Tactical Cyber Threat Intelligence: Identifying Maturity Development Successes and Complications

Sijmen Schenk: 180166172

12 March 2022

Submitted as part of the requirements for the award of the
MSc. in Information Security
at Royal Holloway, University of London.

Supervisor: Dr. Konstantinos Markantonakis

Information Security Group
Royal Holloway, University of London
Egham, Surrey, TW20 0EX
United Kingdom

Anti-Plagiarism Declaration

I declare that this dissertation is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statement on plagiarism in the General Regulations for Awards at Graduate and Masters Levels for the MSc in Information Security, and in accordance with it, I submit this project report as my own work.

Signature: Date: 12-03-2022

Acknowledgements

I want to extend gratitude to the people who supported me during this dissertation process, with special thanks to my project supervisor Dr Konstantinos Markantonakis.

This project could not have come together without my past and current cybersecurity co-workers' help and the fantastic participation provided by my interview respondents. You know who you are, and I will always be grateful for the opportunity presented to me; I hope this dissertation will serve you in a meaningful way.

This project was driven forward through the motivation provided by my wife Desiree and my daughters Nova and Yuna. Their daily support helped me through the many hours needed to complete the MSc. program.

Abstract

Cyber Threat Intelligence (CTI) has developed into a decisive factor in security operations. Accurate intelligence allows stakeholders to prioritize rare investigative resources on the most significant threats. In successful cases, this led to effective investigation, attribution, prosecution, and conviction of malicious actors. 2022 will be an essential year for the CTI discipline. It will bring CTI's further development within the NIST framework and its adoption as a control into the ISO 27002 standard, further formalizing its future significance [1], [2].

This dissertation aims to make a threefold contribution to this field. Firstly, by providing a practical and up to date introduction into the (cyber)intelligence field without requiring previous knowledge, and secondly by performing phenomenological research to identify the successes and challenges encountered when adopting and maturing CTI programs. These experiences were gathered through interviews with eight leading organizations that developed CTI capabilities within the Netherlands within the last ten years. The dissertation will end with a more extensive reflection on the identified best practices and open-source tooling and present them in a logical implementation order. This approach can be considered an alternative strategy to augment current programs or as a starting point to make CTI feasible for smaller-scale organizations without requiring significant financial investment.

Keywords: Cyber Threat Intelligence | Military Intelligence| CERT | SOC | Maturity | Strategic | Operational | Tactical| Structured Analytics | Analysis of Competing Hypotheses| Threat Intelligence Platform| Indicator of Compromise | Intelligence Courses of Action | Open-Source

Contents

List of Figures 8

List of Tables 8

Abbreviations 9

Executive Summary 11

Chapter 1: Introduction, Objectives and Approach of this Dissertation 12

1.1 Statement of Objectives 13

1.2 Motivation 13

1.3 Methodology 14

1.3.1 Introduction 14

1.3.2 Semi-Structured Interviews 14

1.3.3 Literature Analysis 14

1.3.4 Online Conference Participation 15

1.4 Document Outline 15

Chapter 2: General Introduction of Intelligence Concepts 16

2.1 The Traditional Origin of Intelligence 17

2.2 Definitions for Intelligence and Intelligence Analysis. 19

2.3 The Intelligence Lenses of Collection, Processing and Analysis 20

2.4 Identifying Stakeholders and their Requirements: PIR and SIR 21

2.5 Levels of Intelligence, the Traditional Intelligence Perspective 22

2.6 Cyclic Nature of Intelligence Production 23

2.6.1 Iterative Nature of the Intelligence Production Process 23

2.6.2 Acting on Military Intelligence: Courses of Action 24

2.7 Confidential Information Sharing in Traditional Intelligence 25

Chapter 3: Introduction to Cyber Threat Intelligence 26

3.1 The Origins of Cyber Threat Intelligence 27

3.2 Levels of Intelligence, the CTI Intelligence Perspective 28

3.3 Overlap in Traditional Intelligence Tradecraft and CTI 29

3.4 The Cyber Kill Chain 30

3.5 The Pyramid of Pain 31

3.6 CTI Courses of Action 33

3.7 Confidential Information Sharing in CTI 34

3.7.1 Information Sharing in Informal Trust Groups 34

3.7.2 Information Sharing in Formal Trust Groups 34

3.7.3 Confidential Information Sharing in CTI: Traffic Light Protocol 35

3.8 Automating CTI – Threat Intelligence Platforms, Feeds and Services 37

3.8.1 Threat Intelligence Platforms 37

3.8.2 Threat Intelligence Data Feeds 37

3.8.3 Threat Intelligence Services 38

3.9 Distinguishing Levels of CTI Maturity 39

Chapter 4: Identified Successes and Challenges in CTI Implementations 41

4.1 Interview Methodology 42

4.1.1 Participants 42

4.1.2 Distribution of Respondents Origin 43

4.1.3 Structure of the Interviews 44

4.2 Interview Findings 46

4.2.1 Summary of the Interview Responses 46

4.2.2 Findings of the Pre-Implementation Phase: Defined Objectives for the CTI Program 47

4.2.3 Primary Stakeholders Assigned to the CTI Program 49

4.2.4 Involvement of External Expertise to Define the Program 50

4.2.5 Collaborations with Peers at Initiation of the Program 50

4.2.6 Distinction of Objectives by Intelligence Level 51

4.2.7 Maturity Development and Timeline Expectations 52

4.2.8 Staffing Size of Organisations 53

4.2.9 Education and Training Resources Leveraged to aid Maturity 54

4.2.10 CTI Tooling Known and Leveraged by Respondents 55

4.2.11 Adoption of Structured Analytical Techniques in the Program 56

4.3 Interview Findings: Complications Identified During CTI Adoption 57

4.3.1 Overall Complications During CTI Implementation 57

4.3.2 Complications Relating to People Factors 58

4.3.3 Complications Relating to Process Factors 58

4.3.4 Complications Relating to Technology Factors 60

4.4 Interview Findings: Overall Reflections after CTI Adoption 61

4.4.1 Reception of the CTI Program 61

4.4.2 Significant Benefits Achieved 61

4.4.3 Feedback and Continual Improvement in CTI Programs 62

4.4.4 Resulting Level of CTI Maturity Achieved By these Organisations 64

Chapter 5: Analysis of Interview Findings and Potential Improvements 65

5.1 Section One: People 66

5.1.1 Staffing Issues - Considering Fusion Teams or Dual Hat Analysts 66

5.1.2. Analytical Cohesion Between Analysts – Introducing Structured Analytics 67

5.2 Section Two: Processes 71

5.2.1 Structuring the Intelligence Collection Process 71

5.2.2 Structuring the Analysis Process 73

5.3 Section Three: Technology 74

5.3.1 MISP 74

5.3.2 Dutch National Cert Resources: The National Detection Network and ISIDOOR 76

5.3.3 OpenCTI 77

5.4 Section Four: Information 78

5.4.1 MITRE ATT&CK Framework 78

5.4.2 Open-Source Threat Intelligence Libraries 80

5.4.3 Helping Stakeholders Understand Uncertainty in Intelligence 81

Chapter 6: Conclusion 84

6.1 Conclusion 85

6.2 Further Research 86

6.3 Closing Remarks and Diagram of Findings 87

Bibliography - References 89

Appendix A: Interview Introduction and Questions 96

Appendix B: Additional CTI Capabilities Mentioned by Individual Respondents 99

List of Figures

Figure 1 - The Battle of Waterloo, June 18th, 1815, by William Sadler. Depicting Arthur Wellesley, the Duke of Wellington. The defeat of the French forces of Napoleon Bonaparte. The last major battle (Public Domain Image [4]) 10
Figure 2 Intelligence Lenses Model Joint National Intelligence Support, DOD Appendix D [30] 20
Figure 3 Traditional Levels of Intelligence and their purpose and timeliness 22
Figure 4 The Intelligence Process – DOD JP2-01 Publication[30] 23
Figure 5 CTI Levels of Intelligence and their Purpose 28
Figure 6 Lockheed Martin Cyber Kill Chain [46] 30
Figure 7 David J. Bianco - Pyramid of Pain[48] 31
Figure 8 STIX data model, an example from stixproject.github.io about [67] 38
Figure 9 CTI Capability Maturity Model - Marco Lourenco ENISA [9] 39
Figure 10 CTIM approach to maturity from the CTIM Whitepaper [68] 40
Figure 11 Sector Origin of Interview Respondents 43
Figure 12 Respondents Organization Global FTE 43
Figure 13 Stated Objectives for the CTI Initiative 47
Figure 14 Primary Stakeholders Defined 49
Figure 15 Training Material in Use 54
Figure 16 Usage of CTI Tools 55
Figure 17 Structured Analytical Techniques 56
Figure 18 Complications Identified During Implementation of Program 57
Figure 19 Organisational Level of CTI Maturity Achieved 64
Figure 20 ACH Example Richard J Heuer, Psychology of Analysis [26] 68
Figure 21 Mind Map Example for the CTI Domain 70
Figure 22 Bow Tie Example On Risk Management. 70
Figure 23 Intel471 GHIR Collection Plan [81] 72
Figure 24 MISP Overview screen [106] 74
Figure 25 MISP Event Entity Example [106] 75
Figure 26 OpenCTI Graphical Dashboard [117] 77
Figure 27 Navigator view of the MITRE ATT&CK model [118] 79
Figure 28 DeTTECT Framework [119] 79
Figure 29 APT Groups and Operations Spreadsheet [121] 80
Figure 30 Scales of Uncertainty – Weiss [124] 82

List of Tables

Table 1 COA Matrix according to the NATO Comprehensive Operations Planning Directive[36] 24
Table 2 CTI Defensive Courses Of Action 33
Table 3 Proactive ACH Table for Malware Infection 69
Table 4 Evaluation of Source Reliability [125] 83
Table 5 Evaluation of Information Content [125] 83

Abbreviations

ACH: Analysis of Competing Hypotheses
ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge
CERT: Computer Emergency Response Team
CIA: the United States Central Intelligence Agency
CIRCL: Computer Incident Response Center Luxembourg
CISO: Chief Information Security Officer
COA: Courses of Action
CTI: Cyber Threat Intelligence
DOD: United States Department of Defence
ENISA: European Union Agency for Cybersecurity
FIRST: Forum for Incident Responders and Security Teams
IOC: Indicator of Compromise
ISAC: Information Sharing and Analysis Center
MISP: Malware Information Sharing Platform
NATO: North Atlantic Treaty Organisation
NCSC: Nationaal Cyber Security Centrum (The national CERT of the Netherlands)
NDN: Nationaal Detectie Network (Dutch NCSC's National Detection Network)
NOC: Network Operations Center
NSA: United States National Security Agency
OODA: Observe, Orient, Decide, Act
OSINT: Open Source Intelligence
OSS: United States Office of Strategic Services (CIA Predecessor)
PIR: Priority Intelligence Requirements
SIR: Secondary Intelligence Requirements
SOC: Security Operations Center
TIBER: Threat Intelligence Based Ethical Red-teaming
TIP: Threat Intelligence Platform
TLP: Traffic Light Protocol
TTP: Tools Techniques and Procedures of an actor

References and style guide

The following formatting rules apply to this paper.

The default font of this document will be Calibri font size 11, with headers derived from this.
References are cited according to the IEEE referencing standard [3].
Citations will be annotated with parenthesis and the Italic format: '*citations*'.
Terms fundamental to the understanding of this dissertation are highlighted in **bold text.**

Figure 1 - The Battle of Waterloo, June 18th, 1815, by William Sadler. Depicting Arthur Wellesley, the Duke of Wellington. The defeat of the French forces of Napoleon Bonaparte. The last major battle (Public Domain Image [4] *)*

> *"One of the surest ways of forming good combinations in war should be to order movements only after obtaining perfect information of the enemy's proceedings. In fact, how can any man say what he should do himself if he is ignorant of what his adversary is about?*
>
> **General Antoine-Henri de Jomini, Summary of the Art of War, 1838** [5].

Executive Summary

Maturity in Cyber Threat Intelligence Implementations

The analytical data required for this dissertation was gathered by interviewing the key CTI stakeholders of eight organisations. All organisations were based in the Netherlands and had adopted and developed internal CTI capabilities within the last ten years. Five organisations were part of the private sector, and three were part of the Dutch government sector.

The main finding is that all interviewed respondents had developed an effective CTI program where the CTI team leveraged the SOC as their primary stakeholder. After adopting the program, all eight organizations could consume intelligence from external parties and integrate this into their SOC processes. The consumption of external intelligence can be deemed the first tier of maturity. The second tier of maturity is the internal creation of new intelligence, and five respondents were able to achieve this. The third tier of maturity is the moment when the self-created intelligence is disseminated to a broader audience outside of the organization on a structural basis. Two organizations had achieved this level, and they were the longest-running teams (more than five years) with the highest analyst headcount (respectively, nine and twelve analysts).

- All eight interview respondents leveraged the Open Source Circl.Lu (Luxembourg CERT) developed MISP (Malware Information Sharing Platform). This open-source CTI platform makes automated CTI accessible to a broader audience.
- All three interviewed government entities were involved with the Dutch National CERT's 'Nationale Detectie Network; (National Detection Network), a network of sensors that can aggregate network data to help the organisation identify potential intrusion attempts. This network can serve as a great example to other National CERT's that may consider developing similar capabilities.
- Though commercial tools and data sets were in use by all but one respondent, all eight respondents also leveraged open-source tools and were able to gain significant benefits from them. The CTI open-source community has become a thriving environment rich with freely available tools and threat intelligence data.

Based on these findings, it is likely that at this stage of CTI development, the availability of free, open-source CTI tools, datasets and process methodologies has made CTI feasible for small scale organizations without requiring significant investments. This initiative can be as small as joining local government initiatives, setting up an open-source MISP and providing MISP access to the SOC/CERT to perform correlation on internal logging. While this may require a relatively minor investment in time, this integration is likely to enhance the security posture and effectiveness of the SOC process by providing enriched contextual intelligence on SOC findings and thus help perform effective triage.

It can be expected that the CTI domain will continue to receive significant open-source community development interest in the future. This dissertation has identified that similar to our interview participants, any organisation interested in adopting CTI can expect to see significant benefits by assessing what is available on a free community basis before committing to long-term commercial programs.

Chapter 1: Introduction

Objectives and Approach of this Dissertation

Contents:

1.1 Statement of Objectives
1.2 Motivation
1.3 Methodology
    1.3.1 Methodology Introduction
    1.3.2 Semi-Structured Interviews
    1.3.3 Literature Analysis
    1.3.4 Online Conference Participation
1.4 Document Outline

This chapter introduces the dissertation subject. It will describe our research objectives, the motivation for choosing this particular research subject and the methodological approach leveraged to perform our analysis to identify novel findings.

1.1 Statement of Objectives

This dissertation aims to analyse how CTI is practically implemented within Dutch organizations and identify areas of improvement. In this dissertation, we will try to achieve the following objectives.

- Create an accessible introduction to the traditional intelligence discipline, which requires no previous knowledge.
- Present the current state of the CTI field, its standard methodologies, processes and how this field compares and contrasts to the traditional intelligence field.
- Conduct interviews to assess the experiences of teams in the Netherlands that have implemented CTI in the last ten years.
- Analyse interview findings to identify shared successes and complications. Where possible elaborate on the recognised successes and complications.
- Identify the relevant tools, training material, and methodologies used by these CTI teams
- Provide an outlook on potential future research and developments for this field.

1.2 Motivation

As a technical cybersecurity practitioner for over ten years, I have first-hand experience on how organisations struggle to respond to threats manifesting in the information security domain. Within the last six years, the field of CTI, formerly known as ‘Incident Intelligence’, has developed into a dedicated discipline with its own landscape of processes, tools and training methodologies.

The CTI discipline informs organisations on what the relevant context of threats really means to them and how they can respond accordingly. In doing so, CTI enhances a variety of other cybersecurity disciplines such as incident response, forensics, hunting, red-teaming, and risk-related domains, amongst others. As a student of the Royal Holloway University of London, I wanted to use this dissertation opportunity to investigate how Dutch organisations are leveraging this new discipline and which shared successes and complications could be identified. I intend to help further develop this field by identifying and analysing the current CTI best practices amongst the respondents.

The CTI domain is a new discipline for which academic research has only developed for the last ten years. At this time, there is still frequent ambiguity within this developing field [6]. The purpose of this dissertation is to reflect on applied CTI practices that were able to deliver actionable results and to identify the specific methodologies, processes, tooling and techniques that produced these results. Additionally, for some problem areas identified by the interview participants, alternative solutions or directions for future research will be presented.

Though not its primary intent, due to the practical perspectives presented, this dissertation may also serve as a starting point for future organizations to define their own CTI program and set practical objectives based on identified best practices and experiences.

1.3 Methodology

1.3.1 Introduction

Academic research on CTI maturity is being performed [7], [8], but the majority of research subjects are high-level and process-driven. Limited qualitative research could be found that investigated practical implementation experiences. There is also minimal research focused on how tactical level threat intelligence is performed within the daily operations of CTI teams [9].

1.3.2 Semi-Structured Interviews

The semi-structured interview methodology was selected because it would allow for phenomenological research, which offered depth and flexibility within the individual interviews. Eight interviews were performed with team leads and senior analysts of different CTI teams in the Netherlands. This had the aim to identify the direction of their developing programs and lessons learned. A comprehensive description of the interview methodology and process is provided in chapter 4.1. Interview Methodology. The interview approach was verified to comply with the research ethics required by the Royal Holloway University of London and signed off accordingly [10].

Interview findings were analysed and compared, and the results fed into further research aimed at identifying potential improvements based on more traditional intelligence literature or recent insights into CTI [11], [12], [13], [14].

1.3.3 Literature Analysis

- At the start of this dissertation process, an initial broad literature analysis concentrated on identifying the most significant sources on traditional intelligence, CTI and maturity development-related literature. This aimed to describe current research in these fields and place our analysis within the proper context. This also influenced the choice for semi-structured interview methodology and helped define the interview scope, questionnaire and respondent selection process.

