EUROPEAN UNION AGENCY
FOR CYBERSECURITY


```
  },
  {
    "entry": [
      {
        "description": "Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather
        "expanded": "Scanning",
        "value": "scanner"
      },
      {
        "description": "Observing and recording of network traffic (wiretapping).",
        "expanded": "Sniffing",
        "value": "sniffing"
      },
      {
        "description": "Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).",
        "expanded": "Social Engineering",
        "value": "social-engineering"
      }
    ],
    "predicate": "information-gathering"
  },
  {
    "entry": [
      {
        "description": "An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised
        "expanded": "Exploitation of known Vulnerabilities",
        "value": "ids-alert"
```


PROACTIVE DETECTION – SURVEY RESULTS

MAY 2020

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

AUTHORS

Piotr Białczak, Paweł Pawliński, Krzysztof Rydz, CERT Polska / NASK and Rossella Mattioli, ENISA

ACKNOWLEDGEMENTS

ENISA performed this study with the help of the contractor NASK and with the input from the members of the CSIRTs Network and other operational communities who contributed to this project. In particular we would like to thank the following persons for their input: Georgios Psykakos (CERT-EU), Marcin Dudek (CERT Polska), Michał Strzelczyk (CERT Polska). Finally, we would like to thank everyone that answered the survey: your input was crucial for this study.

LEGAL NOTICE

COPYRIGHT NOTICE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As of April 2020 there are more than 500 incident response teams in Europe[1]. These teams need every day to improve the prevention, detection and analysis of cyber threats and incidents. As envisioned by the NIS Directive[2] and in the Cybersecurity Act[3] ENISA is tasked with assisting the CSIRTs Network[4] and the Member States in improving the prevention, detection and capability to respond to cyber threats and incidents by providing them with knowledge and expertise. For these reasons ENISA aims with this study to provide an inventory of available methods, identify good practices and recommend possible areas for growth and attention to improve the proactive detection of network security incidents in EU.

In this respect **proactive detection of incidents** is defined as the **process of discovery of malicious activity in a team's constituency through internal monitoring tools or external services that publish information about detected incidents, before the affected constituents become aware of the problem**. In 2011, ENISA published the first version of a study "Proactive detection of network security incidents"[5]: The current project builds and expands on this. It aims to provide a complete inventory of all available methods, tools, activities and information sources for proactive detection of network security incidents, which are used already or potentially could be used by incident response teams in Europe nowadays.

In doing so, ENISA asked members of the CSIRTs Network and other operational communities to contribute to this project by responding to an **online survey**. The survey gathered information on what is currently used or planned to be implemented by incident response teams. The goal was to **understand goals and expectations of respondents, as well as challenges in implementing available measures. The results help identifying future areas for growth and improvement**. The results of the survey provide an overview of the usage of the different tools and insight on the most common systems deployed in-house, the most often used measures, the level of effort and expertise needed to deploy these systems and other various aspects. For example, the **most common measures are sandboxes and network intrusion detection systems and the least common are cloud monitoring systems**. **The type of tools most often evaluated as excellent belong to systems for aggregation, correlation and visualization of logs and other event data**. **25% of respondents are fully satisfied with their current set of tools but they underlined problems with interaction of different systems (including clear application programming interface API documentation, standards of data exchange and data formats).** These issues cause problems with correlation of data, as different formats and sources are hard to deploy in one monitoring system. Moreover **most of the tools lack automatic classification of output** and there are also problems due to the lack of good practices on implementation, policy and deployment of the measures.

Regarding information sources, all categories covered by the survey are indicated as commonly used and relatively easy to maintain, with the lower level of requirements for repositories of malware samples. According to the answers**, most relevant information sources are feeds of malware URLs and the most accurate are feeds of infected machines (bots). Feeds of malware URLs and information sharing platforms are regarded as having the most timeliness. Feeds of phishing sites are considered as the most complete**. Another

[1] ENISA CSIRTs by Country - Interactive Map https://www.enisa.europa.eu/csirts-map
[2] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[3] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[4] www.csirtsnetwork.eu/
[5] https://www.enisa.europa.eu/topics/csirt-cert-services/proactive-services/proactive-detection/proactive-detection-of-incidents

interesting finding was that **half of the teams who responded to the survey can process all incoming information, however only high priority incidents are handled.** Only 15% of the teams can fully handle the information, while 35% of the teams are overwhelmed with it. In general the **biggest gap of the available information sources is the insufficient context, i.e. poor information completeness** .**The second important challenge is format and taxonomies**. It refers both to the varied formats, protocols and API used by information providers but also perceived lack of common classification of events and inconsistent identifiers. **A major area for improvement is better sharing of information from constituents. The main problem that prevents teams from using various information sources is also the fact that their integration requires investment of time and many teams face insufficient human resources.**

Moreover, in this document it is provided the comparison of the 2019 online survey results with the 2011 edition in order to provide insights about changes in CSIRT teams' experience using measures and information sources for proactive detection of network incidents. The comparison showed **rise in percentage of CSIRT teams satisfied with information sources they had, from 4% in 2011 to 15% of the teams in 2019**. Also the **number of teams capable of processing all incoming information (but handling only high priority incidents) was nearly on the same level.** However, the number of **teams receiving too much information** to handle it properly increased **from 11% in 2011 to 35% of the teams in 2019.** The comparison of usage of different categories of tools showed that the **adoption of spamtrap systems, NIDS, sandbox systems and passive DNS monitoring increased between 2011 and 2019**. **Network flow monitoring, network telescope, server and client honeypots usage decreased** between the analysed years. The comparison of information sources provided in both editions of the surveys showed that the **number of information sources grew, as well as their types, but also majority of the sources from 2011 are no longer available, superseded by new ones or having ceased to operate.** The comparison also **identified issues with correlation of data, standardisation of formats and interaction between tools/systems. These problems were addressed by some projects, however 8 years separating the surveys show that it is still not resolved.**

1. INTRODUCTION

In 2011, ENISA published the study entitled “Proactive detection of network security incidents” [6] and in 2019, with this study the aim is to understand what has changed in the last eight years and map the current situation among incident response teams in Europe. The objectives are to provide an inventory of available methods, identify good practices and recommend possible areas for growth and attention to improve the detection of network security incidents in EU.

Throughout this study, as in the 2011 study, **proactive detection of incidents** is defined as the **process of discovery of malicious activity in a team's constituency through internal monitoring tools or external services that publish information about detected incidents, before the affected constituents become aware of the problem.**

1.1 CONTEXT OF THE WORK

For more than fifteen years ENISA has been supporting Member States and CSIRT communities to build and advance their CSIRT capabilities. Individual teams which represent different sectors and businesses, as well as existing CSIRT communities, are indispensable elements of this shared responsibility and endeavour.

ENISA’s incident response support portfolio of work is related to setting up, running and developing capabilities of Computer Security Incident Response Teams (CSIRTs) in Europe. There are currently more than 500 CSIRTs listed in the ENISA Inventory[7]. The goal is to identify common practices across the EU to improve operational cooperation and information exchange. The primary audience are the CSIRTs Network[8] members, their leadership and the incident response community at large.

The NIS Directive[9] in Article 12 establishes the CSIRTs Network[10] “to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation”. The CSIRTs Network is a network composed of EU Member States’ appointed CSIRTs and CERT-EU[11] (“CSIRTs Network members”). ENISA is tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination upon request.

Moreover, with the EU Cybersecurity Act, ENISA is also mandated to increase operational cooperation at EU level and asked in Article 6 “Capacity-building” to assist Member States in their efforts to improve the prevention, detection and analysis of cyber threats and incidents and Article 7 “Operational cooperation at Union level” in advising on how to improve their capabilities to prevent, detect and respond to incidents.

In 2011, ENISA published the first version of “Proactive detection of network security incidents”[12]: The current project builds upon this study and aims to provide a complete inventory of all available methods, tools, activities and information sources (hereafter ‘measures’) for

[6] https://www.enisa.europa.eu/topics/csirt-cert-services/proactive-services/proactive-detection/proactive-detection-of-incidents
[7] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map
[8] https://csirtsnetwork.eu/
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[10] http://www.csirtnetwork.eu/
11 CERT-EU is a Computer Emergency Response Team or CSIRT and its constituency is composed of all the EU Institutions, Agencies and Bodies. Its offices are in Brussels.
[12] https://www.enisa.europa.eu/topics/csirt-cert-services/proactive-services/proactive-detection/proactive-detection-of-incidents

proactive detection of network security incidents, which are used already or potentially could be used by incident response teams in Europe nowadays.

