EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA CYBERSECURITY THREAT LANDSCAPE METHODOLOGY

JULY 2022

ABOUT ENISA

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

CONTACT

To contact the authors, please use etl@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Eleni Tsekmezoglou, Rossen Naydenov, Marianthi Theocharidou, Apostolos Malatras - European Union Agency for Cybersecurity

CONTRIBUTORS

Gert-Jan Bruggink, Maarten Toelen, Sergio Carrillo, Vasileios Mavroeidis

ACKNOWLEDGEMENTS

We would like to thank the Members and Observers of the ENISA ad hoc Working Group on Cyber Threat Landscapes for their valuable feedback and comments in validating this methodology. We would also like to thank the ENISA Advisory Group and the National Liaison Officers network for their valuable feedback.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-579-1, DOI 10.2824/339396

TABLE OF CONTENTS

1. INTRODUCTION

Policy makers, risk managers and information security practitioners need up to date and accurate information on the current threat landscape, supported by threat intelligence. The EU Agency for Cybersecurity (ENISA) Threat Landscape report has been published on an annual basis since 2013. The report uses publicly available data and provides an independent view on observed threats agents, trends and attack vectors.

ENISA aims at building on its expertise and enhancing this activity so that its stakeholders receive relevant and timely information for policy-creation, decision-making and applying security measures, as well as in increasing knowledge and information for specialised cybersecurity communities or for establishing a solid understanding of the cybersecurity challenges related to new technologies.

The added value of ENISA cyberthreat intelligence efforts lies in offering updated information on the dynamically changing cyberthreat landscape. These efforts support risk mitigation, promote situational awareness and proactively respond to future challenges.

Following the revised form of the ENISA Threat Landscape Report 2021[1], ENISA continues to further improve this flagship initiative.

ENISA seeks to provide targeted as well as general reports, recommendations, analyses and other actions on future cybersecurity scenarios and threat landscapes, supported through a clear and publicly available methodology.

By establishing the ENISA Cybersecurity Threat Landscape (CTL) methodology, the Agency aims to set a baseline for the transparent and systematic delivery of horizontal, thematic, and sectorial cybersecurity threat landscapes. The following threat landscapes could be considered as examples.

- **Horizontal threat landscapes,** such as the overarching ENISA Threat Landscape (ETL), a product which aims to cover holistically a wide-range of sectors and industries.
- **Thematic threat landscapes,** such as the ENISA Supply Chain Threat Landscape, a product which focuses on a specific theme, but covers many sectors.
- **Sectorial threat landscape,** such as the ENISA 5G Threat Landscape, focuses on a specific sector. A sectorial threat landscape provides more focused information for a particular constituent or target group.

"By establishing a methodology to develop threat landscapes, ENISA aims to set a baseline for the transparent and systematic delivery of horizontal, thematic, and sectorial cybersecurity threat landscapes"

Recognising the significance of systematically and methodologically reporting on the threat landscape, ENISA has set up an ad hoc Working Group on Cybersecurity Threat Landscapes[2] (CTL WG) consisting of experts from European and international public and private sector entities. The scope of the CTL WG is to advise ENISA in designing, updating and reviewing the methodology for creating threat landscapes, including the annual ENISA Threat Landscape (ETL) Report. The WG enables ENISA to interact with a broad range of stakeholders for the purpose of collecting input on a number of relevant aspects.

The overall focus of the methodological framework involves the identification and definition of the process, methods, stakeholders and tools as well as the various elements that, content-wise, constitute the cyberthreat Landscape (CTL).

[1] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends
[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes

1.1 OBJECTIVES

The objective of this methodology is to describe a systematic process for data collection and analysis, which is to be used for the formation of Cybersecurity Threat Landscapes (CTLs).

The methodology aims to address the following questions:

- what is the structure (components and contents) a threat landscape should follow?
- how should the targeted audiences be determined?
- how should the data be collected?
- how should the data be analysed?
- how should the products be disseminated?
- what is the process for collecting feedback?

1.2 OVERVIEW OF METHODOLOGICAL APPROACH

For the purpose of the methodology, ENISA's approach focusses on collaboration, starting with the collection of various inputs, performing analysis, interacting with key stakeholders and providing clear recommendations for the improvement of the CTL.

As shown in *Figure 1*, the content of our reports is continuously assessed by ENISA analysts and the Working Group is periodically consulted. The final draft report is then reviewed and discussed with ENISA stakeholders, such as the ad hoc Working Group on Cybersecurity Threat Landscapes (CTL WG), the ENISA National Liaisons Officers Network and the ENISA Advisory Group (AG), to validate the direction of the CTL. The final step of the process is the published CTL report.

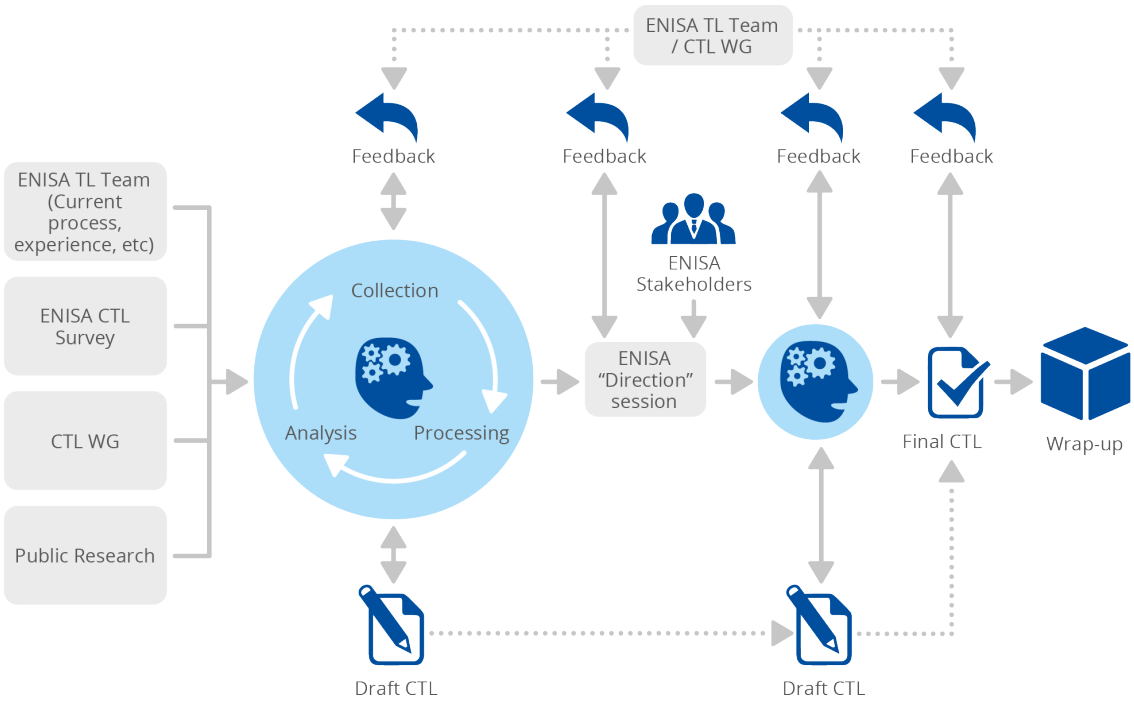

Figure 1: High level overview of ENISA CTL methodology

1.3 SCOPE

The methodology presents how ENISA produces the annual ETL. It can however be used for other purposes, such as short technical threat landscapes or sectorial threat landscapes based on existing needs and requirements. In general, the first and fundamental question that should be considered is '***what is the scope of the threat landscape***' and the second one '***what is the target audience and the aim'***. From the answers to these two questions, all other elements

of the threat landscape will stem and will support decision-making on what is included in the threat landscape, how it is analysed, processed and how strategic insight is inferred.

To produce a threat landscape, a wealth of information and data sources are used. The collected sources are currently based on the sources that ENISA has identified in its analysis. The sources may need to be updated, although the methodology should be able to accommodate them. The sources part in this methodology might need to be updated to include any new types of sources, as well as their weighted trust value.

The visual illustration presented above displays the various elements of the process of developing the ETL methodology and the different areas of focus that have been consolidated in the various steps of the process. For the development of the methodology, ENISA worked with the active participation, input, review and validation of the CTL Working Group. The process involves planning the requirements for the threat landscape (scope, target audience, objective), identifying and validating the different types and formats of information sources from both internal and external stakeholders, such as ENISA internal staff as well as the CTL Working Group. The collected data are processed and analysed before the cybersecurity threat landscape is produced and disseminated.

1.4 CYBERTHREAT LANDSCAPE DRIVING PRINCIPLES

The following considerations and principles are considered critical when generating and disseminating a CTL. Every CTL should be:

- **Actionable**: the CTL should increase stakeholders' awareness of threat situations, support their decision-making processes and improve their proactive, active defence, and retroactive postures against cyberthreats. This can be achieved at both strategic and operational levels. ENISA focuses on this aspect of the ETL by providing cybersecurity recommendations for different categories of threats in its reports, at both operational level and at strategic level. The operational aspect is covered by delivering the basis for the development of a mitigation strategy for prevention against and response to a given threat. The strategic high level aspect is covered in its annual review of the threat landscape. When delivering thematic or sectorial threat landscapes, the countermeasures proposed reflect the specificity of the sector or the thematic topic under analysis.

ETL provides actionable recommendations

- **Timely**: Time influences a report's actionability, especially when a report also accounts for tactical or operational information. The periodicity of a report is influenced by its scope, criticality and the stakeholder requirements it addresses. Based on those criteria, reports can be published monthly, quarterly, biannually or annually as examples.

ETL presents a yearly overview of incidents, but also thematic and sectorial threat trends

- **Accurate**: a report's accuracy depends on the information received, processed, correlated and analysed. ENISA reflects on the information input strategy and scores the quality of sources based on their accuracy, relevancy and comprehensiveness, the types of presentation format (e.g. report or machine-readable formats) and focus areas (e.g. sector, adversary country, activity groups, cyberthreats, threat agents). This is

ETL has included in the methodology the collection of feedback. ENISA cross-checks incidents based on various sources of data and their trust levels

also of particular importance when ENISA produces sectorial threat landscapes since their input strategy will need to be refined accordingly. In addition, the accuracy of the report is directly influenced by the quality of analysis and the inferences derived.

