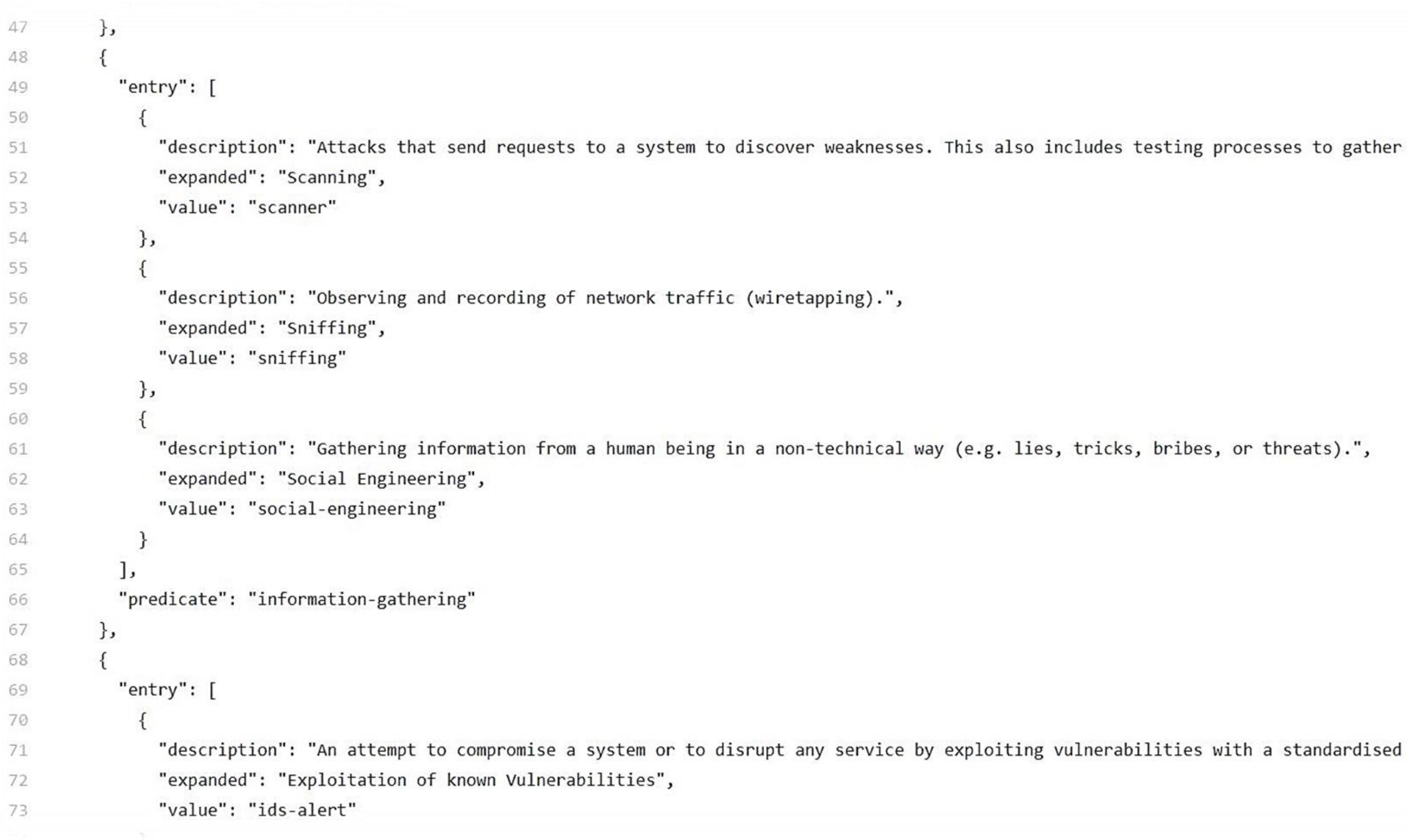
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



```
        },
        {
          "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 - GOOD PRACTICES GAP ANALYSIS RECOMMENDATIONS

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

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

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 entitled “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.

The results of the 2019 survey and comparison with the 2011 edition have been already covered in the first document of this series already available on the ENISA website. In second document, also already available on the ENISA website, we provided an overview of **available methods, tools, activities and information sources** for proactive detection of network incidents that were inventoried and evaluated. **The present document covers the good practices identified, gap analysis and recommendations.**

The **gap analysis identified fields for potential additional work and analysis**. This includes **data harmonization, automated malware analysis, cloud monitoring, sector-specific measures and information sources, routing monitoring and automated collection of spam.** Measures such as honeypots, network telescopes and monitoring of DNS requests are not universally deployed. 75% of the survey’s respondents provided measures which their organisations lacked. **Main obstacles include 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 and data privacy regulations**. When regarding information sources, the respondents indicated **insufficient context of information, including lack of confidence level and how information was obtained, different formats, protocols and APIs providing information, along with inconsistent identifiers and common classification**.