1.2 OBJECTIVES OF THE STUDY

The objectives of this project are to:

- provide an inventory of available methods, tools, activities and information sources for proactive detection of network incidents,
- identify good practices and recommend possible areas for growth with attention for new and already established incident response teams in Europe
- draft a list of key recommendations for policy makers in order to improve the detection of network security incidents in EU.

Figure 1: Information sources and measures covered by the study

The results of this project are provided in the three parts. The **first part** contained the

- survey among incident response teams in Europe
- comparison with 2011 survey

The **second part**, the current document, covers:

- inventory of available methods, tools, activities and information sources for proactive detection of network incidents
- evaluation of identified measures and information sources

The **third part** covered:

- analysis of gathered data
- recommendations for policy makers in order to improve the detection of network security incidents in EU

Furthermore, the **current project has two formats: one is the present document which gives an overview of the findings and the other is a living document hosted on GitHub**[13] which aims to represent a point of reference to identify or reassess appropriate measures for proactive detection of incidents for new or well-established teams.

1.3 DEFINITIONS

1.3.1 Proactive versus reactive detection of incidents

As stated in the introduction and as previously used in the 2011 study, proactive detection of incidents is meant as a **process of discovery of malicious activity in a CSIRT team's constituency, before the affected constituents become aware of the problem.** On the other hand, when a CSIRT team receives an incident report, its role is only reactive - to respond accordingly to the report. In such perspective, a proactive approach can help in detection of incidents at an early stage of the attack or even before it happens.

1.3.2 Measure versus information source

In this study, "measure" is defined as a set of systems, tools and technologies deployed and used by CSIRT teams to provide information about features of a monitored network**.** Whereas "**information source**" is defined as **a source of data independent of the system producing it and consumed using its own, abstract method** as in the 2011 study. The main difference between these two categories is that tools and systems constituting measures have to be deployed and maintained in order to provide information, while the information source is provided as a service by other entity.

1.4 PREVIOUS ENISA WORK ON THE TOPIC

Since 2005, ENISA has been supporting Member States and CSIRT communities in the EU to build and advance their incident response capabilities with handbooks, online & onsite trainings and dedicated projects[14]. ENISA's portfolio of work is related to setting up, running and developing capabilities of Computer Security Incident Response Teams (CSIRTs). The goal is to identify common practices across the Union to improve operational cooperation, preparedness and information exchange for the next generation of cyber-attacks. More info can be found at https://www.enisa.europa.eu/csirt-services

[13] https://github.com/enisaeu/IRtools
[14] https://www.enisa.europa.eu/topics/csirts-in-europe

Relevant ENISA deliverables and activities comprise:

- Orchestration of CSIRT Tools[15]
- Reference Security Incident Taxonomy Working Group[16]
- Exploring the opportunities and limitations of current Threat Intelligence Platforms[17]
- Actionable Information for Security Incident Response[18]
- Standards and tools for exchange and processing of actionable information[19]
- Detect Share Protect - Solutions for Improving Threat Data Exchange[20]
- Proactive Detection of Network Security Incidents – Honeypots[21]
- Proactive Detection of Network Security Incidents – Data feeds – internal and external[22]

Moreover, the following relevant trainings are also available on ENISA website:

- Proactive incident detection: handbook and VM[23]
- Automation in incident handling: handbook and VM[24]
- Honeypots: handbook and VM[25]
- Presenting, correlating and filtering various feeds: handbook and 2 VMs[26]

[15] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational
[16] Reference Security Incident Taxonomy Working Group - RSIT- WG https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force
[17] ENISA, "Exploring the opportunities and limitations of current Threat Intelligence Platforms", 2018, https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms
[18] ENISA, "Actionable Information for Security Incident Response", 2015, https://www.enisa.europa.eu/publications/actionable-information-for-security
[19] ENISA "Standards and tools for exchange and processing of actionable information" https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information
[20] ENISA, "Detect Share Protect - Solutions for Improving Threat Data Exchange", 2013, https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs
[21] ENISA, "Proactive Detection of Network Security Incidents – Honeypots", 2012, https://www.enisa.europa.eu/publications/proactive-detection-of-security-incidents-II-honeypots
[22] ENISA, "Proactive Detection of Network Security Incidents – Data feeds", 2011, https://www.enisa.europa.eu/publications/proactive-detection-report
[23] ENISA, "Proactive incident detection training", https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#proactive-incident-detection
[24] ENISA, "Automation in incident handling training", https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#automation_incident
[25] ENISA, "Honeypots training", https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#honeypots
[26] ENISA, "Presenting, correlating and filtering various feeds training",https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#presenting--correlating-and-filtering-various-feeds

1.5 METHODOLOGY

This section describes the methodology used in different parts of the analysis.

Figure 2: Methodology

- Phase 1, 2 and 3 are detailed below.
- Phase 4 is detailed in “Proactive detection - Measures and Information sources”.
- Phase 5 and 6 are detailed in “Proactive detection - Gap analysis good practice and recommendations”.
- Phase 6 was performed collecting the input of the CSIRTs Network, the experts mentioned in the acknowledgements and via ENISA content approval workflow.
- Phase 7 is the publication on the ENISA website and GitHub repository.

1.5.1 Desktop research

Different knowledge sources were reviewed in order to provide an initial list of measures for proactive detection of network incidents. Particular tools and information sources were grouped into categories to give a more general overview independent of single tools. The goal was also to focus on the most crucial features, helping in proactive detection, provided by such a measures or type of tools.

For all categories open source examples have been identified and provided. The lists excluded ticketing/incident handling tools (like Request Tracker[27]), information sharing platforms (like MISP[28]) and forensics tools.

The above mentioned tools are covered in different extent by other ENISA activities and deliverables mentioned in the section 1.4.

1.5.2 Survey

ENISA asked members of the CSIRTs Network[29], TF-CSIRT[30] and FIRST[31] to contribute to this project by filling a survey on EU survey platform[32] available from 15th of October to the 29th of November 2019.

This survey aimed to gather information on methods, tools, activities and information sources currently used or planned to be implemented by incident response teams. The aim was to understand goals and expectations of respondents, as well as challenges in implementing available measures. The results will help to identify areas for growth and improvement and will allow to suggest recommendations for future developments.

1.5.3 Comparison with 2011 survey

The 2019 edition of the survey focused on different aspects of proactive detection of network incidents than the 2011 edition. Both surveys had different structure and some questions covered different matters. However, the results were compared according to the similarity of the questions, which was discussed for each analysed feature. When questions were too distant, only overlapping answers or results were taken into consideration. The comparison was performed using the obtained statistical results, but it also discussed the results on concrete answers.

[27] https://bestpractical.com/request-tracker
[28] https://www.misp-project.org/
[29] www.csirtsnetwork.eu/
[30] https://tf-csirt.org/
[31] https://www.first.org/
[32] https://ec.europa.eu/eusurvey/

2. SURVEY RESULTS

ENISA asked members of the CSIRTs Network[33], TF-CSIRT[34] and FIRST[35] to contribute to this project by completing a survey on the EU survey platform[36], available from 15th of October to the 29th of November 2019.