2. CTL METHODOLOGY

A cyberthreat landscape (CTL) represents information or intelligence on past, current and future events, allowing audiences to have a contextual understanding of the threats they face. In order to understand what content a CTL should contain or what taxonomies should be used, one must first understand how the CTL is produced. An 'intelligence-driven' approach adopts practical and useful lessons from the intelligence community to produce the CTL, for example allowing authors to explicitly translate what audiences and stakeholders would like to understand from their CTL (e.g. intelligence requirements) to the respective answers (e.g. findings of analysis)..

The following figure details a high-level structure for such a process within ENISA.

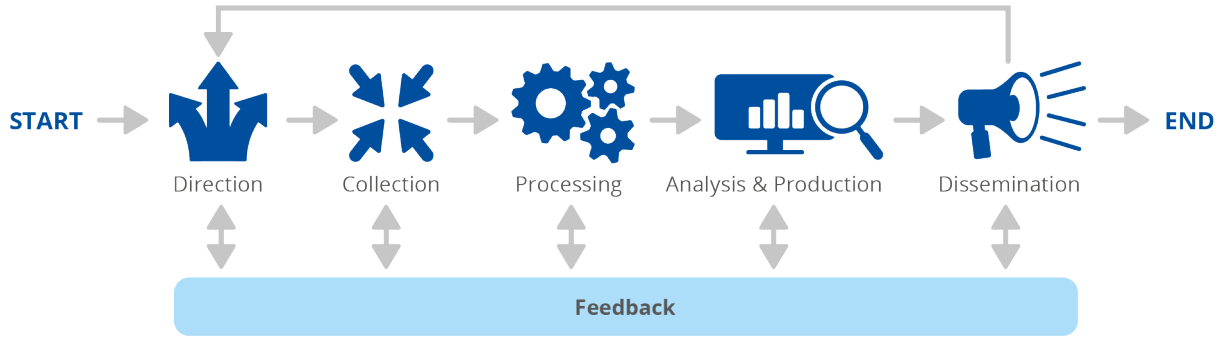

Figure 2: Overview of ENISA CTL methodology

The ETL serves as a recurring example case that illustrates how the methodology is applied in practice.

The upcoming chapters detail the different elements as highlighted in the figure above. Each chapter breaks down relevant topics to consistently produce a CTL and, in each chapter, we explicitly refer to how the methodology is satisfied in the context of the ENISA flagship ETL report.

2.1 DIRECTION

The aim of this first step is to establish the purpose, the audience and the stakeholders of the CTL report. By establishing these requirements and by taking into consideration the underlying legal context, we can then define what are the intelligence requirements for the report, what type of information we will need, who might be the stakeholders to provide the information and to whom the end product would be addressed.

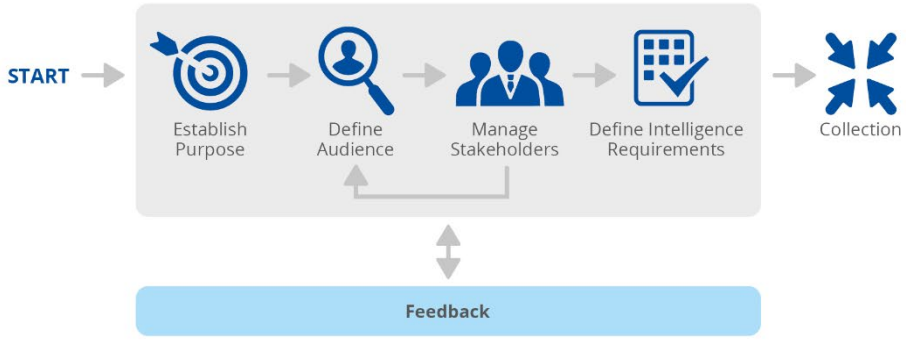

Figure 3: CTL direction definition process

2.1.1 Establish CTL Purpose

To explore the different types of components that make a CTL deliverable, it is important to first establish why authors develop a CTL. The reasoning, purpose and objective dictates what is inserted into the deliverable and what is not. It will also explicitly dictate whether the author needs to produce a CTL or not.

ETL Purpose:

- strategic decision-making,
- risk management,
- policy making,
- prioritising policy recommendations,
- identifying opportunities for training, exercises and capacity building.

Following a meta-analysis performed by ENISA and its CTL working group, all CTLs appear to have a common purpose: sharing information useful to aid cyber defences.

2.1.2 Define Audience

Once the purpose for a CTL is established and the deliverable is commissioned then the audience is considered. The audience for the CTL should be as follows.

- **Strategic**: information about general risks or developments associated with threats that can be used to drive a high-level strategy. Consumed by security strategist or other senior decision-makers, it can even reach board level.
- **Tactical**: information about tactics, techniques and procedures used by threat actors to conduct their attacks. This information is consumed by architects (network, system, product or process), security control owners and HR related roles, red/blue/purple teams, incident responders, threat hunters and digital forensics.
- **Operational**: information about precursory and indicatory signals of impending attacks. Usually generated by monitoring the threat environment, even from events in the real world, it is consumed by incident responders and high-level security staff, such as security managers.
- **Technical**: observed objects associated with specific threats, usually identified during response to an incident or through forensic processes and typically feeds preventive and monitoring solutions. It is ideally consumed through technical and automated means, and is consumed by administrators, security operations centre analysts and forensic experts.

The document structure can also be used to send a signal to the targeted audience. In the introduction to the deliverable the persons to whom a particular CTL is addressed should be explicitly mentioned. In our analysis we identified that for high-level audiences (e.g. when using strategic analysis), a summary and references to key research assessments should be provided. Additionally, different sections of the CTL should be addressed at different levels. As an example, there could be a separate annex that details references to the MITRE ATT&CK®[3] in a graphical way, so detection engineers may explore this more effectively.

The content and sharing or classification level of the CTL is very dependent on the defined audience and vice versa.

ETL Audience:

- *Policy-makers, e.g. the European Commission*
- *Supervisors, e.g. the Member States*
- *Implementers, e.g. the industry*

In some cases, the Member States could be policy makers or implementers as well.

2.1.3 Identifying and Managing Stakeholders

By breaking down stakeholders in the CTL, authors can immediately identify who needs to be engaged. These could, for example, be parties that need to provide input, to be consulted for policy input or to dictate what chapters should be detailed in the final deliverable. Additionally, stakeholders need to be appointed for validation purposes. In some cases, the validators might be the same as the target audience but not necessarily. *Figure 4* displays a practical example how ENISA's stakeholder landscape could be visualised using a matrix.

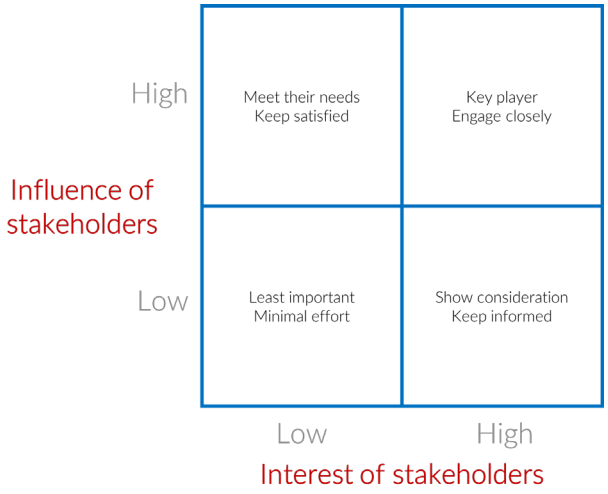

Figure 4: CTL stakeholder mapping[4]

Here are examples of different players.

- **High-influence, High-interest** – these are stakeholders that provide information, can influence the CTL and have high-interest in the product. An example would be Member States. They (through the CSIRT network for example) provide information, have high influence and also use the product to plan their resources. These stakeholders need to be kept satisfied with the product and be always included in the process.
- **High-influence, Low-interest –** these are stakeholders that usually have their own resources and therefore may not be so interested in the product. Their involvement will be beneficial for the product,

[3] https://attack.mitre.org/
[4] Mendelow, A. (1991). Stakeholder mapping. Proceedings of the 2nd International Conference on Information Systems, Cambridge, MA

therefore they need to be kept in the loop and engaged, if possible. An example would be the industry, where many companies might have their own processes and produce their own CTL.

- **Low-influence, High-interest –** these stakeholders might not have high the means to contribute to the product but can use it for their own purposes, such as to plan their resources. They need to be kept informed of the result. An example of such stakeholders might be vendors of information security. They may focus their efforts, based on the results of the CTL.
- **Low-influence, Low-interest –** these stakeholders would not be able to provide any contribution to the CTL and also would not have a use for it.

Given ENISA's complex stakeholder ecosystem, establishing a simple stakeholder overview allows for a quick understanding of who should be engaged with when they are producing their flagship report. This understanding ultimately results in a reduction of the time required to produce a CTL, by for example, reducing the number of review cycles from stakeholders who should be engaged and those who should not. This is achieved through giving each respective stakeholder a role, where they should be engaged.

Example ETL Stakeholder overview:

- *Cyber Threat Intelligence Working Group (CTL WG)*
- *Advisory Group (AG)*
- *National Liaison Officers (NLO)*

2.1.4 Define Intelligence Requirements

Scope

It is important to define the scope of the report. For example, in the case of an incident, ENISA is interested in questions such as the following.

- Which system(s) and/or asset(s) are affected by the incident?
- What sectors of the industry and/or citizens are affected?
- Are we interested in the geographic spread, e.g. More than one country or region?
- What is the impact of the incident, with different levels of economic, physical, digital, reputational and social effects?
- Who is the threat actor?
- What is the threat actor's motivation?
- What are the different tactics, techniques and procedures used?

Once important directional aspects are established such as purpose, audience and stakeholders, it is time to dive into the details. What questions does the CTL deliverable need to answer?

ETL answers these questions:

- *Which sectors are affected?*
- *What is the impact of the incidents?*
- *Who is the threat actor?*
- *What is the motivation?*
- *What are the TTPs used?*
- *What are the vulnerabilities exploited?*
- *What are the trends (sectors, sophistication, etc.)?*
- *What countermeasures can be applied?*

The following definition can be used to define an **intelligence requirement**:

Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence.[5]

It is important to note the distinction between what is needed to produce an intelligence product (production requirement), and what information needs to be collected to answer the production (intelligence requirement). In general, production requirements usually come from stakeholders, posing a more abstract question. To make this more workable, this production requirement is translated into multiple intelligence requirements, breaking down the main question into separate chunks, answerable by the production team. See the following examples.