- A secondary literature analysis was performed after the analysis of the interviews had been completed. The goal of this second analysis was twofold.
    - On the one hand, the identified successes and complications were assessed on how they compared and contrasted with the traditional intelligence literature. This had the aim to determine if lessons learned in the traditional intelligence literature could be repurposed for the CTI field, as for the traditional intelligence discipline, large numbers of research papers on maturity development are already available.
    - The second objective was to identify the novel processes, methodologies and tools leveraged by the respondents. The respondents identified very recent initiatives that were significant contributors to the success of their CTI program. Many of these initiatives had only been developed within the last two years. Because of this, some of the information collection was performed on non-academic sources, as these initiatives are so new that they are rarely mentioned in academic literature.

1.3.4 Online Conference Participation

The interview analysis phase identified significant interests for the Dutch National Cert's NDN program and the Luxembourg Cert's MISP platform. These communities held online conferences within our dissertation research period that were open to public participation.

- The Dutch National Cert held a ten-year anniversary conference for its NDN platform. This was a three-day conference. Participation in this conference allowed for a better understanding of the purpose of the NDN project and allowed for questions to be raised directly to NDN project members and NDN participants [15].

- The MISP project held its 6th Annual Summit, and its online recording was made publicly available during the dissertation research period [16]. This resource helped identify upcoming developments for MISP and verify interview findings [17].

1.4 Document Outline

Chapter One: Objectives and Approach of this Dissertation
This chapter describes the overall dissertation objectives and methodologies leveraged.

Chapter Two: General Introduction of Intelligence Concepts
This starting chapter will introduce the traditional intelligence field. We will approach this field by introducing significant historical developments and methodologies. This will contain foundational concepts on which later reflections on (cyber) intelligence tradecraft will be based.

Chapter Three: Introduction to Cyber Threat Intelligence
This chapter will introduce the novel field of CTI, its commonly used processes, tools and methodologies and describe how this compares and contrasts with the traditional intelligence field from which most of its methods originated.

Chapter Four: Identified Successes and Challenges in CTI Implementations
After introducing the CTI domain, this chapter will present the results of our interviews. These interviews were held with respondents who developed CTI teams within the Netherlands and will identify their approach and the successes and challenges that these respondents encountered.

Chapter Five: Analysis of Interview Findings and Potential Improvements and Mitigations
The identified successes and challenges will serve as a starting point for further analysis of common successes lessons learned and, where possible, suggest mitigations to improve the adoption of CTI programs. This will involve insights from historic intelligence literature and novel developments from recent CTI research.

Chapter Six: Conclusion
This dissertation will end with a final chapter to reflect on the derived conclusions and overall contributions made to this field. This will also describe limitations in our research and potential subjects for future research.

Chapter 2

General Introduction of Intelligence Concepts

Contents:

2.1 The Traditional Origin of Intelligence
2.2 Definitions for Intelligence and Intelligence Analysis
2.3 The Intelligence Lenses of Collection, Processing and Analysis
2.4 Identifying Stakeholders and their Requirements: PIR and SIR
2.5 Levels of Intelligence, The Traditional Intelligence Perspective
2.6 The Cyclic Nature of Intelligence Production
    2.6.1 Iterative Nature of the Intelligence Production Process
    2.6.2 Acting on Military Intelligence: Courses of Action
2.7 Confidential Information Sharing in Traditional Intelligence

Before the domain of cyber threat intelligence is introduced in Chapter Three, an introduction to the traditional intelligence discipline will be provided. Cyber threat intelligence originated from the traditional intelligence discipline and still shares many underlying fundamental concepts. This chapter will introduce these concepts and provide the reader with the context necessary to interpret the specific findings relating to cyber threat intelligence maturity development.

This chapter will start with a brief historical introduction to traditional intelligence development, followed by an introduction to the traditional intelligence methodologies and models relevant to this dissertation.

2.1 The Traditional Origin of Intelligence

This chapter will start with a brief historical introduction to the military intelligence process and how this was interpreted at different times. This will lead into the fundamental Western military intelligence literature from which our current CTI statecraft is derived. This is not meant to be an exhaustive interpretation but is provided to illustrate significant events selected by the author that underline historical insights and the evolving understanding of the discipline of intelligence.

Sun Tzu, The Art of War: 5th century BC
Sun Tzu was the Chinese military leader who authored 'The Art of War[17]', considered the oldest military treatise globally. Sun Tzu emphasized the significance of accurate, timely information about the adversary. While not defined as intelligence at the time, Sun Tzu developed this field of espionage statecraft to the degree that was not seen before. On intelligence, Sun Tzu wrote:

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

In historic times, the distribution of friendly and hostile forces was often a decisive factor in achieving victory. Sun Tzu relied on a network of spies and informants to gather intelligence and spread false information to distract his adversaries. The Art of War did not specify processes or methodologies; however, Sun Tzu emphasised the importance of intelligence's actionability. By this, he meant that fundamentally, intelligence should feed into a decision that the recipient can act on. The influence of The Art of War in current military doctrine is evident by it being recommended and sometimes mandatory reading for most military academies. The Art of War has solidified the significance of Intelligence in modern Western military doctrines [18], [19]**.**

Carl von Clausewitz: Intelligence in the 19th century,
In the 19th century, the meaning of intelligence was more accurately defined by Carl von Clausewitz, a Prussian military commander and military theorist. Clausewitz defined three core principles of war in the book 'On War' [20]. Clausewitz's third principle was '*In short, most intelligence is false*'. The meaning of this statement was that within Clausewitz's literature, he identified a fundamental degree of uncertainty in all things related to war. He named this concept the 'fog of war', which he described as the following:

"*War is the realm of uncertainty; three-quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth".*

This quote identifies the underlying meaning meant by Clausewitz. The process of intelligence analysis requires a skilled, sensitive and discriminating approach because fundamentally, it will always deal with uncertainty.

Clausewitz's military theory significantly influenced the Prussian military doctrines, and his insights have made their way into military doctrine leading up to both World Wars [21]**.**

The specific meaning of intelligence has developed throughout the ages. In the last century post World War 2, the intelligence discipline received academic interest and became more formalized and theoretical. A prominent Western contributor to this development was Sherman Kent.

Sherman Kent on Intelligence: 1940 - 1980

Sherman Kent was a history professor at Yale University who served in the United States Central Intelligence Agency and its predecessor, the Office of Strategic Services[22]. Kent was deeply involved in the development of modern intelligence analysis and is sometimes named 'the father of intelligence analysis' by advocating analysis through a methodical qualitative scientific method. He has made significant academic contributions to the intelligence field, most notably his book *'Strategic Intelligence for American World Policy',* which became a de-facto standard for Western intelligence agencies [23] [11].

In one significant assessment during the Cuban missile crisis, Kent was proven wrong. The hypothesis that the Soviet Union would not place ballistic missiles in Cuba was met with a high confidence rating by the analysts that Kent was directing within the CIA. To their surprise, and against their analysis, the placement of ballistic missiles occurred, which led to the Cuban missile crisis [24].

From an operational perspective, this may be considered a failure for Kent; however, from a methodological perspective, this further affirms that the uncertainty variable will always be a significant factor for intelligence. Intelligence recipients should understand that every intelligence product is based on several hypotheses that deal with degrees of uncertainty and that alternative hypotheses should continually be assessed and considered. However, no intelligence deliverable can ever be considered entirely predictive of future events.

Richard Heuer on Structured Analytical Techniques: 1950 - 1990

Richard 'Dick' J. Heuer Jr. was a lecturer at the United States Central Intelligence agency, where he worked for over 45 years [25]. Heuer was a rigorous analyst and asserted that intelligence analysis should be structured to provide objective analysis and repeatability by different analysts. Heuer identified eight techniques for Structured Analytical Techniques, which could lead to high-quality intelligence analysis and minimize the influence of personal bias in making objective assessments. Heuer's work later helped popularize intelligence analysis in general, including adopting intelligence within business practices (business intelligence).

Compared to Kent's scientific method, which was more of a quantitative approach to intelligence. The methods developed by Heuer allowed for more analyst driven qualitative interpretations as well, albeit through a structured analytic methodology to maintain analytical integrity [14], [26].

This serves as the end of our historical introduction and provides several relevant insights. Sun Tzu identified the significance of the **actionability** of information (it leads to decisions) to make it a usable form of intelligence. Clausewitz presented the concept of a 'fog of war', which represents the **fundamental uncertainty** underlying all intelligence observations and analysis. Kent further developed the intelligence discipline by applying a **rigorous scientific approach** to analysing information and pursuing a quantitative scientific approach to intelligence analysis. Heuer built on Kent's principles and solidified the importance of **structured analytical techniques to prevent bias** in intelligence analysis and create objectivity and repeatability to the analysis process while also allowing for qualitative assessment to be made based on human insights.

2.2 Definitions for Intelligence and Intelligence Analysis.

Before advancing into specific intelligence processes, an introduction will be provided to the definitions adhered to in this dissertation. As the field of (military) intelligence has developed and changed over time, it has also struggled to adhere to well defined and broadly accepted definitions.

On Intelligence:

Intelligence has several definitions, which can lead to problems of interpretation. The CIA investigated this in a case study to reach a consensus on their internal interpretation [27]. For our purpose, we will adhere to the following definition as it is somewhat context neutral and will help us holistically approach this field when applying it to traditional as well as information security domains in subsequent chapters. This definition originates from SANS Course FOR578 on CTI, which has developed into one of the more foundational training courses on CTI [28]**.**

"Intelligence is the collecting and processing of information about a competitive entity and its agents, needed by an organization or group for its security and well-being."

The following definition will be used when we refer to intelligence analysis.

On Intelligence Analysis:

Intelligence analysis is the methodical process by which an analyst tailors information into intelligence. CIA Analyst and professor Rob Johnston performed an extensive investigation among intelligence staff in the United States to aggregate common knowledge. He identified the following widely shared statement, which matches our requirements going forward [29].

"Intelligence Analysis is the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret social-cultural context."

Reporting on Intelligence:

There can be confusion on the difference between a conventional report and a piece of intelligence. For our exploration of this field, the explicit description and analysis of alternative hypotheses, including the underlying degrees of uncertainty, will differentiate intelligence products from traditional reporting.

"A report presents data and answers; an intelligence product presents hypotheses."

Intelligence products should contain estimative analytical language, alternative hypotheses, and gaps in the identified hypothesis where possible. This allows the reader to make its own assessment of the intelligence presented and minimizes interpretation bias.

Having defined Intelligence, Intelligence analysis, and the Intelligence deliverable, we can start to address additional specifics on Intelligence tradecraft.

2.3 The Intelligence Lenses of Collection, Processing and Analysis

A standard conceptual model of intelligence production represents the application of filtering lenses that narrow the flow of external information into distilled intelligence.

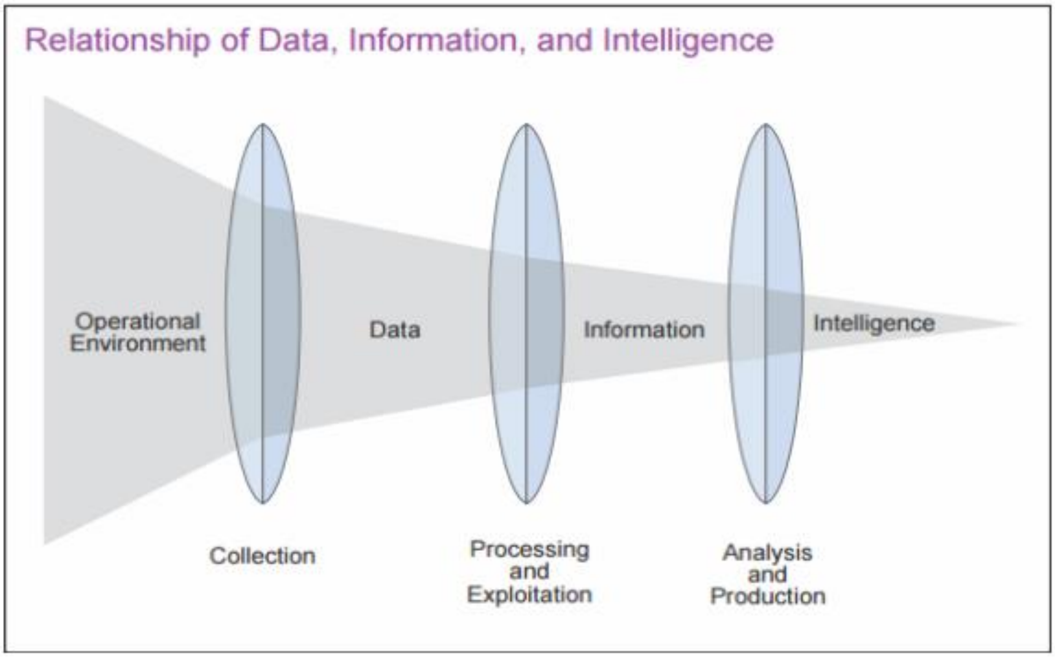


Figure 2 Intelligence Lenses Model Joint National Intelligence Support, DOD Appendix D [30]

The concept presents three distinct phases and activities.

- **The initial stage of Collection.** This first stage means a broad selection to filter away irrelevant data on a high level. In larger intelligence organisations, a dedicated team performs the collection process. This process can also involve the (large scale) ingestion of data through a structured collection plan, after which automated filtering is performed.
- **The secondary stage is Processing and Exploitation**. At this stage, data collection is scrutinized to identify what is applicable and relevant to our specific intelligence purpose. This can be done by filtering for timeliness, technology vector, geopolitical origin, or other relevant variables.
- **The final stage is the actual analysis and production process.** This process is performed on the subset of information gathered during processing and exploitation. At the end of this linear process, the end product of (finished) intelligence remains and can be provided to the intelligence stakeholder that requires this deliverable [31], [32].

2.4 Identifying Stakeholders and their Requirements: PIR and SIR

Intelligence is not created for its own sake. Before the process can start, a stakeholder must be designated, and their intelligence requirements must be specified. A stakeholder can be an individual such as the CISO or another organization, such as a Security Operations Center performing daily monitoring and response activities. Regardless of the specific audience, the next step will be for the intelligence team to identify and define the requirements of the desired intelligence product. These requirements are defined as PIR's and SIR's [33].

Priority Intelligence Requirements (hereafter referred to as PIR)
PIR's are the specific and primary intelligence requirements for our stakeholders. If our stakeholder is our organization in general, an example of a PIR can be: 'Which geopolitical developments can potentially affect our market situation in Central Asia in the upcoming five years.

In this high-level PIR, we have already specified a temporal scope of five years, a geographical region of coverage and an area of interest being geopolitical developments. This PIR can serve as an initial starting point from which we can derive our Secondary Intelligence Requirements, which will be more specific.

Specific Intelligence Requirements (hereafter referred to as SIR)
SIR's are the derived specific information requirements. In the above scenario, some potential SIR's can be:

- Which areas of industry in Central Asia are most significant to our organization?
- Which diplomatic, legal or industrial developments are we expecting in Central Asia in the upcoming five years?
- Which regulatory frameworks are expected to change, potentially affecting our organization's market in Central Asia in the upcoming five years?

Once the PIR's and SIR's for our stakeholders are defined, we can start designating our collection plan where we identify which sources we will leverage and in what way, to gather the high-level information for further processing [30], [34], [35].

It is not uncommon for PIR's and SIR's to have a recurring scope whereby a periodic update to the intelligence assessment is required, for example, a quarterly update. It is also possible that a stakeholder wishes to be alerted on significant changes to the stated PIR or SIR. To deliver this up to date intelligence may require continuous monitoring of the area of interest.

2.5 Levels of Intelligence, the Traditional Intelligence Perspective

The military command structure from which most traditional intelligence doctrine originates is rigidly structured to assign different levels of responsibility. Within policy and intelligence, this is frequently distinguished in three primary levels, Strategic, Operational and Tactical. The three distinguishing levels can be visualized using a pyramid.

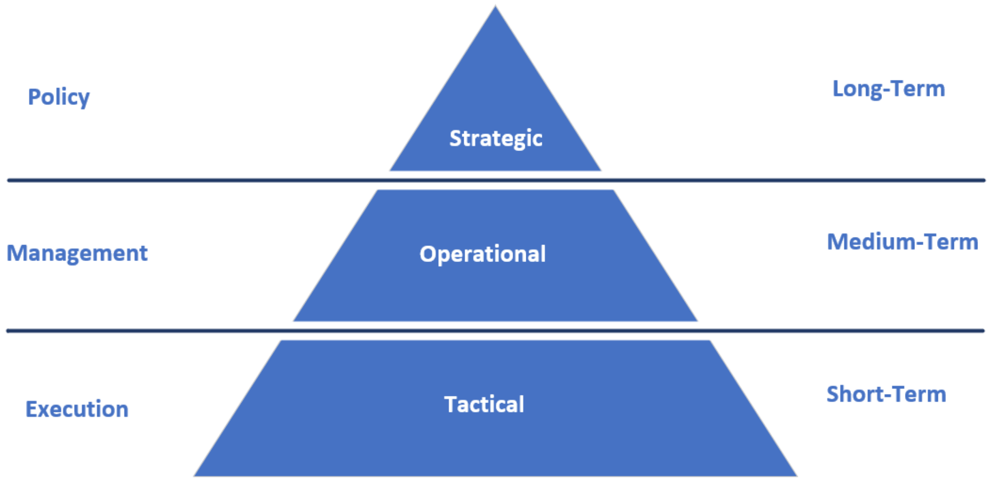


Figure 3 Traditional Levels of Intelligence and their purpose and timeliness

Strategic intelligence is intelligence required to formulate strategy, policy, and military plans and operations at national and theatre levels. Stakeholders at this level are the senior military and civilian leaders and the highest echelons of politics and military command. The types of intelligence deliverables are long term estimates and prognoses that can help support a new policy. Because of this, many intelligence products are scoped to encompass multi-year developments. An example could be an intelligence analysis on the Chinese Belt and Road initiative, which is a five-year strategic plan on which the Peoples Republic of China will focus their efforts. Accurate assessments on this subject can provide a long term intelligence benefit to our organization as it may influence our industry for several upcoming years [34]**.**

Operational intelligence is intelligence required for planning and conducting campaigns and major operations to accomplish strategic objectives within theatres or areas of operations. The stakeholders are often the military commanders on-site responsible for planning their specific campaigns. The deliverables are of a shorter time estimate and more specifically detailed as they must help military command coordinate plans on a more granular level. Examples can be observations of logistical preparations by an adversary that may indicate a build-up of troops. Though this observation by itself is not a direct tactical threat, it can be an indication of future operations. The timespan of Operational Intelligence often falls between months, up to a year [34].