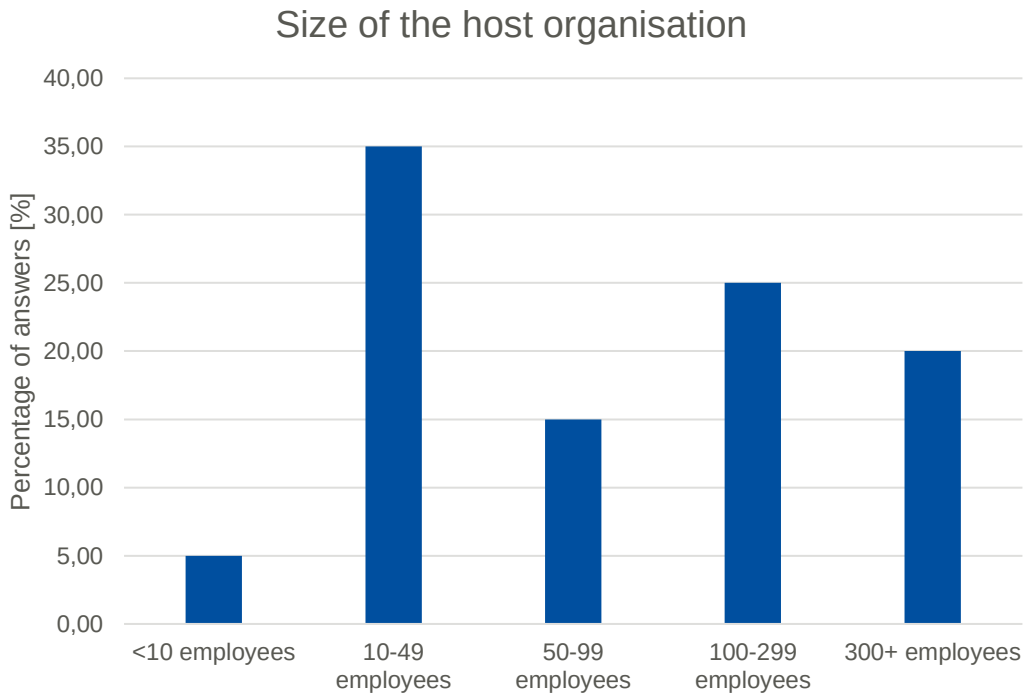
This survey aimed to gather information on the methods, tools, activities and information sources currently used or planned to be implemented by incident response teams. The aim was to understand goals and expectations of respondents, as well as challenges in implementing available measures. The results will help to identify areas for growth and improvement and will allow to suggest recommendations for future developments.

Answers provided by the surveyed teams indicate what problems with proactive detection of network incidents the teams face. The provided insight was used as a help in performing a gap analysis and in identification of common shortcomings. The survey results are presented below.

2.1 RESPONDENTS PROFILE

The survey was answered by 20 teams. The size of the respondents' host organisation is presented in fig. 3.

Figure 3: Size of the host organization.

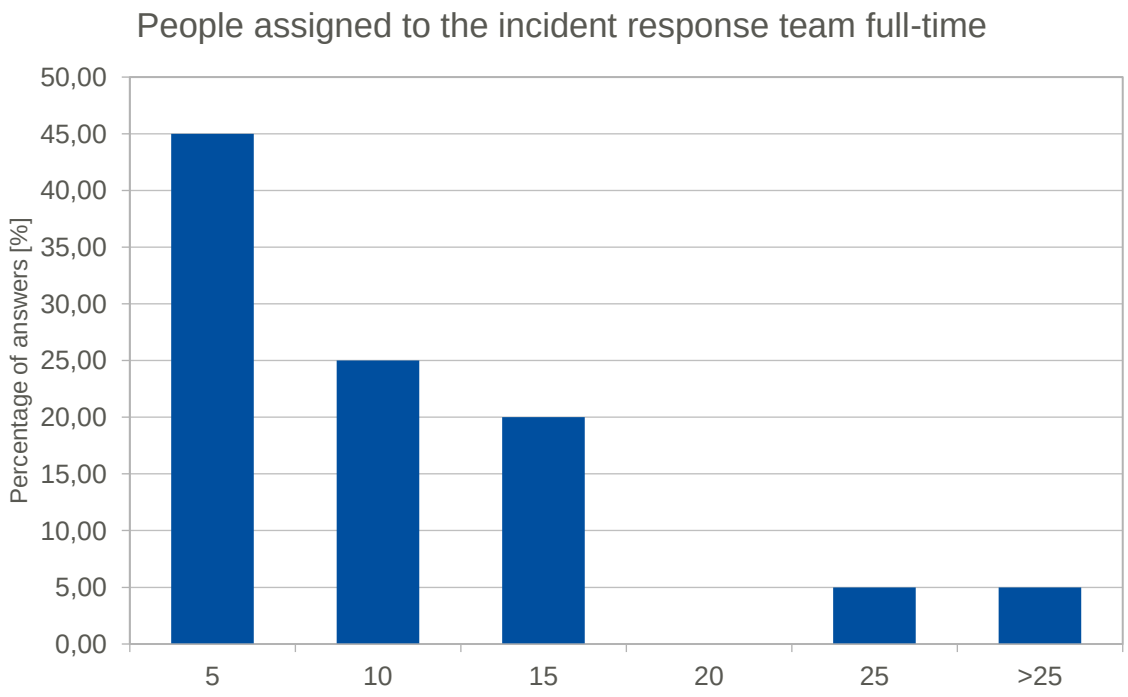


For 35% of teams, the host organisation employs between 10-49 people, which is followed by 25% of teams associated with organisations employing 100-299 people. Only one team (5%)

[33] www.csirtsnetwork.eu/
[34] https://tf-csirt.org/
[35] https://www.first.org/
[36] https://ec.europa.eu/eusurvey/

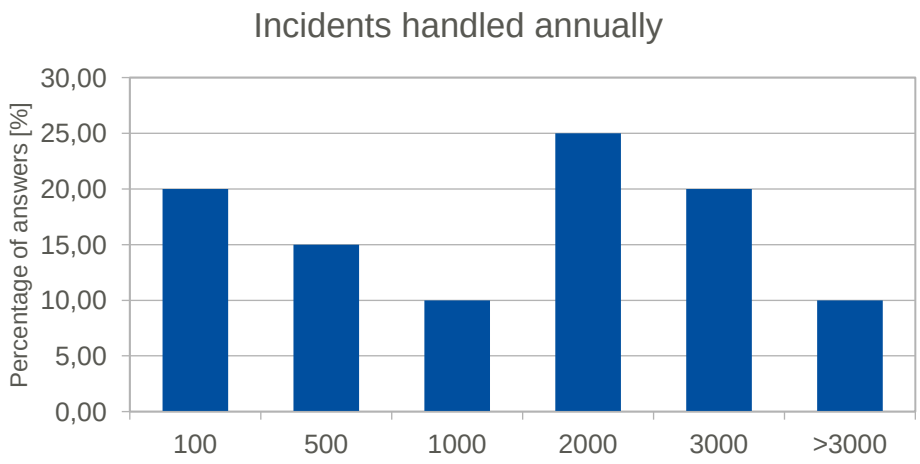
is located in an organisation with less than 10 people. No organisation is smaller than 10 people. Fig. 4. presents number of people who are assigned to the incident response team full-time.

Figure 4: Number of people assigned to the incident response teams full-time.



Almost half of the teams (45%) has up to 5 people assigned to manage incident response full-time, this includes one team, which stated that it has no person assigned to it full time. Additionally one team has 200 people assigned to handle incident reports. Fig. 5. shows the number of incidents handled by the teams annually.

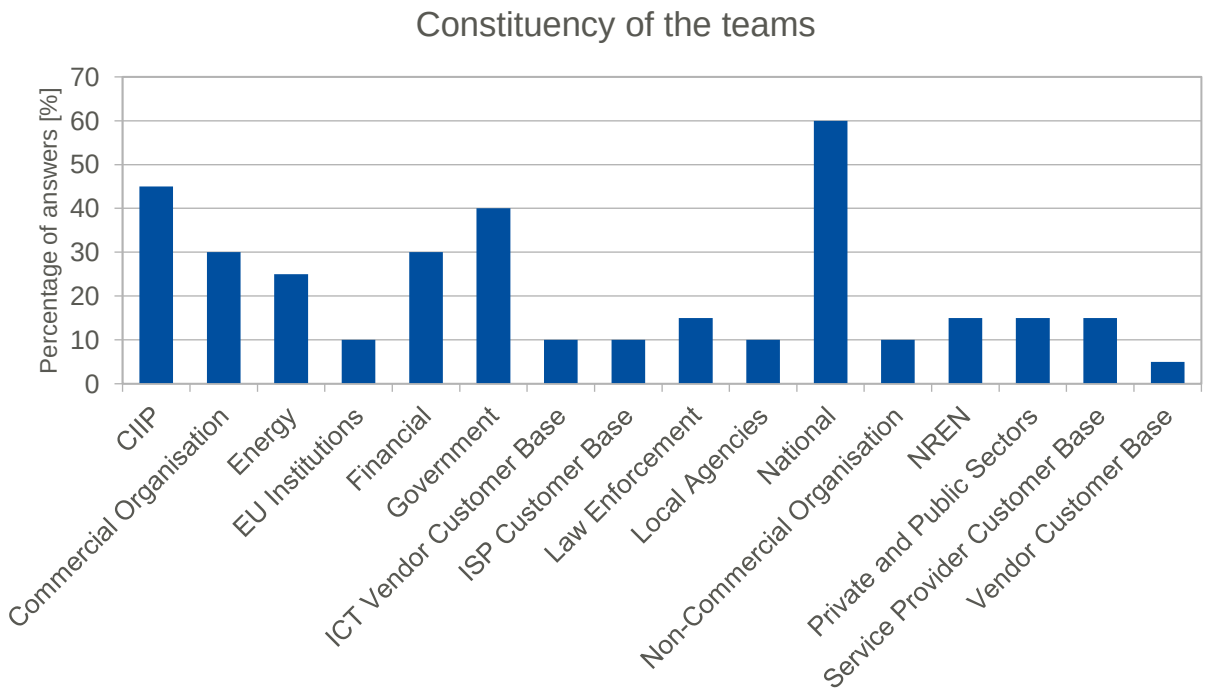
Figure 5: Number of incidents handled by the teams annually



20% of teams (4 answers) handle up to 100 incidents per year. This includes two teams with 4 incidents and one team with 10 incidents in a year. **25% of the teams handle between 1001-2000 incidents annually.** Two answers (10% of the teams) stated at least 3000 incidents

handled: one was exactly that number and the second one was 100 000 incidents. Fig. 4 presents constituency of the teams. Please note that percentages do not add, because multiple answers could be selected.