ETL Intelligence Requirement

1. How many ransomware campaigns were observed in the last 12 months?
2. What ransomware campaigns where specifically targeting European entities?
3. How many campaigns, to a certain extent, have been attributed?
4. What tactics and techniques are employed in attributed campaigns, when mapped against MITRE's ATT&CK framework?

Period

Here the period for which the collected data should be considered is defined. Usually, it specifies the time frame for which we collect the data.

ETL is produced based on the collection of information from July in the previous year to July in the current year.

[5] Intelligence requirement. (n.d.) Dictionary of Military and Associated Terms. (2005)

Deliverable components

When producing a CTL there are numerous ways of structuring the findings. There is no 'right way', just the way that is in line with the CTL's purpose, stakeholders and audience. Additionally, how the final deliverable would look like, e.g. machine readable only, graphs, etc. should be explored as this would have an impact on the dissemination process.

The most common approaches to structure CTL content are:

- **Internal orientation**: following the internal requirements, using them as guidance for the CTL,
- **External orientation**: exploring traditional standards for research papers or documents from other external entities, using similar and recognisable structures for a CTL.

Currently, the ETL is delivered following a combination of both internal and external orientation with regards to its structure and content.

2.2 COLLECTION

The collection process generally entails the coordination of a significant number of operations, including the establishment of strategic objectives, (priority) intelligence requirements and the subsequent collection requirements or plans as well as the continuous evaluation of identified information sources in order to ensure actionable intelligence[6]. Information can be collected from different data sources (publicly available reports, subscription services, information shared by cybersecurity vendors, public feeds etc.) before they are processed and transformed into actionable intelligence.

In this context, this step of the methodology deals with the data collection requirements, and the planning and validation of the data sources. Finally, it includes the actual collection of data from the sources before they can be processed in the next phase.

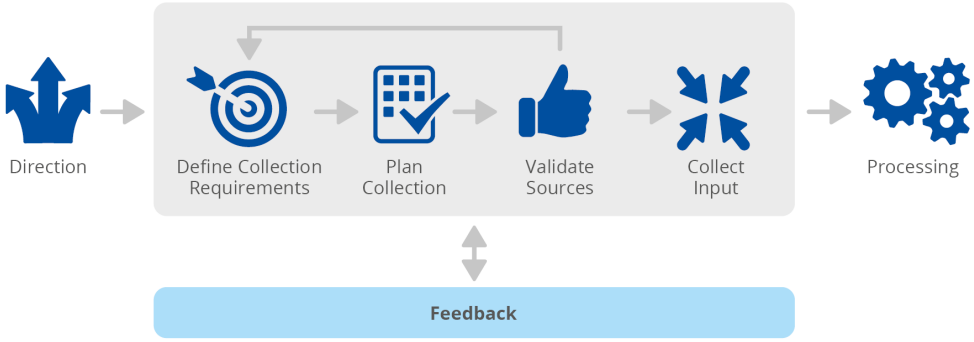

Figure 5: CTL data collection process

2.2.1 Define collection requirements

Having established the needs and expectations of the stakeholders, the next step in the process is to define the data collection requirements. In order to do that, it is important to have clarity and to reflect on the cyberthreat intelligence requirements and objectives or, in other words, identify and break down the information that needs to be collected to meet the requirements.

In practice this implies that the CTL team will need to identify what data is required to meet the intelligence requirements and from where this data can be collected. This can be external collection, such as cyberthreat

[6] X., "Chairman of the Joint Chiefs of Staff Intelligence Manual", U.S. Department of Defence (2012).

intelligence providers or knowledge sharing groups, or internal collection, such as access to procured threat feeds, cyberthreat intelligence providers or specific monitoring solutions.

An example how this would work in practice is present in the table below.

Intelligence requirements	Collection requirements
What ransomware campaigns were specifically targeting European companies?	• Consult ransomware campaign repository from VENDORTOOL_$ • Open-source feeds publishing ransomware campaign specifics. • Liaison with European knowledge sharing groups • Other sources
Timeframe for collecting the data	February to April
Types of incidents	Verified incidents covering EU specific sector

Table 1: Example of defining data collection requirements

ETL Intelligence collection requirements:

- Vendor Cyberthreat Intelligence (CTI)
- Member States shared CTI
- Open-source intelligence (OSINT)
- Internal monitoring systems and tools (e.g. Open Cyber Situational Awareness Machine (CSAM))

2.2.2 Collection planning

The data collection requirements are usually stored in an Intelligence Collection Plan (ICP), listing all intelligence requirements, mapping that to the source(s) and allowing the author to start planning the collection. This listing helps visual representation and efficient measurement. In addition, it allows teams to immediately spot overlaps or gaps, so that they can act accordingly. This is crucial in a CTL, especially for consistent collection as deliverables are produced periodically (e.g. yearly). The collection of data should be for a specific period. This period should be included in the initial requirements.

While information-gathering might seem like a repetitive task at first glance, it is essential to foresee an adequate level of continuous evaluation and redundancy in order to ensure that if an information asset fails, it is replaced by a duplicate or complementary asset that can meet the established collection demand[7].

An indicative intelligence collection plan is presented in *Table 2* below. The sources can be either static or dynamic and most of them are based on open-source intelligence. Open-source intelligence (OSINT) is a term that can carry a lot of different meanings, depending on the context and operationalisation thereof. Theoretically, it is described as all intelligence derived from publicly accessible data that is collected, exploited, and distributed to the proper audience in order to meet intelligence objectives or collection requirements[8].

[7] J. AMMONS, 'How to Use MITRE ATT&CK to Improve Threat Detection Capabilities' Gartner (2021).
[8] X. "What Is Open-Source Intelligence and How Is it used?" Recorded Future (2019).

In the context of Cyberthreat Intelligence (CTI), hundreds of data sources and tools are publicly available on the internet or in the wider cybersecurity community. In order to avoid information overload and to maximise the value of this abundance of information for a CTL, a structured and continuous source-assessment will help in preparing a good collection plan.

Based on the direction of the CTL, we define what types of sources we will need and use. The different types of data have the following characteristics.

- **Operational** – tends to contain a lot of technical details such as IP addresses, URLs, Domains, etc. This information usually becomes obsolete quite fast.
- **Tactical** – contains information about the ways a certain malware or group is using information such as scanning for specific services or specific software installed, or connections to specific domains. The latter is considered a tactic that a malware or group can use.
- **Strategic** – contains information which is usually based on trends and direction of where an entity might want to go. Usually, this type of data is not going to change in a short period of time.

In this regard, an analysis - based on research and market feedback - and a selection of existing CTI tools is deemed necessary for the selection of CTI products or services that can provide the type of intelligence anticipated based on the defined purpose, audience and stakeholders of a CTL. CTI providers offer products or services not directly comparable, as they can provide different types of intelligence, cover different threat areas, or focus on different CTI aspects to a variable degree. Therefore, a comparative review and analysis of the available tools, focusing on the functionalities and services offered, highlighting strengths and weaknesses, is a significant step before choosing the appropriate CTI tools that can support data collection. Some reflections and criteria that could be taken under consideration are the following:

- General overview of CTI vendors for a quick assessment of their tools and offerings;
- Product or service offerings of CTI vendors, e.g. some providers mainly produce technical or operational intelligence or focus on delivering ‘cyber watch’ services;
- Spotlight focusing on the perceived ability of the vendor to provide strategic CTI;
- Spotlight focusing on the perceived ability of the vendor to provide tactical CTI;
- Timing of the delivered CTI, e.g. is it provided on a timely basis (yearly, monthly, etc.), or after an incident has been identified?

Source	Type of data	Collection time
CTI providers	Operational, tactical	All year
Institutional stakeholders	Strategic	Periodically on an annual basis
Social media	Operational, strategic, tactical	All year
Data feeds	Operational, strategic, tactical	All year
Cybersecurity news	Operational, strategic, tactical	All year
Vulnerability disclosure	Operational, tactical	All year
Academia	Operational, strategic, tactical	All year
Deep/dark web	Operational, strategic, tactical	All year

Table 2: An indicative intelligence collection plan

ETL intelligence collection plan

Source	Type of data	Collection time
ENISA OSINT data **(e.g. social media, data feeds, cybersecurity news, vulnerability disclosure, academia, deep/dark web**	Operational, strategic, tactical	All year
ENISA Situational Awareness intelligence data	Strategic, tactical	Periodically on an annual basis
Member states' incident reporting tool (CIRAS)	Strategic	Once annually
CTI provider	Operational, tactical	Periodically on an annual basis
Institutional stakeholders	Strategic	Periodically on an annual basis

2.2.3 Validate Sources

The cybersecurity ecosystem of the European Union is complex and multi-layered, cuts across an array of national and EU policy areas – such as justice and home affairs, the digital single market and research policies[9]. Moreover, the EU is heavily invested in public-private cooperation, which is structured in various cooperation formats. While this complex structure – and division of powers – certainly results in some challenges, it also offers a unique opportunity from a CTL perspective in that intelligence collection can draw upon various trusted and mutually reinforcing sources.

ETL Distinguishes:
- *Internal sources*
- *Institutional sources*
- *External sources*

Internal sources include anything from internal people, processes and technology assets providing input to intelligence requirements. This is mostly relevant in cases where a CTL is produced by ENISA, to build situational awareness reports.

[9] X., "Challenges to effective EU cybersecurity policy", European Court of Auditors (2019)

Institutional sources – represent the numerous EU institutional actors within cybersecurity and their envisaged interrelationships with ENISA. This includes, but is not limited to CERT-EU, Network and Information Security Directive Cooperation Group, CSIRT Network, EUROPOL.

External sources include anything that is collected externally by ENISA. For example, technical indicator repositories, social media, forums. External sources can be categorised as open-source or closed source. External sources provide:

- **Raw or processed data**: data sources can differ greatly. For example, these could be a data provider that delivers output on demand, a tool that can be queried manually or a forum that needs to be visited and interacted with manually.
- **Information, based on data they themselves collected and/or processed**: providers having access to extensive telemetry, for example end point vendors, regularly analyse and establish interesting insights for (potential) clients. This information is published in periodic reports, some of them being CTLs themselves.
- **Finished intelligence products, based on data and information collected, processed, analysed, and disseminated**: the transition from information to intelligence, at least in concept, is mostly done by companies who understand how to produce it.

