enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CONTACT

EDITORS

CONTRIBUTORS

ACKNOWLEDGEMENTS

LEGAL NOTICE

COPYRIGHT NOTICE

“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”

Horizontal threat landscapes,

Thematic threat landscapes,

Sectorial threat landscape,

1.1 OBJECTIVES

-
-
-
-
-
-

1.2 OVERVIEW OF METHODOLOGICAL APPROACH

Figure 1

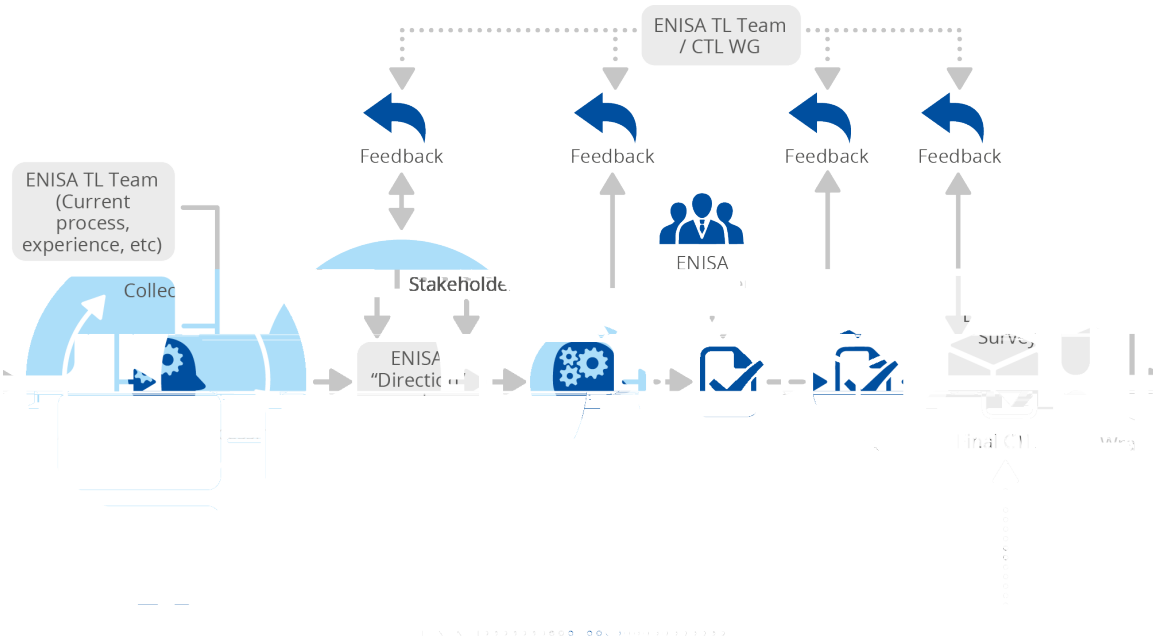

Figure 1: High level overview of ENISA CTL methodology

1.3 SCOPE

what is the scope of the threat landscape

what is the target audience and the aim'