Key recommendations for CSIRT teams are firstly to consider implementing a measure for proactive detection of network incidents such as **endpoint monitoring with SIEM systems, network monitoring with NIDS systems, but also network flow logging, analysis of DNS and media monitoring**. Secondly, to maintain a **roadmap of information sources that are most relevant to the team’s operations and evaluate available offerings on the marke**t.

[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

To perform proactive detection of network incidents, CSIRT teams require appropriate skills, time, tools and resources. Part of these are the responsibility of the CSIRT host organisation, however some actions can be suggested to be evaluated at European level. These include **development of improvements in the tooling ecosystem, data harmonization, vendor-neutral and open source focused trainings, evaluation of information sources and interoperability between tools and systems**.

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

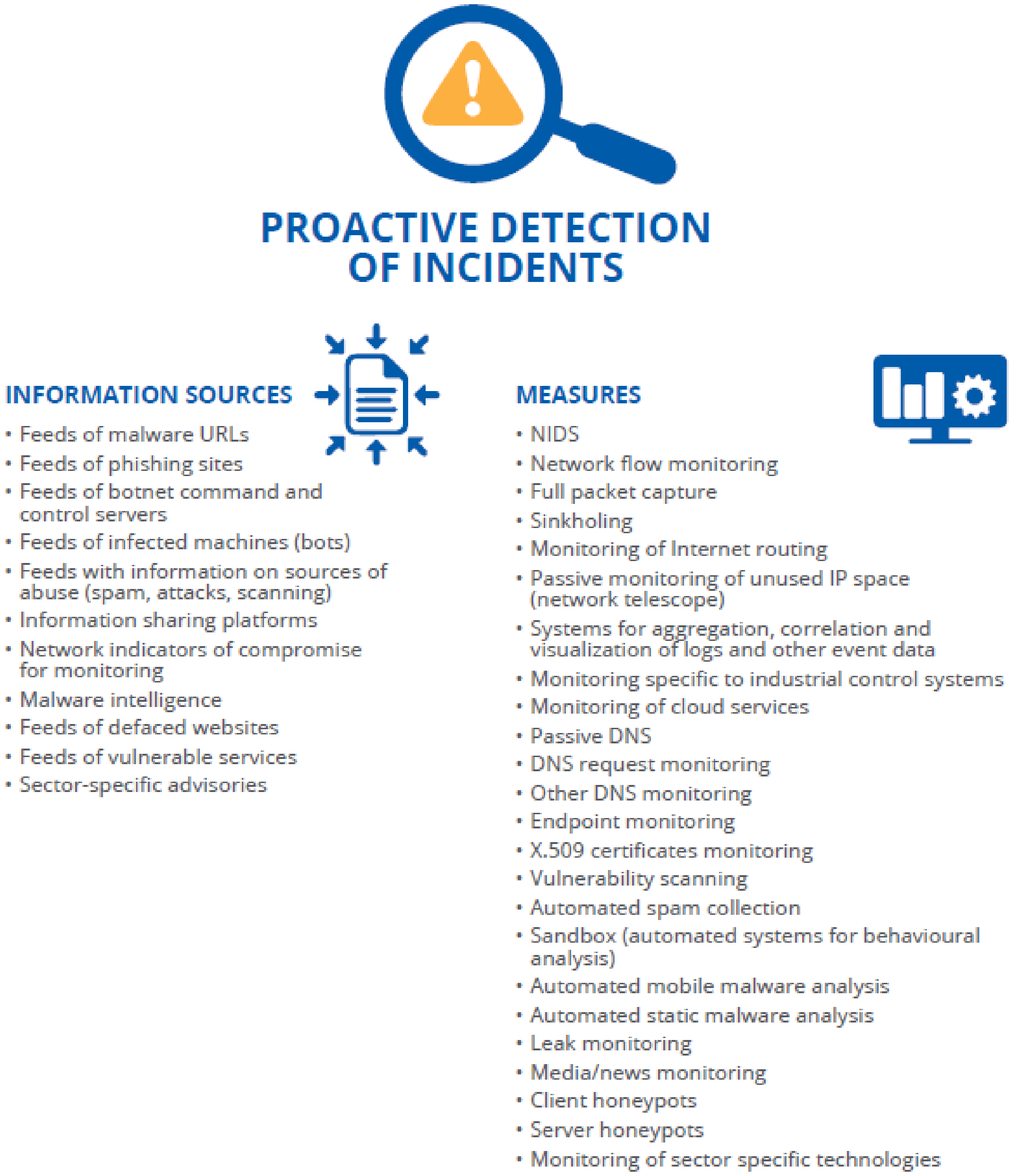
proactive detection of network security incidents, which are used already or potentially could be used by incident response teams in Europe nowadays.