Contextualising should be done at the time of collecting, with source trust levels, as described in the next section. Contextualising is usually taken from the direction and purpose of the report.

2.2.3.1 Confidence or Trust levels

At this phase of data collection the trust level should be established. The trust levels should be as follows.

Low Confidence: an event that is supported with available information. The information is likely single sourced and there are known gaps in collection or in the information itself. However, it could be a good assessment that is supported. It may not be finished intelligence though and it may not be appropriate to take it as the only factor in making a decision.

Moderate Confidence: an event that is supported with multiple pieces of available information and collection gaps are significantly reduced. The information may still be single sourced but there are multiple pieces of data or information supporting the hypothesis. The gaps in the collection or in the information have been accounted for although it has not been possible to address all of them.

High Confidence: an event is supported by a predominant quantity of the available data and information, it is supported through multiple sources, and the risk of collection gaps are all but eliminated. High confidence assessments are almost never single sourced. There will likely always be a collection gap even if it is not known but everything possible has been accounted for and the risk of that collection gap has been reduced, i.e. even if we cannot collect information in a certain area it is all but certain that it would not change the outcome of the assessment.

As a general starting rule for ENISA threat landscapes, institutional sources are deemed to be high confidence, internal sources medium level confidence, and external sources deemed to be low confidence.

ETL high-level confidence data collection:
- *CIRAS incident reporting*
- *EU Institutions, Bodies and Agencies*

2.2.4 Input data collection

The actual collection does not require an extensive breakdown. Here the analysts collect the relevant data to start processing and analysing according to the requirements set in the previous phases.

2.3 PROCESSING

Data processing is generally known as the process of converting acquired data into a format that is suitable for human-centric analysis and the output of intelligence. In this stage, the collected data is converted into formats that intelligence analysts may use to generate intelligence products in a more efficient manner[10].

Having collected a large amount of data of different types, formats, granularity, trust levels etc., the real challenge is figuring out what to do with this plethora of information and how to separate credible threats from false positives that tie up resources and waste precious time. After all, threat intelligence is useful only if you can analyse and act on it in a timely manner. These considerations are part of the analysis step and will be further discussed later.

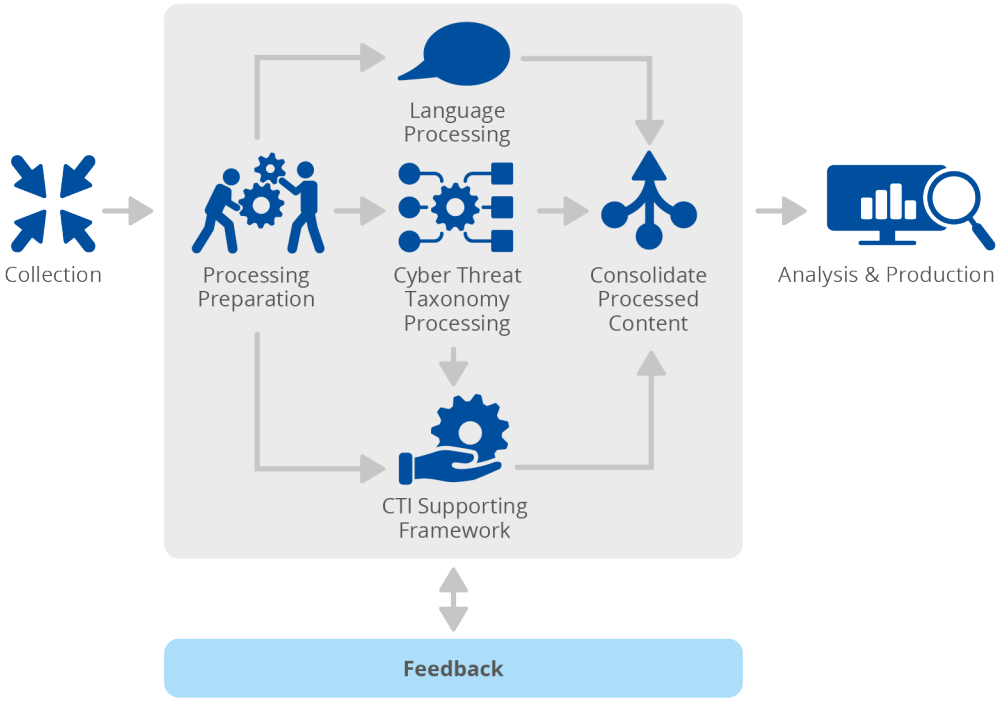

Figure 6: CTL data processing process

In the context of CTL this part of the process could focus, for example, on translating data or information to a common language, transforming large volumes of data into usable form or structuring TTP (Tactics, Techniques, Procedures) data sets according to MITRE ATT&CK® or other similar frameworks, all part of this phase. This processing could – among others – include the (manual) correlation of data that was collected by threat intelligence platforms with report-based sources, the (manual) structuring of TTP data sets according to the MITRE ATT&CK® framework and other processing and analytical capabilities.

[10] D. McDowell, Strategic Intelligence: A Handbook for Practitioners, Managers, and Users, (2008, Scarcrow Press)

The ETL data processing involves the correlation of data collected from open sources (OSINT) by means of situational awareness, threat intelligence platforms, the ENISA CTI providers and other report-based open sources for the structuring of TTP data sets according to the MITRE's ATT&CK framework and other processing and analytical capabilities.

2.3.1 Preparation for processing

The data processing of all collected information is being prepared and planned in accordance with the defined CTL objectives and ambitions, outlining and contextualising priority intelligence requirements in order to ensure that the CTL delivers actionable and credible intelligence. A close inter-relationship between the processing and analysis phases of the CTL should be followed, by giving feedback from the analysis phase to the processing.

2.3.2 Language processing

When developing a CTL, the author needs to decide upon the language to be used. Although this might sound trivial, it could introduce challenges that need to be addressed accordingly. For example, when collecting reports in English from published open source threat reports, there is a risk that sources written in other languages could be excluded. Similarly, when collecting articles in various languages, they must be processed into a single coherent language to meet the needs and objectives of the analysis.

The ETL is currently taking into consideration sources in all European languages and is being delivered in English, though it has been translated to other languages in previous years.

2.3.3 Cyberthreat taxonomy

Another important element of the methodology for delivering CTL is the definition of 'content taxonomies' as the classification used to structure the cyberthreat ecosystem. This is crucial for processing as this dictates the structure of how collected data are organised and historical data sets are developed. In this phase, one can observe the immense importance of having consequent taxonomies and frameworks to produce reliable and consistent output.

In March 2021, ENISA conducted a survey intended for the improvement of ENISA's yearly CTL by collecting the requirements and needs of its stakeholders. Following input from this survey (major outcomes of the survey are presented in Annex A), several suggestions were made by relevant stakeholders to consider additional taxonomies. A list of existing cyberthreat taxonomies follows.

- **ENISA Threat Taxonomy**[11]**:** established and published in 2016, the ENISA threat taxonomy became the guiding principle for future CTLs and the standard for threats referenced within ENISA. Currently the taxonomy is under revision for the purpose of developing a more mature framework, an ontology, considering not only the technical aspects of the cyberthreat ecosystem but also its socio-economic aspects.

- **Alignment with other ENISA initiatives**: ENISA launches multiple initiatives each year to improve the current approach to managing risk, for example, risk management aspects[12] that provide templates for

[11] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view
[12] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management?tab=publications

organisations to work with. Despite the fact that some of these components may be outdated, the approaches and taxonomies suggested are still valid to this day.

- **Alignment with other EU-centric research programs**: at the end of 2020, the European Commission published a proposal for a revised Directive on Security of Network and Information Systems (NIS2 Directive[13]), to update and replace the NIS Directive[14] (Directive (EU) 2016/1148) which was the first horizontal cybersecurity legislation at EU level. This proposal replaces and develops the original NIS Directive and is one of the most important EU cybersecurity legislations. This directive also adopts and provides several taxonomies, which will be considered for future ENISA CTLs.

- **JRC Taxonomy[15] (based on NIST):** published in 2019, the JRC taxonomy represents extensive research on taxonomies, documents and regulations in the field. The focus of this taxonomy is on the domains of cybersecurity, the economic sectors that can be affected by cybersecurity incidents and technologies and use cases. The JRC taxonomy was expected to be used for the classification of domains for incidents and for the economic sectors impacted or where a possible impact could be present.

- **ENISA Cyber Incident Taxonomy[16]** (Blueprint, High-level): published in 2018, this simple and high-level taxonomy was proposed to classify cybersecurity incidents at the strategic and political level in response to the requirements in the Cybersecurity Act (CSA). The document was developed by the NIS Cooperation Group (NIS CG) work stream 7 on large scale cybersecurity incidents. This taxonomy is to be used for the purpose of coordinating responses to incidents at Union level carried out in the framework of the arrangements for Integrated Political Crisis Response (IPCR). The scope of this taxonomy is cybersecurity incidents in general, for the sake of completeness. The taxonomy has two core parts: the nature of the incident i.e. the underlying cause that triggered the incident, and the impact of the incident i.e. the impact on services in which sector(s) of the economy and society.

- **ENISA Reference Incident Classification Taxonomy[17]**: published in 2018, this taxonomy was the result of initiatives in collaboration such as the annual ENISA/Europol European Cybercrime Centre (EC3) Workshop which involved Computer Security Incident Response Teams (CSIRTs), Law Enforcement Authorities (LEAs), ENISA, and Europol EC3. Other examples include the eCSIRT.net taxonomy[18] which was developed in 2003, and the eCSIRT.net mkVI taxonomy[19] which is an adaptation of the original eCSIRT.net taxonomy.

The ETL is currently delivered using the ENISA cyberthreat taxonomy that is under review and adaptation to encompass all existing work to capture the needs of the ETL. The cyberthreat ontology that is under development will be made publicly available.

2.3.4 CTI frameworks

Currently, several CTI frameworks exist that support structures for cyberthreats. Each has different focus areas, which makes them have specific uses. Whether a CTI team should use the Cyber Kill Chain® or the MITRE ATT&CK® is a

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN
[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148
[15] https://publications.jrc.ec.europa.eu/repository/handle/JRC118089
[16] https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf
[17] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
[18] http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6
[19] https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

decision to be made in order to efficiently capture and organise intelligence based on the threat taxonomy used and the requirements set during the direction and planning phase of the CTL process.