1.4 CYBERTHREAT LANDSCAPE DRIVING PRINCIPLES

- **Actionable**

ETL provides actionable recommendations

- **Timely**

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

- **Accurate**

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

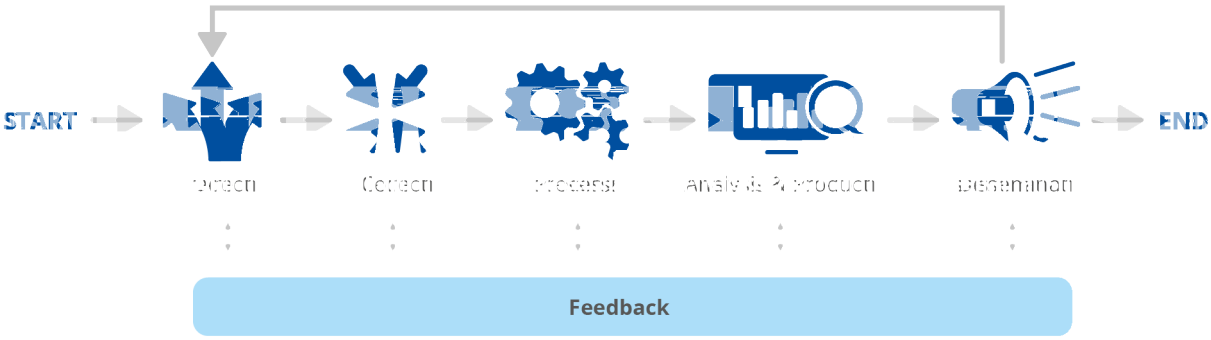

Figure 2: Overview of ENISA CTL methodology

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

2.1 DIRECTION

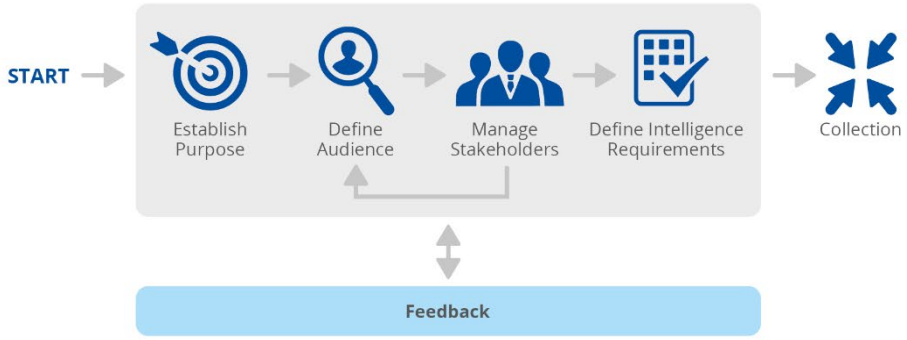

Figure 3: CTL direction definition process

2.1.1 Establish CTL Purpose

ETL Purpose:

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

2.1.2 Define Audience

- **Strategic**
- **Tactical**
- **Operational**
- **Technical**

2.1.3 Identifying and Managing Stakeholders

Figure 4

Figure 4: CTL stakeholder mapping[4]

High-influence, High-interest

High-influence, Low-interest 0 Tw 2.227d (ep)13.3 (s)-o 0.7 (i)1nt)2

Low-influence, High-interest –

Low-influence, Low-interest –

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

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?*

intelligence requirement

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

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

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

Deliverable components

- **Internal orientation**
- **External orientation**

2.2 COLLECTION

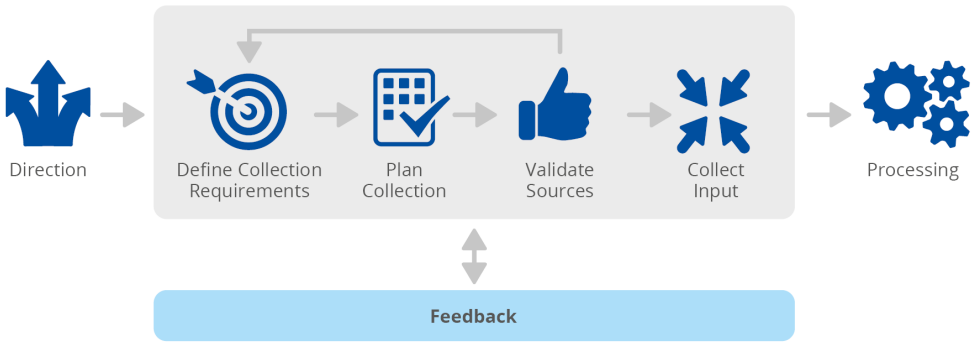

Figure 5: CTL data collection process

2.2.1 Define collection requirements

Intelligence requirements	Collection requirements
What ransomware campaigns were specifically targeting European companies?	• • • •
Timeframe for collecting the data	
Types of incidents	

Table 1: Example of defining data collection requirements

2.2.2 Collection planning

Operational

Tactical

Strategic

Source	Type of data	Collection time
CTI providers		
Institutional stakeholders		
Social media		
Data feeds		
Cybersecurity news		
Vulnerability disclosure		
Academia		
Deep/dark web		