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



PROACTIVE DETECTION OF INCIDENTS

INFORMATION SOURCES

- Feeds of malware URLs
- Feeds of phishing sites
- Feeds of botnet command and control servers
- Feeds of infected machines (bots)
- Feeds with information on sources of abuse (spam, attacks, scanning)
- Information sharing platforms
- Network indicators of compromise for monitoring
- Malware intelligence
- Feeds of defaced websites
- Feeds of vulnerable services
- Sector-specific advisories

MEASURES

- NIDS
- Network flow monitoring
- Full packet capture
- Sinkholing
- Monitoring of Internet routing
- Passive monitoring of unused IP space (network telescope)
- Systems for aggregation, correlation and visualization of logs and other event data
- Monitoring specific to industrial control systems
- Monitoring of cloud services
- Passive DNS
- DNS request monitoring
- Other DNS monitoring
- Endpoint monitoring
- X.509 certificates monitoring
- Vulnerability scanning
- Automated spam collection
- Sandbox (automated systems for behavioural analysis)
- Automated mobile malware analysis
- Automated static malware analysis
- Leak monitoring
- Media/news monitoring
- Client honeypots
- Server honeypots
- Monitoring of sector specific technologies

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** covered:

- 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**, the current document, covers:

- 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

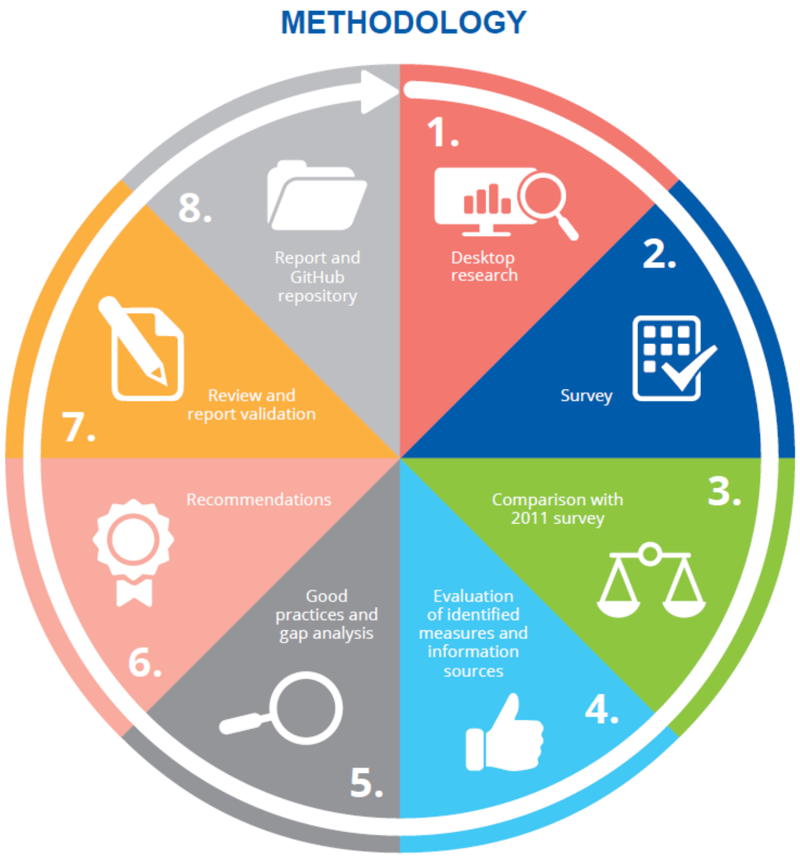
[25] ENISA, “Honeypots training”, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#honeypots

[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


METHODOLOGY
1.
Desktop research
2.
Survey
3.
Comparison with 2011 survey
4.
Evaluation of identified measures and information sources
5.
Good practices and gap analysis
6.
Recommendations
7.
Review and report validation
8.
Report and GitHub repository

- Phase 1, 2 and 3 are detailed in “Proactive detection – Survey results”.
- Phase 4 are detailed in “Proactive detection – Measures and information sources”.
- Phase 5 and 6 are detailed below.
- 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 Good practices and gap analysis

Good practices and gap analysis were based on desktop research, survey results and feedback from CSIRT teams. They were also extended with own experience of project team in proactive detection of network incidents. This analysis helped identify common problems, and some methods to resolve them. Good practices were proposed to take into account different constituencies, capabilities and resources of the CSIRT teams.

1.5.2 Recommendations

Proposed recommendations are a result of the prolonged analysis, which began with desktop research, then analysis of the survey, evaluation of the identified measures and information sources, and gap analysis. Personal experience of the project team with proactive detection of network incidents and discussions with other CSIRT teams on this subject (beside of this study), helped to enrich the proposed recommendations. Overall, they provide high level overview of our findings and conclusions resulting from the study.

2. GOOD PRACTICES AND GAP ANALYSIS

The following sections contain the conclusions of the study, based on the performed desktop research, analysis of the survey results and consultations with the CSIRT community.

2.1 RECOMMENDED MEASURES

As teams differ in the size and type of their constituencies, services they provide and resources available, they have different needs and priorities for detection measures. While there is no single solution that could be recommended to all of them, a set of guidelines is proposed below that should be applicable for the majority of teams: enterprise, governmental and national.