It is important to note that the application of any framework assists the production of reliable statistics. Once a framework is selected, data or information collected can be visited yearly and future CTLs can produce and explore historical research or forecasting research. Some well-respected CTI frameworks are mentioned below.

- **MITRE ATT&CK®**: is a globally-accessible knowledge base of the tactics of adversaries and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government and in the cybersecurity product and service community.

- **Cyber Kill Chain®**[20]: developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the Intelligence Driven Defence® model for the identification and prevention of activities related to cyber intrusions. The model identifies what the adversaries must finish doing in order to achieve their objectives. The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures.

- **MITRE CVE®**[21]: the mission of the CVE® Program is to identify, define and catalogue publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalogue. The vulnerabilities are discovered then assigned and published by organisations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritise and address the vulnerabilities.

- **OASIS Cyber Threat Intelligence (CTI) STIX™**[22]: one prominent threat intelligence representation and sharing standard is Structured Threat Information eXpression (STIX™) and its counterpart relay mechanism, Trusted Automated Exchange of Intelligence Information (TAXII). In 2021 STIX™ was released as an OASIS Standard. The working group that developed STIX™ is the OASIS Cyber Threat Intelligence Technical Committee (OASIS CTI TC). STIX™ is an ontology and a language that describes cyberthreats and observable information. It enables organisations to share cyberthreat intelligence in a consistent and machine-readable manner (STIX™ is expressed in JavaScript Object Notation - JSON), allowing them to better understand what computer-based attacks they are most likely to see and anticipate and/or respond to those attacks faster and more effectively. STIX™ has influenced the underlying format for the representation of different platforms for threat intelligence.

The following considerations should be taken into account.

- **There is no single silver bullet framework**. The single most important thing is that current CTL content should be matched to pre-selected frameworks. This could be that some elements of a CTL refer to framework A because this is more suitable for data analysis, while framework B is adopted to support input for strategic analysis.

- **Be wary of the implications due to betting on a single framework**. Sometimes selecting a single framework for structuring the entire CTL, for example focussing almost entirely on MITRE ATT&CK® or other similar framework, can yield great benefits, such as the content is so structured that it is immediately actionable for any defender. On the other hand, this also introduces a narrow scope, as it is only relevant for the audience for which the framework is intended.

[20] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[21] https://cve.mitre.org/
[22] https://www.oasis-open.org/committees/cti

- **Reconsider the framework used**. Reassessing whether the selected framework meets the purpose and objectives set during the direction and planning phase of the CTL can be controversial and challenging though necessary.

2.3.5 Consolidate processed content

Consolidating processed content consists of forming all available processed data into a more efficient usable form. It might consist of the format conversion of pure data, language translation, evaluating the relevance and reliability of data, to name a few. Data consolidation also ensures the elimination of redundancies and data errors.

2.4 ANALYSIS & PRODUCTION

Analysis and production is the key step. This is where data is put into context and analytical abilities and cyberthreat intelligence can make a difference. This is where data is put into context following processing. During this phase, the CTL team is trying to answer all the questions that have been raised in the requirements section. Additionally, the team will be trying to identify gaps that could potentially be then used for creating recommendations, based on past ENISA recommendations and other sources

In this step, the team conducts expert analysis to be able to provide meaningful conclusions based on the collected information. Based on these conclusions, considering the entire threat landscape including cybersecurity policies, market standardisation and certification efforts, capacity building exercises and trainings and operational cooperation, the Agency produces actionable recommendations as well as cybersecurity measures.

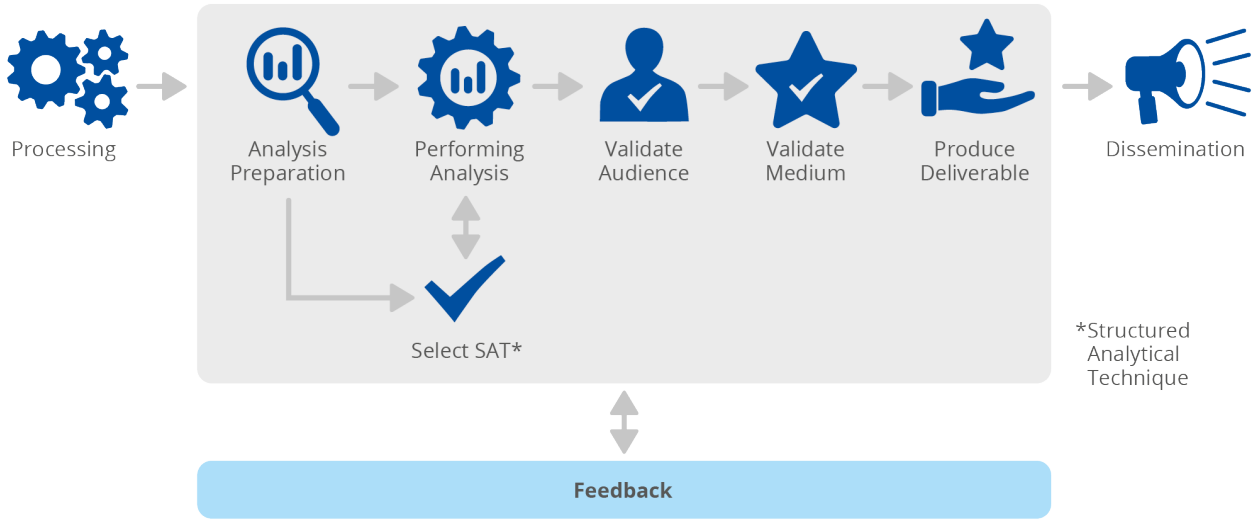

Figure 7: CTL data analysis and production process

2.4.1 Analysis preparation

To prepare and decide upon matters related to analysis, one should reflect upon the analytical techniques to be used during the process of analysis. There are different methodologies that one can employ to perform the analysis, e.g. a manual analysis, an automated analysis or a mix of automated and manual, a hybrid mode. Manual analysis typically involves different teams looking at a data set and trying to reach conclusions. The automated analysis usually requires the data to be imported into specific tools which then produce the analysis. With the recent developments in Artificial Intelligence (AI) this type of analysis will become very useful in producing reports.

Although the CTL relates directly to both the audience and the stakeholders, it is important to reiterate that here the audience becomes crucial. When the content is written for each threat, one can easily describe it for a generic audience while specific audiences will lose interest in the CTL. For example, an executive might only have time to discuss a simple list of threats while a risk manager will go to great lengths to establish if a particular threat warrants certain countermeasures to mitigate associated risk. Including outlines for specific audiences and reasons for certain analytical choices greatly improves the readability for the audience.

2.4.2 Structured Analytical Technique (SAT) selection

When producing a CTL, the application of Structured Analytical Techniques (SATs) can prove very valuable. By SAT we refer to the 'mechanism(s) by which internal thought processes are externalised in a systematic and transparent manner so that they can be shared, built on and easily criticised by others[23]'. The aim of SAT is to help the analysts and developers of CTLs to build and expand their thinking in a structured way, and advance their judgement by removing any bias, so that the quality of intelligence analysis is improved and therefore trust in the results of the analysis is increased.

According to *The Five Habits of the Master Thinker*[24], intelligence analysts employ a range of methods and analytic techniques, which can be grouped into four broad categories based on the nature of the analytic methods used and the type of data that are available, i.e. unaided expert judgment, structured analysis, quasi-quantitative analysis and empirical analysis.

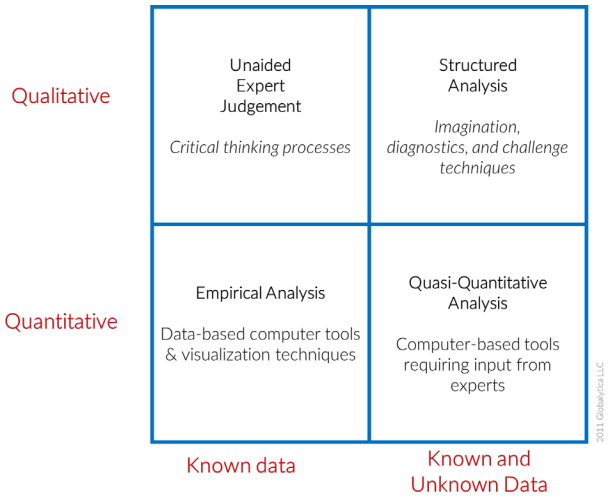

Figure 8: Analysis approaches[25]

Techniques from two or more of these categories can be employed when producing a CTL, depending on the data available. For example, a quantitative analysis can be performed when sufficient empirical data is available. In the case when the CTL development team lacks sufficient empirical data needed for the analysis, they can follow a quasi-quantitative analysis.

Currently the ETL is based on unaided expert judgement often referred to as traditional analysis, which entails critical thinking and expert reasoning, but also on structured analytical techniques.

2.4.3 Performing analysis

As mentioned at the analysis preparation step, there are different methodologies that one can follow to carry out the analysis, i.e. manual analysis, automated analysis or a mix of automated and manual analysis as in a hybrid mode. For example, one can follow the Delphi approach, i.e. forming working groups with specific experts assigned as rapporteurs to improve the overall process through consensus. When applying Structured Analytical Techniques[26]

[23] Heuer and Pherson, Structured Analytic Techniques for Intelligence Analysis, 2019
[24] Pherson, Randolph H. 'The Five Habits of the Master Thinker'. Journal of Strategic Security 6, no. 3 (2013): 54-60. DOI: http://dx.doi.org/10.5038/1944-0472.6.3.5
[25] Pherson, Randolph H. 'The Five Habits of the Master Thinker'. Journal of Strategic Security 6, no. 3 (2013): 54-60. DOI: http://dx.doi.org/10.5038/1944-0472.6.3.5
[26] Authors Richards J. Heuer, Richards J. Heuer Jr., Randolph H. Pherson, Publisher CQ Press, 2010, ISBN 1608710181, 9781608710188

(SAT) analysts intuitively think about how they think, whether a certain technique is required and how to visualise output.

The challenges that may be faced during analysis can be related to a potential lack of confidence in the data and information collected, to the multiple authors and experts involved, to the need to produce reliable content and statistics to mention a few. In this respect, some considerations to be taken include:

- **Checking your assumptions:** establish key assumptions, understand when to challenge them;
- **Considering alternatives:** consider alternative explanations or hypotheses for all events;
- **Consider inconsistencies:** look for inconsistent data that provides sufficient justification to quickly discard a candidate hypothesis or address the inconsistency;
- **Consider the key driver:** focus on the key drivers that best explain what has occurred or what is about to happen;
- **Focus on context:** anticipate the needs of stakeholders and understand the overarching context within which the analysis is being done.