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**		
ENISA Situational Awareness intelligence data		
Member states' incident reporting tool (CIRAS)		

2.2.3 Validate Sources

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

Internal sources

Institutional sources

External sources

- **Raw or processed data**
- **Information, based on data they themselves collected and/or processed**
- **Finished intelligence products, based on data and information collected, processed, analysed, and disseminated**

2.2.3.1 Confidence or Trust levels

Low Confidence

Moderate Confidence

High Confidence

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

2.2.4 Input data collection

2.3 PROCESSING

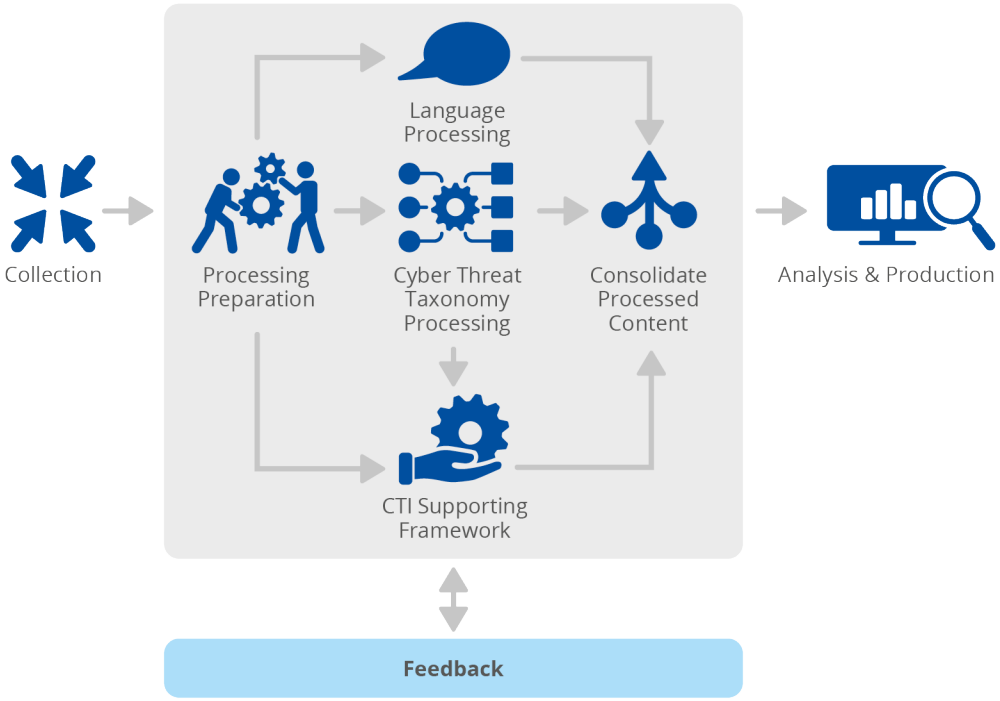

Figure 6: CTL data processing process

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

2.3.2 Language processing

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

- **ENISA Threat Taxonomy :**

- **Alignment with other ENISA initiatives**

- **Alignment with other EU-centric research programs**

- **JRC Taxonomy[15] (based on NIST):**

- **ENISA Cyber Incident Taxonomy[16]**

- **ENISA Reference Security Incident Classification Taxonomy[17]**

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

- **MITRE ATT&CK®**

- **Cyber Kill Chain®**

- **MITRE CVE®**

- **OASIS Cyber Threat Intelligence (CTI) STIX™** [22]