Figure 6: Constituency of the teams



60% of the teams represent national CSIRTs, 45% CIIP and 40% governmental. The vendor customer base is represented only by one team (5%).

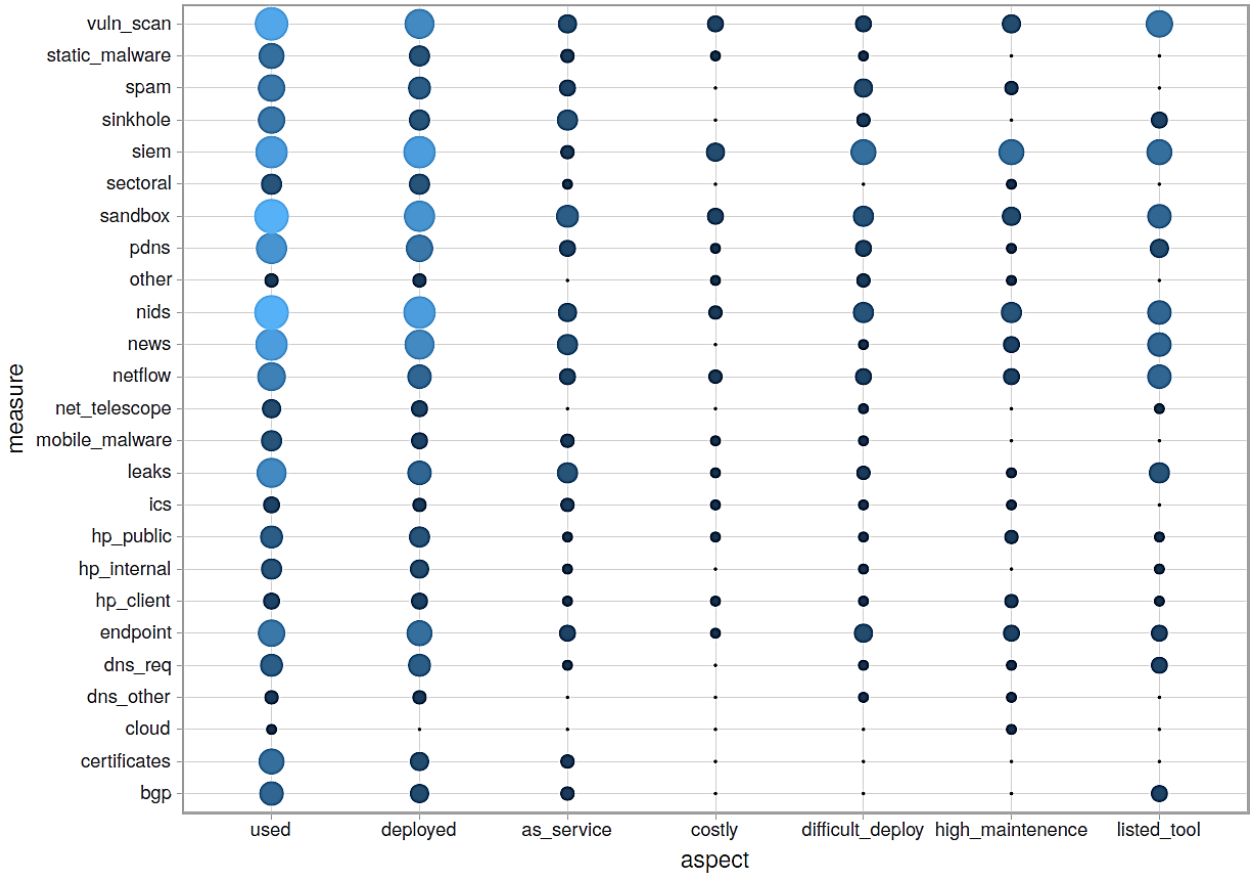
Please note that percentages do not add up to 100%, because multiple answers could be selected.

2.2 MEASURES FOR PROACTIVE DETECTION OF NETWORK SECURITY INCIDENTS

2.2.1 Adoption of measures

Respondents' opinions about various measures for proactive detection of network incidents is presented in fig. 7.

Figure 7: Adoption of measures.



The results of the survey show that **all of the identified measures have some real-life use**, however the adoption levels vary significantly. The **most common measures are sandboxes and network intrusion detection**, followed by vulnerability scanners, SIEM platforms, Passive DNS systems and news monitoring. The **least common are cloud monitoring systems**, followed by other DNS monitoring systems. The list of measures proved to be sufficiently extensive, as all additional tools for proactive detection suggested by participants could be mapped to one of the categories (if they were in scope at all).

The **most common systems deployed in-house by the teams are SIEM and NIDS systems**, followed by vulnerability scanners and news monitoring. The least often deployed measure is cloud monitoring.

The most often used measures, when used as an external service, are sandbox systems, followed by sinkhole, news monitoring and leaks monitoring systems**. The least often used measures in as a service scheme are network telescope,** other DNS monitoring systems and cloud monitoring systems.

2.2.2 Evaluation of measures

The teams evaluated the **financial cost of measures** (including licenses, hardware and services). According to the answers the **most costly are SIEM systems**, followed by vulnerability scanners and sandbox systems.

When asked whether measures required **significant effort and/or expertise to implement/deploy**, the teams identified **SIEM systems as the most difficult**. This measure

was followed by sandbox and NIDS systems. **The least problematic are sectoral monitoring systems, cloud monitoring systems, X.509 monitoring systems and BGP monitoring systems.**

The teams also evaluated whether the measures require substantial **effort to maintain**. **SIEM systems were identified as having the highest requirements**, followed by NIDS systems. **The least level of maintenance** requirements are needed by **static malware analysis systems**, sinkhole systems, network telescopes, mobile malware analysis systems, and server honeypots in internal networks, X.509 monitoring systems and BGP monitoring systems.

The teams were also asked about the **usage of the tools or services** from the list of examples provided for particular measure. Answers identified examples of **vulnerability scanners as the most commonly used among the teams**. They were followed by SIEM systems, sandboxes, NIDS, news monitoring systems and network flow monitoring systems**. The least used were static malware analysis systems**, spam systems, sectoral monitoring systems, mobile malware analysis systems, industrial control systems monitoring systems, other DNS monitoring systems, cloud monitoring and X.509 monitoring systems.

Based on the responses about **additional tools used by the teams**, the following tools were added to the inventory: **BGPmon[37], Nessus[38], Velociraptor[39], Sigma[40], Winlogbeat[41] and Taranis[42]**. Some of the answers referred to tools that are used for incident response, information processing or incident management but they were not included in the inventory, since these activities do not fit in the scope of this study.