Tactical intelligence is intelligence that is required for planning and conducting tactical operations. It is very detailed and focuses on short term developments that can affect our immediate ongoing operations. This type of intelligence can be directly applied to the tactical planning process and help our stakeholders to conduct battles or special missions. Examples can be the advance of opposing forces, their logistical situation, and the intermediate terrain they will cover.

2.6 Cyclic Nature of Intelligence Production

The intelligence lenses are a conceptual model representing the filtering nature of the intelligence collection and analysis process. The overall intelligence production process is more extensive and is sometimes represented as a cyclic process, similar to the intelligence lenses but with additional phases for planning and dissemination and surrounded by a continuous feedback loop.

- This process starts with **Planning and Direction**. This identifies stakeholders, PIR's and SIR's
- A high-level collection plan is compiled, and the **Collection** process is executed.
- On this broad collection of data, **Processing and Exploitation** is performed to define specific information relevant to answer our stakeholder's PIR's and SIR's.
- **Analysis and Production** is performed on the filtered subset of information to create intelligence products,
- In the final phase of **Dissemination and Integration,** our products are presented to our stakeholders and integrated into their decision-making process.

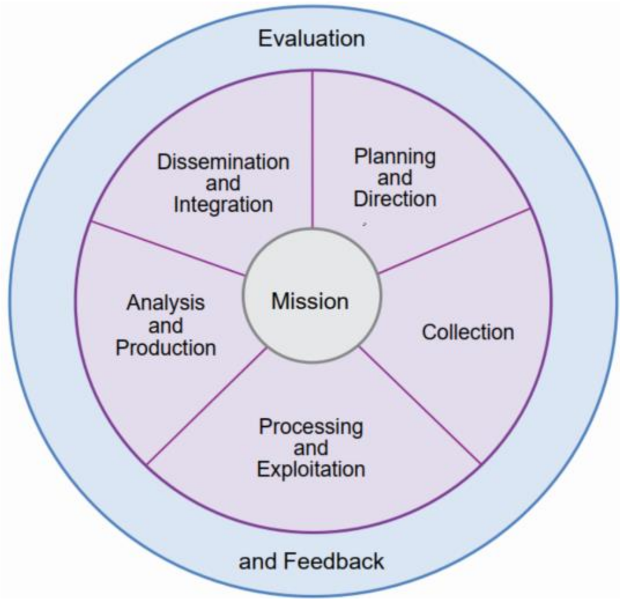


Figure 4 The Intelligence Process – DOD JP2-01 Publication[30]

2.6.1 Iterative Nature of the Intelligence Production Process

In this model representation, each phase is surrounded by an **Evaluation and Feedback** phase. This implies a continuous reflection on the relevance of the deliverable before it progresses further in the cycle. In the end, the stakeholder's feedback decides whether the intelligence was suitable. Though the intelligence production cycle is generally iterative, it may also have to return to an earlier stage if the information is deemed not fit for purpose or if external circumstances have changed.

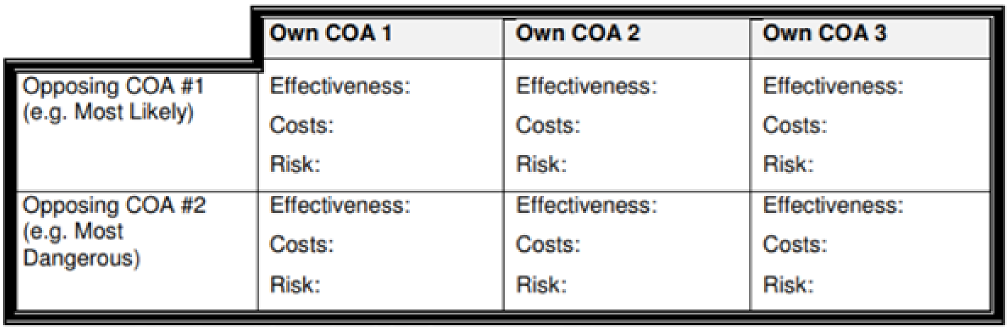
The final phase of dissemination and integration is essential because it provides feedback on the efficacy of our information. This feedback will provide context for the planning and direction phase of the next intelligence cycle and may lead to a rescoping of PIR or SIR [33].

2.6.2 Acting on Military Intelligence: Courses of Action

A phase that often follows the intelligence reporting phase is the development of Courses of Action (hereafter referred to as COA's). This means that the commander leverages the intelligence sources to plan potential future operations.

COA's will be defined both on the current actions available to the commander and based on potential situations that may materialize in the future. COA's are also compiled for likely adversary activity so that follow-up defensive COA's can also be proactively assessed and planned [30], [34].

COA's are often represented in a COA matrix, for which an example is provided below.



	Own COA 1	Own COA 2	Own COA 3
Opposing COA #1 (e.g. Most Likely)	Effectiveness: Costs: Risk:	Effectiveness: Costs: Risk:	Effectiveness: Costs: Risk:
Opposing COA #2 (e.g. Most Dangerous)	Effectiveness: Costs: Risk:	Effectiveness: Costs: Risk:	Effectiveness: Costs: Risk:

Table 1 COA Matrix according to the NATO Comprehensive Operations Planning Directive[36]

The NATO Comprehensive Operations Planning Directive identified the role of the COA as the following, with CPG meaning the 'Commanders Planning Guidance' (or overall mission goals) and the JOPG being the Joint Operations Planning Group, which for our purposes represents a part of the intelligence team [36].

The purpose of the final portion of the Operational Estimate is to determine how best to carry out operations that will accomplish the mission effectively and efficiently. Guided by the Commander, the JOPG will develop a set of COAs, all of which will accomplish the mission effectively according to the Commander's intent, including that expressed through his operational design and CPG [36].

COA's serve as an actionable derivative of the intelligence process. The concept of the COA will be revisited in chapter 3.5 CTI Courses of Action COA's to present its significance to the domain of CTI.

2.7 Confidential Information Sharing in Traditional Intelligence

Western government standards on intelligence sharing are generally based on security clearance and the levels of confidentiality assigned to individual pieces of information. The clearances are personally assigned after formal vetting processes have been followed, the level of access is assigned on a need-to-know basis. Designated data custodians are tasked with marking the information with the appropriate security levels. Compromises of the information sharing regulation can incur criminal penalties, deemed a deterrent to information leakage [37].

Commonly the levels of: "*Top Secret, Secret, Confidential and Unclassified*" are used as the basis, and derived sub-categorizations can be added to this. An example of a sub-category can be for information that falls under additional categorization, such as atomic research, which can also be subject to international export restrictions.

Within the United Kingdom, This type of information will likely have a double security classification such as 'Top-Secret – Atomic' [38]. In contrast, the United States will use the overall Restricted Data label to identify a sensitive sub-type of information [39]. Already this identifies that national government interpretations can have different ways of handling and classifying these categories and that these labels frequently do not align between nations.

Situations can be significantly more complex when partners within the information-sharing initiative are not part of the same international collaborations or have different information categorization schemes. As an alternative, new classifications can be agreed on, such as NATO-Secret, EU-Confidential, or even ISAF-Secret if related to a specific mission.

For example, Norway is part of NATO and may be privy to NATO Secret information. Norway Is, however, not a member state of the European Union[40]. This means that intelligence shared within a confidential EU military collaboration will not by default be available to Norway and will likely have to be reclassified for them. However, this will likely involve multiple data custodians (one for each intelligence partner), significantly complicating this process.

Because of the above complexities, traditional information sharing standards have seen limited development. Any organization wishing to improve on this will have to re-assess a massive amount of historically classified data and would be invested in a long-term operation where a legacy classification scheme and its historic intelligence will still be around. In chapter 3.6 Confidential Information Sharing in CTI, an alternative approach will be presented that describes how this problem is addressed within the CTI field.

Chapter 3

Introduction to Cyber Threat Intelligence

Contents:

3.1 The Origins of Cyber Threat Intelligence
3.2 Levels of Intelligence, the CTI Perspective
3.3 Overlap in Traditional Intelligence Tradecraft and CTI
3.4 The Lockheed Martin Cyber Kill Chain
3.5 The Pyramid of Pain
3.6 CTI Courses of Action
3.7 Confidential Information Sharing in CTI
3.7.1 Information Sharing in Informal Trust Groups
3.7.2 Information Sharing in Formal Trust Groups
3.7.3 Confidential Information Sharing in CTI: Traffic Light Protocol
3.8 Automating CTI: Threat Intelligence Platforms, Feeds and Services
3.8.1 Threat Intelligence Platforms
3.8.2 Threat Intelligence Data Feeds
3.8.3 Threat Intelligence Services
3.9 Distinguishing Levels of CTI Maturity

Chapter Two introduced the traditional field of (military)Intelligence and how intelligence teams create intelligence products to help their stakeholders make decisions. This chapter will introduce the specifics of the Cyber Threat Intelligence discipline and how this discipline came into being. It will describe the specific purpose of CTI, its leading methodologies and specific techniques that often came together either as a derivative from traditional intelligence techniques or as a combination of novel community best practices.

The combination of Chapter Two on traditional Intelligence and Chapter Three on Cyber Threat intelligence serves as an up-to-date introduction to the field of CTI and its origins, without requiring knowledge of either domain. This serves as the first novel contribution of this dissertation.

3.1 The Origins of Cyber Threat Intelligence

It is hard to identify when CTI was first introduced conclusively, as the act of gathering intelligence from computer and networking sources, in general, has been around for many decades. Additionally, the phrase cyber has become a common buzzword that is frequently used to draw attention to subjects to which it does not apply.

One notable event that ratified the phrase was when in 2011, the United States Congress proposed the 'Cyber Intelligence Sharing and Protection Act' bill [41]. The objective of this bill was to help the United States government investigate digital attacks and allow for the sharing of cyber information between the United States government and private companies in the technology sector. Though the bill in its first iteration did not pass congress approval, it did serve as a notable event when Western governments started to introduce legislation that would allow the sharing of threat intelligence between government and the private sector.

Unfortunately, the definition of CTI tends to be misinterpreted at times [31]. CTI grew from a need to more effectively collaborate in cybersecurity incident response activities. Because of this, many initial developments were not formalized and were mostly community-driven as they grew out of direct operational necessity. The most commonly adopted practices were later embraced by more formal communities such as FIRST (the Forum for Incident Response & Security Teams) [42], ENISA [43], and similar initiatives after which they became de-facto standards for (National) CERTS and (government) organisations [44]. The rapid commercialization of the CTI domain has led to a push from vendors to present novel interpretations of CTI to distinguish their products, but this has sometimes introduced further confusion and conflicting interpretations.

For the intents and purposes of this dissertation, the following definition of CTI will be used, as it is broad and supports a holistic approach to this subject.

Cyber threat intelligence is what cyber threat information becomes once it has been collected, evaluated in the context of its source and reliability, and analysed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information. '

Like all intelligence, cyber threat intelligence provides a value-add to cyber threat information, which reduces uncertainty for the consumer while aiding the consumer in identifying threats and opportunities. It requires that analysts identify similarities and differences in vast quantities of information and detect deceptions to produce accurate, timely, and relevant intelligence [45].

3.2 Levels of Intelligence, the CTI Intelligence Perspective

The Cyber Threat Intelligence literature has also embraced the three main tiers in levels of intelligence. Often each level serves to answer the questions of a different stakeholder [28], [44].

Strategic Intelligence can be considered the product of long term trends and observations that can forecast future policy requirements; these products generally have relevance more than six months ahead and are aimed at stakeholders such as the CISO and Board members.

Operational Intelligence is actor profiling and attribution and (multiple) campaign tracking with the intent to identify or predict similar behaviour. This intelligence is based on tactical level observations identified as recurring between activities.

Tactical Intelligence directly deals with forensic observables such as file hashes, IP addresses, DNS and other infrastructure artefacts (identified as 'indicators of compromise'). These intelligence products are primarily aimed at the SOC, CERT, and CTI teams as they can aid in detection and forensic investigation but frequently have a short-term relevance of less than a month. Once identified as malicious, observables tend to be modified by the adversary.

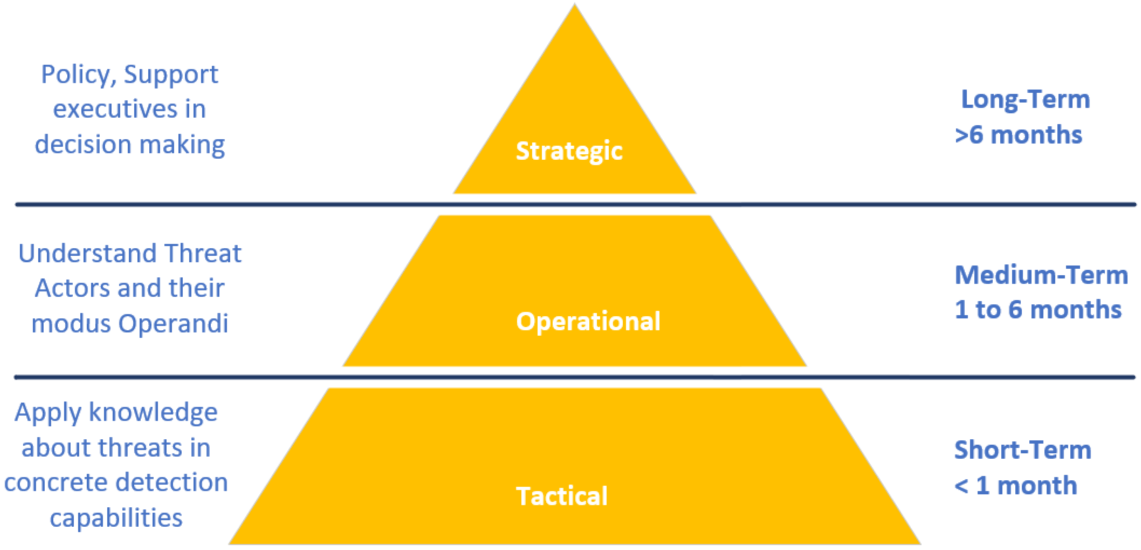

Policy, Support executives in decision making
Strategic
Long-Term >6 months
Understand Threat Actors and their modus Operandi
Operational
Medium-Term 1 to 6 months
Apply knowledge about threats in concrete detection capabilities
Tactical
Short-Term < 1 month

Figure 5 CTI Levels of Intelligence and their Purpose

A common heuristic to apply these different levels of Cyber Threat Intelligence is the following:

When dealing with adversary activities,

***Strategic** Level Applies to*	***The Who and Why***	*(describing the actor and motivation)*
***Operational** level applies to*	***The How and Where***	*(describing the campaign and methods)*
***Tactical/Technical** applies to*	***The What***	*(describing technical evidence)*

3.3 Overlap in Traditional Intelligence Tradecraft and CTI

The application of intelligence analysis within a specific domain frequently follows a fundamental intelligence process that is agnostic to the domain to which it is applied. The before mentioned traditional intelligence methodologies have been successfully applied to many specialistic fields of application. We will describe a few examples.

- Human Intelligence (HUMINT) is intelligence from human interaction.
- Communications Intelligence (COMINT), intelligence from communication sources.
- Geospatial Intelligence (GEOINT) is derived from imagery and geospatial information analysis.
- Technical Intelligence (TECHINT), intelligence of a specific technical nature such as weapon and equipment capabilities.

These areas leverage the same high-level intelligence methodologies such as the Intelligence Cycle, the Intelligence Lenses, definitions for PIR and SIR and many more fundamental intelligence processes. Each sub-field also augments this discipline with its own specific tradecraft specific techniques. For example, with HUMINT, psychological methods are often involved in shaping and enhancing the HUMINT tradecraft techniques.

Intelligence Fusion

Another benefit of a shared underlying methodology is that different areas of intelligence can be combined to enhance an overall assessment. It is not uncommon for an extensive intelligence product to have originated from different intelligence disciplines. These different perspectives can serve to strengthen or challenge the proposed hypotheses. Combining multiple intelligence disciplines is called Intelligence Fusion, and this phrase is also used to identify multi-disciplinary intelligence teams as ‘Fusion Teams’. Fusion Teams will be further described in chapter 5.1.1 Fusion teams.

CTI is one of the newest domains that is now being integrated within this overall intelligence framework. Because of this, most literature that is of a high-level methodologic nature will also apply to CTI. CTI is sometimes described as being in its infancy, and repurposing proven intelligence methodologies fills the knowledge gaps until more extensive CTI specific processes can be developed [6].

Some fields can offer significant synergy; for example, if the purpose of an investigation is to identify a specific threat actor and describe their perceived motivation. The critical analysis can be supported by high-level models originating from either the HUMINT or law enforcement domain. An example can be the: “*Means, Motives and Opportunities*” approach to describe an actor's perceived intent and motivation.

CTI should, as such, not be considered as a completely novel field but can be addressed as another domain to which high-level intelligence processes will also apply. Apart from re-applying traditional tradecraft, the CTI domain has started developing its specific methodologies, for which several examples will be presented.

3.4 The Cyber Kill Chain

A ‘kill chain’ is a military phrase for target identification and destruction processes. Lockheed Martin repurposed this terminology in 2011 to apply to computer intrusions. This model is commonly known as the Cyber Kill Chain [46], [47]. We will introduce this model and refer to this methodology later in the document as it has several uses for Cyber Threat Intelligence.

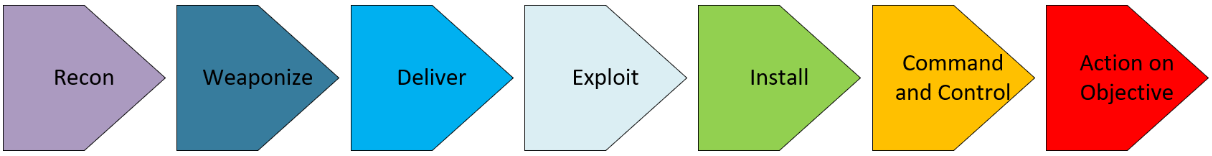


Figure 6 Lockheed Martin Cyber Kill Chain [46]

The seven identified phases consist of the following:

Reconnaissance
The intruder researches and identifies their target; this can be passively or by actively interacting with the target.