- **There is no single silver bullet framework**

- **Be wary of the implications due to betting on a single framework**

- **Reconsider the framework used**

2.3.5 Consolidate processed content

2.4 ANALYSIS & PRODUCTION

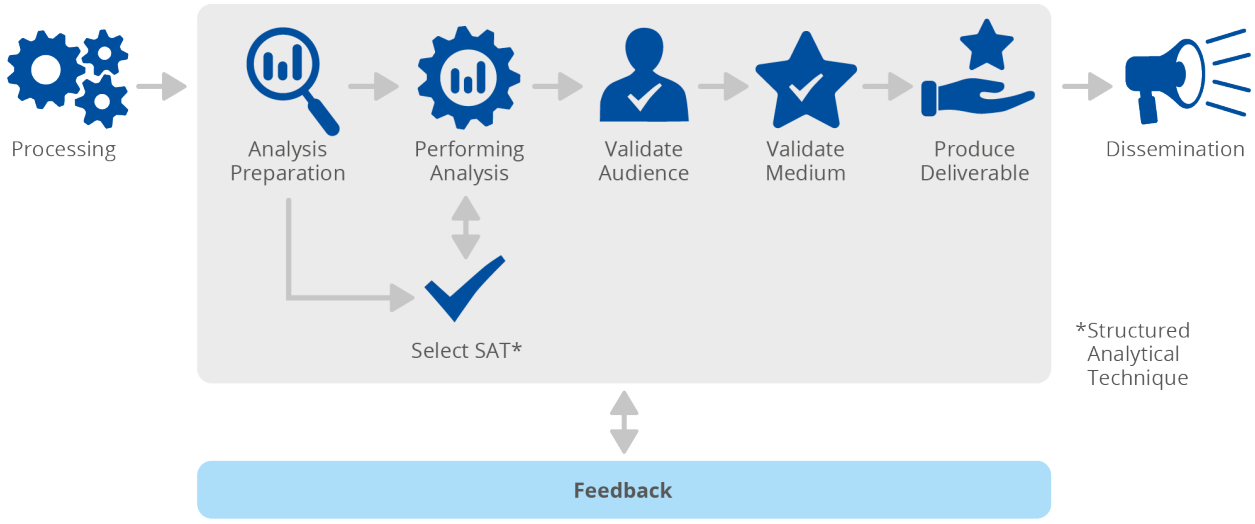

Figure 7: CTL data analysis and production process

2.4.1 Analysis preparation

2.4.2 Structured Analytical Technique (SAT) selection

The Five Habits of the Master Thinker

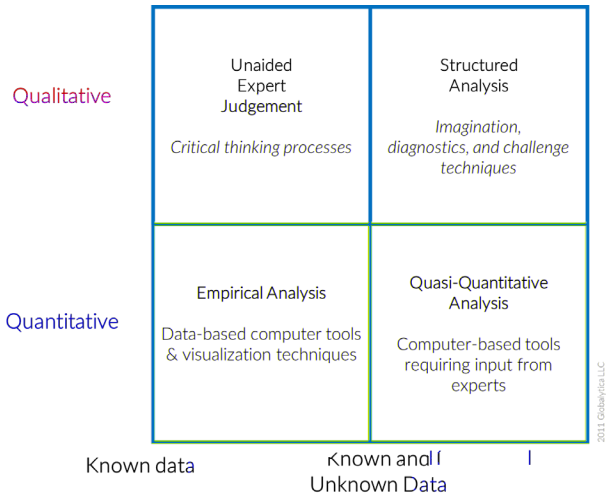

Figure 8: Analysis approaches[25]

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

- **Checking your assumptions:**
- **Considering alternatives:**
- **Consider inconsistencies:**
- **Consider the key driver:**
- **Focus on context:**

