OSINT and free tools. Further research is therefore suggested on evaluation of such data and tools to support national CSIRTs on what data and tools to use.

The detailed breakdown statistics are shown in Figure 5.

Theme 3: Reporting and sharing of information about cyber incidents

The interview data also revealed a trend in reporting and sharing information about cyber incidents between victims and non-CSIRT organisations with national CSIRTs,[82] as well as the reasons behind such a trend. All seven interviewees from MyCERT mentioned that not all victims and organisations in their constituency (Malaysia) would actually report cyber incidents to MyCERT due to several reasons. The main reason — reported by all MyCERT interviewees but one — is that victims and non-CSIRT organisations

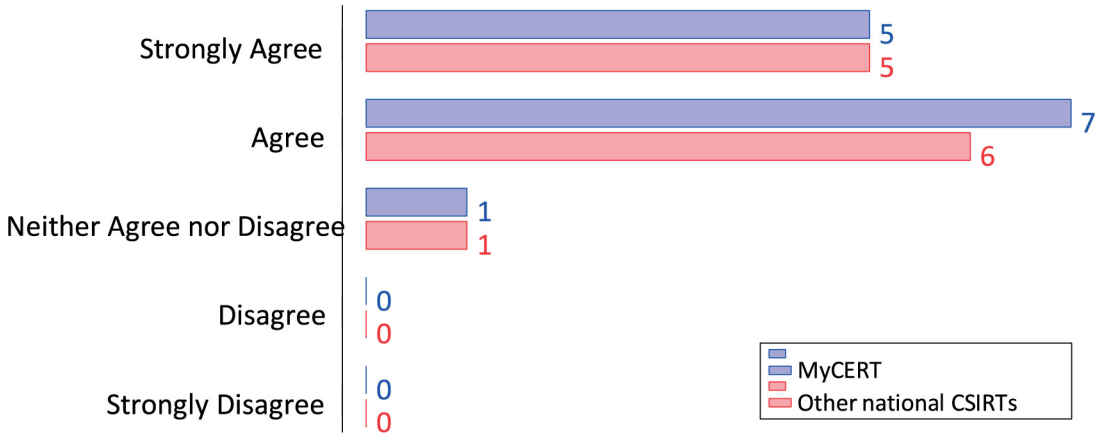

Figure 4: Survey participants' perceptions on usefulness of public data and OSINT tools for national CSIRTs

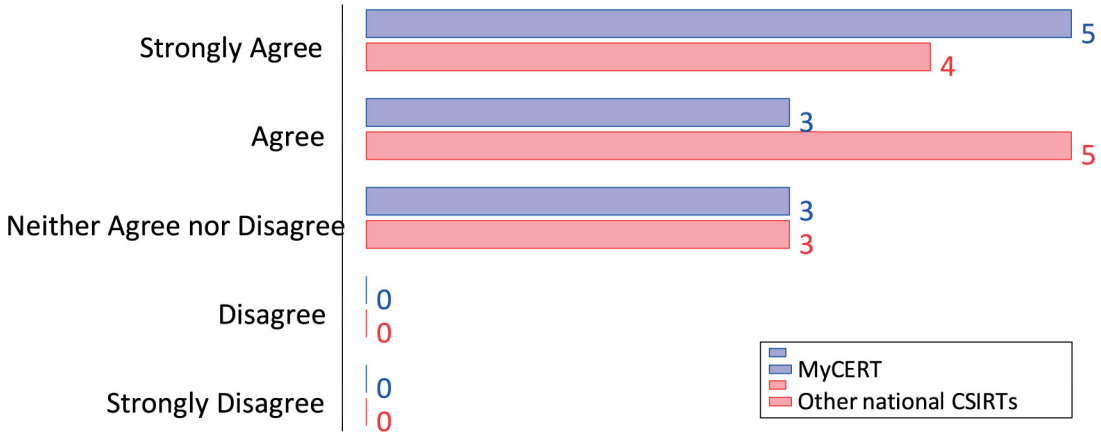

Figure 5: Survey participants' perceptions on whether combining public data and closed-source data could often lead to better results for incident investigation

are concerned about potential reputational damage due to the publicity of reported incidents. The following five other reasons were also mentioned (each by one interviewee): 1) stringent internal policies on data privacy and information disclosure in some organisations; 2) some victims and organisations believed that they could handle cyber incidents themselves; 3) organisations may hire third-party experts to respond to cyber incidents; 4) home users do not report incidents due to privacy concerns and other personal reasons; and 5) the data needed for reporting an incident may not be available. One interviewee also mentioned that some organisations reported cyber incidents without detailed information about the incident because they only wanted to obtain more related information from MyCERT.