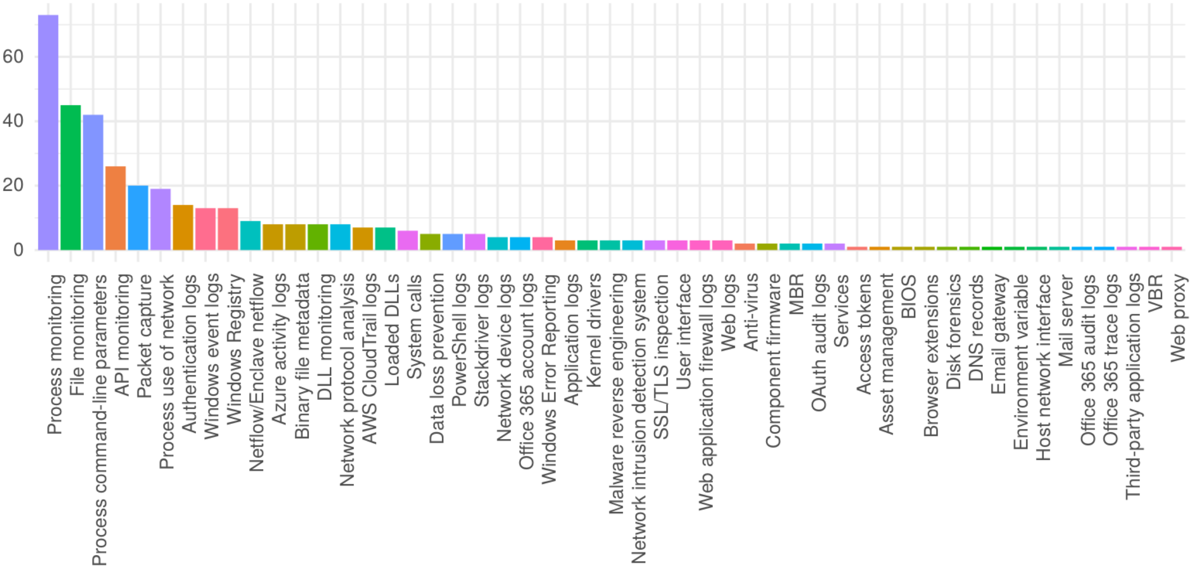
2.1.1 Monitoring of local infrastructure

In the last decade, development of **endpoint monitoring** could be seen as a growing trend in the industry. Collection and analysis of various types of logs from servers, workstations and other devices is not new and has been a standard practice for a long time. However, this type of monitoring has seen substantial improvements in wide practice: nowadays teams collect more detailed information about host activity (for example all process executions, registry writes, mutex creation) and the coverage of monitored devices increased to cover not just critical assets, such as production servers, but also computers and appliances of the end users.

This development both supported and was fuelled by the industry-wide rise of the proactive approach to defending against adversaries to catch them at an early stage of an intrusion (so called “threat hunting”). As part of this approach, practitioners share methods of detecting specific suspicious behaviours that can indicate an ongoing attack and one of the outcomes of this collaboration is the development of the ATT&CK knowledge base curated by MITRE[27]. Looking into specific data sources that ATT&CK defines as options for detection, it is clear that the large majority correspond to the endpoint monitoring, which is illustrated in Figure 1. This is consistent with the results of the survey, **endpoint monitoring has the second-highest perceived importance for the proactive detection of incidents.**

[27] https://attack.mitre.org

Figure 3: Distribution of data sources mentioned in the ATT&CK repository



Despite its value, this measure has certain drawbacks, which can limit its uptake or the scale of deployment inside an organisation. **Primarily, the amount of data that can be collected from even a medium-sized network can be large, which means that a team needs to make a trade-off between the level of detail, coverage and cost of backend to store and index the logs. Secondly, the deployment of collection agents across a large fleet of diverse devices can be a significant IT challenge.**

In general, for any team that has direct authority over the infrastructure of its constituency and can collect such information, it is recommended to invest in having good coverage of endpoint monitoring. Additionally, a team should put extra consideration into tuning the types of events that are collected and the level of detail that is logged to obtain the optimal results given the resource constraints.

Storing logs without effective ways to analyse them will not be sufficient to detect early signs of an attack. Therefore it is not surprising that **systems for aggregation, correlation and visualization of logs play a crucial role**. This was also reflected by the fact that this category of tools received the **highest utility rating in the survey**.

It is important to note that **this measure includes, but is not limited to, SIEMs since other tools that can be used for the same goal** may not necessarily have this term commonly associated with them. The key feature of these systems is enabling analysts to efficiently query vast amounts of log-like data and facilitate both hunting and incident response workflows.