2.4.4 Validate CTL

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

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

-
-
-
-

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

-
-

-
-
-

Textual formats

Machine-readable formats

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

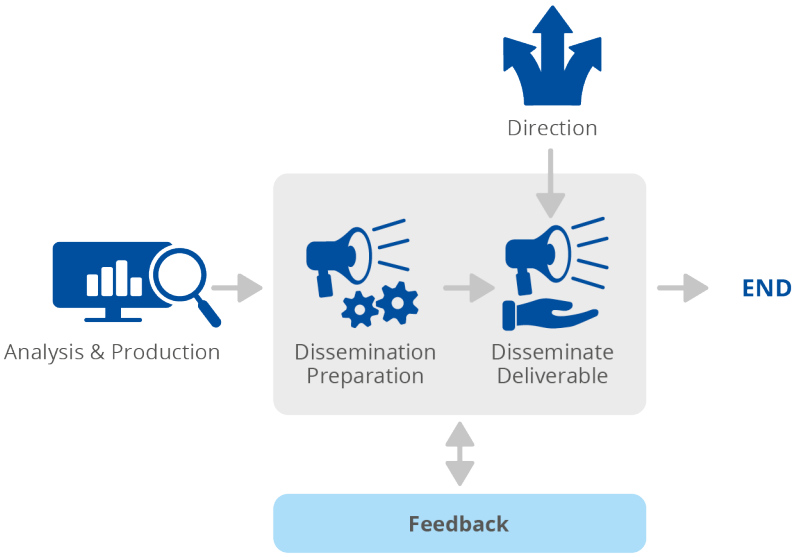

Figure 9: CTL dissemination process

2.5.1 Prepare dissemination

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

2.6 FEEDBACK

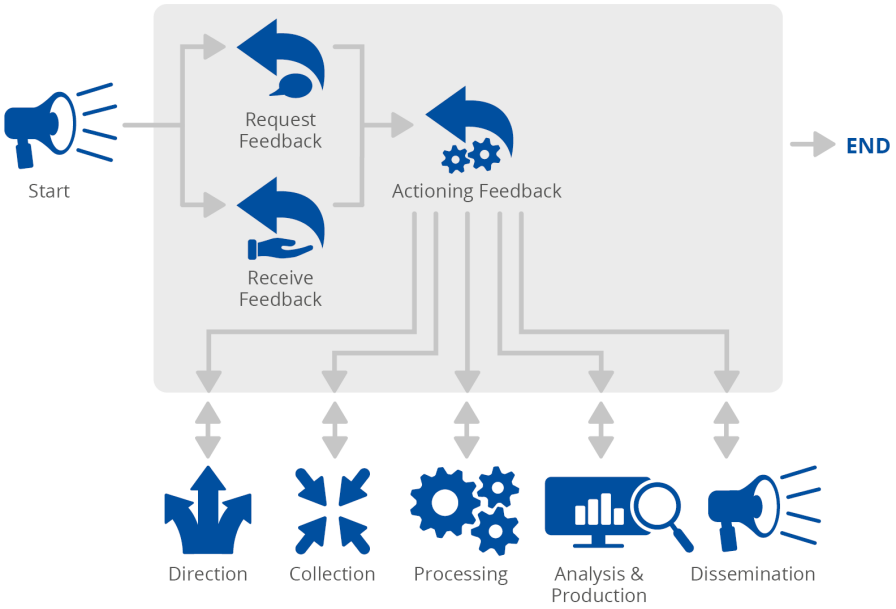

Figure 10: CTL feedback collection process

2.6.1 Requesting feedback

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

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

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.