The trend of lack of incident reporting revealed by MyCERT interviewees was confirmed by interviewees from other national CSIRTs. Four interviewees mentioned the difficulties in getting victims and non-CSIRT organisations to report cyber incidents to their national CSIRT. One interviewee from CERT.at mentioned that Austria has a regulation that mandates cyber incident reporting in Austria.[83]

Non-MyCERT interviewees also mentioned a number of reasons contributing towards the lack of reporting, and these

are not all the same as those suggested by MyCERT interviewees. One interviewee from CERT-PH (Philippines' national CSIRT) stated two main reasons for the lack of reporting: the lack of trust especially from private sectors on the national CSIRT, and the lack of knowledge about the national CSIRT (CERT-PH was in service for only three years at the time of the interview). A third reason mentioned by a SWITCH-CERT interviewee is that victims may be afraid of being blamed for the incident:[84]

> 'It is not just the problem of customer trust. It is more like having fear to be blamed if somethings happens. I think they have fear that someone would blame, that it happened to you, how could it be.' (Interviewee, SWITCH-CERT)

Overall, the lack of incident reporting and sharing of incident data by victims and non-CSIRT organisations provides some suggestions on why national CSIRT staff often consider closed-source data to be insufficient for incident investigation (as identified in Theme 4). This observation also provides a partial answer as to why it would be necessary for national CSIRT staff to acquire more information from public data (as identified in Theme 1).

Theme 4: Common operational challenges faced by national CSIRTS

The interviewees also talked about the challenges faced by national CSIRTs. Such challenges can be grouped into three areas: 1) public data; 2) OSINT and free tools; and 3) resources (see Table 4). Note that some interviewees also mentioned less relevant challenges or challenges based on inaccurate information, eg some issues about closed-source data and an insufficient budget to purchase commercial tools, and one based on an inaccurate claim of an open-source tool. Such irrelevant and problematic 'challenges' are excluded from the discussion here. Some challenges represent isolated or very subjective opinions of one or just a few interviewees, which were excluded as well. Such selective synthesis ensured challenges discussed here are common and representative for all national CSIRTs.

The challenges are largely self-explanatory. They also reflected the major areas for governments, industry and security researchers to focus on, in order to help the work of national CSIRTs. Among all the challenges, validation of public data and tools emerged as the two most important ones.

FURTHER DISCUSSIONS

The results from the online survey and the semi-structured interviews provide sufficient evidence to answer the two RQs mentioned in the first section. For RQ1, it is clear that the use of public data, OSINT and free tools is popular within most (if not all) national CSIRTs, independent of attributes such as region, size, cultural background and level of maturity. Although the survey and the interviews did not give a complete set of public data sources, OSINT and free tools, participants' responses showed a wide range of such data sources and tools used by national CSIRT staff. There is a general agreement that closed-source data is insufficient to support incident investigation within national CSIRTs. This means there is a real need for good-quality public data. It is a common practice for national CSIRT staff to validate public data before using it for their work. For RQ2, most national CSIRT staff participated in the study felt that public data is very useful as additional sources to provide richer information and intelligence, especially when combined with closed-source data. The need and proven usefulness of public data justify the wide use of OSINT tools among national CSIRT staff. In addition, many tools used by national CSIRT staff are free ones, for both OSINT and non-OSINT purposes. The usefulness of some free tools is considered comparable

Table 4: Operational challenges related to public data, OSINT and free tools, synthesised from interviews

Area	Number of interviewees			Challenge
	MyCERT	Other national CSIRTs	Total	
Public data	5	3	8	Lack of validated public data that can be considered reliable
				The huge amount of (public) data, making it difficult to find useful information
				Lack of sufficient data shared by some organisations (eg some users of MISP do not actively share data)
OSINT + free Tools	4	2	6	Lack of officially validated tools that can be used by CSIRTs
				Usability issues of some tools (eg limited or broken features)
				Lack of enough tools to process unstructured data
				Lack of tools that can process big data at high speed (eg for real-time netflow analysis)
Resources	4	1	5	Insufficient manpower (eg due to loss of competent staff)
				Insufficient skills and expertise (eg on OSINT tools and data analytics)

to similar commercial tools, indicating that it is possible to operate a national CSIRT without dependencies on (expensive) commercial tools.