Of course, this measure also has its drawbacks, primarily cost and human resources. **The benefit of log aggregation is as good as the data that is collected, which means that a team would want to integrate as many inputs and log as much data as possible**. However, **license costs of commercial solutions and hardware requirements for storage and indexing can put limits on how much data can be ingested in practice. Secondly, these tools are typically complex and large deployments need dedicated staff to deploy and maintain them, integrate new inputs, tune configuration, etc. A small team with a large constituency might find these costs challenging.**

Regardless of advancements of other detection methods, **network monitoring remains a baseline measure for catching threats**. Tooling in this area is mature, implementing advanced methods for traffic analysis and analysts had over two decades to acquire experience with these technologies. **Network monitoring can be safely recommended as one of the first measures a newly established team should start from, before moving into more demanding or specialized areas.**

NIDSs are perhaps the most conventional but also definitely useful tools at a team's disposal. Quality of generated alerts depends on the rules that are used, however in general vendors can provide a reasonably good coverage of widely-known threats and timely updates. **Intrusion detection systems are generally straightforward to deploy and use, however "noise" (false positives) can be a problem in daily operation.**

Even better visibility into all network activity can be obtained by implementing flow monitoring. Similarly to endpoint logs, flows can be useful for hunting and anomaly detection but are also essential for supporting incident investigations. Deploying flow monitoring across even a large organization might be significantly cheaper (in hardware, time) compared to other similar measures which makes this a very attractive tool for many teams.

Teams that want to collect more information on network activity than flows can provide should consider upgrading or complementing it with full packet capture. Availability of payloads might be invaluable for detecting some types of behaviour or investigations, however it comes with a much higher cost to store all of the collected traffic and a challenge to deploy sniffing across the network. For this reason, this measure is much less popular than other forms of network monitoring. **It is still recommended, at least for critical parts of the infrastructure,** however but other measures are likely to be of a higher priority given budget and time constraints.

Given the importance of domains for operation of all IT systems but also attackers' infrastructure, **monitoring of DNS requests can provide plenty of opportunities for early detection**. A somewhat less popular measure, it focuses only on a specific application (DNS) so cannot replace other network monitoring tools however it can complement them very well without the overhead of installing agents or sniffing infrastructure. **Easy deployment is also one of the reasons this measure can be recommended even for teams with very limited resources.**

It is worth pointing out that nowadays, even with all the network monitoring measures deployed looking just at the network level on its own is not sufficient, given the growing popularity of end-to-end encryption, steganography, complex and dynamically changing traffic patterns, etc. Nevertheless, **logs from both endpoint and network monitoring can and should be inputs for systems for aggregation, correlation and visualization to create a comprehensive picture of activities in the organization.**

2.1.2 Other types of monitoring

Apart from monitoring that is typically used for detecting threats within the organization's infrastructure, there are multiple useful measures that can be deployed by teams regardless of their constituency type.

One of such obvious and simple to implement activities is **media and news monitoring**, which **includes sources like technical blogs, mailing lists and other forums where advisories, intelligence or observations are shared. This common process which can be recommended for all kinds of teams allows to stay up to date on major events, overall trends and have basic situational awareness.** News monitoring is usually associated with financial costs, however designated staff will have to allocate time to follow the information feeds, triage reports and summarise them for the rest of the team. Automation tools can help with minimizing the time spent on handling these tasks and there are ones that are available for free or are released as open source. In particular, the Taranis-NG project that is currently under development by European teams is expected to provide a good set of functionality in this regard. Taranis-NG is a complete rewrite of the original Taranis tool that was created by NCSC-NL but is no longer under active development. Its official open source release is scheduled for the second half of 2020.

On a more technical level, **behavioural malware analysis in sandboxes is a typical part of daily activities.** This simple way of investigating suspicious files is used both for classification (network defence) and understanding the malware itself (intelligence). It is a very common measure, with multiple vendors offering appliances and online services (often used according to the survey) but also with open source tools available for local deployment. While useful, sandboxes have fundamental limitations which mean that some malware analysis capacity has to be eventually developed anyway in a team.

Passive DNS is a very good source of intelligence, essential for linking adversaries' infrastructure and supporting investigations. Its value is well understood in the community which translates into wide adoption across teams, multiple commercial and non-profit providers. It is also worthwhile to deploy a passive DNS sensor in own networks to obtain data that might be unique to the organization and not available from third-parties**. Certificate monitoring is a similar measure that focuses on the data from X.509 certificates instead of DNS.** While useful, this type of monitoring is more recent, which means that there are still fewer teams using it and fewer providers to choose from**. Certificate monitoring is recommended for all teams that already use passive DNS, as the next step in building their capabilities.**

Another very common measure is **vulnerability scanning**. By definition, **it is a very good match for the proactive approach, as it allows identification of vulnerabilities before they are exploited by attackers.** In practice results can be varied, which is reflected in different opinions regarding its usefulness. Still**, it is definitely recommended for enterprise and governmental teams for periodic scanning of the infrastructure they monitor. Even teams with external constituencies, especially national, can employ scanning on a large scale (when envisioned in their mandate), however this is more difficult to set up and appropriate notification channels to distribute the vulnerability reports must be in place for this approach to be effective.**

Finally, **sinkholing can be a simple but effective measure for targeting particular known threats.** Internally, effects can be similar to what can be accomplished with NIDS, meaning detecting hosts connecting to command and control domains or IPs. A different deployment model can be used for takedowns of botnets or other malicious infrastructure but such actions are usually taken by teams that have capabilities to conduct this type of anti-crimeware activities.