2.2.3 Evaluation of the usefulness of example tools

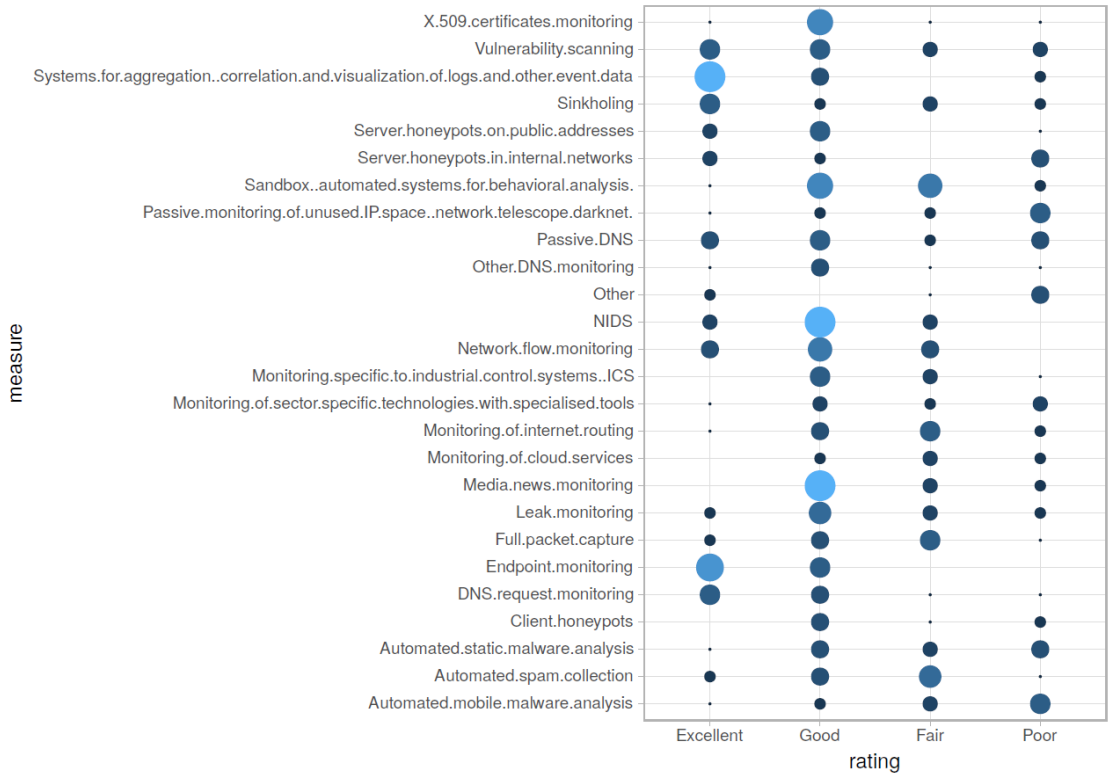
Example tools of all measures were evaluated by the teams using below scale:

- **Poor:** Information provided by measures in this category is not useful for proactive detection for your team. Note: data can still be useful during incident analysis, for example to provide more context for pivoting.
- **Fair:** There are cases when your team used measures in this category to detect incidents proactively, but it is quite rare.
- **Good:** Measures in this category are often useful to detect incidents in your constituency.
- **Excellent:** For your team, measures in this category are very important to proactively detect incidents.

The results of the evaluation are presented in fig. 8.

[37] https://bgpmon.net/
[38] https://www.tenable.com/products/nessus
[39] https://www.velocidex.com/
[40] https://github.com/Neo23x0/sigma
[41] https://www.elastic.co/downloads/beats/winlogbeat
[42] https://github.com/NCSC-NL/taranis3

Figure 8: Evaluation results.



The example tools most often evaluated as **excellent belong to the systems for aggregation, correlation and visualization of logs and other event data** measure, followed by endpoint monitoring.

The majority of example tools were evaluated as good. These include **NIDS systems, media/news monitoring, but also X.509 certificates monitoring and sandbox systems**.

Tools most often rated as fair include sandbox system and automated spam collection. This is the second most chosen rating by the teams.

Finally, some tools were evaluated generally poor. These include automated mobile malware analysis, passive monitoring of unused IP space and server honeypots in internal network.

Overall, the provided example tools are evaluated as good or excellent by the teams, with some exceptions rated as fair or poor. Examples of tools for endpoint monitoring and systems for aggregation, correlation and visualization of logs and other event data measure, are very important for the teams in proactive detection of network incidents.

2.2.4 Deficiencies in measures

25% of respondents were fully satisfied with their current set of measures. On the other hand, **75% of respondents provided measures which their organization lacks**. One team provided answers mentioning lack of SOC division and compliance with international standards. Other teams identified lack of:

- endpoint monitoring,

- X.509 certificates monitoring,
- cloud monitoring (including configuration compliance, asset management),
- flow monitoring,
- DNS request monitoring,
- dynamic mobile malware analysis,
- network telescope monitoring,
- logging systems with sufficient retention and correlation capabilities,
- system for OS identification from network traffic.

As main obstacles respondents indicated insufficient financial and human resources, lack of management support, insufficient (or lack of) law authority, trust issues with implementation, lack of expertise, lack of cooperation of the network owners, high network load, data privacy regulations, problem with license models for iOS and lack of products for that platform, problems with deployment and support, problems with constituency coordination, in terms of onsite deployment and maintenance, vendor cooperation and quality delivery.

2.2.5 Gaps in tooling

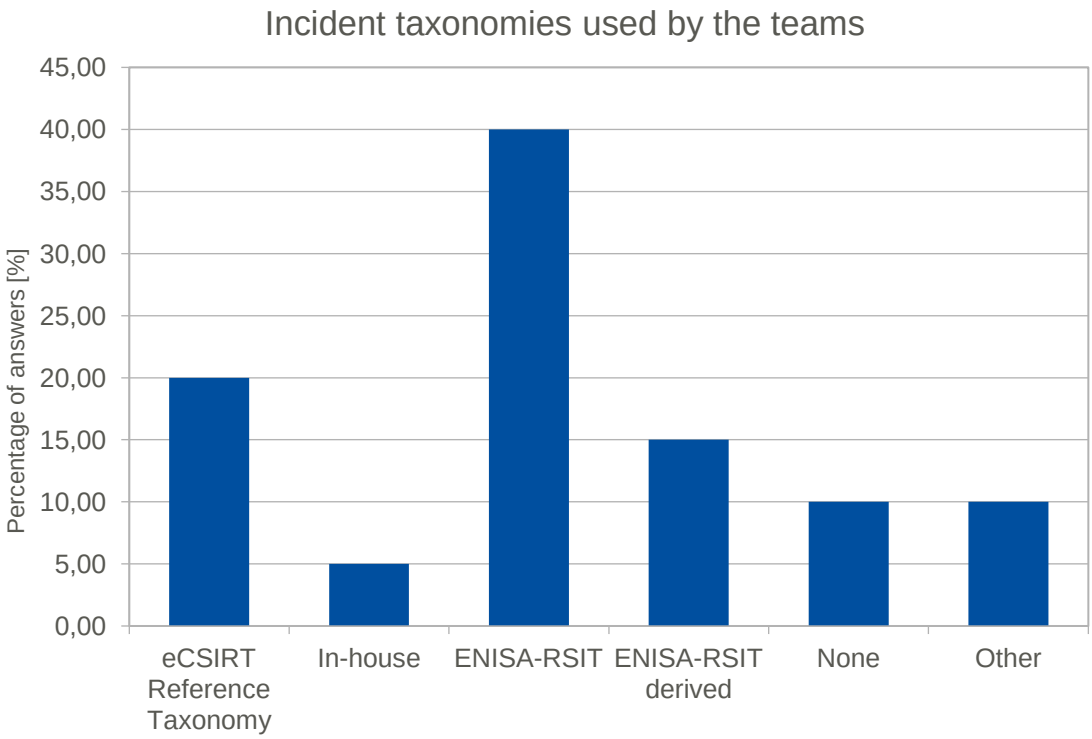
Respondents identified some gaps in tooling. These include **problems with interaction of different systems (including clear API documentation, standards of data exchange and data formats**), lack of privacy aware data structures. These issues cause problems with correlation of data, as different formats and sources are hard to deploy in one monitoring system. Furthermore, **tools lack automatic classification of output.** Also some of the teams identified problems in their constituency - as it prevents them from monitoring of some networks. The answers indicated also **problems with good practice on implementation, policy and deployment of the measures.**

Respondents also shared comments about **gaps in open source and commercial tooling**. The main identified issue is the **higher requirement of human resources for deploying and management of open source systems**, whereas commercial tooling is too expensive for budgets of some organizations. Also vendors often require the sharing of IOCs/signatures/samples.

2.2.6 Taxonomy used to categorize collected data

The teams provided answers about taxonomies used to categorize collected data. Their breakdown is presented in fig. 9

Figure 9: Incident taxonomies used by the teams.