In addition to the positive findings summarised above, participants of the study also commented on the problems and operational challenges related to the use of public data, OSINT and free tools. Among all the challenges, two are of particular importance. First, public data, OSINT and free tools are still used in a very ad hoc manner; more standardised and systematic approaches are still to be established. Second, even though national CSIRT staff do validate public data before using it, the validation process is also mostly done on an ad hoc basis, without a generally accepted standard procedure. Therefore, further research is necessary on establishing standard processes and guidelines to support national CSIRT staff to use public data, OSINT and free tools more effectively and efficiently.

Similar to other related empirical studies in the field of information security,[85,86] this study also has a couple of limitations. First, the number of participants (25) and the number of national CSIRTs covered (13, including the national CSIRT of two anonymised participants) are both relatively low, which can affect the generalisability of the results reported. Second, some participants were reluctant to reveal some information about operational practices at their national CSIRT due to privacy and confidentiality concerns, which limited the completeness of the information collected through the study and could make some findings less representative.

Both limitations should not be major issues considering two facts: 1) participants' responses are mostly aligned with each other for all key aspects; and 2) the main findings are logical and they match the experience of the first author as an employee of MyCERT for over 20 years. The study calls for the security community to conduct further research to cross-validate these findings.

CONCLUSION

The prevalence of cyber security incidents makes it imperative for a coordinated effort to handle them efficiently. This is one of the

key roles of CSIRTs, especially at the national level. The main aim of the study presented in this paper is to obtain a better understanding of how national CSIRTs operate in terms of the use of public data, OSINT and free tools, and how staff perceive their usefulness — a less-studied topic in the research literature.

Through an online survey and a number of follow-up semi-structured interviews with 25 participants from 13 national CSIRTs, the study led to three main findings. First, the active use of public data, OSINT and free tools at national CSIRTs was confirmed. Second, public data, OSINT and free tools are perceived to be useful by national CSIRT staff. Third, the study also revealed a number of operational challenges, particularly related to: 1) the ad hoc use of public data, OSINT and free tools; and 2) the ad hoc nature of the validation process of such data and tools. The findings indicate that more research is needed to help support more effective and efficient use of public data, OSINT and free tools; to create more useful public data sources; to develop more useful OSINT and free tools; to develop more standardised and systematic processes, as well as suitable frameworks for evaluating and recommending public data sources, OSINT and free tools.

APPENDIX A: SURVEY QUESTIONNAIRE

How National CERTs Use Public Data and OSINT Tools: Operational Practices

[Participant Information Sheet]
[Consent Form]
*Mandatory questions.
Please answer all of the following questions. You can come back to edit your answers before submitting the survey.

A. Basic information about participant

1. What is your gender?
   - ☐ Male
   - ☐ Female
   - ☐ Other

2. How many years have you worked in the national CERT? Please select from the drop-down list.
   - ☐ 1
   - ☐ 2
   - ☐ 3
   - ☐ 4
   - ☐ 5
   - ☐ 6
   - ☐ 7
   - ☐ 8
   - ☐ 9
   - ☐ 10 years or more

3. In your experience, what type(s) of data do you deal with in your incident handling work?
   - ☐ Close-source data
   - ☐ Public data
   - ☐ Other type of data

4. Can you name all the tools you use in the national CERT and for what purpose (task) do you use the tools? For example, name of the tools you use to conduct log analysis or malware analysis. Please state of these are free or commercial tools?

B. Information about data received and OSINT (Open-Source Intelligence) tools

5. What type of close-source data you have access from different organisations or victims who report cyberattack?

6. Do you think the close-source data that you have access to is sufficient for your investigation?

☐ Yes
☐ No

If No, can you provide what are the insufficiencies?

7. Do you receive data from other national CERTs and other cyber security organisations?

☐ Yes
☐ No

Can you provide the names of the national CERTs and the cyber security organisations and the type of data you receive from them?

8. Besides the close-source data from reporting victims, do you also use public data to facilitate analysis?

☐ Yes
☐ No

9. [If the answer to Question 6 is yes] Can you list all types of public data you use to facilitate your analysis?

10. [If the answer to Question 6 is yes] For each type of public data, can you briefly explain from where and how you collect it?

11. [If the answer to Question 6 is yes] how often do you combine? Can you give the estimated percentage of incidents analysed using a combination of public and close-source data?

12. [If the answer to Question 6 is yes] Do you often get better results in your analysis when you combine data from public and close sources, instead of using just data from one type of source?

☐ Strongly agree
☐ Agree
☐ Neither agree or disagree
☐ Disagree
☐ Strongly disagree

13. When you use public data in your analysis, do you verify the validity and authenticity of the public data to make sure the data is trusted and reliable?