The GitHub inventory[28] contains more measures[29], all of them have some adoption and large majority have received positive usefulness ratings. **Teams need to review their needs and prioritize measures according to their needs and capabilities.** For example honeypots can be useful for early detection of emerging threats however a team should have a good understanding how data obtained that way can be used in the internal workflows.

2.2 RECOMMENDED INFORMATION SOURCES

Similarly to implementation of measures for proactive detection, the choice of information sources ultimately depends on the needs of a particular team. However, **for the categories of the data sources identified in this project[30] it is common, and would be recommended for**

[28] https://github.com/enisaeu/IRtools
[29] https://github.com/enisaeu/IRtools/blob/master/measures_and_tools.md
[30] https://github.com/enisaeu/IRtools/blob/master/information_sources.md

the majority of the teams, to collect all types of information listed for the purpose of early detection of threats. Comprehensive detection simply requires that information is obtained about different aspects of threats.

For example: it is possible to learn about a malware infection by detecting connections to a URL hosting malware, a beacon being sent to a command and control server or an abuse notification from a sinkhole operator. Even if the end result might be the same, it is preferable to have information from all of the sources, since each increases the chance that a potential incident will be caught as early as possible.

A category of sources that requires special mention are sharing platforms[31]. In contrast to traditional feeds of information where teams act only as consumers, these platforms allow participants (organisations, but also individuals) to add their own IoCs, observations and other data and engage in multilateral exchanges.

The main benefit of sharing platforms, assuming they have an active user community, is that they contain rich information from a variety of sources aggregated in a single system. It means that nowadays, a single platform can replace multiple feeds or bilateral exchanges that teams had to rely on in the past. Therefore the main guidance for both new and established teams is to **take full advantage of this approach, by ensuring that they are able to exchange information with their peers, have a good grasp of the content that is available and sharing their own findings.**

Of course not a single information sharing platform, even a very popular one, will ever contain all intelligence that teams need, so integration of additional sources is still needed. Given the large number of options, **the main recommendation is to employ an evaluation method that would allow to compare different offerings, taking into account not just the cost, but also the quality of the content and effort required to integrate it into the workflows used within the team.** Relevant to the topic, ENISA published in 2018 “Exploring the opportunities and limitations of current Threat Intelligence Platforms”[32].

A category of information that might be lower on the list of priorities for new teams is **malware intelligence**[33]. While **essential for teams with developed malware analysis capabilities**, coordinating teams or the ones that outsource malware analysis might find it less useful.

Finally, **abuse reports** [34](sources of attacks, spam, etc.) are considered less useful in general for some of the teams. It is true that these sources are not useful against advanced adversaries and mostly contain data on hosts that have been infected with common crimeware. Nevertheless, **even if not essential for network defence, these reports are an important and sometimes unique way of learning about constituents or infrastructure that needs to be cleaned up before they cause more damage. Especially for coordinating CSIRTs, large-scale notifications based on this type of information is a core part of their activities.**

2.3 GAP ANALYSIS

Some of the measures and information sources have been rated lower than expected, which raises questions whether the current offerings sufficiently address the needs of teams.

One such case is the area of **automated malware analysis** in general. Mobile malware analysis in general and static malware analysis received low scores for detection of threats, similarly malware intelligence sources were scored below average. These measures are also

[31] https://github.com/enisaeu/IRtools/blob/master/information_sources.md#information-sharing-platforms
[32] https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms
[33] https://github.com/enisaeu/IRtools/blob/master/information_sources.md#malware-intelligence
[34] https://github.com/enisaeu/IRtools/blob/master/information_sources.md#feeds-with-information-on-sources-of-abuse-spam-attacks-scanning

less used by the teams in general, despite the fact that malware is one of the most important threats facing security practitioners. This situation indicates **a possible area for improvement, both on the tooling side and in the context of skills of the teams themselves. To provide exact recommendations, a more detailed analysis would be required**.

Another area for investigation are measures specific to **cloud monitoring**. Services offered by cloud providers such as CDN, computing, storage, but also many more application-level services are continuously growing in importance as the IT in general becomes increasingly dependent on them. It seems that such outsourced services are much less frequently monitored than local infrastructure and, at the same time, results of the implemented monitoring do not fully meet teams' expectations. While the survey does not provide a sufficient detail to determine the exact reasons for this situation, there might be a couple of possible factors at play: insufficient tooling, lack of expertise, limited adoption of cloud services among respondents or, in the case of coordinating teams, no authority to monitor cloud infrastructure. Determining the actual reason would require a separate project focused on how cloud infrastructure is used by European companies and what the relevant threats and defences are. Some relevant efforts[35] are available on ENISA website such as 2016 ENISA report "Exploring Cloud Incidents"[36].

More work is also required to get a **better understanding of sector-specific measures and information sources**. They are used by fewer of the teams, which is expected, however the usefulness has been also rated below average. Given the variance between sectors, understanding this situation would require interviewing representatives of the particular sectors and this could be an opportunity to explore for future ENISA efforts.