2.4.4 Validate CTL

The CTL products need to be validated before being released and disseminated to the relevant audience. Validation is meant in the form of review and the provision of feedback, commenting and fine tuning. In this way, a high degree of assurance is established that the outcome of the CTL development process is of high quality, i.e. the CTL product is meeting its predetermined specifications and quality attributes.

The ETL is validated by the ENISA CTL Working Group, a group that consists of experts from European and international public and private sector entities. Validation is also achieved through other internal and external stakeholders i.e. ENISA Management Team (MT), National Liaison Officers (NLO), Advisory Group (AG).

2.4.5 Validate dissemination medium

There are various mediums that can be used for disseminating a CTL. This is something to be defined during the initial directions step. At this stage, the dissemination medium needs to be validated to ensure that it is fit for purpose. For example, the CTL can be delivered through download-via-our-website features, by establishing dedicated interactive websites or publishing key findings directly on social media. The medium can also be crucial for receiving new input or feedback. For example, audiences will be able to provide feedback on social media as well as being asked to provide comments via email.

The ETL is delivered primarily through:
- The ENISA website
- Press releases on major news websites
- Social media
- E-mail to ENISA stakeholders, e.g. National Liaison Officers (NLO), Advisory Group (AG), CTL working group

2.4.6 Deliverable production

Once the analysis is completed, findings are documented and the final deliverable is created. This produces a deliverable, where the findings are stored in a certain structure[27] after collection and analysis. Before the final text is compiled to produce the CTL,

- Text must be compiled for each threat;
- The text must be combined into one or several documents;
- The document(s) must be reviewed (internal, expert group, management approval, proof reading).
- Final edits are undertaken, followed by promotion.

Currently, the basic ETL structure includes:

- *A generic description of the cyberthreat as it has been assessed in the reporting period;*
- *A list of interesting points with important points, observations or developments that have been found with regards to the threat;*
- *Observed trends and main statistics for the threat that describe whether the threat is increasing in frequency, is decreasing or is stable;*
- *A list of specific attack vectors for a particular threat;*
- *A list of threat agents using these threats;*
- *An indicative list of incidents related to the threat category;*
- *A reference to the MITRE ATT&CK® framework for a given threat;*
- *A reference to the geographical spread of this cyberthreat in relation to the EU, namely at a near, mid or global scale;*
- *A list of recommendations and mitigation vectors that can be launched to reduce exposure to this threat;*
- *A list of authoritative resources, indicating the main, more indicative references or reports that have mentioned elements of the threat.*

A generic cyberthreat landscape template, as well as a reference template for the three types of CTLs, i.e. horizontal, thematic and sectorial threat landscapes, are provided in the Annex.

Format

This methodology identifies two different broad categories of presentation formats for cyberthreat intelligence: textual (prose documents) and machine-readable. Multiple approaches or formats for producing and disseminating a CTL exist that belong to one of the aforementioned categories. For example:

- briefings or requests for information
- blog posts

[27] Current ETL report structure, ENISA.docx

- threat landscapes or threat reports
- ad-hoc reports
- intelligence provided in machine-readable formats.

Textual formats

With regards to textual CTLs, introducing reference (semi-standardised) presentation or output templates is a necessary task. Reference templates provide several benefits, such as consistency in writing composition and semi-standardising a repetitive process. In addition, an output template is designed based on stakeholder requirements and the messages the producer and, in this case, ENISA wants to deliver (answers to stakeholder questions). As a result, a presentation or output template is influenced by and influences the processes of intelligence collection and analysis as it interprets the stakeholders' requirements for intelligence. For example, a reference template infers what information should be gathered, processed, analysed and, finally, the way it is to be represented.

Machine-readable formats

Machine-readable representation formats provide defenders with the means to operationalise and share cyberthreat intelligence. Using dedicated software, defenders use machine-readable formats to increase the delivery speed of cyberthreat information and intelligence and enable machine-oriented processing (collection, normalisation, correlation) and analysis.

Such formats and their counterpart software for collecting, processing and analysing data and information (threat intelligence platforms - TIPs) often integrate with other technological solutions to derive additional threat context and seamlessly inform defence components and human agents about detecting, preventing or mitigating attacks. This demonstrates why many intelligence producers, in addition to traditional reporting methods, also offer their technical observations in machine-readable formats. In addition, standardised approaches for representing cyberthreat intelligence in a machine-readable format enable interoperability and allow defenders to share and consume intelligence across organisational and geographical boundaries more seamlessly.

It is also a misconception that the representation of threat intelligence and the sharing of standards and threat intelligence platforms are only used to disseminate technical artefacts. The security communities have started transitioning to using machine-readable formats to share more context around adversaries, which was previously performed mainly by publishing threat reports. Technological advancements have allowed us to be able to fully transfer the content of a textual report to a structured machine-readable counterpart. Still, it is the case that only organisations that are highly mature in cybersecurity and resources can use such approaches.

Currently the ETL is produced in text format (pdf) and is enriched with infographics providing a visual representation of the results of analysis.

2.5 DISSEMINATION

Dissemination is the part of the intelligence cycle that delivers the CTL products to the appropriate stakeholders after analysis and production is complete. When reviewing practices related to the management of the dissemination of intelligence, one should consider issues related to the format of dissemination, its timeliness and automation.

Dissemination can be done in an automated way using tools or through narrative processes using formats such as reports, briefings, e-mails etc. This needs to be decided when planning the dissemination of the CTL product. Usually, based on stakeholder requirements, intelligence can be disseminated through public or private channels such as public releases with reports, briefings, blog posts, emails, social media, sharing machine-readable feeds using digital transports or a dedicated threat intelligence platform.

For example, in terms of dissemination, a CTL could be delivered in Structured Threat Information Expression (STIX™), Malware Information Sharing Platform (MISP) or some other custom-made schema. Other options that need to be considered are associated with the method of dissemination. For instance, the CTL could be delivered using Application Programming Interface (API), in file format (e.g. JavaScript Object Notation (JSON), CSV, spreadsheet, pdf, doc file etc.), or via feeds.

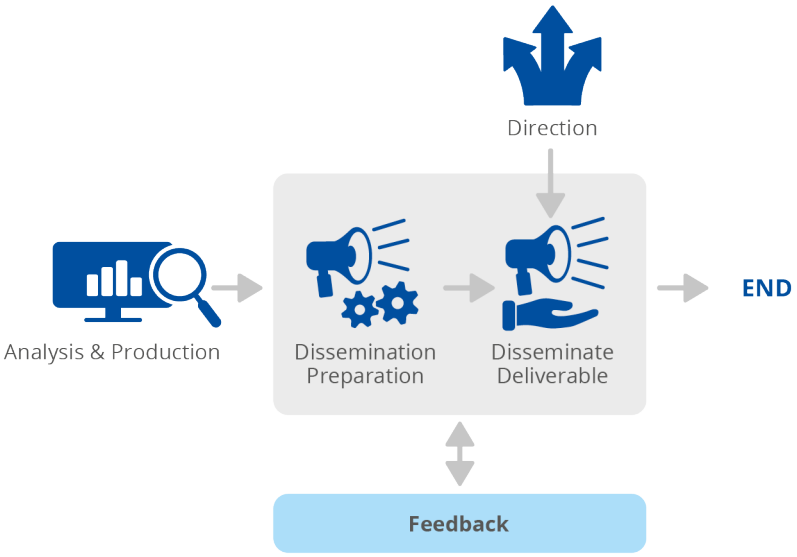

Figure 9: CTL dissemination process

2.5.1 Prepare dissemination

At this stage, one should choose the model of interaction with the intended audience. There are three models to explore interaction with a CTL audience: push, pull or interactive. All the models have different values, so choosing one should be aligned with the requirements, audience and objectives of the CTL.

One of the challenges for ENISA's CTL is that different interactions are chosen at different stages of producing the CTL. There is much interaction with expert groups, such as stakeholders and working groups during production. When the document is finalised it is then published to the audience.

2.5.2 Disseminate CTL deliverable

This is the actual dissemination of the CTL product based on the different parameters that have been discussed and decided upon in the previous steps. Engagement with the CTI community would be beneficial, which would mean using social channels, e.g. Twitter, LinkedIn, or other means of community engagement. Additionally, this step of the process can also feed the direction or planning phase of the CTL in the sense that after dissemination, feedback, comments, observations, reflections, ideas can be received from the different audiences on how to advance the CTL produced. The means of receiving this feedback may vary depending on the medium through which a CTL is disseminated.

2.6 FEEDBACK

Collecting and acting on received feedback is vital for improving the CTL products and services offered. The feedback can touch upon the content of the CTL (direction, data collection, analysis method), the format, the components, the structures, the tools used, the CTL taxonomies, the frequency of production and other relevant matters.

The feedback, either positive or negative, can highlight a number of areas, as perceived by the relevant recipients and audience, in which a CTL development team may do well or fall down. The feedback received should be handled bearing in mind the initial objectives of the given CTL and the CTL development team should act accordingly. Having a clear and detailed understanding of the individual needs of the various CTL audiences can be enforced by putting in place a constant feedback loop. Maintaining a continuous stakeholders' feedback communication process throughout all the individual phases of the CTL development lifecycle is key to the success of the CTL.