Weaponization
The actor develops or tailors a malicious payload malware for the victim environment; this may also involve setting up command and control servers or crafting a lure to deceive the victim.

Delivery
Delivery is the actual transmission of the payload to the victim. This is the first phase that the defender can potentially identify.

Exploitation
The payload is activated; the target device is exploited.

Installation
The initial payload performs a backdoor functionality allowing persistent access to the actor. Additional capabilities can be deployed here.

Command and Control
In this phase, the actor’s command and control channel will communicate with the malware to provide remote access to perform activities on the host or perform the lateral movement to another target.

Actions on Objective
The actor now has a foothold in the environment and can perform their objective. The action often leads to (information)theft, destruction or intrusion of another target.

The kill chain can be considered an iterative model. This means that the kill chain progresses through the phases iteratively and that defenders can thwart any of the phases, leading to the rest of the compromise not progressing further.

3.5 The Pyramid of Pain

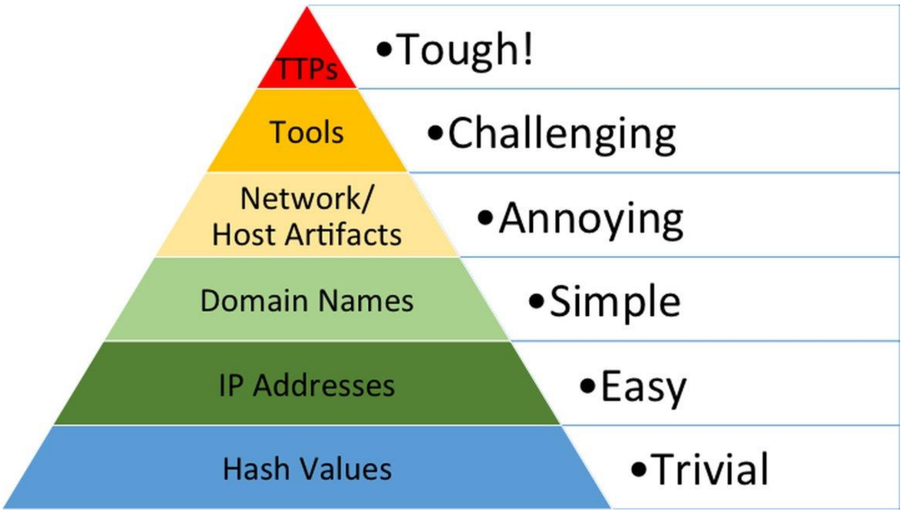


Figure 7 David J. Bianco - Pyramid of Pain[48]

The Pyramid of pain is a conceptual model developed by David J. Bianco to describe the severity of impact that our CTI evidence can have on an adversary's operations. This is a technical model specific to the field of CTI, which will be described from the bottom up [28] [48].

Level 6 Hash Values:
Hashes are in frequent use within digital forensics. Hashes represent specific files, and within CTI, they are most frequently used to identify malicious files. This allows defenders to share this hash value as a signature for the file to quickly identify the presence of this file without having to share the entire volume of data. Though useful for us as forensic evidence, our knowledge of a specific hash is of minimal cost to the actor as they can quickly generate new hashes. It is trivially easy to change hashes from the actor's perspective by flipping insignificant bits or adding random data to their files.

Level 5: IP Addresses:
IP addresses can be used to identify network communication. It can indicate an adversary's staging server or command and control channel. Network data can significantly aid defenders because they can use perimeter network devices to filter this IP from reaching our systems. From the attacker's perspective, the presence of thousands of malicious IP addresses in typical resale makes them easy to replace, and an actor frequently has different IP's available to him. Not all IP addresses are similar. IP addresses from foreign locations with poor online reputations (due to past malicious activities) will hold a low value to the attacker. On the other side of the spectrum, dedicated bulletproof hosting that is not reshared between actors can have high value to our attacker [49].

Level 4 Domain Names:
Actors can easily register DNS records, and registrars are abundant. The potential for automation has led many actors to leverage pseudo-random domain generating algorithms. Some top-level domain registrars even allow automated API-driven registrations, leading to the fully automated generation of attack infrastructure [48].

The actor has an advantage when using DNS instead of IP's for addressing command and control channels. Suppose the malware in question directs to a DNS entry instead of an IP address. Should the IP address become unavailable, the actor can redirect the DNS entry to a new IP without losing connectivity to their malware. For defenders, domain names hold a similar value to IP addresses; they can aid in identifying malicious activity. However, they are considered a re-usable item from the actor's perspective.

Level 3 Network / Host Artifacts:
Network and host artefacts are specific artefacts created by adversary activities on our networks or hosts.

An example of a network artefact could be a specific pattern of traffic that is unique to the adversary's command and control protocol. We may identify and block future activities by identifying the behaviour and setting up a network detection rule. It may also help us identify historic compromises in our network logging.

An example of a host-based artefact could be a specific bit-pattern integral to malware used by our malicious actor. Defenders can write detection rules such as YARA (YARA is an acronym meaning Yet Another Random Acronym), a regular expression alternative frequently used for malware research[50]. By filtering a large set of files with this YARA rule, defenders can potentially identify malicious files, regardless of other data present within the file. Because of this, similar detection rules are of significant use to defenders, making them far more helpful than file hashes. For our adversary, these detection rules are far more problematic. If the actor wants to continue their operations without being detected, they will have to rewrite the malware and the networking protocol configuration to aid evasion. This time-intensive process requires more testing to confirm whether their new protocol or file structure is still effective and can significantly burden our adversary.

If CTI teams can create intelligence at this pyramid level, it can severely undermine an adversary's operations. Because it is uncommon for malicious actors to change their configurations frequently, reliable evidence can potentially apply to several intrusion attempts.

Level 2: Tools
Tools are a collection category of the different tools that the actor leverages at different phases of his intrusion. These can be both malicious files and benign files used to facilitate access. Overall, this is the modus-operandi that our actor is familiar with to perform his compromise

Suppose our intelligence initiative can identify the tools being used by our actor. In that case, this may aid us in setting up detection rules that identify specific behaviour with non-malicious files, even before actual malicious files are being used. From a Kill Chain perspective, this can mean that some reconnaissance or lateral movement activity may already be identified and potentially stopped before the deployment of the malicious files takes place.

For the threat actor, it is problematic if the victim is aware of the actor's tools. Changing over to new tools (both malicious and benign) will require that our actor re-assesses his entire attack methodology and require a significant retraining period.

Level 1: TTP, Tactics Techniques and Procedures
The highest level of the pyramid of pain is the TTP, which is our malicious actor's overall business case. It contains their toolkit and the overall techniques they perform to compromise victims. Within TTP, defenders can also deduce perceived objectives and targets that the actor prefers. It may also identify language used or any other interesting context that can describe an actor's behaviour. TTP's may also contain the actor's day and time preference for operations, potentially indicating geographic location.

If defenders effectively establish high confidence TTP for our actors. This may aid victims in early detection of activities and can also help support attribution, which can help law enforcement prosecute an actor by tying together several compromises.

From a threat actors' perspective, exposure on this level is highly detrimental to their effectiveness. Suppose an actor wants to mitigate against this exposure. In that case, they will have to start their malicious operations from a blank slate and develop new tactics, techniques and procedures to be no longer identifiable or attributable. From a CTI perspective, this is the highest level of significant evidence [28] [47]**.**

3.6 CTI Courses of Action

Similar to the traditional intelligence courses of action described in chapter 2.6.3. Acting on Military Intelligence: Courses of Action, analysts can also identify courses of action available to the attackers and defenders in the cyber domain. When used defensively, this can map potential mitigation capabilities and the respective processes or tooling that delivers this capability. The COA Matrix below is an example, though it is not exhaustive.

Well-developed COA's are highly valuable to CTI. They can suggest potential follow-up activities and identify potential gaps in security capabilities. Similarly, they serve as a starting point to define well established Standard Operating Procedures (SOP) for incident response teams [51].

Defensive Courses of Action (Actions available to the defender to thwart attackers)

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web Analytics	Firewall ACL		Tarpits	Sinkhole	
Weaponization	NIDS	NIPS				
Delivery	Vigilant User	Proxy/Mail Filter	Host AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	Reduced privileges	AV	Tarpits		
C2	HIDS	Firewall ACL	NIPS	Sinkhole	DNS Redirect	Hack Back
Actions on Objectives	Audit Log			Quality of Service	Honeypot	Hack Back

Table 2 CTI Defensive Courses Of Action

Models like the COA matrix can be derived from the intelligence products delivered by the CTI team and may serve to recommend follow-up activities when malicious activities are identified [28].

3.7 Confidential Information Sharing in CTI

Information sharing within the CTI domain was mainly developed through the community-driven necessity for sharing incident response information. Trusted peer organizations would inform each other on ongoing compromises or observed activity and collaboratively work on solutions. Because of the informal nature of these agreements, there are many different interpretations on intelligence sharing within CTI. This chapter will present some of the methods that are seeing wider adoption.

3.7.1 Information Sharing in Informal Trust Groups

An example of an informal sharing model is peer-invitation trust groups. Examples can be malware researchers who collaborate to analyse newly identified samples in a confidential environment. An example of this is the Malpedia trust group [52].

These groups often have a vouching system whereby a public application is either not possible or not automated, and explicit vouches by members who know and trust an individual are to gain access.

Informal sharing circles align with interest groups, and some larger scale trust groups may even have different subgroups to specialize in areas of interest. The membership of the trust group is on an individual basis and is based on personal merit; it is not tied to any corporate position, and membership remains valid when the individual leaves to work for another organization.

3.7.2 Information Sharing in Formal Trust Groups

Government initiatives
Government and semi-government frequently create their own trust groups. Within the Netherlands, the Dutch NCSC, the 'National Cyber Security Centre Netherlands, is the official government agency (National CERT) that represents the national cybersecurity interests and provides central coordination. The Dutch NCSC also organizes conferences and provides public threat reports and landscapes to the Dutch public. They also help to bring peer groups together.

The Dutch NCSC has peer groups for industry sub-sectors; each is served with tailored intelligence applicable and actionable to their industry. They have a specific emphasis on critical infrastructure [53].

Multinational Initiatives
The MISP project or Malware Information Sharing Platform is an excellent example of a government-driven initiative to promote information sharing. MISP is a web-based sharing platform that is open to everyone and falls under the GNU free software standard [54]. The MISP system already incorporates free public threat feeds that disseminate CTI data by default.

Additional MISP threat feeds can be acquired commercially or through invitations into other sharing circles. Some examples of sharing circles can be, for instance, industry initiatives or initiatives from the local National CERT. This will be further investigated in chapter 5.3.1 MISP.

Commercial (Global) initiatives

Industry ISAC (Information Sharing and Analysis Center)

The United States ISAC is a commercial organization that serves as a trusted intermediate between industry peers. The central ISAC organization hosts several sharing platforms distributed to specific sub-ISAC groups. These exist for the majority of industries, such as the Financial Services ISAC (FS-ISAC), the Energy Sector ISAC (E-ISAC), Aviation (A-ISAC) and many more.

Membership requires a recurring fee and a thorough vetting process. Acceptance will see the member be introduced to international peer organizations and allow them to participate in dedicated ISAC conferences to meet their peers, form trusted bonds and collaborate in information sharing.

FIRST

The Forum for Incident Response and Security Teams is a formal trust group. This is a global non-profit initiative to develop the community's ability to perform incident response. Membership requires that an organization be vetted as a credible and reliable incident response team. Though the FIRST organization is a non-profit, fees are paid to maintain standing, and members can also receive specialized information security training [42].

3.7.3 Confidential Information Sharing in CTI: Traffic Light Protocol

As described in chapter 2.7 Confidential Information Sharing in Traditional Intelligence, formalized nationally regulated sharing standards can be confusing and error-prone because the regulation does not apply supranationally.

CTI is performed in a collaborative domain. Organizations frequently observe malicious activity that can also affect their peers and competitors. To ease the process of sharing intelligence in informal circles, the Traffic Light Protocol (TLP) was introduced by the cybersecurity non-profit organization FIRST [55].

Though TLP is informal, it can be considered the de-facto standard for CTI information sharing. It has seen adoption by both formal and informal threat intelligence organisations. The TLP standard is officially endorsed by the United States Cybersecurity and Information Agency (CISA) and the European ENISA. FIRST is the official custodian of the standard[56], [57].

This adoption has also led to the TLP standard being a default compartmentation feature in threat intelligence tools, platforms and feeds, further promoting its usage.

TLP follows a few simple rules:

- Only the original author of the information can define what TLP level is assigned to his product.
- Only the author may eventually change the TLP level to a lower threshold if the information is deemed less confidential in time.
- Though an informal standard, the breach of TLP confidentiality will exclude the individual from the trust group and negatively affect a person's standing within trust communities. Severe or recurring offences may even get the individual or the organization banned.

Several levels (or colours) are distinguished in the Traffic Light Protocol.

TLP: RED

The most sensitive information is identified as TLP: Red, and it is designated the formalized text header "**TLP: Red**" this header can be affixed to the information. The header is most frequently applied to the top of each page or message. The level of TLP: Red implies that the information is only meant for the initial circle of distribution. People may not reshare this information outside of the initial distribution group. Frequently this information is transmitted verbally as e-mail systems may not be confidential due to external administrative access. Examples of TLP: Red information can be organizations sharing explicit evidence on breaches within their organization. They warn their peers and provide evidence artefacts to perform a local investigation or mitigate compromise.

Sensitive breach information risks potential reputational damage to the affected organization, so this information distribution is frequently limited to only the individuals explicitly stated by the author. This information may not be reshared or distributed internally. Only the TLP: Red appointed audience may act on it directly, and the information is not to be mentioned externally.

TLP: Amber

TLP Amber has the format header " **TLP: Amber** " and is the second tier of confidentiality. This level can be broadly interpreted as a 'need to know' basis. It is not uncommon for intelligence notifications to have a TLP: Amber chapter of investigative indicators and a TLP: Red segment explaining the sensitive context. An example would be to share information that is important to perform investigative activities but lacks the context on potential victim attribution. A CTI analyst who is part of a TLP: Red information distribution circle may ask the original author of the intelligence whether the indicators without context can be shared internally under Amber so that their local SOC can perform their investigation. This way, the Red context can stay with the CTI team, but the wider SOC team can act on the Amber derived observables.

TLP: Green

TLP: Green " **TLP: Green** " is information that is not confidential but should only be distributed by reliable sources. An example could be that an organization publishes their quarterly figures. However, only the publication on the official organization website is authoritative as third party distribution may be manipulated and is unwanted.

TLP: White

Unclassified and unrestricted information can be provided under TLP White with the format header" **TLP: White** " this implies that the information may be distributed freely, but its content should not be manipulated. Examples of TLP: White information consists of investigations that no longer hold a confidential nature or whose primary intelligence value has already diminished but may still serve to inform a greater community.

Chatham House Rule and TLP

TLP rated information is sometimes supplemented with the acronym CHR, which implies Chatham House Rules. This implies that the intended recipients are free to leverage the information but may not identify the sender's identity or affiliation or any of the other participants [58].

3.8 Automating CTI – Threat Intelligence Platforms, Feeds and Services

3.8.1 Threat Intelligence Platforms

A TIP (Threat Intelligence Platform) is a software platform that allows CTI analysts to ingest threat intelligence data and work on it directly. Most TIP's support the ability to ingest automated feeds, enrich the data, and then correlate the findings on another dataset, often the endpoint telemetry of the network. As such, the TIP can identify known bad indicators and verify whether these were observed in the defender's network environment. This information can support potential incident response activities [59], [60].

The interview respondents provided extensive replies on technical threat intelligence, specifically on their usage of TIP's (Threat Intelligence Platforms) and threat feeds. All eight interview respondents leveraged MISP, an open-source TIP described in chapter 5.3.1. MISP. Two respondents also leveraged OpenCTI. This is an alternative open-source TIP with some capability overlap with MISP. OpenCTI will be described in chapter 5.3.3. OpenCTI.

3.8.2 Threat Intelligence Data Feeds

Threat intelligence can be disseminated in several ways. This can take the shape of extensive reports with supporting intelligence assessments, or merely data feeds that only share the relevant indicators relating to a piece of malicious evidence. To automate large scale dissemination and ingestion of these feeds, two specific CTI data standards exist, STIX and TAXII. These standards were developed by the MITRE corporation [61] in collaboration with the United States Department of Homeland Security[62] and have become the de-facto standard for the sharing of threat intelligence data. The standards saw a joint development to enhance their interoperability [63].

Trusted Automated eXchange of Intelligence Information - TAXII is a transport protocol that allows users to subscribe to or disseminate feeds. TAXXII has several capabilities to ease traffic flow [64].

Structured Threat Information Expression - STIX is an XML or JSON based data format that provides objects to describe cyber intrusions. STIX can be used to describe technical observables, targets, threat actors, campaigns, and the specific activities performed in an intrusion. The objects have a logical relation to each other and the overall intrusion process. STIX is a lightweight protocol that can efficiently share large volumes of threat intelligence. It also allows threat intelligence analysts to compare STIX objects with each other to identify potential similarities within campaigns. Most TIP's support integration with these threat feeds, and some TIP' some pre-configured with subscriptions to free open-source threat intelligence feeds based on STIX data.

The latest version of STIX (2.1 and JSON based) defines 18 STIX Domain Objects, which are the supported entity types. A more extensive description of the STIX and TAXXI model can be found here; this was a presentation by the US Department of Homeland Security at the 2016 FIRST[42] symposium in Munich. This presentation elaborates on both STIX and TAXXI and their integrations.

Collaborative Threat Feed Initiatives

It is typical for industry collaboration initiatives such as ISAC's [65] to aggregate and disseminate threat intelligence to their constituents. A similar initiative is the Dutch national CERT's 'Nationale Detectie network[66]' this initiative will be presented in chapter 5.3.2.