☐ Yes
☐ No

If yes, how do you verify the validity and authenticity of the public data? For example do you validate with other national CERTs, with other trusted parties or validate the data using some validation tools?

If No, what is the reason for not validating the public data?

14. In your daily practices, do you collaborate with others to obtain public data needed?
☐ Yes
☐ No
If yes, please provide with whom you collaborate and what public data you obtain through such collaborations?

15. In your daily practice, how do you conduct analysis of the public data?
☐ Manual
☐ Automated
☐ Semi-automated
Please explain briefly how you conduct the analysis. For example, if you select Manual in the above list, how you conduct analysis of the data. If you select Automated and Semi-automated, please name the tools used and their functionalities.

16. Do you use any OSINT tools in your daily operation?
☐ Yes
☐ No
If yes, please list the specific OSINT tools you are using and for what purposes or tasks?

17. Can you briefly explain from where you obtained the OSINT tools?

18. Do you agree that public data and OSINT tool are useful for national CERTs?
☐ Strongly Agree
☐ Agree
☐ Neither agree or disagree
☐ Disagree
☐ Strongly disagree

C. CHALLENGES IN THE NATIONAL CERT YOU ARE WORKING FOR

19. What are the challenges you face in obtaining close-source data in your work?

20. What are the challenges you face in analysing close-source data you receive?

21. What are the challenges you face in obtaining public data for your work?

22. What are the challenges you face in analysing public data for your work?

23. What are the challenges you face in obtaining OSINT tools for your work?

24. What are the challenges you face in using OSINT tools for your work?

END OF SURVEY

APPENDIX B: QUESTIONS FOR SEMI-STRUCTURED INTERVIEWS

Note: The semi-structured interviews will follow the survey structure, with the purpose to get more information on the answers participants provided in the survey. Each interview will last for about 1 hour and the interview will be audio-recorded, with participant's permission. Such interviews will be mostly conducted remotely.

Basic Information about participant

1. In your current position, what type of work do you do in the national CERT?
2. How do you gain your skills and expertise in incident handling?
3. Have you attended any security trainings? If yes, what type of trainings?
4. In your experience, can you give examples of different types of data you had handled in your work?
5. Can you share how you handle an incident in the national CERT, starting from receiving an incident until resolution of the incident?

Information about data received and OSINT Tools

6. Do you think national CERTs must not always rely on close data for incident analysis and why?
7. Can you name any policy the national CERT has on the usage of public data and OSINT tools? If yes, why such a policy in place?
8. How does the national CERT encourage their analyst to use public data and OSINT tools?
9. Can you briefly describe how do you conduct analysis using tools in the national CERT? For example, a tool you use to analyse logs, or analyse malware.
10. What do you do or how do you resolve the issue of insufficiency in the close data?

11. How do you access the different type of close-source data from victims or organisations who report cyberattack to the national CERT?
12. How can national CERTs benefit by combining close data and public data in incident analysis?
13. Can you give examples of incidents that achieved better results in your analysis when you combine data from public and close sources, instead of using just data from one type of source?
14. Can you share a case study of how you had used public data and OSINT tool to resolve an incident successfully, due to unavailability or insufficiency of close data?
15. Why do you need to use public data on top of the close data you receive from victims (complainants)?
16. Could you elaborate why public data and OSINT tools are useful or not useful for national CERTs?
17. How can national CERTs better optimize OSINT tools in their daily operation?
18. How can national CERTs better optimize public data in their daily operation?

Challenges in the national CERT

19. How can national CERTs overcome the challenges in using public data and OSINT tools?
20. What could be the reason that hinders national CERTs from using public data and OSINT tool?
21. Why don't some organisations and victims report incident to national CERTs?
22. Why don't some organisations and victims share closed data when they report incidents to national CERTs?
23. How can national CERTs give assurance to organisations and victims to encourage reporting incidents?
24. How can national CERTs give assurance to organisations and victims to encourage sharing closed data in their incident reports?
25. What are other challenges the national CERT faces in terms of data (close and public data) and tools in your constituency?