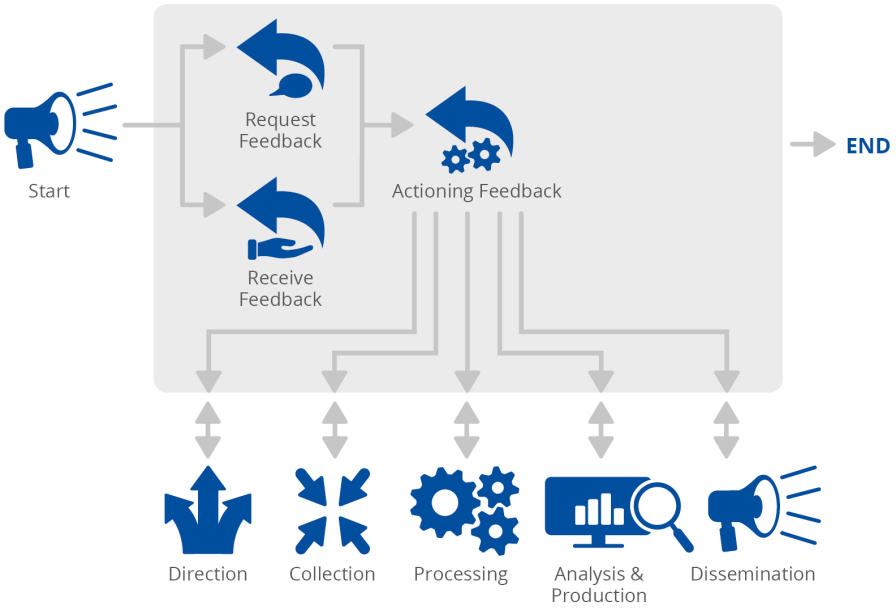

Figure 10: CTL feedback collection process

2.6.1 Requesting feedback

There are various ways to ask for feedback. Feedback on the CTL can be received continuously, meaning without being requested, or on an ad-hoc basis (e.g. through a survey) when the CTL development team is reviewing the CTL or considering a revamp or major changes that could have a key impact on the output.

In 2021, ENISA conducted a survey to enable it to improve ENISA's yearly CTL by collecting the requirements and needs by its stakeholders. The feedback collected was used to extract and formalise requirements to be considered in its long-term strategy and its revised methodology for threat landscapes.

2.6.2 Receiving feedback

When following the push model for dissemination, authors of the CTL will undoubtedly receive feedback. This can be either by email, social media or in person. In addition to understanding 'who' is providing the feedback, it is always

relevant to collect as much feedback as possible. Sometimes even the smallest suggestions can lead to great long-term improvements.

ETL feedback extracted from the survey ENISA conducted in 2021:
- ETL assisted the most in awareness raising;
- The majority of participants asked for the strategic orientation of the ETL;
- The sections of the report on threats, trends and recommendations are considered essential for the ETL and further development on these is highly encouraged.

2.6.3 Actioning feedback

Actioning feedback is probable the most important step, as it involves deciding on the actions to be made after adopting the comments received. Feedback received on a regular basis or an ad-hoc basis is not immediately actionable as it requires some processing by the CTL team beforehand. This takes time and sometimes this time is not included in the estimates for production resources.

To further improve acting on the feedback collected, it is crucial to have more insight into who provided it. This can include CTL audiences but also stakeholders. Having a more granular understanding helps the making of conscious choices on what feedback to action and what to ignore. Once the feedback is processed, suggestions can be made to the relevant parties who can decide on the matter and what improvements are to be approved or rejected.

For the ETL, the input received from the ETL stakeholders was actioned through the ENISA CTL Team that maintains a feedback registry, but also through the experts of the CTL working group.

3. FUTURE WORK

The ENISA methodology provides a high-level overview of how to produce a CTL. In a way this is a living document. To that extend the Agency is always looking for feedback and ways to improve and update the methodology, thus increasing transparency and trust in the CTL work. The process is attempting to be exhaustive, although certain elements of the methodology such as the data sources and the analysis are not described exhaustively, as they are subject to confidentiality.

The reason for publishing the ENISA methodology is to enable other entities themselves to be able to produce similar products. That way ENISA is helping the community to mature and achieve a higher level of cybersecurity, which is also one of the main objectives of the Agency.

The ENISA CTL methodology consists of the following steps:

1. Direction
2. Data Collection
3. Processing
4. Analysis and Production
5. Dissemination

Feedback is incorporated in all steps of the CTL methodology.

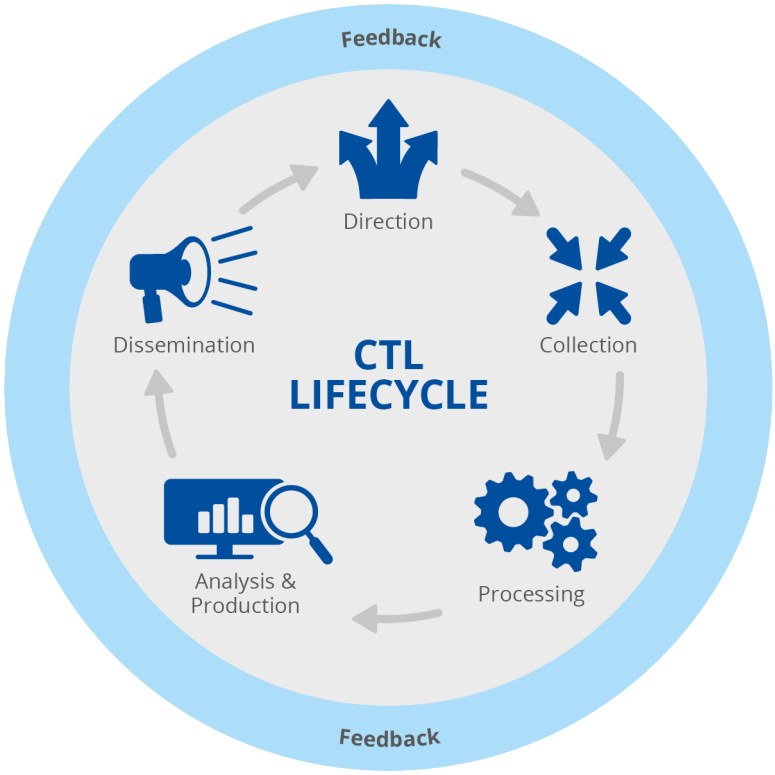

Figure 11: Methodological approach for the development of cybersecurity threat landscapes

3.1 MOVING TOWARDS AUTOMATED INFORMATION PROCESSING

Currently, the methodology involves a lot of manual work. Although human interaction and analysis will still be a part of the process for a long time, most of the work could be automated. For example, different solutions specialise in one or more areas to identify, collect, preserve, process, review, analyse and produce electronically stored information (ESI).

Such solutions would allow for the efficient processing, cross-validation and analysis of a variety of ESIs that are currently used to shape the CTL, ranging from common information sources such as Outlook and Microsoft Data to more dynamic or esoteric sources like OSINT and (vulnerability) databases. In this context, these automated solutions could enable the exploration of patterns, trends and relationships within unstructured and structured data with the objective of uncovering insights and intelligence that will enable stakeholders to respond to future cybersecurity challenges proactively or reactively.

Additionally, Artificial Intelligence (AI) is increasingly influencing people's everyday lives and playing a key role in digital transformation through its capabilities. The benefits of this technology are significant and will have a notable effect on the production of the CTL. Indeed, having an AI able to collect and provide analysis based on predefined requirements will significantly speed up the process of producing a CTL.

A ANNEX: 2021 ETL STAKEHOLDER SURVEY REVIEW

Following the revised form of the ENISA Threat Landscape Report 2020, ENISA wishes to continue and further improve this flagship report. In particular, ENISA seeks to provide targeted as well as general reports, recommendations, analyses and other actions on future cybersecurity scenarios and threat landscapes, supported by a clear and publicly available methodology and IT tools.

To this end, in March 2021, ENISA conducted a survey intended for the improvement of ENISA's yearly CTL by collecting requirements and needs of its stakeholders. The feedback collected was used to extract and formalise requirements to be considered in the long-term strategy and a revised methodology for threat landscape(s).

The current annex lists all output extracted from the survey. The list below is structured with specific topics addressing aspects of the ETL, as deemed relevant.

1. Enhancements that would increase the added value for ENISA's CTL

- **Unique content:** several suggestions were made (also shown below in this list) to position ETLs better, highlighting their unique content. Examples include moving from breaking down threats individually towards groups that use their capabilities (techniques, procedures) and intent to do 'XYZ', thus causing the threat. Another example could be more content as part of coordination between member states, such as having position papers from each country on a particular topic. Integrating the ETL with other EU professionals in security or PPP would provide more perspective on how an all EU effort is allocated to combat the current and future threat landscape.
- **Sectoral expertise:** respondents suggested collaboration with constituents could also be explored through client cases and case studies in order to improve sectoral understanding for specific sectors (railways in particular). Vertical views of industries would promote the unique position of ENISA when addressing critical sectors (and others as established in the EU NIS Directive).
- **Trend analysis**: many comments suggested the report would benefit from increased trend analysis, some saying that it deserved a separate component chapter in the ETL. This could be expressed visually with infographics. There is a strong desire to effectively monitor trends in threats across European countries.
- **Contextualisation**: several comments highlighted the desire for more context. Previous comment included the industry, yet some respondents believe the threat landscape should also be contextualised within the European policy forecast. This could include forecasts for the specific NIS sectors.
- **CTI frameworks**: it is noted that the use of frameworks, such as MITRE ATT&CK®, has improved over the years but that they are not yet integrated into the ETL. Suggestions were made to include summaries of techniques, tactics and procedures (TTPs) used by certain adversaries – mapped against the framework. This could also be potentially showcased from an ENISA perspective. This could then include a horizontal view of all TTPs observed, targeting stakeholders and industries, in an actionable format.
- **Adversarial understanding**: stepping towards an adversarial frame of mind will yield great benefits in deeply understanding threats. This can include identifying specific adversary profiles, active in Europe, breaking them down based on their capabilities and intentions. This would also allow progress towards an EU catalogue of attack techniques.

2. Improvements that would improve the ETL's current structure and/or components

   - **Revisit multiple document strategy:** multiple downloads and information fragmentation over several documents received mixed results (predominantly negative). Probably started as a good initiative but the division adds unnecessary complexity. Respondents do appreciate the thematical reports and suggest keeping the reports on specific topics yet integrate them more effectively into the main ETL; for example, by showcasing a deep dive into one of the topics that has been marked in the main ETL for development in the coming year.
   - **Document structure**: tying into point #1, mixed results were shared on the structure. Some suggested the current structure is excellent, while others said it was too complex.
   - **Automated consumption**: multiple suggestions were made for improving the 'machine' readability of the CTL report. This could include parts of structured texts that are machine readable or the use of standardised frameworks that can be parsed. This could integrate with other formats, such as an interactive application.
   - **Use the annex more effectively**: some comments suggested moving parts of long pages, such as technical and detailed content, to an annex to save room content-wise.
   - **Relevant components in the current format:** feedback received for each subject area considered as most relevant:
     - Threat trends (100%)
     - Observed threats (97%)
     - Threat vectors (97%)
     - Recommendations (94%)
     - Threat agents (89%)
     - Impact assessment (86%)
     - Emerging technologies (85%).