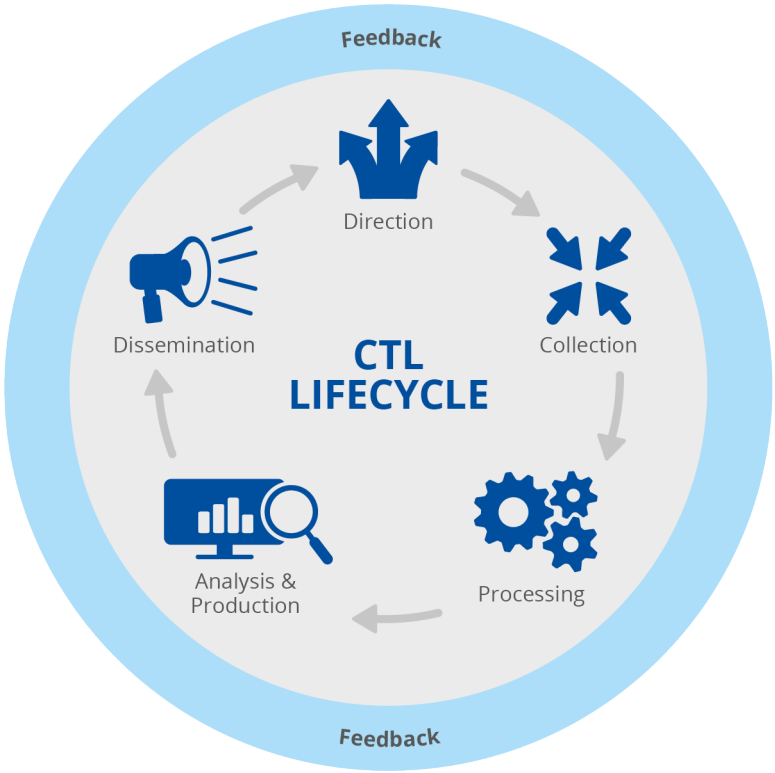

Figure 11: Methodological approach for the development of cybersecurity threat landscapes

3.1 MOVING TOWARDS AUTOMATED INFORMATION PROCESSING

- **Unique content:**
- **Sectoral expertise:**
- **Trend analysis**
- **Contextualisation**
- **CTI frameworks**
- **Adversarial understanding**

- **Revisit multiple document strategy:**

- **Document structure**
- **Automated consumption**

- **Use the annex more effectively**
- **Relevant components in the current format:**
    -
    -
    -
    -
    -
    -
    -

- **Analysis techniques applied:**

- **Recommendations**

- **Actionability**

- **META analysis:**

- **Trend analysis:**

- **Quantification:**
- **Forecasting**

- **Longer term tracking**

- **Scenarios**
- **Case studies**
- **Impact assessments**
-

- **Taxonomies used:**

- **Expertise:**

B.1 GENERIC CYBERTHREAT LANDSCAPE TEMPLATE

-
- *strategic*

  tactical
- *tactical* *for each actor type*

- **Threat groups or activity groups**
  -
  -
    -
    -
  -
  - *tactical*
  -

- **Cyberthreats**
  - *trends*
  -
  - *tactical*

- **Defensive recommendations**
  -

- **Appendices:**
  -
  -
  -
  -

B.2 HORIZONTAL THREAT LANDSCAPE TEMPLATE

Figure 12: Horizontal threat landscape template

B.3 THEMATIC THREAT LANDSCAPE TEMPLATE

Figure 13: Thematic threat landscape template

B.4 SECTORIAL THREAT LANDSCAPE TEMPLATE

1. INTRODUCTION

2. 5G STAKEHOLDERS

3. 5G NETWORK DESIGN AND ARCHITECTURE

4. 5G VULNERABILITIES

6. 5G THREATS

7. THREAT AGENTS
8. RECOMMENDATIONS/ CONCLUSIONS

A ANNEX: ASSETS MAP
B ANNEX: THREAT TAXONOMY
C ANNEX: DETAILED VULNERABILITIES IN THE CORE NETWORK
D ANNEX: DETAILED VULNERABILITIES IN NETWORK SLICING
E ANNEX: DETAILED VULNERABILITIES IN THE RADIO ACCESS NETWORK
F ANNEX: DETAILED VULNERABILITIES IN NETWORK FUNCTION VIRTUALIZATION – MANO
G ANNEX: DETAILED VULNERABILITIES IN SOFTWARE DEFINED NETWORKS
H ANNEX: DETAILED VULNERABILITIES IN MULTI-ACCESS EDGE COMPUTING
I ANNEX: DETAILED VULNERABILITIES IN THE PHYSICAL INFRASTRUCTURE
J ANNEX: DETAILED VULNERABILITIES IN IMPLEMENTATION OPTIONS
K ANNEX: DETAILED VULNERABILITIES IN MNO PROCESSES
L ANNEX: DETAILED VULNERABILITIES IN VENDOR PROCESSES
M ANNEX: DETAILED VULNERABILITIES IN SECURITY ASSURANCE PROCESSES

Figure 14: Sectorial threat landscape template

ABOUT ENISA

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