References and Notes

1. Koivunen, E. (2010), "'Why Wasn't I Notified?": Information Security Incident Reporting Demystified', Information Security Technology for Applications: 15th Nordic Conference on Secure IT Systems, NordSec 2010, Espoo, Finland, 27th–29th October, Revised Selected Papers (Lecture Notes in Computer Science, Vol. 7127), Springer, pp. 55–70, available at https://doi.org/10.1007/978-3-642-27937-9_5 (accessed 23rd November, 2021).
2. Nyre-Yu, M., Gutzwiller, R. S. and Caldwell, B. S. (2019), 'Observing cyber security incident response: Qualitative themes from field research', Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Vol. 63, SAGE, pp. 437–441, available at https://doi.org/10.1177/1071181319631016 (accessed 23rd November, 2021).
3. Ahmad, R. A. and Hashim, M. S. (2011), 'The Organisation of Islamic Conference—Computer Emergency Response Team (OIC-CERT): Answering Cross Border Cooperation', Proceedings of the 2011 Second Worldwide Cybersecurity Summit, IEEE, p. 5, available at https://ieeexplore.ieee.org/document/5978783 (accessed 23rd November, 2021).
4. Wara, Y. M. and Singh, D. (2015), 'A Guide to Establishing Computer Security Incident Response Team (CSIRT) for National Research and Education Network (NREN)', *African Journal of Computing & ICT*, Vol. 8, No. 2, p. 8.
5. Killcrece, G., Kossakowski, K-P., Ruefle, R. and Zajicek, M. (2003), 'Organizational models for computer security incident response teams CSIRTs', Handbook CMU/SEI-2003-HB-001, Carnegie Mellon University, Pittsburgh, PN, available at https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14099.pdf (accessed 23rd November, 2021).
6. Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M. and Perl, S. J. (2014), 'Computer Security Incident Response Team Development and Evolution', *IEEE Security & Privacy*, Vol. 12, No. 5, pp. 16–26, available at https://doi.org/10.1109/MSP.2014.89 (accessed 23rd November, 2021).
7. Hove, C., Tarnes, M., Line, M. B. and Bernsmed, K. (2014), 'Information Security Incident Management: Identified Practice in Large Organizations', Proceedings of the 8th International Conference on IT Security Incident Management & IT Forensics,

pp. 27–46, available at https://doi.org/10.1109/IMF.2014.9 (accessed 23rd November, 2021).
8. Metzger, S., Hommel, W. and Reiser, H. (2011), 'Integrated security incident management – Concepts and real-world experiences', Proceedings of the 6th International Conference on IT Security Incident Management and IT Forensics, pp. 107–121, available at https://doi.org/10.1109/IMF.2011.15 (accessed 23rd November, 2021).
9. Werlinger, R., Muldner, K., Hawkey, K. and Beznosov, K. (2010), 'Preparation, Detection, and Analysis: the Diagnostic Work of IT Security Incident Response', *Information Management & Computer Security*, Vol. 18, No. 1, pp. 26–42, available at https://doi.org/10.1108/ 09685221011035241 (accessed 23rd November, 2021).
10. *Ibid.*, ref. 2.
11. *Ibid.*, ref. 3.
12. Hellwig, O., Quirchmayr, G., Huber, E., Goluch, G., Vock, F. and Pospisil, B. (2016), 'Major Challenges in Structuring and Institutionalizing CERT-communication', Proceedings of the 2016 11th International Conference on Availability, Reliability and Security 2, pp. 661–667, available at https://doi.org/10.1109/ARES.2016.57 (accessed 23rd November, 2021).
13. *Ibid.*, ref. 2.
14. Alberts, C. J., Dorofee, A. J., Killcrece, G., Ruefle, R. and Zajicek, M. (2004), 'Management Processes for CSIRTs: A Work in Progress', Technical Report CMU/SEI-2004-TR015, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PN, available at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153 (accessed 23rd November, 2021).