Two measures that proved to be slightly less common and lower rated than their importance would suggest are **routing monitoring and automated collection of spam**. In both cases **it is likely that the quality and features of the available services and tooling do not fully meet the teams' expectations. Therefore also these could be a topic for further investigation and improvement.**

Honeypots, in general, are a tool that seems to be still used by a subset of teams, with mixed results. Historically, the main issue with the deployment of honeypots has been that most of them are designed primarily as a research tool: the interpretation of data needs time and so might maintenance. Despite the development of the market, including the emergence of multiple vendors of the so called "deception" technologies, which are usually honeypot-based, it **seems that this measure has not gained widespread adoption yet. All of this applies to network telescopes, which can be simply considered non-interacting honeypots**.

Finally, a simple measure that can yield good results, but is still not universally deployed is **the monitoring of DNS requests**.

The surveyed teams identified **gaps in tooling**. **Firstly, the problem with interaction between different systems and tools, which includes the lack of clear API documentation and lack of standards of data exchange and data formats, extended with lack of privacy aware data structures.** This results in higher workload needed to deploy systems correlating information in different formats depending on the source system. **Secondly, the tools often do not provide an automatic classification of output. Thirdly, many systems/tools lack information about good practice implementation, policy and deployment of the measures.**

[35]https://www.enisa.europa.eu/publications#c5=2010&c5=2020&c5=false&c2=publicationDate&reversed=on&b_start=0&c6=cloud&c10=Cloud+and+Big+Data
[36] https://www.enisa.europa.eu/publications/exploring-cloud-incidents

The surveyed teams also identified gaps in open source and commercial systems. In their opinion, open source systems require more human resources for deployment and management, while commercial solutions are too expensive for some organisations or require sharing of Indicators of Compromise.

75% of the respondents provided measures which their organisations lack. These include:

- 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.

Main obstacles preventing the implementation of these measures were identified as insufficient financial and human resources, lack of management support, insufficient (or lack of) legal authority, trust issues with implementation, lack of expertise, lack of cooperation of the network owners, high network load, data privacy regulations, problem with licence 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.

According to the survey respondents, available information sources do not provide sufficient context, that is information completeness is poor. The provided information often lacks details on how it has been obtained or what confidence level it presents. Also **available information sources provide data using different formats, protocols and APIs. Adding to this lack of common classification of events and inconsistent identifiers, deployment and usage of currently available information sources requires higher levels of work, thus more human and hardware resource**s.

The analysis of the 2011 survey with the current edition provides many insights on changes and trends of proactive detection of network incidents. A detailed comparison is presented in survey document: here, only major gaps will be discussed**. Firstly, the increase in the number of measures and information sources shows development of different monitoring domains,** both in standard environments, popular in 2011, but also previously non-existent or niche**. Secondly, the adoption of some measures increased, including spamtrap systems, NIDS, sandbox systems and passive DNS monitoring.** While the adoption of measures such as network flow monitoring, network telescope monitoring and honeypots decreased. **Thirdly, both survey editions indicated problems with the correlation of data, standardisation of formats and interaction between tools/systems.** While these issues were addressed during the 8 years separating the surveys, the responses by the surveyed teams show that it is still an unresolved problem.

Apart from the above analysis of the measures and information sources for proactive detection, some non-technical issues arise with proactive detection of network incidents. They were indicated by the teams in the survey. **Firstly, some of the teams stated that they did not have sufficient legal authority. Secondly, due to changes in privacy laws, privacy protection plays a substantial role in proactive detection.** It includes the lack of tools supporting a sufficient level of privacy, but also an enforced change in methods of accessing some data, for example WHOIS information. **Thirdly, the teams indicated unwillingness to cooperate, as it can be seen between the teams and clients.** Lack of management level support is also an issue encountered by the teams - without such support, deployment of many measures and information sources presented in this study is hard. The reason is that the deployment requires human and hardware resources and without management support, these are impossible to obtain. Even with such support, shortages of manpower are felt by the teams, however this issue is known to the entire IT field.

3. RECOMMENDATIONS

3.1 KEY RECOMMENDATIONS FOR CSIRT TEAMS

The previous chapter contain multiple specific recommendations for the teams for early detection of threats. To summarise the main conclusions, **these are the top four proactive measures that most CSIRT teams should consider implementing**:

Endpoint monitoring with SIEM

For teams with authority to directly monitor the IT infrastructure in their constituency, **very good visibility can obtained by collecting detailed logs from servers, workstations and other devices.** The collection should be **complemented by deploying a centralized system that allows an easy search through the data for suspicious patterns of behaviour**, the approach commonly referred to as **hunting**.

Network monitoring

Network monitoring, while often insufficient on its own, is still a basic measure that should be implemented in all monitored networks. Apart from standard network intrusion detection appliances or software with up-to-date rulesets, **detection capabilities will be greatly improved if all network flows are logged.** Full packet capture is not a must, due to its cost and increasingly common end-to-end encryption.