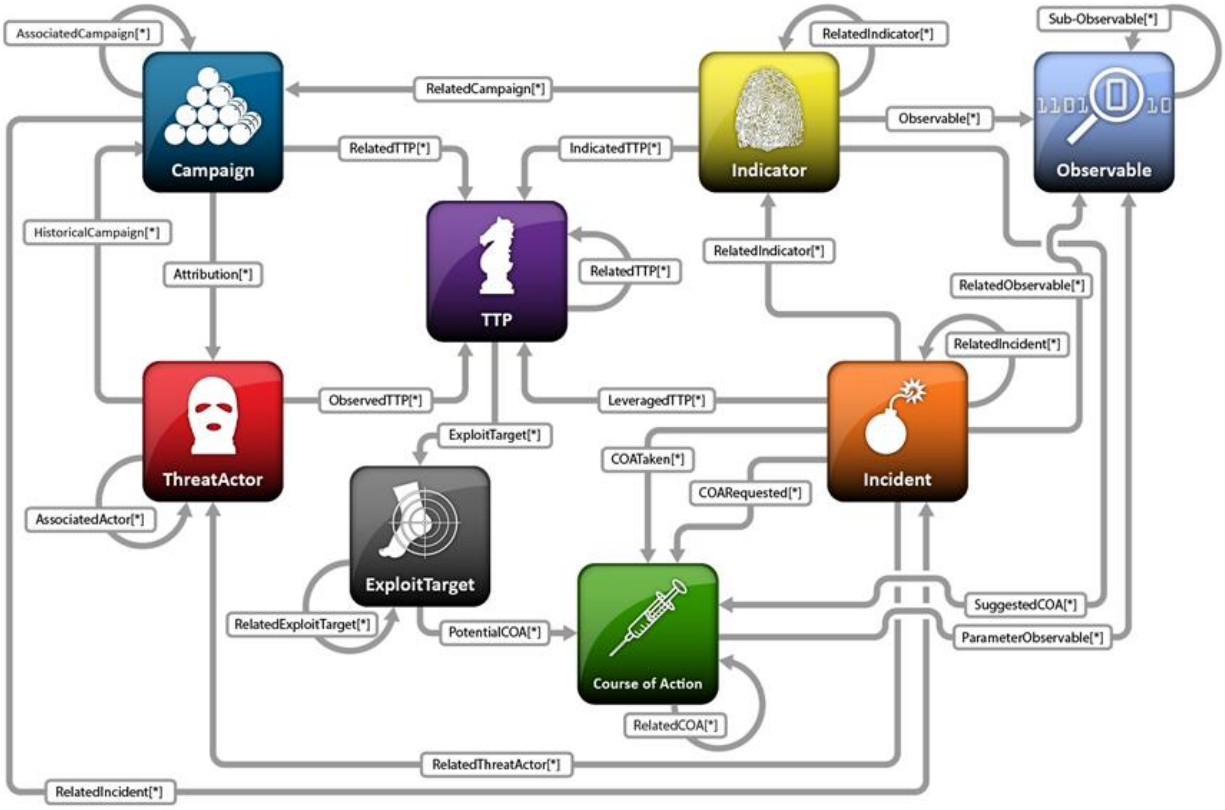


Figure 8 STIX data model, an example from stixproject.github.io about [67]

Commercial Threat Feeds

Most commercial threat intelligence providers provide their intelligence in subscription-based threat feeds. Examples of this are Mandiant, FoxiIT, Intel471, and many more, as it is a developing landscape.

Non-Commercial Threat Feeds

Non-commercial initiatives are free threat feeds provided as a public service by sources such as Abuse.CH, Bambanek Consulting, Shadowserver. They are community-driven initiatives.

3.8.3 Threat Intelligence Services

Apart from self-managed threat intelligence platforms, it is also possible to acquire a threat intelligence service provider to provide these services on your behalf. Outsourcing CTI can be a suitable option for smaller organisations that lack the workforce or expertise to staff a CTI team. This model has several benefits as it can allow the organisation to state the explicit performance goals of the delivering entity. Similarly, the delivering entity may serve multiple organizations within the same industry or sector, thus providing additional benefits due to its more extensive coverage.

This model of threat intelligence services is now also being provided directly through large scale IT infrastructure offerings such as Microsoft Azure. or Amazon Web Services. Within this environment, the threat intelligence data is provided as an additional service on top of the existing cloud infrastructure. This provides the benefit that the organisation can expect fewer implementation issues than an in-house implementation on self-managed resources.

3.9 Distinguishing Levels of CTI Maturity

ENISA on CTI Maturity

At the ENISA conference on Threat Intelligence in 2018, ENISA's lead cyber security analyst Marco Lourenco presented an approach to designating the overall level of organisational CTI maturity in four stages [9]. The presentation is publicly available through ENISA[43].

Four levels are distinguished to rate the maturity phases.

Level 1 - Initial	Unpredictable and reactive	Descriptive outlook
Level 2 - Managed	Developed but inconsistent, often reactive	Predictive outlook
Level 3 – Repeatable	Processes are measured and controlled	Predictive outlook
Level 4 – Optimized	Focus on process improvement	Pre-Emptive outlook

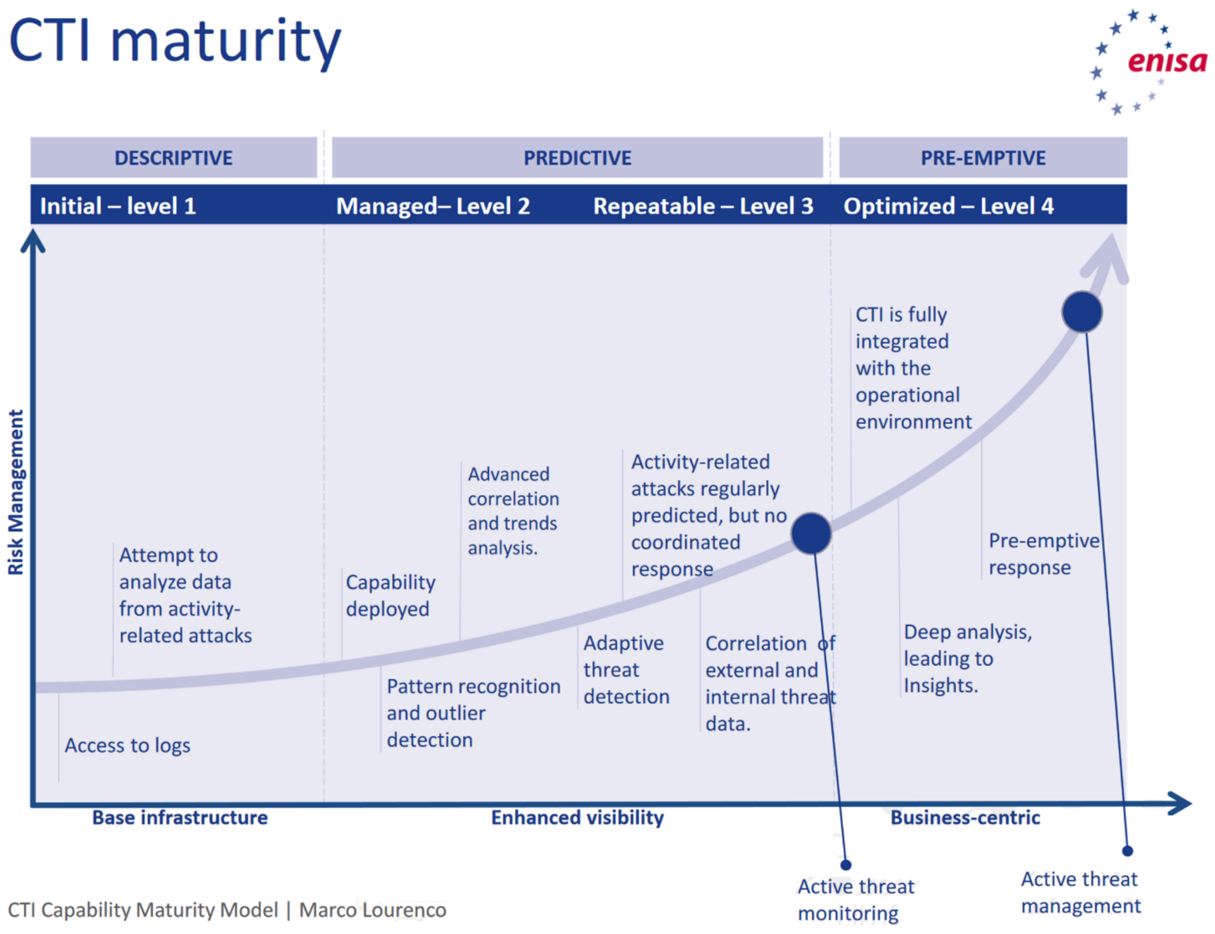

CTI maturity
enisa
DESCRIPTIVE
PREDICTIVE
PRE-EMPTIVE
Initial – level 1
Managed– Level 2
Repeatable – Level 3
Optimized – Level 4
Risk Management
Access to logs
Attempt to analyze data from activity-related attacks
Capability deployed
Pattern recognition and outlier detection
Advanced correlation and trends analysis.
Adaptive threat detection
Activity-related attacks regularly predicted, but no coordinated response
Correlation of external and internal threat data.
CTI is fully integrated with the operational environment
Deep analysis, leading to Insights.
Pre-emptive response
Base infrastructure
Enhanced visibility
Business-centric
Active threat monitoring
Active threat management
CTI Capability Maturity Model | Marco Lourenco

Figure 9 CTI Capability Maturity Model - Marco Lourenco ENISA [9]

ENISA's CTI Capability Maturity Model also contained scorecards for each phase of Planning, Collection, Production, Evaluation and Dissemination that can be individually graded. The model is intended to assess the entire CTI environment.

CTI Maturity according to CTIM, the Cyber Threat Intelligence Maturity Platform

An alternative model for CTI Maturity was presented by the Cyber Threat Intelligence Maturity Platform (further abbreviated to CTIM) [68]. CTIM is a research collaboration between the Hasso Plattner Institute of Germany and the Dutch university of TU Delft [69], [70]. This initiative has developed several models and toolkits for organisations to assess their maturity. Their whitepaper 'Measuring Your Cyber Threat Intelligence Maturity' proposes a six-step approach. [71]. Similar to ENISA, CTIM offers several tools for organisations to assess and structure their CTI maturity, and their publications have been made freely available on their website.

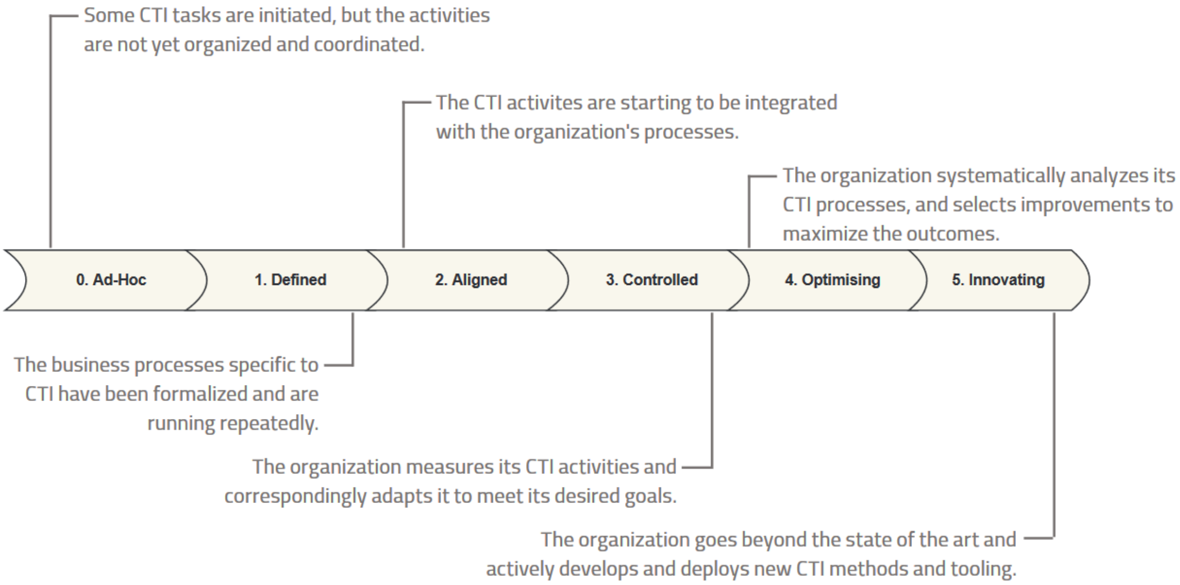

Some CTI tasks are initiated, but the activities are not yet organized and coordinated.
The CTI activites are starting to be integrated with the organization's processes.
The organization systematically analyzes its CTI processes, and selects improvements to maximize the outcomes.
0. Ad-Hoc
1. Defined
2. Aligned
3. Controlled
4. Optimising
5. Innovating
The business processes specific to CTI have been formalized and are running repeatedly.
The organization measures its CTI activities and correspondingly adapts it to meet its desired goals.
The organization goes beyond the state of the art and actively develops and deploys new CTI methods and tooling.

Figure 10 CTIM approach to maturity from the CTIM Whitepaper [68]

Models like these can help organizations steer the maturity development of their overall programs, including their strategic and operational level ambitions. For the intents and purposes of this dissertation, a simplified description will be used that represents the maturity of tactical level CTI in three levels.

Level 1: Intelligence Consumption
The organisation can consume intelligence products provided by third parties.
Level 2: Intelligence Creation
The organisation has a collection and analysis process to perform intelligence creation.
Level 3: Intelligence Dissemination
The organisations can consistently deliver their self-created intelligence products to third parties.

Chapter 4

Identified Successes and Challenges in CTI Implementations

Contents:

4.1 Interview Methodology
- 4.1.1 Participants
- 4.1.2 Distribution of Respondents Origin
- 4.1.3 Structure of the Interviews

4.2 Interview Findings: Analysis of the Pre-Implementation Phase
- 4.2.1 Summary of the Interview Responses
- 4.2.2 Defined Objectives for the CTI Program
- 4.2.3 Primary Stakeholders Assigned to the CTI Program
- 4.2.4 Involvement of External Expertise to Define the Program
- 4.2.5 Collaborations with Peers at Initiation of the Program
- 4.2.6 Distinction of Objectives by Intelligence Level
- 4.2.7 Maturity Development and Timeline Expectations
- 4.2.8 Staffing Size of Organisations
- 4.2.9 Education and Training Resources Leveraged to aid Maturity
- 4.2.10 CTI Tooling Known and Leveraged by Respondents
- 4.2.11 Adoption of Structured Analytical Techniques in the Program

4.3 Interview Findings: Complications Identified During CTI Adoption
- 4.3.1 Overall Complications During CTI Implementation
- 4.3.2 Complications Relating to People Factors
- 4.3.3 Complications Relating to Process Factors
- 4.3.4 Complications Relating to Technology Factors

4.4 Interview Findings: Overall Reflections after CTI Adoption
- 4.4.1 Overall Reception of the CTI Program
- 4.4.2 Significant Benefits Achieved
- 4.4.3 Feedback and Continual Improvement in CTI Programs
- 4.4.4 Resulting Level of CTI Maturity Achieved By these Organisations

After introducing cyber threat intelligence and its traditional intelligence origins, this chapter will present the findings identified in eight interviews. The interviews were held with stakeholders who worked in cyber threat intelligence and developed internal cyber threat intelligence teams. The interviews were of a semi-structured informal form, where each participant was asked the same set of questions provided in Appendix A: Interview Questions.

This chapter will identify the shared successes and complications of these teams. The novel insights gained by analysing the practical implementation experiences of these organisations will serve as this dissertation's second contribution to further the academic field of cyber threat intelligence.

4.1 Interview Methodology

4.1.1 Participants

This dissertation aims to answer the main research question: ’How Cyber Threat Intelligence is practically implemented within Dutch organizations’. The aim was to gather phenomenological data on the experiences of eight organisations that have gone through CTI adoption in the last ten years. The analytical data required to answer this question was gathered by interviewing the key CTI stakeholders of eight organisations.

This number of respondents was intended to be no bigger than ten respondents to remain feasible for the scope of this dissertation project and allow for more depth in individual questioning and analysis.

There was an added advantage to exclusively limiting the peer group to Dutch organisations, as all respondents’ organisations had their CTI team (legally) based in the Netherlands. Due to this joint national base, all respondents had to account for the same regulatory and legal landscape. This is relevant because CTI operations rely on the collection and analysis of (personal) data, which for these respondents occurs within the same national legal framework (most significantly the Dutch AVG ‘Algemene Verordening Gegevensbescherming ‘ [72]) and the overarching EU based (GDPR) legal framework [73]. This common factor is beneficial for our research as various local laws and regulations could have introduced deviation in the legal bandwidth nationally dissimilar respondents would otherwise operate in, thus making comparisons less representative.

Respondent Identification

Starting in September 2021, internet searches were performed to identify representatives in the Dutch CTI community. This search took place through online searches for CTI related phrases concerning the Netherlands. This involved organisational profiles, publications, blogs, CTI conferences and mentions of CTI within organisations on their websites; this was followed up with searches on LinkedIn. Representatives of Dutch organisations invested in cybersecurity were also directly approached to identify whether they had CTI teams and could provide contact details of the CTI staff that could potentially participate in these interviews.

To limit participation to respondents that were in a suitable position to provide representative answers, the participants had to meet the following criteria:

- A participant was involved in setting up or helping to build up a dedicated CTI team in the last ten years and is currently employed in this position.
- The respondent was in a senior position to assess the overall situation of the CTI program.
- The organisational entity must be based in the Netherlands.
- The respondent is willing to discuss their successes and complications under anonymity for themselves and their organisations.

Fifteen organisations were identified that could match the requirements. Publicly visible representatives of these CTI teams were directly approached and asked for participation. These respondents were also asked whether they knew other potential respondents interested in participating in this dissertation project. This helped identify more potential participants.

Respondent Selection

A selection of ten respondents that matched the requirements was made through purposive sampling to create diversity between industries, scale and sectors. These ten respondents were formally invited and received the interview questions beforehand; eight respondents were interviewed. The remaining two respondents could not accommodate the interview within the designated timeframe.

4.1.2 Distribution of Respondents Origin

The respondents' sectors varied between government entities (three) and commercial entities (five), as exhibited in figure 13.