15. Sfakianakis, A., Douligeris, C., Marinos, L., Lourenço, M. and Raghimi, O. (2019), 'ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends, Technical Report', available at https://doi.org/10.2824/622757 (accessed 23rd November, 2021).
16. West-Brown, M. J., Stikvoort, D., Kossakowski, K-P., Killcrece, G., Ruefle, R. and Zajicek, M. (2003), 'Handbook for Computer Security Incident Response teams (CSIRTs), 2nd edn', Technical Report Handbook CMU/SEI-2003-HB-002. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PN, available at https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf (accessed 23rd November, 2021).
17. European Commission (2009), 'Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience. Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection', available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52009DC0149 (accessed 23rd November, 2021).
18. European Parliament and European Council (2016), 'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union', available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed 23rd November, 2021).
19. See Enisa, 'CSIRTS in Europe', available at https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network (accessed 23rd November, 2021).
20. International Telecommunication Union (ITU), 'National CIRT', available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx (accessed 23rd November, 2021).
21. ITU chooses to use a slightly different term for CSIRT: computer incident response team (CIRT). Another widely used term is 'computer emergency response team' (CERT), which was used by many national CSIRTs. This paper uses CSIRT because this is the most widely used term in the research literature and in the EU NIS Directive.
22. Kassim, S. R. M., Abu, Dd S. and Omar, A. M. (2019), 'Measuring the Effectiveness of Phishing Detection Tool: Comparative Study on Pattern Matching and User Rating', *Journal of Computers*, Vol. 14, No. 4, pp. 302–310, available at https://doi.org/10.17706/jcp.14.4.302-310 (accessed 23rd November, 2021).
23. Kassim, S. R. M. and Zakaria, W. Z. A. (2014), 'Automating Big Data Analysis: Malaysia CERT Experience', Proceedings of the Tokyo International Conference on Engineering and Applied Sciences.
24. Kassim, S. R. M., Zakaria, W. Z. A. and Alta, N. M. K. M (2016), 'Exploitation of Android Mobile Malware in Phishing Modus Operandi: A Malaysia Case Study', Proceedings of The Second International Conference on Electronics and Software Science (ICESS2016), SDIWC, pp. 47–55, available at http://d.researchbib.com/f/4nBGp2ZwDhpTEz.pdf (accessed 23rd November, 2021).
25. Mokaddem, S., Wagener, G. and Dulaunoy, A. (2019), 'AIL – The design and implementation of an Analysis Information Leak framework', Proceedings of the 2018 IEEE International Conference on Big Data, pp. 5049–5057, available at https://doi.org/10.1109/BigData.2018.8622074 (accessed 23rd November, 2021).
26. One may argue that public data does not have to be freely available, as long as anyone can have access to it (possibly after paying a fee). In this paper, public data is defined as data that can be obtained for free, in order to have a more focused scope. This is also the understanding of many people and organisations when they talk about 'public data', eg Google Public Data Explorer, available at https://www.google.com/publicdata/directory [accessed 23rd November, 2021]). Note that a narrower definition of 'public data' refers to open data from public bodies only, which is considered too narrow.
27. *Ibid.*, ref. 18.
28. Jaatun, M. G., Bodsberg, L., Grøtan, T. O. and Moe, M. E G. (2020), 'An Empirical Study of