40% of teams use the new Reference Security Incident Taxonomy (RSIT)[43], the product of a TF-CSIRT WG and supported by ENISA, and another 15% of teams use taxonomy derived from it, giving overall 55%. Another 20% of teams uses eCSIRT reference taxonomy[44] [45]. One team did not provide any answer and another one stated it did not use any taxonomy - these answers are categorised as “None” and consist of 10% of answers. VERIS[46] and an in-house developed taxonomy are used by one each. Finally, only one respondent specified multiple MISP taxonomies and galaxies[47] as their main approach.

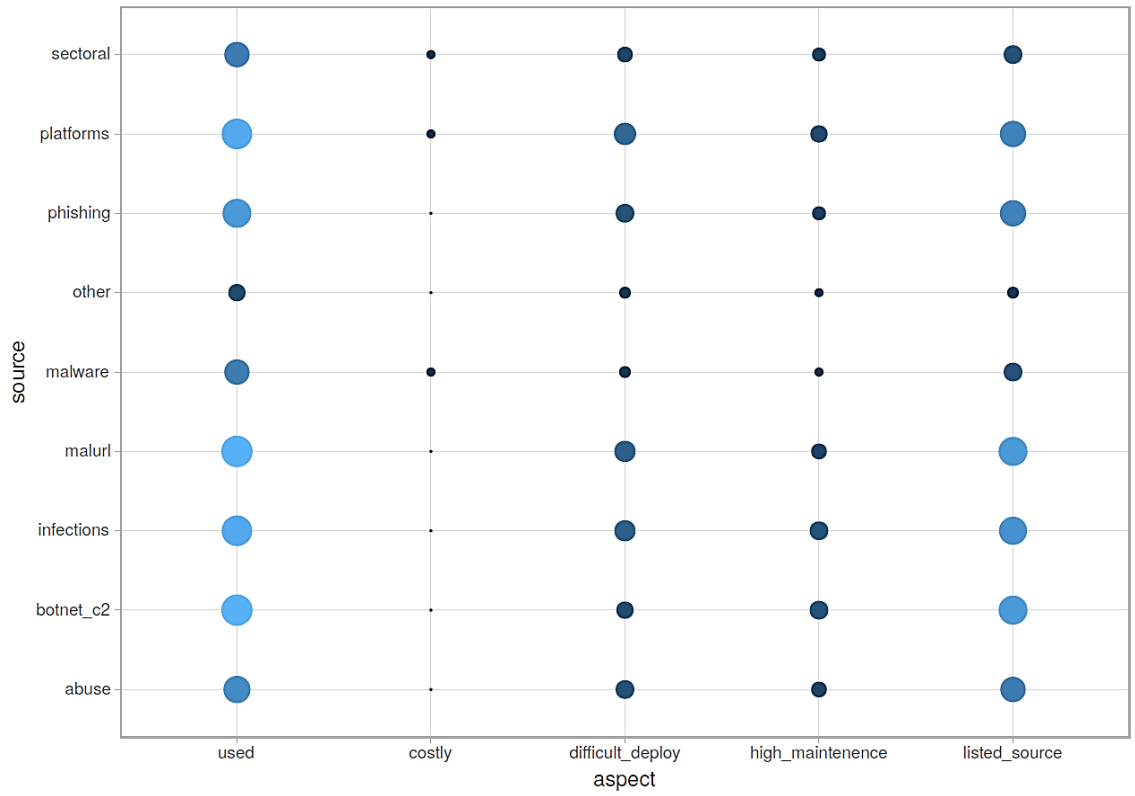
2.3 INFORMATION SOURCES FOR PROACTIVE DETECTION OF NETWORK SECURITY INCIDENTS

2.3.1 Usage of information sources

The teams have provided answers regarding various aspects of information sources for proactive detection of network incidents. The results are presented in fig. 10.

[43] https://github.com/enisaeu/Reference-Security-Incident-Taxonomy-Task-Force
[44] http://www.ecsirt.net/
[45] The RSIT taxonomy was developed using eCSIRT.net as a starting point.
[46] http://veriscommunity.net/
[47] https://github.com/MISP/misp-taxonomies

Figure 10: Usage of information sources.



The provided categories of information sources are commonly used by the teams. Only sector specific, repositories of malware samples, feeds with information on sources of abuse and other structured types of information sources categories are less often used.

All information source categories are perceived as relatively cheap when considering financial cost (licenses, hardware, and services) in comparison to other categories. Only information sharing platforms, repositories of malware samples and sector specific advisories were identified as having slightly higher cost.

The teams evaluated requirement of effort and/or expertise to integrate the information source categories. **The lowest level of effort has been assigned to the repositories of malware samples and other structured types of information sources categories. The highest requirements have feeds of malware URLs, feeds of infected machines (bots) and information sharing platforms.**

All information source categories are indicated as relatively easy to maintain, with the lower level of requirements for repositories of malware samples and other structured types of information sources categories.

The examples of information sources listed in the survey are commonly used by the teams. Only examples of repositories of malware samples and sector specific advisories are less often used by the teams.

The respondents also provided a list of information sources which were not specified in the survey. These include **commercial threat intelligence sources, search engine queries with queries, inter-sectoral data exchange via MISP, client reports, and governmental CSIRT reports.**

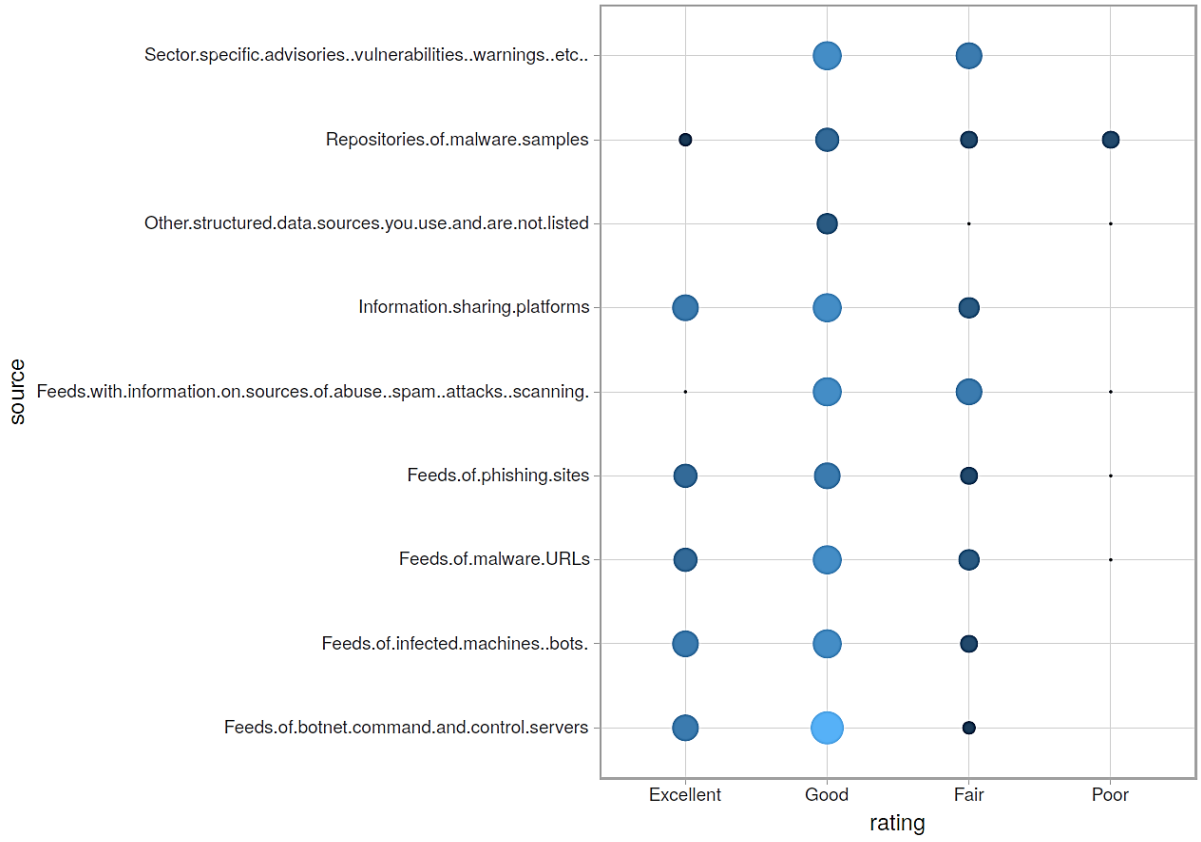
2.3.2 Usefulness of information sources

The respondents evaluated usefulness of information source examples provided with the survey. Following criteria were used:

- **Poor:** Information provided by sources in this category is not useful for proactive detection for your team. Note: data can still be useful during incident analysis, for example to provide more context for pivoting.
- **Fair:** There are cases when your team used sources in this category to detect incidents proactively, but it is quite rare.
- **Good:** Sources in this category are often useful to detect incidents in your constituency.
- **Excellent:** For your team, sources in this category are very important to proactively detect incidents.