3. Improvements suggested on the current efforts in analysis (leading to the actual content in the deliverable)

   - **Analysis techniques applied:** many respondents wished to see improved analytical techniques applied to generate the ETLs. When a dedicated process is constructed, references to the analytical method used can be easily included.
   - **Recommendations**: in general, respondents are happy with recommendations provided in the ETL. To improve these commendations, it was suggested that current recommendations focus more explicitly on mitigation measures and strategic reflections on their effectiveness.
   - **Actionability**: some respondents commented that ETL recommendations are mostly too generic. The ETL seems oriented towards consumption, forcing readers to decide how to act on specific threats themselves. Improvements should be made on actionable 'things to do' beyond recommendations. These could include the creation of scenarios based on events observed across Europe or following up on specific techniques used by adversaries (matched against MITRE ATT&CK®).
   - **META analysis:** comparisons of different sources to contextualise threat topics and themes better have been suggested by some respondents. An example for this could be comparing ENISA's view with the views of Asia-Pacific countries or America on the current threat landscape.
   - **Trend analysis:** some respondents underlined the need for improvements in trend analysis. This includes past, current and future topics, and highlighting differences between qualitative and quantitative approaches. Examples include trends in adversaries, the state of CTI or emerging threats. Trend analysis would also include the implications of future technologies for threats in Europe.
   - **Quantification:** several respondents requested more quantifiable content. These could be metrics or economic parameters, preferably from EU entities.
   - **Forecasting**: currently ETL reports often include summary analyses of past and current events. Several respondents requested better analysis of future threats, for example, making predictions and looking ahead – allowing stakeholders to build their strategic understanding of threats.
   - **Longer term tracking**: several respondents suggested tracking certain threats over a longer period, including their evolution. This implies the improvement of the longer-term data used.

4. What specific content should be explored further in future ETLs?

   - **Scenarios**: multiple moves towards a scenario approach were suggested as well as scenarios to look out for.
   - **Case studies**: several respondents suggested that incident write-ups should be improved. This could include industry reports or peer research, potentially including support from the respondents themselves.
   - **Impact assessments**: some respondents suggested that the ETL should more specifically address how the ETL can be used to perform impact assessments at the end on the client side.

5. From what perspective should the ETL be written?

   - Respondents suggested that the ETL should mostly be strategic (80%), followed by operational (61%) and technical/tactical (53%). It is important to note that the focus area ENISA will select will also reflect the content included in the ETL. For example, one could create separate documents focused on specific audiences or included different chapters in single reports.

6. What suggestions were made regarding the taxonomies used?

   - **Taxonomies used:** content should be mapped against multiple threat intelligence frameworks, not just MITRE ATT&CK® but also the diamond model. Next, it should also be mapped against ENISA related best practices such as ETL incident reporting standards. This will allow for much improved benchmarking, which was also requested by the stakeholders.

7. Other relevant notes

   - **Expertise:** a small number of respondents suggested that industrial threats to Europe is an underrepresented topic. ENISA's role in addressing this lack of understanding can be more important than it already is.

B ANNEX: REFERENCE TEMPLATES

Introducing (semi-standardised) presentation or output templates for reference is an important element when delivering CTL. Reference templates provide several benefits, such as consistency in writing composition and semi-standardising a repetitive process. In addition, an output template is designed based on stakeholder requirements and the messages the producer wants to convey. As a result, a presentation or output template is influenced and influences the collection of intelligence and the analytic processes as it interprets the stakeholder requirements as regards intelligence. For example, a reference template infers the information that should be gathered, processed, analysed and, finally, the way it is to be represented.

A generic cyberthreat landscape template, as well as reference templates for the three types of CTL (i.e. horizontal, thematic and sectorial threat landscapes) are provided as examples in the following sections based on respective ETL reports. These references are meant to indicate the elements to consider including when producing a CTL and need to be adapted to meet the peculiarities of different use cases.

B.1 GENERIC CYBERTHREAT LANDSCAPE TEMPLATE

This section presents a generic reference template for a CTL report. The template provided can be modified, i.e. sections can be omitted or others can be added, and can generally be adapted to support the production of different types of threat landscapes according to the needs and purposes of the audience and intended stakeholders.

- **Cover Page**: title, reporting period, publication date, TLP and reference or DOI)
- **About the organisation**
- **Objective(s) of the report**: what's within the scope of the report, its objectives and the target audience
- **Methodology and approach**: the methodology used to produce the report, including information about the datasets such as the different types and amounts. Stakeholders that contributed information can be named.
- **Acronyms and glossary**
- **Table of contents**
- **Executive summary**: the overall risk-based understanding of the threat horizon, including forecasts, assessments, key takeaways, top insights, most important observations or findings and trends.
- **The sector (if applicable)**
    - Identification of the sector (an explanation or description of the industry sector).
    - The specificity of the sector (presenting the different stakeholder groups, critical functions or assets pertinent to the industry sector). For each category, a mini (or full) threat landscape can be provided.
        - It is most common for a report on the threat landscape of an industry sector to present overviews of the different threat landscapes pertinent to stakeholder or critical function groups. Those can be perceived as mini threat landscapes within the main threat landscape report and include content similar to the ones provided in executive summaries, identification of relevant adversaries and their characteristics (e.g. motivations and capabilities), noteworthy incidents and attack vectors.
        - A threat matrix can be populated that describes the risk an adversary poses to the critical function or stakeholder. Such an approach translates directly to the tactics, techniques and procedures used in attacks.
- **Threat actor categories or types**
    - The status of activity [regarding cybercrime, nation-state threats, insiders, hacktivists, etc.] over the reporting period for a particular industry sector.

- Information about the characteristics of a threat actor category or type such as motivations, capability and objectives.
- Trends and most noteworthy incidents (briefly). From a *strategic* point of view, to emphasize the importance of the incidents, the report can describe the impact in terms of financial losses, downtimes and number of affected stakeholders. From a *tactical* perspective, the important characteristics of an attack can be described briefly.
- From a *tactical* point of view, ATT&CK heatmaps or ATT&CK lists *for each actor type* can be included to indicate the most common TTPs targeting the sector.

- **Threat groups or activity groups**
  - An overview of adversaries that target the sector.
  - Details on groups that have been observed to be active in the reporting period.
    - The groups need to either target the sector directly or, if they are opportunistic, it should have been assessed that their operations will affect entities and stakeholders or functions within the industry sector.
    - Categorisation is possible based on actor types and motivations.
  - Significant incidents can be described.
  - From a *tactical* perspective, ATT&CK heatmaps or ATT&CK lists or tables for each adversary group can be included to indicate their most common TTPs.
  - Mitigations when possible (for example when an activity group corresponds to a particular malware) can be provided for more technical audiences.
- **Cyberthreats**
  - Describe cyberthreats relevant to the sector, including *trends*, attack vectors and recommended (high-level) mitigations pertinent to the threat.
  - For each threat, major incidents can be described concisely (a tabular format can be used).
  - From a *tactical* (more technical) perspective, ATT&CK heatmaps or ATT&CK lists or tables for each cyberthreat can be included to indicate most common TTPs.
- **Defensive recommendations**
  - Due to the unique technological environments of the sectors and their critical functions and stakeholders, the report can provide and describe best practices for defence.
- **Appendices:** information that may not need to be part of the main document, such as details for technical audiences.
  - List of sector incidents with references
  - TTPs - (e.g. the MITRE ATT&CK® Framework could be used)
  - Commonly used tools
  - CVE weaponisation

B.2 HORIZONTAL THREAT LANDSCAPE TEMPLATE

This section presents a sample of a reference template for horizontal threat landscape reporting, based on the annual ENISA Threat Landscape report[28] as published in 2021.

Table of Contents
Executive Summary

1. THREAT LANDSCAPE OVERVIEW
1.1 Prime Threats
1.2 Key Trends
1.3 EU Proximity of Prime Threats
1.4 Major Threats per Sector
1.5 Methodology
1.6 Structure of the Report

2. THREAT ACTOR TRENDS
2.1 State-Sponsored Actors
2.2 Cybercriminals
2.3 Hacker-For-Hire Actors
2.4 Hacktivists

3. RANSOMWARE
3.1 Trends
3.2 Recommendations
…
ANNEX A: MITRE ATT&CK
ANNEX B: MAJOR INCIDENTS

Figure 12: Horizontal threat landscape template

[28] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

B.3 THEMATIC THREAT LANDSCAPE TEMPLATE

This section presents a sample of a reference template for thematic threat landscape reporting, based on the ENISA Threat Landscape for Supply Chain Attacks report[29] as published in 2021.

Table of Contents
Executive Summary

1. INTRODUCTION
2. WHAT IS A SUPPLY CHAIN ATTACK?
2.1. Taxonomy of Supply Chain Attacks
2.2. Attack Techniques Used To Compromise a Supply Chain
2.3. Supplier Assets Targeted by a Supply Chain Attack
2.4. Attack Techniques Used to Compromise a Customer
2.5. Customer Assets Targeted by a Supply Chain Attack
2.6. How to Make Use of the Taxonomy
2.7. Supply Chain Taxonomy and other Frameworks

3. THE LIFECYCLE OF A SUPPLY CHAIN ATTACK
4. PROMINENT SUPPLY CHAIN ATTACKS
4.1. Solarwinds Orion: It Management and Remote Monitoring
4.2. Mimecast: Cloud Cybersecurity Services
4.3. Ledger: Hardware Wallet
4.4. Kaseya: IT Management Services Compromised With Ransomware
4.5. An Example of Many Unknowns: SITA Passenger Service System

5. ANALYSIS OF SUPPLY CHAIN INCIDENTS
5.1. Timeline of Supply Chain Attacks
5.2. Understanding the Flow of Attacks
5.3. Goal Oriented Attackers
5.4. Most Attack Vectors to Compromise Suppliers Remain Unknown
5.5. Sophisticated Attacks Attributed To Apt Groups

6. NOT EVERYTHING IS A SUPPLY CHAIN ATTACK
7. RECOMMENDATIONS
8. CONCLUSIONS

Figure 13: Thematic threat landscape template

[29] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

B.4 SECTORIAL THREAT LANDSCAPE TEMPLATE

This section presents a sample of a reference template for thematic threat landscape reporting, based on the ENISA Threat Landscape for 5G Networks report[30] as published in 2020.

Table of Contents

[30] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

Figure 14: Sectorial threat landscape template

TP-09-22-217-EN-N

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-579-1
doi: 10.2824/339396