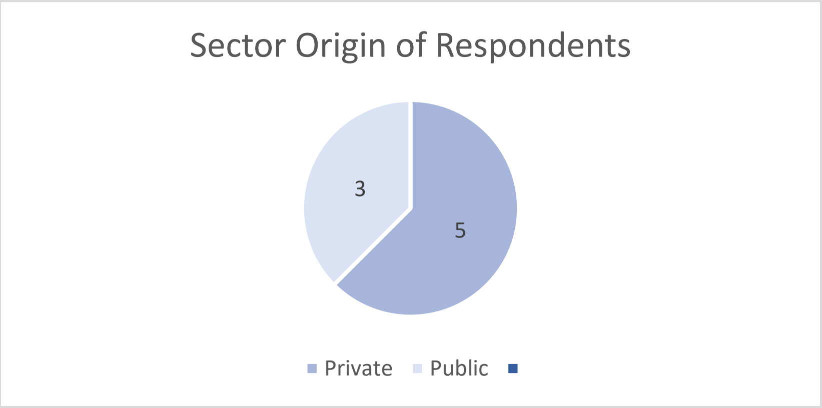


Figure 11 Sector Origin of Interview Respondents

There was a wide divergence in respondents' organization size. This differed between small organizations with less than 50 total FTE (Full Time Employees) and global enterprise-level organizations with more than 200,000 FTE. The average accounted for 68,500 FTE. The distribution is represented in figure 14.

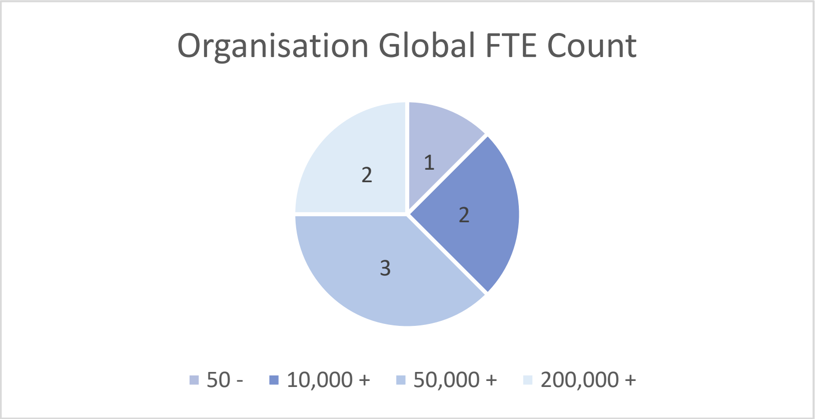


Figure 12 Respondents Organization Global FTE

Respondents Industry Sector

Three respondents were part of government organisations within the Netherlands. The five private sector organisations originated from IT services and consultancy (three), retail, and communications.

Age of the CTI Initiatives

The oldest CTI team had been active for more than ten years; the most recent participant had only just started on-boarding analysts and was only three months into its program when interviewed.

4.1.3 Structure of the Interviews

To observe how organizations leveraged CTI, semi-structured informal interviews were performed. This meant that every respondent was provided with the same set of 25 base questions to compare responses. The intent was to perform phenomenological research, whereby the implementation experience of the respondents, at this specific point in time, could be approached holistically. [74], [75]. This type of research is described as the following: *"A phenomenological approach is a form of qualitative enquiry that emphasizes experiential, lived aspects of a particular construct – that is, how the phenomenon is experienced at the time that it occurs"* [76].

The set of questions consisted of reflexive and open-ended questions that allowed the respondent to share novel insights and, where relevant, allowed the interview to deviate from the central questions into new areas of interest. The introduction to the open questions was intended to be unbiased on what CTI possibly meant to gather different interpretations of what CTI means to different organizations. The Simula Research Laboratory paper 'An analysis of semi-structured interview methodology' was used as the main guideline of the interview process and for drafting the questions [77] in addition to William C. Adam's Handbook of Practical Program Evaluation [78]. The number of 25 total questions was chosen because it would allow for the interviews to take place within one hour to heighten participation rates.

The questions were divided into five main categories, for which sub-questions were compiled. Three specific implementation phases were distinguished. These phases were deemed relevant to identify insights respondents may have gained as the program developed.

1. The first category was about the scoping and planning of the CTI program before actual adoption. It dealt with expectations, planning, timelines, stakeholders and other pre-stated objectives.

2. The second category was about the experience gained in the implementation process. Its purpose was to identify any deviations and how these were addressed.

3. The third category reflected on the moment the actual implementation was deemed complete (by the respondent). This involved any lesson learned in the overall implementation process. In cases where the CTI implementation was not deemed to be finalized, the respondent was asked to reflect on the experiences up to that point in time.

4. The fourth category consisted of open-end questions relating to tooling, processes, training and overall insights; this was not restricted to a specific time phase.

5. The final category was the interview's conclusion with two open-ended questions about any additional subjects the respondent deemed significant to discuss. At this stage, respondents were also asked about whether they had identified potential future developments for the CTI field in general.

After the drafting of the interview structure, an initial pilot interview was undertaken to verify the accuracy of the questions. After analysing the preliminary findings, a slight modification on the order and phrasing of the questions was performed. This was because two questions were related to each other but were presented in an illogical order. The definitive questions are presented in Appendix A: Interview Questions.

Anonymity

Anonymity was foundational in letting respondents open up about complications as these findings could reflect on maturity issues affecting their organization. Care was taken to create an atmosphere of trust and ensure confidentiality. To support this but still allow for data processing, starting at the interview, the respondents would only be identified by a unique pseudonym (letter) going forward. The interviews were opened by re-iterating the respondents' anonymity, confidentiality, and data processing requirements to ensure they understood the interview conditions.

Ethics

Before the formal initiation of the dissertation, the interview approach was verified to align with the research ethics as required by the Royal Holloway University of London and signed off accordingly [10].

Interview Process

All respondents received the same introduction e-mail with the interview questions a week before the scheduled interviews. This e-mail further explained the considerations relating to anonymity, data destruction and the analysis process. This also served to receive the respondent’s approval for participation.

Providing the questions upfront was intended to allow the respondents to reflect on the questions and make the interview time more efficient. This had a positive effect as three respondents were prepared with written notes. One respondent had verified answers within their internal team to reach a consensus on the response.

After the interview, the respondents received the interview transcripts to provide their feedback and final approval for processing. During later analysis, clarification questions were sent to several respondents. These questions were also answered, and the results were incorporated into the analysis.

In the end, eight out of the ten approached respondents were successfully interviewed.   All interviews were conducted professionally with cooperative and positive respondents. Where possible, the interviews were conducted face to face, but for three respondents, this was not feasible; these interviews were performed using video conferencing software from within confidential environments. The interviews took place between August 2021 and December 2021.

Analysis of findings

Answers were grouped by each question and compared between respondents. In case of ambiguity in analysis, the respondents were approached for additional clarification.

4.2 Interview Findings

This chapter will start with a summary of the overall notable findings, and these will be further elaborated on in subsequent chapters.

4.2.1 Summary of the Interview Responses

- All respondents had predefined objectives before the CTI program started.
  - For all eight respondents, the main objective for the CTI team was to integrate CTI capabilities with SOC/CERT processes.
  - Seven respondents identified that their CTI program played a significant role in providing vulnerability assessments to their organisations.
  - Five respondents had assigned their CTI teams a strategic advisory objective from the start.
  - Four respondents had external customers or peers intended to be served with the intelligence consumed or created by the CTI teams.
  - Automation was deemed a priority objective for three respondents.
  - One team had defined a specific multi-year roadmap from the start.

- For all respondents, the primary stakeholders of the CTI program were the internal SOC/CERT teams.
- The Dutch National Cert NCSC was also designated a primary stakeholder for all three interviewed government entities. These teams were also integrated into the 'Nationale Detectie Network' sensor system described in chapter 5.3.2 Dutch National Cert Resources: The National Detection Network.
- None of the teams had leveraged external expertise to set up the CTI initiative. Two respondents intentionally did not involve third parties to prevent potential external influence and bias. One respondent regretted this as it may have accelerated some of their integrations.
- The average team size was 6.7 analysts. The smallest team consisted of two analysts, and the largest consisted of twelve; those were dual-hat positions where people had other tasks besides CTI.
- The most common challenge was that infrastructure integration with the CTI tooling was more involved than expected, and for four respondents, this caused them to overrun their time plan. Two respondents had changed their tooling requirements since their start as their initially defined requirements were not accurate for the eventual integration.
- Respondents were aware of structured analytical techniques, primarily Analysis of Competing Hypotheses, but this was considered too time-intensive for daily operations.
- Seven respondents were actively using the MISP platform, and one respondent was still working on its implementation.
- Five respondents were invested in using the MITRE ATT&CK taxonomy to enhance intelligence deliverables; two respondents had not used it but were aware of its potential.
- The primary training resource for all respondents was the SANS 578 training course.
- All respondents adhered to the Traffic Light Protocol format for information sharing.

4.2.2 Findings of the Pre-Implementation Phase: Defined Objectives for the CTI Program

Respondents were asked how they prepared for the adoption of the CTI program. All respondents had explicitly specified objectives before the start of their program.

Diversity of CTI Objectives

- All eight respondents had defined the primary objective that the CTI program is to deliver intelligence to the organisation's internal SOC or CERT teams.
- Seven respondents leveraged CTI to deliver some degree of vulnerability management, brand monitoring or data leakage investigations. However, this was not considered their core objective and was one of several deliverables they were responsible for in serving the organisation. One respondent was still in the early stages of their implementation and was considering but yet undecided on providing vulnerability management services.
- Five organisations were set up to provide a strategic advisory role to their organisations. One respondent described this as the following:*" We consider CTI to be not just tactical/technical threat response but also Cyber Security Research & Development which aids future strategic decision making."*
- Two respondents explicitly defined a focus on automation as a core objective at the program's start.
- One respondent leveraged the CTI team to make threat landscapes that fed into multi-year roadmaps, which the general security organization used for planning. This also involved serving the risk management organisation with tailored CTI deliverables. In this process, the CTI team collaborated with the Chief Information Security Officer's team and directly worked on the advisory products.

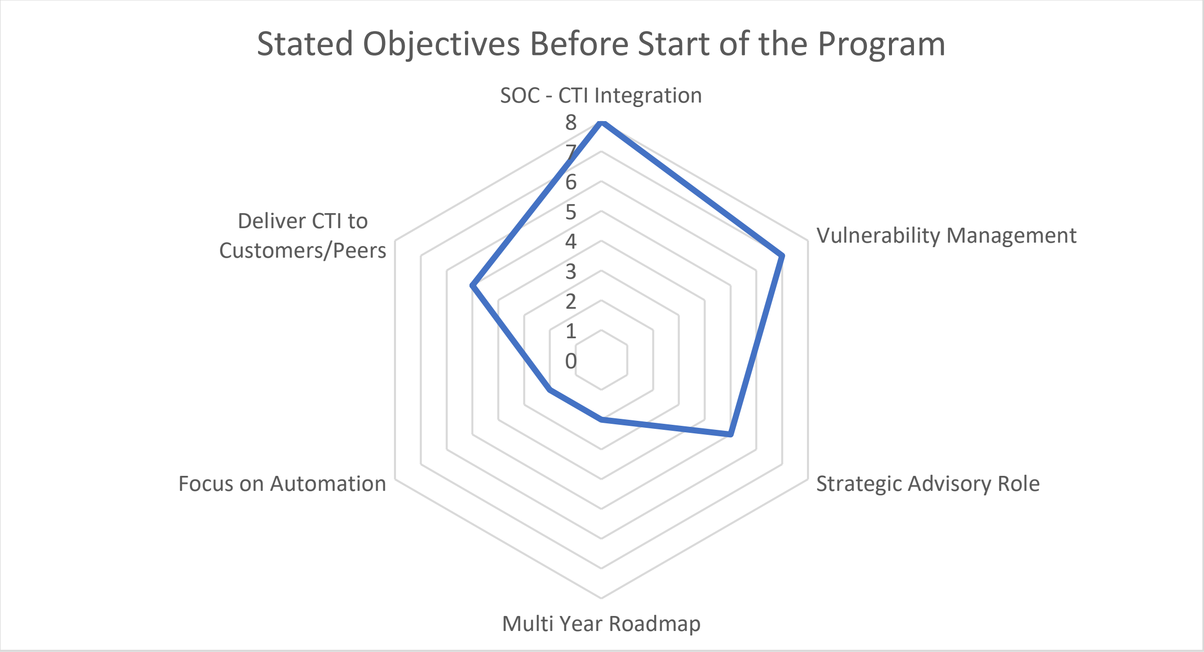


Figure 13 Stated Objectives for the CTI Initiative

Degrees of Integration with the SOC/CERT Capability and Additional Potential Objectives

The interview audience reached a consensus on aligning the CTI team to serve the SOC/CTI processes and integrate with this team. Several methods were identified in which the CTI team integrated with their SOC/CERT teams.

- With one respondent, this went as far as designating the entire CTI team as CERT and not distinguishing between Incident Responders, Forensics or CTI staff. All team members were expected to perform CTI within their operations, with some analysts being more involved in CTI than others.
- For another organization, the CTI team reports in daily physical 'operations room' meetings (morning and afternoon), where active investigations are collaborated on between SOC and CTI. This team has implemented analysts with a 'double hat' position, with two senior SOC analysts working part-time for the CTI team while also operating as liaisons between the respective teams.

These novel approaches for integrating Dual-Hat positions will be elaborated on in chapter 5.1.1 Staffing issues - Considering Fusion Teams or Dual Hat Analysts.

Respondents were asked whether alternative objectives were considered for the program and if they were aware of other potential objectives that could be delivered through CTI. This provided us with several perspectives on CTI adoption.

- One respondent's peer organization is leveraging CTI as a curated newsfeed for vulnerability management. This was described as a lightweight service that could be quickly developed and fed the organization specifically with tailored vulnerability assessments. This type of CTI service would lend itself to outsourcing to a threat intelligence service provider.
- Another alternative was to set up the CTI team to perform operational risk management. This example described this as an independent expert group positioned next to the CISO. In this role, the objective was less tactical but more strategic to inform and drive policy, with the core stakeholder being the CISO and without integrating with SOC/CERT processes.
- One respondent mentioned a peer who leveraged CTI primarily to perform brand monitoring and data leakage investigations. A third-party threat intelligence service provided this service. The respective organization was a small-to-medium business organization with commercial interests, but their staffing was not set up for an internal CTI capacity.
- One respondent mentioned an ambition to present a '*single pane of glass view'* on the entire security posture. This exceeded the CTI domain, as the intent was to perform exposure management and support the C level and Risk Management team on all manner of threats. This also included non-cyber related (geo)political, physical, legal and fraud intelligence subjects, surpassing the information security domain.
- One success shared by a respondent was a comment on a successful collaboration that could become a future objective: *"We were very successful in implementing CTI in a Red Team/Hunting team integration. They were very close partners in our processes."* Integrating CTI with Red Teaming was also mentioned by another respondent who described the TIBER Framework (Threat Intelligence Based Ethical Red teaming) as an example of how this is leveraged in their organisation. The TIBER framework will be described in Appendix B: Additional CTI Capabilities Mentioned by Individual Respondents.

4.2.3 Primary Stakeholders Assigned to the CTI Program

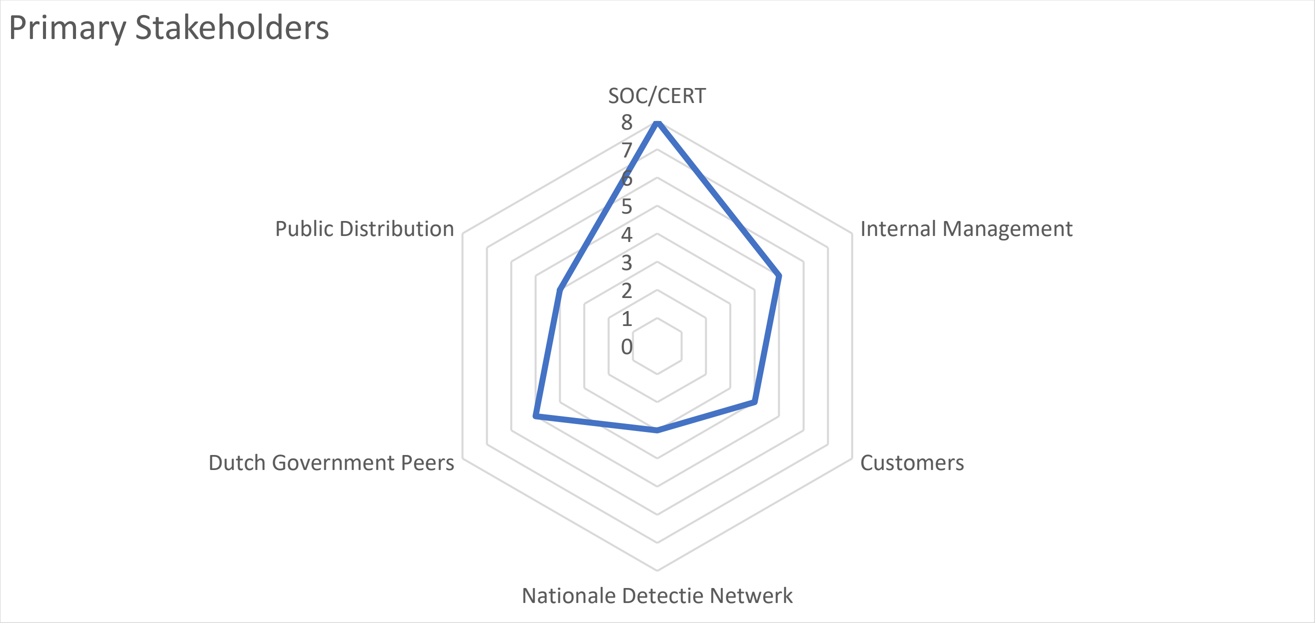


Figure 14 Primary Stakeholders Defined

Respondents were asked about the primary stakeholders assigned to the project. All respondents had explicitly defined stakeholders before the initiation of the program. This is relevant because it aligns with the intelligence literature, which defines that intelligence is not done for its own sake but must always be primarily driven by a stakeholder to support decision-making [79].
There was significant overlap with the stakeholders designated and the primary objectives defined for the CTI programs amongst respondents.

- All interview respondents identified the SOC or CERT of the organization as the primary stakeholder. (Within our analysis, no further distinction will be made between SOC and CERT as for the intents and purposes of our analysis; it will be defined as the part of the security organization where security events are identified and investigated and where technical level indicators can be consumed.) This implies a shared focus on tactical level CTI.