The results are presented in fig. 11.

Figure 11: Usefulness of information sources.



The provided examples of information sources are mostly regarded as excellent or good. The exceptions are repositories of malware samples, feeds with information on sources of abuse and sector specific advisories. They are seen also as fair or poor (when regarding the repositories of malware samples).

2.3.3 Satisfaction with defined aspects of information sources (including comments)

The respondents evaluated satisfaction regarding information sources used by their teams. The following criteria were used in the survey:

- **Relevance**: Relevant sources provide information that is mostly applicable for protection of your constituency. Not relevant sources might provide data outside the scope of the services offered by the team or about sectors or regions not in your area of interest.

- **Accuracy**: Accurate sources are trustworthy/reliable. Inaccurate ones bring high risk of false positives, attacks that have never happened or other erroneous information.

- **Timeliness**: Timely sources provide information on threats as they occur, with minimal delay and have high availability. Sources that introduce significant delay, provide stale information or are often not available are not useful for proactive detection.

- **Completeness**: Complete information should have enough context/details to allow for detection of incidents. Incomplete information lacks details that are essential for detection and defense, for example timestamps or addresses.

Information sources most commonly perceived as relevant belong to feeds of malware URLs, followed by feeds of phishing sites and feeds of botnet command and control servers. **The most accurate, according to the answers, are feeds of infected machines (bots),** followed by feeds of malware URLs. **The most timeliness are feeds of malware URLs and information sharing platforms. Feeds of phishing sites are regarded as having the highest completenes.**

The respondents provided observations regarding relevance, accuracy, timeliness and completeness of the data sources. Firstly, the **teams observe an increase of false positives with the increase of size of sharing community.** According to the respondents it is particularly true in the education/research sector, where environment and user behavior is very diverse. Secondly, **timestamps of events are missing,** that is information when the event started and when ended. Without such information, teams cannot determine whether the incident was handled.

2.3.4 Evaluation of capabilities to handle the current amount of information

The teams evaluated their capabilities to handle the current amount of information, both in terms of available personnel and tools**. Half of the teams can process all incoming information, however only high priority incidents are handled.** An increase of information would increase the number of low priority incidents without analysis. 35**% of the teams stated that they receive too much information to handle it properly,** what causes that some is ignored or discarded. Finally, **15% of the teams can fully handle the amount of information they receive or collect and could handle even more.** None of the teams provided answer that they handle current amount of information, but would not be able to handle much more.

It is an important observation, that **only 15% of the teams can fully handle the information, while 35% of the teams are overwhelmed with it. It is a good starting point for further analysis whether automation/better tools, better formats or more human resources would help these teams.**

2.3.5 Gaps in information sources

In general the **biggest gap of the available information sources is the insufficient context, i.e. poor information completeness.** This includes, but is not limited to, to lacking details on how certain information was obtained or what is the estimated confidence level. The second important challenge is **format and taxonomies**. It refers both to the **varied formats, protocols and API used by information providers but also perceived lack of common classification of events and inconsistent identifiers** (while no specific examples were provided, this might be a problem with malware names).

Other issues reported by some of the respondents include the following:

- **Lack of suitable methods for distributing IoCs to constituents**, in a way that they will actually use it for correlation with the logs from their internal infrastructure. Note: This is not a gap in the information sources as such but more of a general information sharing issue that falls outside of the scope of this study.

- **Insufficient quality (especially false positives) of the open source information sources.** (Answer provided by a non-CSIRTs Network member)

- Both open source and commercial information sources are described as requiring additional effort to provide quality rating.

2.3.6 Advantages of commercial sources

The teams shared their observations about what kind of commercial sources has advantage over open source ones. Commercial offerings were reported as a better source for IDS rules, threat and malware intelligence platforms, vulnerability and Internet scanners, and threat hunting platforms. One team also stated that commercial feeds have better coverage of targeted attacks.

2.3.7 Missing types of information sources in organisations (including obstacles preventing from using them)

The respondents also identified information sources which their organization lacks. A **major area** for improvement is **better sharing of information from constituents.** The importance of this sort of source is obvious, given its relevance for each team**. Other gaps mentioned include information about darknet/darkweb (including Tor .onion services), a feed of compromised websites (including malicious HTML/JavaScript patterns)** that would be actively maintained and information on zero day vulnerabilities. Only two teams are fully satisfied with their current sources and two stated that they lack “a lot” of sources.

The teams also identified HaveIBeenPwned[48], NormShield[49] and Blueliv [50] as information sources used by them, but absent in the list.

The **main problem** that prevents teams from using various information sources is the fact that their **integration requires investment of time and many teams face insufficient human resources**. One of the respondents reported unwillingness of cooperation from the potential providers as another issue blocking obtaining the information needed.

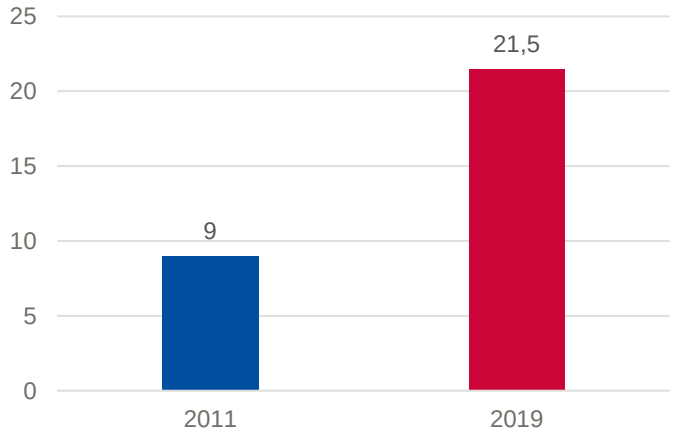
[48] https://haveibeenpwned.com/
[49] https://www.normshield.com/
[50] https://www.blueliv.com/

3. COMPARISON WITH 2011 SURVEY

Results of the survey can be compared to the 2011 edition of the study, when a similar survey was conducted. The 2011 edition was answered by 45 teams, while this edition, by 20 teams.

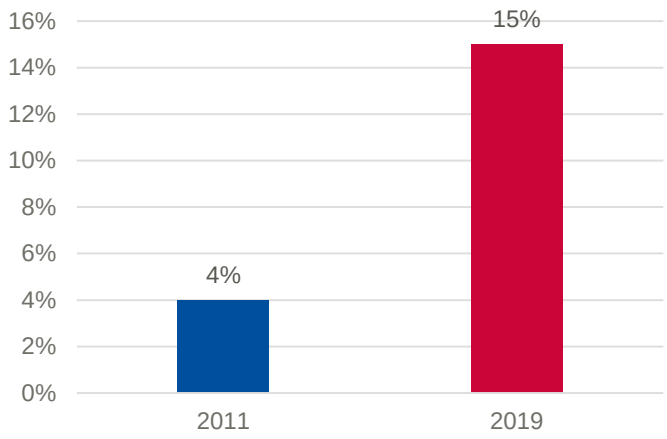
Beginning with respondents' constituency (organisation profile in the 2011 edition), it should be noted that different categories have been used to group the teams. Nevertheless, in 2011 33% of teams represented government/public administration and 32% - the academic sector. In this edition, 60% of the teams indicated they represented the national level, 40% represented the governmental level, and 15% represented NREN institutions. In the 2011 edition financial institutions were represented by 7% of the teams, while in this edition - 30%. When considering the number of incidents handled by the teams annually, in the 2011 edition the range was between 10 incidents to 2 million incidents, while in the 2019 edition it was between 4 incidents to 100,000 incidents. The number of people assigned to the incident response full time in 2011 ranged from 0.5 to 41 (average 9), while in 2019 it was between 0 and 200 (average 21,5).

Figure 11: Number of people assigned to the incident response full time.