CERT Capacity in the North Sea', Proceedings of the 2020 International Conference on Cyber Security and Protection of Digital Services, IEEE, p. 8, available at https://doi.org/101109/CyberSecurity49315.2020.9138865 (accessed 23rd November, 2021).
29. *Ibid*., ref. 9.
30. Mana, P. and Friligkos, V. (2019), 'EUROCONTROL/EATM-CERT Services – Supporting Aviation To Better Manage Cyber Threats', Proceedings of the 2019 Integrated Communications, Navigation and Surveillance Conference, IEEE, Article 1B1, available at https://doi.org/10.1109/ICNSURV.2019.8735282 (accessed 23rd November, 2021).
31. See MISP, 'Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing', available at https://www.misp-project.org/ (accessed 23rd November, 2021).
32. Grispos, G., Glisson, W. B. and Storer, T. (2015), 'Security Incident Response Criteria: A Practitioner's Perspective', available at https://arxiv.org/abs/1508.02526 (accessed 23rd November, 2021).
33. Line, M. B., Tøndel, I. A. and Jaatun, M. G. (2014), 'Information security incident management: Planning for failure', Proceedings of the 2014 8th International Conference on IT Security Incident Management & IT Forensics, IEEE, pp. 47–61, available at https://doi.org/10.1109/IMF. 2014.10 (accessed 23rd November, 2021).
34. Kijewski, P. and Kozakiewicz, A. (2011),' Security Research at NASK: Supporting the Operational Needs of a CERT Team and More', Proceedings of the 1st SysSec Workshop, pp. 96–99, available at https://doi.org/10.1109/SysSec.2011.29 (accessed 23rd November, 2021).
35. Tøndel, A. A., Line, M. B. and Jaatun, M. G. (2014), 'Information Security Incident Management: Current Practice as Reported in the Literature', *Computers & Security*, Vol. 45, pp. 42–57, available at https://doi.org/10.1016/j.cose.2014.05.003 (accessed 23rd November, 2021).
36. International Organization for Standardization (ISO) (2011), 'Information technology — Security techniques — Information security incident management', International standard, ISO/IEC 27035:2011, available at https://www.iso.org/standard/44379.html (accessed 23rd November, 2021).
37. International Organization for Standardization (ISO) (2016), 'Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management', International standard, ISO/IEC 27035-1:2016, available at https://www.iso.org/standard/60803.html (accessed 23rd November, 2021).
38. International Organization for Standardization (ISO) (2016), 'Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response', International standard, ISO/IEC 27035-2:2016,. available at https://www.iso.org/standard/62071.html (accessed 23rd November, 2021).
39. Day, T., Gibson, H. and Ramwell, S. (2016), 'Fusion of OSINT and Non-OSINT Data', in *Open Source Intelligence Investigation: From Strategy to Implementation*, Springer, New York, pp. 133–152.
40. Wells, D. (2016), 'Taking Stock of Subjective Narratives Surrounding Modern OSINT', *Open Source Intelligence Investigation: From Strategy to Implementation*, Springer, New York, pp. 57–65.
41. Fleisher, C. S. (2008), 'Using Open Source Data in Developing Competitive and Marketing Intelligence', *European Journal of Marketing*, available at https://doi.org/10.1108/03090560810877196 (accessed 23rd November, 2021).
42. Lwin, M. O., Lu, J., Sheldenkar, A. and Schulz, P. J. (2018), 'Strategic Uses of Facebook in Zika Outbreak Communication: Implications for the Crisis and Emergency Risk Communication Model', *International Journal of Environmental Research and Public Health*, Vol. 15, No. 9, available at https://doi.org/10.3390/ijerph15091974 (accessed 23rd November, 2021).
43. Odlum, M. and Yoon, S. (2015), 'What Can we Learn About the Ebola Outbreak from Tweets?', *American Journal of Infection Control*, Vol. 43, No. 6, pp. 563–571, available at https://doi.org/10.1016/j.ajic.2015.02.023 (accessed 23rd November, 2021).
44. Quick, D. and Choo, K. K. R. (2018), 'Digital Forensic Intelligence: Data Subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix', *Future Generation Computer Systems*, Vol. 78 pp. 558–567, available at https://doi.org/10.1016/j.future.2016.12.032 (accessed 23rd November, 2021).
45. Lee, S. and Shon, T. (2017), 'Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures', Proceedings of the 2016 Future Technologies Conference, IEEE, pp. 1030–1033, available at https://doi.org/10.1109/FTC.2016.7821730 (accessed 23rd November, 2021).
46. Uehara, K., Mukaiyama, K., Fujita, M., Nishikawa, H., Yamamoto, T., Kawauchi, K. and Nishigaki, M. (2019), 'Basic Study on Targeted E-mail Attack Method Using OSINT', in *Advanced Information Networking and Applications: Proceedings of the 33rd International Conference on Advanced Information Networking and Applications (AINA-2019) (Advances in Intelligent Systems and Computing, Vol. 926),* Springer, New York, pp. 1329–1341, available at https://doi.org/10. 1007/978-3-030-15032-7_111 (accessed 23rd November, 2021).
47. Roohparvar, R. (2020), 'Use of OSINT tools for security and their functions', Infoguard Cyber Security, available at http://www.infoguardsecurity.com/use-of-osint-tools-for-security-and-their-functions/ (accessed 23rd November, 2021).
48. Glassman, M. and Kang, M. J. (2012), 'Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)', *Computers in Human Behavior*, Vol. 28, No. 2,