There was a notable difference in the designated stakeholders between respondents from the commercial sector and respondents from the government sector.

- The respondents of the commercial organizations mentioned the CISO, security officers and risk managers as primary stakeholders to the CTI process; this was not the case for the government respondents as they were not structured this way.
- Four commercial organisations identified external customers as core stakeholders to the process.
- All three government organisations identified government peers as stakeholders.
- Notably, all three government respondents identified the Dutch National Cert's (NCSC) 'Nationale Detectie Network (further abbreviated as NDN) as a primary stakeholder. The Dutch NDN, which translates in English to the National Detection Network, is a Dutch government initiative where network detection sensors are deployed by the Dutch NCSC. Details on NDN will be described in chapter 5.3.2 Dutch National Cert Resources: The National Detection Network [80].

4.2.4 Involvement of External Expertise to Define the Program

Respondents were asked whether they involved external expertise to help define and implement their threat intelligence program.

- None of the respondents leveraged external expertise to shape the program's objectives. Two respondents mentioned leveraging partnerships, but this was limited to tooling and datasets.
- One respondent leveraged an external consultant to assess the validity of newly developed CTI tooling. Though this was not a formal collaboration, it did help shape their tooling selection. This same respondent leveraged the Intel 471 GHIR framework [81] to formalize their processes and stakeholder selection at the start. The Intel471 GHIR will be presented in chapter: 5.2.1 Structuring the Intelligence Collection Process.
- One respondent regretted not having leveraged external expertise earlier.
  "Perhaps we could have involved external expertise earlier; it may have helped to steer direction to more actionable things first. In our approach, these insights had to come from experience in time."
- Two respondents mentioned that not leveraging third parties was a conscious decision to minimize potential external (commercial) influence. The argument was that they were hesitant to expose their program to external preferences and biases and wanted to maintain a self-developed direction for their intelligence program.
- As an elaboration on this question, one of the more mature respondents mentioned intentionally recruiting experienced staff with various former intelligence backgrounds specifically to have different perspectives on how intelligence can be delivered. Having diverse analysis teams is common in traditional intelligence and is often identified as "Intelligence Fusion" this will be briefly introduced in the chapter. 2.2 Overlap in Traditional Intelligence Tradecraft and CTI This concept will be revisited in chapter 5.1.1 Staffing issues - Considering Fusion teams.

4.2.5 Collaborations with Peers at Initiation of the Program

- All government respondents leveraged the Dutch National Cert (NCSC) resources to develop their program. One government partner mentioned a presentation by Dutch Law Enforcement on CTI to having been a pivotal moment in the scoping of the team. The presentation emphasized a tactical/technical focus on deliverables, which aligned with their intended approach.
- Amongst the commercial organizations, the collaboration with peers was limited. One respondent considered their peers competitors and only leveraged direct partnerships with technology providers such as threat intelligence tooling and data providers when signed under non-disclosure Agreements.
- One commercial CTI team had industry embargoes that prohibited sharing sensitive details on how they set up their threat intelligence program and the specific technical configurations of their commercial security solutions. However, this did not prevent them from collaborating with sources from the Dutch National Cert or publicly participating on MISP. This team also publicly shared internally developed open-source tools and processes when this did not fall within embargo regulations.

4.2.6 Distinction of Objectives by Intelligence Level

Respondents were asked whether they distinguished specific CTI processes concerning the intelligence levels that are traditionally identified as tactical, operational and strategic.

Views on Tactical/Technical Level Intelligence

- All respondents agreed that the threat intelligence feeds (containing indicator information) were part of the tactical level. For two respondents, tactical was synonymous with technical, and no further distinction was made between the phrase tactical/technical.
- One government entity had intentionally set up their CTI program with two sub-teams, a tactical level analysis team focused on identifying trends, TTP's, and providing high-level recommendations. They also designated a separate technical team that would deal with the technical side of CTI relating to the indicators, the threat intelligence platform and the distribution of the IOC's. This organization had intentionally not scoped their initiative for strategic or operational as this was not in their area of responsibility.
- The respondent of one commercial organization identified that some of their customers alternated the levels tactical and operational by using the order of operational, tactical, strategic. The respondent identified that this approach was more common within law enforcement and some business environments.

Regardless of the model chosen. When collaborating on intelligence, it should be one of the starting questions on what levels are identified and what they mean to the organisation as differences exist. For the purpose of this dissertation, the traditional intelligence levels will be used as they are more readily adopted within CTI practices.

Views on Strategic Level Intelligence

- Three of the five commercial organisations were managed services providers. All three identified strategic level intelligence to be relevant to advise their customers on long term investments. All three organisations had identified strategic level advisory as an objective at the initiation of the CTI program.
- One of the longest-running CTI teams identified an increasing maturity in operational level intelligence and growth in their internal CTI dataset size and significance. The team could now identify strategic (multiyear) level trends through this. Though not a current priority, this information could help tailor strategic level intelligence deliverables.

4.2.7 Maturity Development and Timeline Expectations

The respondents were asked whether the program's initiation involved a maturity development program and timelines defined for specific maturity objectives.

- Three respondents had a maturity development process envisioned at the program's start. However, none of these respondents had a multi-year approach to this, and it was directed at yearly touchpoints to set new goals. All respondents mentioned that flexibility was a key concern as the overall environment and supporting infrastructure surrounding the CTI teams were expected to change, which had to be accommodated.

MoSCoW method To Define Future Roadmap

One respondent leverages a yearly brainstorm where at least three goals are defined for each high-level CTI process. The brainstorm is open to all people involved with CTI, and there is intentionally no hierarchy amongst participants of this brainstorm. During a team discussion, they assign all the goals into a Must Have, Should Have, Could Have and Would (like to) Have category. This designation is also known as the MoSCoW method [82]. The identified objectives are then voted on before they become part of the formal roadmap for the upcoming year.

Feedback Integrated with the Intelligence Dissemination Process

One respondent leveraged the feedback process of intelligence deliverance to feed the improvement process. Instead of periodically looking back on a set time, they collaborate with peers in their ‘risk intelligence’ group and ensure that the intelligence deliverables produced are actionable for their stakeholders. This process is performed for each intelligence deliverable produced.

This process refers to the intelligence cycle defined in chapter 2.6, Cyclic Nature of Intelligence. It is an interesting approach for organizations where the CTI team can directly collaborate with the stakeholders and their intelligence consumption.

There were notable quotes about this subject.

- *“Cyclic improvement processes are great on paper but much too time-intensive for incident driven CTI”.*

- *“Work on what you need in 3 months. Plan on what you need in 6 months, have a direction on where your overall program will lead to (5 years from now).”*

4.2.8 Staffing Size of Organisations

Respondents were asked about the size of their team, and this was specified to mean actual analysts working on CTI and not supporting positions such as management or engineering.

The dedicated CTI headcount for each respective organization was: 2, 2, 3, 4, 5, 6, 9 and 12, and it is notable that the large team of 12 analysts was the organization that had integrated CTI within their CERT, as this headcount reflects the total size of their CERT.   The organisations with headcounts of 9 and 12 FTE were the two organisations capable of disseminating large scale intelligence and having reached level three of our CTI maturity distinction, which is described in chapter: 3.9 Distinguishing Levels of CTI Maturity

Staffing Issues due to Scarcity

Three respondents identified staffing issues as a primary concern to developing their maturity. CTI expertise is scarce since this field has only been developing for ten years. The loss or addition of an experienced analyst can significantly affect the operational maturity of a team. All respondents identified that recruitment was problematic, specifically finding people with an intelligence background and mature cybersecurity expertise.

Promoting Diversity in Intelligence teams: Intelligence Fusion

Two organisations had intentionally recruited staff with a traditional, non-technical intelligence background; respectively, one organisation recruited a staff member with a background in strategic intelligence. The other organisation had recruited an employee with a military HUMINT (Human Intelligence) background. The intent was to find staff with a fundamental intelligence background and provide additional training to train them in the specific cyber aspects. This also had the aim to benefit from the intelligence experiences outside of the technical field of information security.

The effect of diversity in analytical teams is sometimes identified as 'Intelligence Fusion'. Within the Joint Intelligence Doctrine of the US Department of Defence, this is stated as:
'Fusion is a deliberate and consistent process of collecting and examining information from all available sources and intelligence disciplines to derive as complete an assessment as possible of detected activity. It draws on the complementary strengths of all intelligence disciplines" [34]**.**
This concept will be further explored in chapter 5.1.1 Staffing issues - Considering Fusion Teams or Dual Hat Analysts

When dealing with multi-disciplinary investigations, structured analytical techniques can prevent bias and help align the different intelligence disciplines. Structured analytics will be described in chapter 5.1.2. Analytical Cohesion Between Analysts – Introducing Lightweight ACH.

4.2.9 Education and Training Resources Leveraged to aid Maturity

Respondents were asked about the training resources that they leveraged to train their analysts.

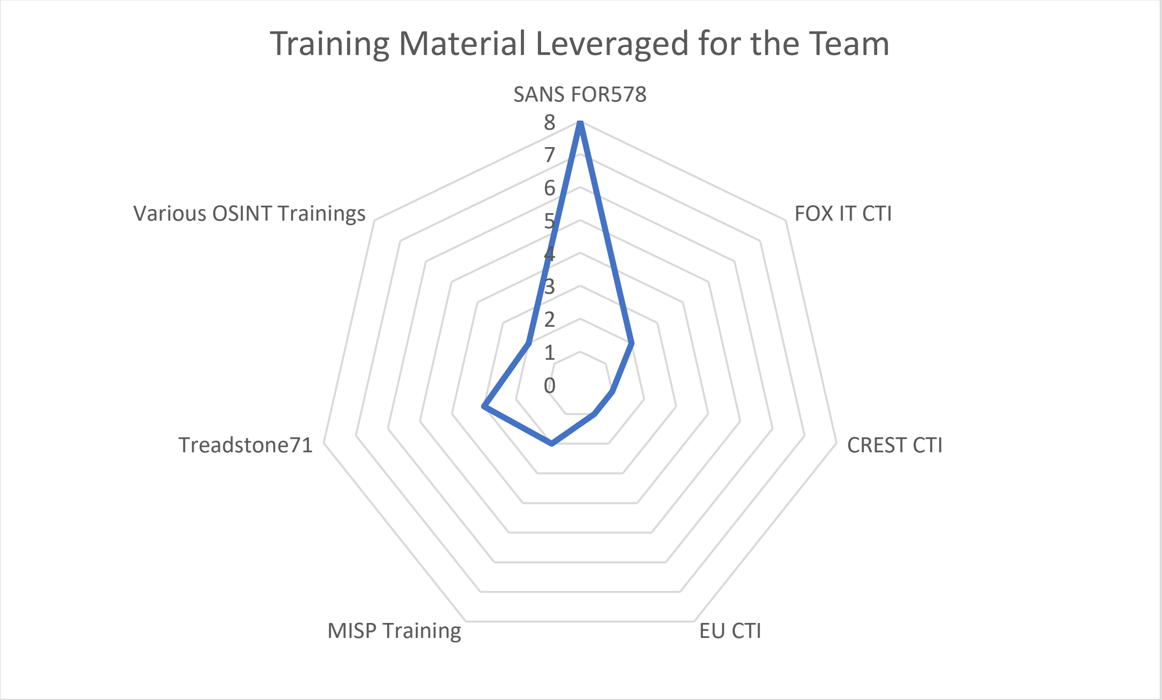


Figure 15 Training Material in Use

This question identified a strong preference for the GIAC, SANS FOR578 Cyber Threat Intelligence program, as this was leveraged by all eight respondents [83].

- Three respondents had used the Treadstone 71 Cyber Intelligence Tradecraft Certification to provide CTI training to their team [84] [85].
- Two organisations used MISP training resources provided by the Luxembourg CERT [86], [87].
- Two respondents used Fox-IT CTI training; this is an in-company training that is not open to individual participants [88]. Both of these teams were within the Dutch government sector.
- Two respondents participated in online OSINT (Open Source Intelligence) training resources. Both found this lacking as it was too focused on social media and not a good match with tactical CTI information requirements, which are more technically inclined.

Individual mentions:

- The EU-CTI certification (provided by the European Union Agency for Cyber Security ENISA) was mentioned as another alternative training source that a respondent was aware of but had not leveraged themself. This program is more of an accreditation program than an individual tactical level CTI training solution[89].
- CREST, the Council of Registered Ethical Security Testers, has an individual accreditation program to become a certified 'registered Threat Intelligence Analyst'; one respondent had looked into this training program but had not participated in it yet [90].

4.2.10 CTI Tooling Known and Leveraged by Respondents

Of specific interest to our interview process were questions 3.5 and 3.6 relating to a respondent's awareness of open-source tooling and which of these tools had seen adoption in their programs. The scope of interest was open-source and free 'community' editions of CTI tooling. All respondents were aware of the availability of some CTI tooling; each team had leveraged several of these tools. **The three most used tools were MISP, the MITRE ATTC&K Framework and Maltego.**

- All respondents were aware of **MISP**. Seven out of eight respondents had an operational MISP implementation. One party was adopting MISP. This identifies MISP as the most used CTI tool among these respondents. MISP will be described in chapter 5.3.1 MISP.
- The **MITRE ATT&CK framework** is a CTI ontology known by seven respondents, with five actively using the ATTC&K methodology and its supporting tooling in their operations. This will be described more extensive in chapter 5.4.1 MITRE ATT&&CK Framework [91].
- **Maltego** was known by five respondents and used by three; it is a graphing analysis tool prepared with API connectors for popular CTI datasets. Maltego is a commercial tool with a free Community Edition with limited capabilities [92].
- The **OpenCTI** platform was known by four respondents, with two having used this. One respondent has OpenCTI in active use. One respondent used it shortly as an intermediate solution for a commercial TIP. OpenCTI will be further described in chapter 5.3.3 OpenCTI.
- **Spiderfoot** is an OSINT/CTI footprinting tool that can identify internet infrastructure; two respondents were aware of this tool and had it in active use.
- **Taranis** is an open-source OSINT too published by the Dutch NCSC. This tool was known to three respondents, and it is in use with two government organizations. Taranis is available from the Github site of the Dutch NCSC. It is also part of the NCSC CSIRT Maturity Kit. [93].
- **Several tools** saw individual mentions; these are provided in Appendix B: Additional CTI Capabilities Mentioned by Individual Respondents.

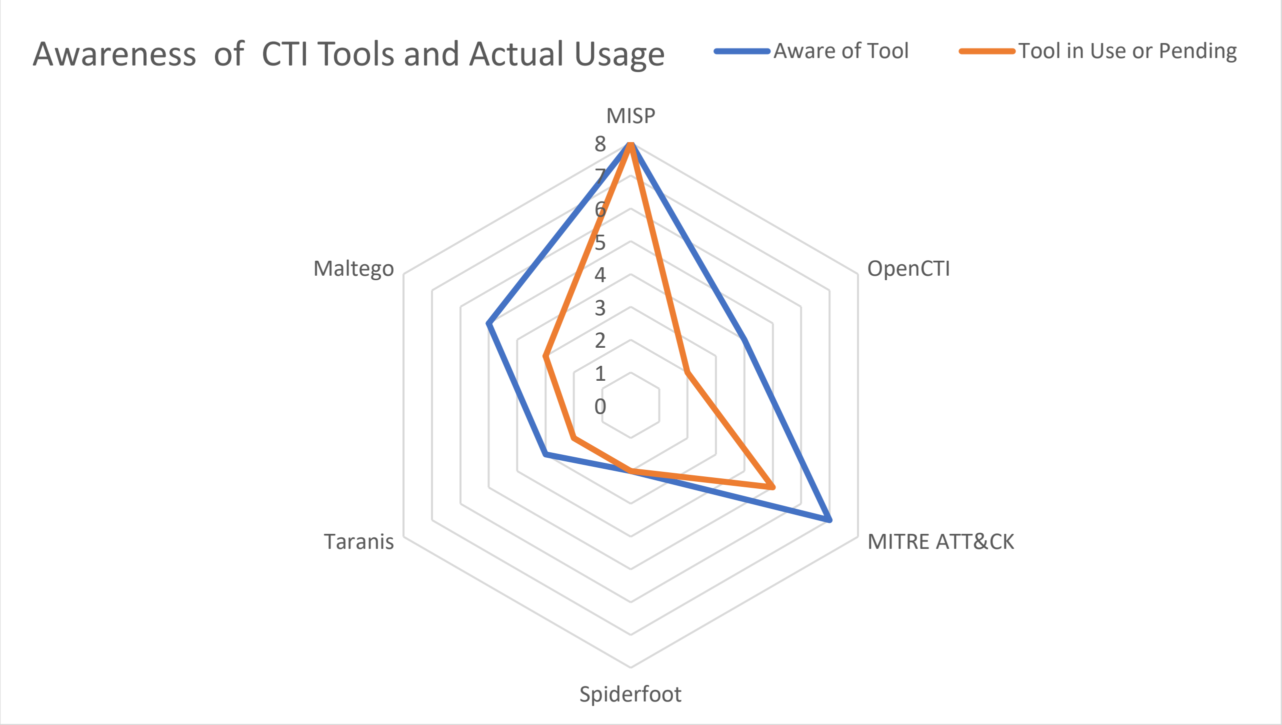


Figure 16 Usage of CTI Tools

4.2.11 Adoption of Structured Analytical Techniques in the Program

Structured analytics are processes that structure the human assessment of information. Within the field of intelligence, there has been a high level of interest in how analysts interpret information. Richard Heuer is notable for having performed a significant amount of research on this subject in his work for the CIA. Many of his publications and books are now in the public domain [14]. Several CTI methodologies involve the application of structured analytics to reduce analyst bias. The respondents were asked whether they were aware of structured analytics and if this saw adoption in their programs.