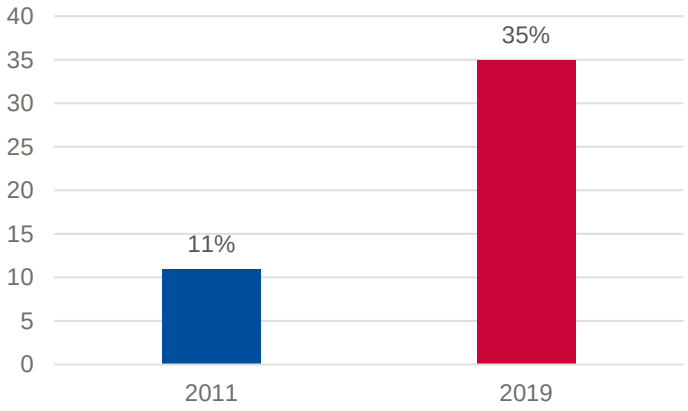
The 2011 survey checked general feelings regarding information sources in the respondent's constituency, while the 2019 survey asked "What type of information sources does your organisation lack?". These two questions are different, however some of the answers could be mapped on each other. **In 2011, 4% of the teams stated that they were fully satisfied with information sources they had, while in the 2019 edition it was 15% of the teams.** In 2011, 47% of the teams stated that they felt general information deficit. It could be compared to the 2019 answers, where 10% teams stated lack of majority of information sources and additional 20% of teams provided information about particular information source types.

Figure 12: Teams stated that they were fully satisfied with information sources they had



Both editions of the survey evaluated capabilities to handle the current amount of information. **The percentage of teams capable of processing all incoming information, however provided that only high priority incidents are handled, is nearly the same in both editions**: 45% of teams in 2011 and 50% in 2019. The number of teams which can fully handle the amount of information they receive or collect and could handle even more decreased from 31% in 2011 to 15% in 2019. **In 2019 35% of the teams stated that they receive too much information to handle it properly, as a result of which some of it is ignored or discarded. This constitutes an increase from 2011, when such an answer was provided by 11% of the teams.**

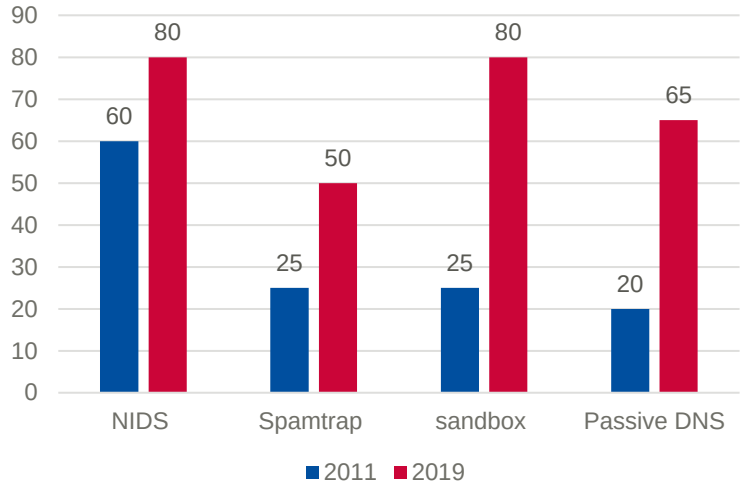
Figure 12: Teams stated that they receive too much information to handle it properly.



The 2011 edition of the survey evaluated usage of different categories of tools for gathering information from the internal network. The 2019 edition used different set of categories, however some of them overlapped**. In 2011, about 60% of the teams used network flow monitoring, in 2019 the level is 55%. NIDS systems were used by about 60% of the teams in 2011, in this year's edition the number increased to 80%**. In 2011, about 40% of the teams used server honeypots, while in 2019 - 25% of the teams used them. In 2011, darknet was monitored by about 30% of the teams, in 2019 it is monitored by 20% of them. **Spamtrap systems were used by slightly more than 25% of the teams in 2011, while in 2019 they are used by 50%. A little more than 25% of the teams used sandbox systems in 2011, while in 2019 the number increased to 80%. Passive DNS monitoring was performed by about 20% of teams in 2011 - in 2019 the number has risen to 65%.** Finally, client honeypots were used by slightly more than 15% of the teams in the previous survey and in 2019 they are used

by 15% of them. **Overall, the adoption of some measures increased, these include spamtrap systems, NIDS, sandbox systems and passive DNS monitoring.** The usage of other measures' decreased, including network flow monitoring, darknet monitoring, server and client honeypots.

Figure 13: Adoption of some measures increased – percentage.



The 2011 edition of the survey asked about the method and priority of acquiring incident-related data about a constituency. The respondents could provide answers on different categories of systems, grouping into internal monitoring, external public sources, commercial sources, closed sources and incoming incident reports. In the 2019 edition of the survey a question about the in-house deployment of measures was asked. The categories of measures do not map on 1:1 scale between the editions of survey, as well as the structure of the answers. Nevertheless, some general observations can be made regarding the comparison of results. In the 2011 edition the teams indicated that the primary source of information about incidents came from incident reports, then from internal monitoring and monitoring of closed sources. Furthermore, internal monitoring was not used at all by about half of the teams**. A majority of the measures from the 2019 edition of the survey can be categorised as internal monitoring** (as stated in the 2011 edition " Systems deployed internally, such as firewalls, IPS or antivirus software."). These measures are adopted between 10% (ICS systems) to 70% (NIDS systems) of the teams. The median of their adoption is 30%, while the average is about 35%. Discrepancy between the results for both editions of the survey can be explained with the usage of different categories of sources and incident reports having been added as answer in the 2011 survey.

Both editions of the survey evaluated examples of information sources for proactive detection of network incidents. However, only three examples of sources can be found in both surveys. The main reason of this misalignment is that during 8 years dividing the surveys, some of the sources ceased to operate or were superseded by newer source types/services. Despite this fact, the surveys can be compared, provided that the examples from the 2011 edition are categorised using groups of the 2019 survey and rating information that has been appropriately aggregated. With the use of such an approach, the best rating in the 2011 survey had feeds of malware URLs, phishing sites, command and control servers and infected machines. These observations are similar to those from 2019 edition. Furthermore, in 2011 some of the categories were not widely represented, for example: repositories of malware samples and sector specific advisories. Also, **the 2019 survey shows that not only the quantity but also the number of types of information sources increased.**

Both versions of the survey asked respondents about a comparison of open source and closed source (2011 edition)/commercial (2019) information sources. Despite the fact that closed source information sources can be non-commercial, that are provided for free, these two categories are regarded as similar in the remainder of this paragraph. In the 2011 edition, the respondents indicated that closed sources provided better accuracy, timeliness, reliability and quality of information. According to the answers the closed sources share information before it is known publicly, however such information is provided less frequently. **In the 2019 edition, the respondents stressed insufficient quality (especially regarding false positive levels) of the open source information sources. Both open source and commercial information sources are described as requiring additional effort to provide quality rating**.

In both editions of the survey respondents shared comments on gaps and missing tools and, depending on the year, services (2011) or information sources (2019). **Firstly, some measures are identified in both editions as absent in the teams inventory, these include network flow monitoring or DNS monitoring. Secondly, a significant difference is seen in the domains of systems, which are identified as generally missing. In 2011, the teams indicated lack of visualisers, IDS/IPS systems, centralised tools for management of different source information, P2P network traffic detection or systems detecting SQLi attacks. Based on answers from the 2019 edition, advancement of some security domains is seen.** Some particular measures were absent in comments to the previous edition, partly due the fact that the associated technologies were still in development or they did not exist. These include: endpoint monitoring, cloud monitoring, dynamic mobile malware analysis or X.509 certificates monitoring. **Nevertheless, in both editions, the respondents identified problems with correlation of data, standardisation of formats and interaction between tools/systems. It is directly connected with lack of sufficient systems for retention and correlation of information. During 8 years separating the surveys these issues were addressed by some projects, however they seem to be still unresolved.**

In both editions of the survey, the teams shared problems facing proactive detection of network incidents: **either to collect information about incidents or preventing them from deploying measures/information sources. In both editions the teams raised legal issues, privacy regulations and problems with incident visibility, due to the fact that the teams do not have control on the monitored network**. They indicated also the unwillingness to cooperate and excessive amounts of data. In 2019, the teams also pointed out insufficient financial and human resources, and problems with lack of good practices on implementation, policy and deployment.

4. GLOSSARY AND ACRONYMS

Please refer to ENISA glossaries and lists of acronyms

- https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/glossary
- https://www.enisa.europa.eu/topics/csirts-in-europe/glossary
- https://www.enisa.europa.eu/media/media-press-kits/enisa-glossary

TP-01-20-306-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

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

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

enisa.europa.eu

ISBN: 978-92-9204-346-9
DOI: 10.2824/01659