pp. 673–682, available at https://doi.org/10.1016/j.chb.2011.11.014 (accessed 23rd November, 2021).
49. Passi, H. (2018), 'Top 10 Popular Open Source Intelligence (OSINT) Tools', Grey Campus, available at https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools (accessed 23rd November, 2021).
50. Pastor-Galindo, J., Nespoli, P., Mármol, F. G. and Pérez, G. M. (2020), 'The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends', IEEE Access, Vol. 8, pp. 10282–10304, available at https://doi.org/10.1109/ACCESS.2020.2965257 (accessed 23rd November, 2021).
51. Krstic, M., Cabarkapa, M. and Jevremovic, A. (2019), 'Machine Learning Applications in Computer Emergency Response Team Operations', Proceedings of the 27th Telecommunications Forum, available at https://doi.org/10.1109/TELFOR48224.2019.8971040 (accessed 23rd November, 2021).
52. *Ibid*. ref. 34.
53. *Ibid*., ref. 2.
54. *Ibid*., ref. 32.
55. *Ibid*., ref. 7.
56. Nouh, M., Nurse, J. R. C., Webb, H. and Goldsmith, M. (2019), 'Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement', Proceedings of the 2019 Workshop on Usable Security (USEC) at Network and Distributed System Security Symposium, pp. 1–11, available at https://doi.org/10.14722/usec.2019.23032 (accessed 23rd November, 2021).
57. See Typeform, available at https://www.typeform.com/ (accessed 23rd November, 2021).
58. Oates, B. J. (2005), 'Researching Information Systems and Computing', SAGE, available at https://us.sagepub.com/en-us/nam/researching-information-systems-and-computing/book226898 (accessed 23rd November, 2021).
59. Sauerwein, C., Pekaric, I., Felderer, M. and Breu, R. (2019), 'An analysis and classification of public information security data sources used in research and practice', *Computers & Security*, Vol. 82, pp. 140–155, available at https://doi.org/10.1016/j.cose.2018.12.011 (accessed 23rd November, 2021).
60. Auerbach, C. and Silverstein, L. B. (2003), *Qualitative Data: An Introduction to Coding and Analysis*, Vol. 21, New York University Press, New York.
61. Braun, V. and Clarke, V. (2006), 'Using Thematic Analysis in Psychology', *Qualitative Research in Psychology*, Vol. 3, No. 2, pp. 77–101, available at https://doi.org/10.1191/1478088706qp063oa (accessed 23rd November, 2021).
62. Adu, P. (2019), *A Step-by-Step Guide to Qualitative Data Coding*, Routledge, New York and London.
63. *Ibid*., ref. 62.
64. *Ibid*., ref. 61.
65. *Ibid*., ref. 62.
66. Two participants chose 'no' when being asked about their experience with public data, but answered 'yes' for another question about validating public data. One of them participated in an interview and clarified that they did use public data. Another participant was not interviewed, but we believe that they also used public data.
67. See Virus Total, available at https://www.virustotal.com/ (accessed 23rd November, 2021).
68. See Shodan, available at https://www.shodan.io/ (accessed 23rd November, 2021).
69. See Google Hacking Database, available at https://www.exploit-db.com/google-hacking-database (accessed 23rd November, 2021).
70. See Censys, available at https://censys.io/ (accessed 23rd November, 2021).
71. One participant reported that he did not validate public data, but during a follow-up interview with him it was clarified that he made a mistake for this question in the survey.
72. Two MyCERT participants used the term 'proof of concept' (POC) for this method, but judging on the first author's knowledge on operational practices at MyCERT, what they meant is validation experiments (eg running a malware sample in a sandbox environment to validate its being malware).
73. Although structured data with an unknown or unsupported format also require bespoke parsing tools, this challenge was not mentioned by any participants.
74. *Ibid*., ref. 32.
75. *Ibid*., ref. 7.
76. Kral, K. (2012), 'The Incident Handler's Handbook', White Paper, SANS Institute, available at https://www.sans.org/white-papers/33901/ (accessed 23rd November, 2021).
77. Ahmad, A., Hadgkiss, J. and Ruighaver, A. B. (2012), 'Incident response teams – Challenges in supporting the organisational security function', *Computers & Security*, Vol. 31, No. 5, pp. 643–652, available at https://doi.org/10.1016/j.cose.2012.04.001 (accessed 23rd November, 2021).
78. *Ibid*., ref. 7.
79. *Ibid*., ref. 8.
80. See GitHub, available at https://github.com/certat (accessed 23rd November, 2021).
81. The free version was available in the past, see https://www.splunk.com/view/SP-CAAAE66 (last accessed 23rd November, 2021) which is no longer available (only free trials for most products from Splunk).
82. There is active information sharing between national CSIRTs, and there are a number of free tools facilitating such sharing, eg MISP and IntelMQ. This aspect was, however, not discussed during the interviews.
83. The interviewee referred to the Netzund Informationssystemsicherheitsverordnung (NISV), available at https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2019_2_215/ERV_2019_2_215.html (accessed 23rd November, 2021), the national law defined according to the EU NIS Directive. The law actually does not mandate compulsory reporting of cyber incidents to CERT.at, but just for incidents with an 'impact on economic and societal activities'

that occur to essential and digital services. All EU member states now have such a legislation.
84. This echoes similar findings from previous research on the blame culture in other contexts, *ibid*., ref. 13 and *ibid*., ref. 24.
85. Kotulic, A. G. and Clark, J. G. (2004), 'Why there aren't more information security research studies', *Information & Management*, Vol. 41, No. 5, pp. 597–607, available at https://doi.org/10.1016/j.im.2003.08.001 (accessed 23rd November, 2021).
86. Sundaramurthy, S. C., McHugh, J., Ou, X. S., Rajagopalan, S. and Wesch, M. (2014), 'An anthropological approach to studying CSIRTs', *IEEE Security & Privacy*, Vol. 12, No. 5, pp. 52–60, available at https://doi.org/10.1109/MSP.2014.84 (accessed 23rd November, 2021).