DNS analysis

Another network-oriented measure is **collection and analysis of DNS traffic**, in particular in the implementation of **passive DNS and DNS requests**. They are useful, easy to deploy and usually do not have a significant financial cost.

Media monitoring

The most straightforward way of maintaining a basic level of situational awareness is **monitoring of publicly available information: social media (especially Twitter), publications and advisories** put by organisations fighting cyber-crime and doing research, individual researchers, traditional media outlets, etc. It does not require any special resources and an analysis of these reports is a good starting point for any new team.

For **external information sources**, providing a short list of recommended providers and types of data is much more challenging due to their variety and the fact that some data are unique and cannot be simply replaced by another source. Therefore the **main recommendation** is to prioritize: **maintain a roadmap of information sources that are most needed for the team's operation and allocate some effort on evaluating available offerings on the market.** When looking for new sources of information, the general observation is that trusted communities can be among the most valuable sources of information, as long as their focus is aligned with the threats that the team is concerned with.

3.2 GENERAL CONCLUSIONS

Proactive detection of threats is important for minimizing damage from intrusions, however it depends on teams' capabilities that are not trivial to develop. Teams require appropriate skills, time, tools and resources to do this job properly.

While it is the responsibility of each organisation to provide sufficient funding for the network defence, there are multiple actions on the European level that can help teams to improve their detection capabilities.

Development of trainings

Systems supporting operations can be of great benefit for effectiveness of a team, however personnel often lack skills and best practices to make full use of what they have available. For expensive commercial solutions, like SIEMs, vendors usually have developed training programmes that address this need. However, for open source tooling, often commonly used and having advanced functionality (for example information sharing platforms), the offering is much more limited. Therefore **ongoing development and wide availability of vendor-neutral and open source focused trainings should be one of the priorities.**

Evaluation of information sources

With the large choice of providers and lack of simple evaluation frameworks, teams have difficulty in making fully-informed decisions on information sources they should focus their integration efforts on. This can be addressed on two levels:

- **Creating an evaluation framework that would simplify selection of sources while optimising for maximum coverage for detection**. This can be in the form of a handbook with a set of general guidelines that a team could apply in its environment and use their threat model for prioritization.
- **Maintaining an up-to-date catalogue of information sources that would be comprehensive enough to support selection of optimal sources while minimizing the effort teams have to spend on understanding the market.** This report should contain multiple examples of external information sources grouped into main functional categories, a detailed analysis of individual ones is beyond the scope of this study. A proper long-term initiative should be launched, preferably including quantitative data analysis as part of the source characterisation.

Both activities should be community-driven, with most of the input coming from teams that work with a wide range of information sources and can share their experiences. European institutions, like ENISA, can help to ensure sustainability of such activities.

Analysis of inadequate measures

Usefulness of some of the measures and information sources were rated below average, which might indicate an area that needs improved tools or better training programmes. These potential shortcomings should be analysed separately in more detail, in order to understand how to address them. Such areas are:

- **Consistent taxonomies, formats and techniques** - Improve interoperability between different tools and enable automatic classification of output and correlation of different data.
- **Sectoral information sources**. Better development of data feeds coming from ISACs could be the key to improved information exchange and build upon existent ENISA efforts[37].
- **Feeds of abuse information**. The role of national CSIRTs and other brokers should be analysed in the context of effective remediation.
- **Automated malware analysis tools** (conventional sandboxes, static analysis tools, mobile analysis) and services providing information about malware. Collaboration on analytical tools and pooling resources to analyse common threats could address this issue to some degree.

Improvements in the tooling ecosystem

Deployment, integration and maintenance of open source tools was identified as a challenge by multiple teams and this observation echoes some of the comments from the survey 8 years ago. In general, the ecosystem of open source CSIRT tools would benefit from improved

[37] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

documentation and guides, which would reduce the human resources that teams must invest into the implementation of proactive detection measures. **Additionally, interoperability between tools would be improved if more tools used consistent taxonomies, formats and APIs. Similar issues also apply to the available external information sources.**

While there is no simple solution for these problems, there are some steps that could improve the situation:

- Provide incentives for developers to continue improvements of their tools, including features that will simplify deployment and operation by end users.
- Support work on the trainings, tutorials and good practice guides that will increase the level of expertise in the community.
- Develop and promote taxonomies that can improve interoperability between different tools and teams.

Finally, the **general recommendation** is facilitating **cooperation between teams on various levels**. Joint initiatives will minimize duplication of work and lead to better allocation of resources that can be used for detection in all teams. This obviously includes sharing of operational information, as threats discovered by one team can help to protect others. However, teams could also engage in joint operation of some measures that are not tied to a local network, such as malware analysis, passive DNS, honeypots and more. While such initiatives have been ongoing for some time, there is still much room for growth in this aspect.

Support on the European level will be beneficial for all teams, however especially smaller teams, with more constrained resources, will be the ones that will benefit most from advances in open source tooling, development of up-to-date inventories and guidelines on detection, and skill development through widely available online or live trainings.

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-01-20-305-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: 978-92-9204-347-6
DOI: 10.2824/21267