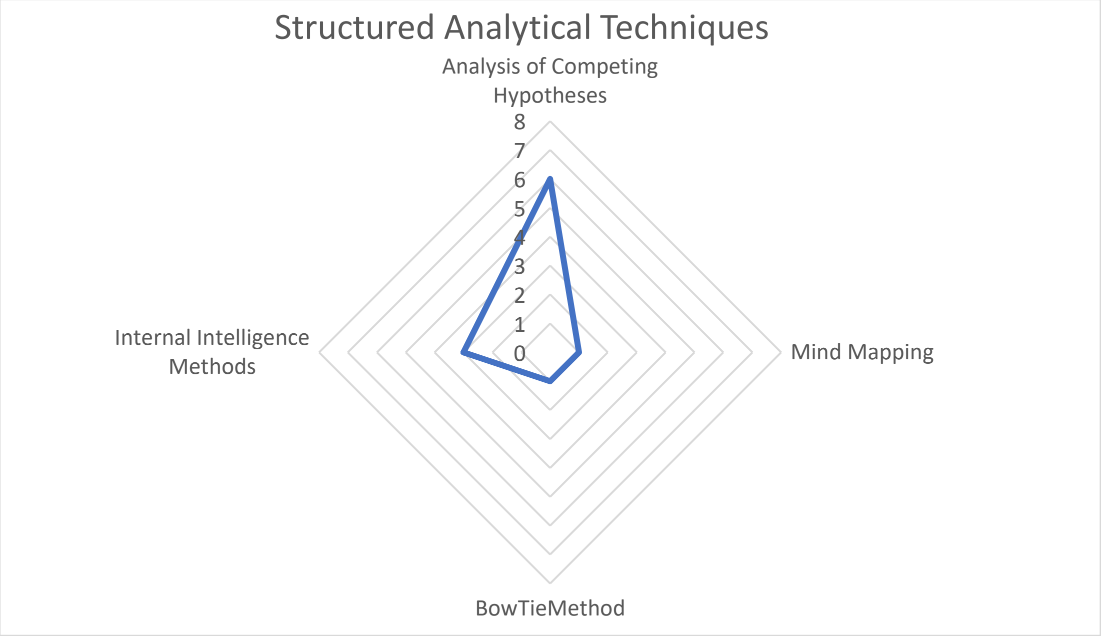


Figure 17 Structured Analytical Techniques

- Six respondents were aware of structured analytical techniques; the most frequently mentioned technique was Analysis of Competing Hypothesis (hereafter referred to as ACH).

  This is not surprising as ACH is part of the SANS FOR578 Cyber Threat Intelligence training course that all respondents leveraged to train analysts[83]. Three participants mentioned having tried ACH, but all three have since retired its use. The reason was that ACH was deemed too time-intensive and could not be easily leveraged for incident-driven CTI analysis. ACH and structured analytics will be described in chapter 5.1.2. Analytical Cohesion Between Analysts – Introducing Lightweight ACH An alternative way to leverage ACH to make it less time-intensive will also be suggested.

- One respondent used the Bowtie Method to define a filter on what information was to be retrieved in the collection phase of the intelligence cycle[94].

- Two respondents mentioned leveraging the MindMap methodology as a structured analytics technique that they had leveraged[95].

- One respondent identified having leveraged structural analytics originating from an internal intelligence program, but due to confidentiality, could not elaborate on the details

4.3 Interview Findings: Complications Identified During CTI Adoption

4.3.1 Overall Complications During CTI Implementation

Respondents were asked whether they identified complications during the adoption of the CTI program. The responses were diverse.

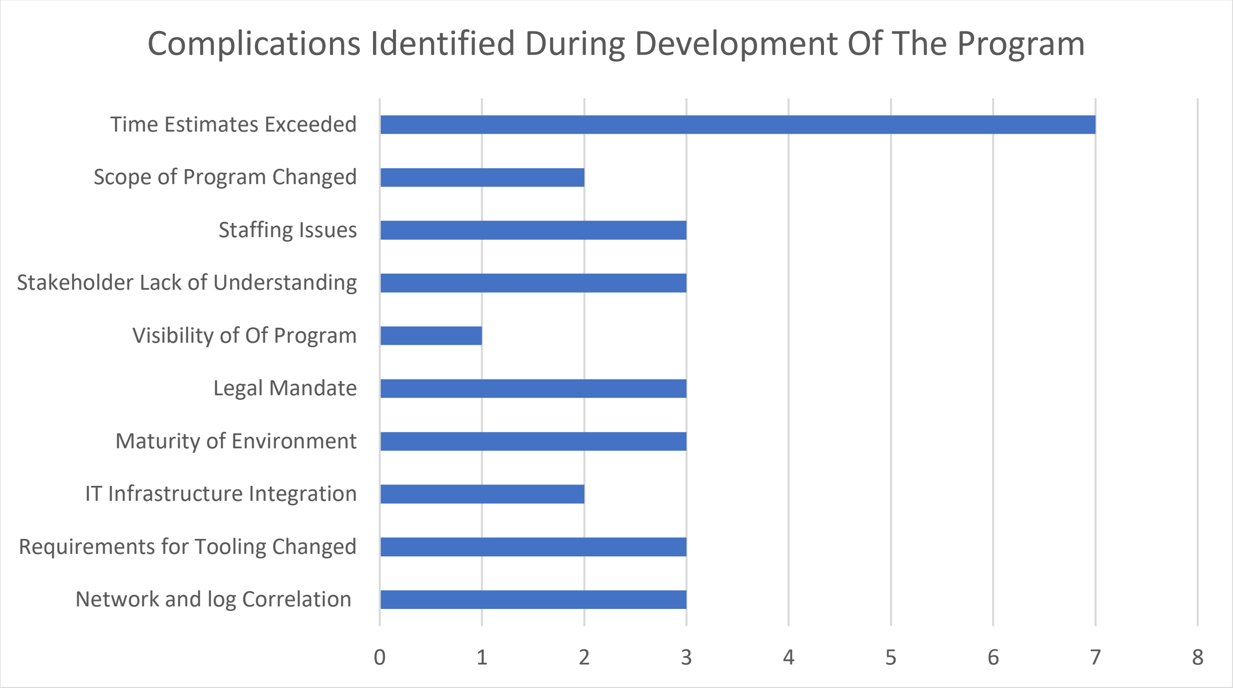


Figure 18 Complications Identified During Implementation of Program

- **Overall Delays in Program Development**
  Four respondents identified that they exceeded their planned timeframe. A further three respondents identified that they were not fixed to specified deadlines but felt the program could have moved faster at some stages and encountered various delays overall. Seven out of eight respondents identified exceeded time estimates. On this subject, one respondent stated: "*Technical, financial and procedural developments did slow down some of our initiatives."*

  One respondent did not identify delays in their adoption. Notably, this respondent was the team-lead of the overall program, and this individual had already supervised two other CTI program adoptions.
  "In our scoping, we already estimated a long-term growth initiative. Because of this, we set our expectations realistically, and we could deliver on our ambitions. This was also because the organization allowed for a long-term initiative."

4.3.2 Complications Relating to People Factors

- **Delay Due to Staffing Complexity**
  One organization had severe issues with staffing during the implementation of the program. They stated that the field is highly contested, and everyone requires experienced analysts. As such, it took more time for the team to be operational. Their insight was:
  "We could potentially have started recruitment earlier to mitigate this problem."
  Alternative approaches to staffing will be described in chapter 5.1.1 Staffing issues - Considering Fusion Teams or Dual Hat Analysts

- **Complexities Due to Stakeholder's Perception of Intelligence.**
  As stated by one of the respondents: '*The potential depth on which CTI can add value depends on the stakeholder's understanding. We can maximize our effectiveness if we get buy-in from all horizontal and vertical stakeholders. We cannot provide intelligence products to a hunting team if they have not already defined some hunting hypothesis and developed capabilities to perform hunting.*'
  This example can emphasize the importance of adequately introducing potential CTI deliverables to the stakeholders.

- On this subject, another respondent stated:
  "*The intelligence understanding of stakeholders was sometimes minimal, requiring some effort to make the purpose of CTI clear".* Suggestions to aid stakeholder understanding will be presented in chapter 5.4.3. Helping Stakeholders Understand Uncertainty in Intelligence.

- **Creating Visibility for the Program**
  One respondent identified lack of visibility as a complication that they were overcoming. When their team was started, their peers within the organisation were not aware of their presence or the purpose of the CTI initiative. The team proactively sent out periodical intelligence reports with a broad scope of interest to increase their visibility which helped them improve on this in time.

4.3.3 Complications Relating to Process Factors

- Two organisations identified a scope change as their program developed.
  - **Addition of new Stakeholders to Involve Non-Government Peers**
    One government respondent has expanded on their original number of stakeholders. This re-scoping was intentional and planned for and led to an increase in their team capacity by growing their team by two analysts (from six to eight). In this expansion, they also started serving intelligence to non-government constituents (near peers), which changed their deliverables' format.
  - **Expansion of CTI Initiative into Forensics and Malware Analysis**
    One organisation has expanded their initial CTI processes into an in-house malware analysis capacity. This integration allows the organisation to investigate malware and derive relevant CTI indicators without leveraging third-party expertise.

- **No Complications or Scope Changes Due to Flexible Programs**
  Four organisations did not identify a formal scope change but did elaborate that their overall program was flexible from the outset. Because of this, the expectation was that they could grow organically into the emerging requirements.

- Three organizations struggled with the complexities of legal mandates.

  - **Complexities of Acquiring Commercial Tools within Government**
    In one case, this involved a government entity that encountered a strict regulation on acquiring commercial threat intelligence, which postponed the adoption of external threat intelligence feeds.

  - **Complexities of Legal Information Sharing from Government to Private Sector**
    One government respondent identified complexities with the legal framework required to share information with third parties. This is based on the laws and regulations relating to data privacy.
    "As a government organization, we had a lot of strict legal mandates for information sharing that we have to adhere to and needed to be formalized before we could start sharing. Due to this, it is difficult for us to communicate out of bounds with peers that we did not already have a formal information-sharing initiative set up with."

  - **Complexities with Commercial Non-Disclosure Agreements**
    Another example involved a commercial organisation with strict non-disclosure clauses. This organisation wanted to contract a threat intelligence provider, but unfortunately, this party could not meet their organisation's legal requirements. Because of this, the project was aborted. The CTI team considered this a significant set-back to their program, as the team had invested much time in selecting and testing this tooling

- One organisation encountered complications due to the lack of maturity in the overarching Organisations

  - **Maturity of the Surrounding Organization**
    One respondent identified the developing maturity of the surrounding team to be one of the main complications. The CTI program was one of the sub-teams in a larger SOC/CERT environment, which also contained penetration testing, security assessments and infrastructure engineering. As the overall organization was still relatively new, the CTI team had to adjust to the changing environment. They were able to compensate for this by not setting too strict guidelines and maintaining flexibility in their program to grow organically in the direction that the surrounding environment required.

4.3.4 Complications Relating to Technology Factors

- Technical integrations provided complications for five out of eight respondents.

    - **Delays by Complex Integration of IT Infrastructure**
      Two respondents identified that during the development of the CTI program, the integration of IT infrastructure was more time-intensive than envisioned. The leading cause identified was dissimilarity of the infrastructure and different ownership, which meant dealing with additional stakeholders that did not have CTI as one of their objectives initially. This delay may have been partially prevented if the stakeholder analysis process had been more extensive and envisioned specific infrastructure partners from the start.

    - **A restart of CTI Tooling Integration Due to Requirements Change**
      Two organizations restarted the integration of CTI tooling because their requirements had changed over time. They did not see how this could have been foreseen. When further specified, the overall program direction was loosely defined. Their actual requirements only became apparent when they started using their tooling.
      "As the program matured, the tooling requirements we set beforehand did not match anymore. By then, we were committed to less optimal solutions. Looking back, there was no way to predict what our requirements would be, but an emphasis on flexibility here is very important."
      "With the knowledge we have now, we may have set our tooling requirements differently (with more flexibility) to better match future requirements."

    - **Delays due to Log Source Integration**
      Log source Integration was a complication for two respondents. They identified dissimilar datasets between their primary log sources, complicating correlation and integration with the TIP. The respondents considered this an oversight on their preparation, as this complication could have been identified at the time.
      'We identified complexities due to the fragmented nature of the surrounding network infrastructure. A historical re-organization merged two separate organizations, each with specific IT requirements and configuration. This integration created a lack of overall commonality in datasets and ownership, which further complicated the aggregation of data sources.'

    - **Complications due to Issues with the Threat Intelligence Platform**
      One respondent identified that they are held back by their Threat Intelligence Platform. The issues stem primarily from TIP features. They specified that this was something that the vendor was informed about but had yet to be resolved.
      "We do not feel sufficiently supported by our Threat Intelligence tooling, as our Threat Intelligence Platform does not deliver on the ability to correlate dissimilar datasets and entities, and did not accommodate for deduplication leading to confusing responses and manual verification. With the intent to increase the number of stakeholders we support, this is a growing concern to us."

4.4 Interview Findings: Overall Reflections after CTI Adoption

4.4.1 Reception of the CTI Program

Six respondents stated that their program implementation could be considered complete; they all consider their CTI program successful at this stage. Two respondents identified that they had not yet reached the stage where they consider their CTI initiative formally adopted as it is still in development.

- *"Our main requirements, such as tooling and staff, are now in position, and this is having an accelerating effect on the rest of the program."*

- *"Integration with the SOC was fundamental since our start-up, and this has been very successful."*

4.4.2 Significant Benefits Achieved

Respondents were asked to reflect on the most significant benefits and successes achieved.

Adoption of CTI by the Surrounding Organization

- *"Visibility to stakeholders has been greatly improved**; we have started with a weekly threat digest and have gotten a lot of good responses on this**. We distribute this to our general public to raise awareness."*
- *"Due to our automation, our intelligence can even automatically feed into risk/compliance requirements and processes, a great success we did not foresee.*

Operational Success with SOC collaboration

- *"Recently, we had an incident to which we could apply our CTI intelligence assessments. We were able to support our engineering teams and incidents responders. The perspective from CTI was unique as we objectively assessed a situation that was about to escalate. Our approach was to gather the facts first and not rumours that influenced the other teams. We developed a theory and investigated this objectively, **this was a great success as we brought in a novel approach,** and we turned out to be correct in our assessment."*
- *"We met our deadlines on the development and delivery of products."*
- *"We re-assessed some data standards* that are in everyday use to make them more feasible for our purposes. This significantly aided our data quality. We maintained a high degree of automation due to our infrastructure decisions. Manual analysis was kept at a minimum, creating a high degree of effectiveness per analyst hour. "*
  ** (*Threat Intel Platform JSON format ingestion*)*

- *"We have great internal collaboration with other security teams; we perform extensive investigations that often become multi-disciplinary—the integration with our SOC process and the direct preventative actions that can be taken with actionable intelligence.* ***We are moving ahead in the kill chain.***

- *‘Implementation is technically complete; however, we are still improving on many levels. Expectations were superseded; we were able to gather talented people who made it work from the start.’*

- *‘Yes, we surpassed initial expectations. But it could always have moved faster.’*

- *‘We are still setting up to a degree. We were able to match some of our expectations. CTI has helped advise some business processes relating to how we acquire tooling, how we respond to threats.’*

- *‘We could report to one of our customers that someone was selling access to a confidential dataset on the dark web. This was a serious investigation for our customer. The listing turned out to be fraudulent and not data stolen from the internal organization. Due to the pro-active nature of the investigation, the organisation’s board was fully aware of the scenario. Media got wind of this, but due to the early warning, they could be answered completely without causing any negative repercussions.’*

- *‘One of our customer's main suppliers/partners was hit by ransomware. But the affected supplier had not informed our customer about this yet. We rapidly helped our customer switch from this supplier to an alternative provider, which massively helped them. They also disconnected all network connections before the breach notification came out. This further reduced their risk pro-actively. We offer organizations the perspective to pro-actively work on things when we notify them of this. This is a completely different perspective than the reactive approach they were used to.’*

4.4.3 Feedback and Continual Improvement in CTI Programs

Respondents were asked whether they had formalized improvement programs to further mature their CTI programs going forward.

- One respondent identified that their incident driven CTI operations did not allow for many separate improvement programs; however, they were very extensive in the dissemination phase when delivering CTI reports. They actively participated in the delivery and usage of the intelligence deliverable and gathered feedback at this stage. In this way, each intelligence deliverable fed into the quality improvement program individually.

- One organisation leveraged CERT maturity processes to develop its CTI team.
  “We have leveraged CERT maturity processes as a knowledge base for our CTI maturity development. This also made sense because we integrated with our CERT team. We found some valuable insights there.” This team referred to the Dutch NCSC CSIRT Maturity Toolkit [93].

Future Development Goals

Respondents were also asked whether they had identified future development goals for their program. This identified some unique insights.

- *'We make high-quality intelligence products, but we do not register the analysed information in a ticket or knowledgebase; because of this, we risk redoing things or not enhancing on past investigations we performed. '*

- *'There is a need for orchestration for some of our processes; I think that will be one of the next maturity phases; to solidify our processes and make them scalable within an automated knowledge base environment.'*

- *'When our program came together, it started with a fixed and dated delivery requirement. This benefited from creating some pressure behind things and making things develop rapidly. Looking back, we may have been served better if we had been given more time to deliver the service before we had the delivery requirement, as it may have helped us restructure some things. '*

- *'We are working on the holistic sharing of threat information to the entire organization. We want to create a centralized data repository available to all staff.'*

- *'Scalability is the main driver now. We want to increase and maintain quality while scaling up our services.'*

One respondent had made significant investments in their data infrastructure, and they foresaw several notable developments on their roadmap, which they specified as the following.

'We have identified several stretch goals for our future development.

- *We hope to integrate the upcoming CACAO* standard into our data feeds*
- *We will Introduce security orchestration into our CTI program and overall security operations.*
- *We are already drafting standards to which our future data requirements will have to adhere. This allows the CTI team to set requirements before other teams acquire new tools and data that cannot integrate with the CTI initiative.*
- *We will increase the number of detection sensors, both by volume and by integrating new log sources and for these, we will integrate YARA rule detection.'*

*The CACAO standard is further described in Appendix B: Additional CTI Capabilities Mentioned by Individual respondents.

4.4.4 Resulting Level of CTI Maturity Achieved By these Organisations

All eight interviewed CTI teams could effectively consume external intelligence at the end of their program integrations. Five organisations were able to create new intelligence themselves. Two organisations were set up to disseminate their self-made intelligence at a large scale to third parties (either customers or peers). These two organisations were the longest-running teams and the teams with the highest analyst headcount (nine and twelve analysts, respectively).

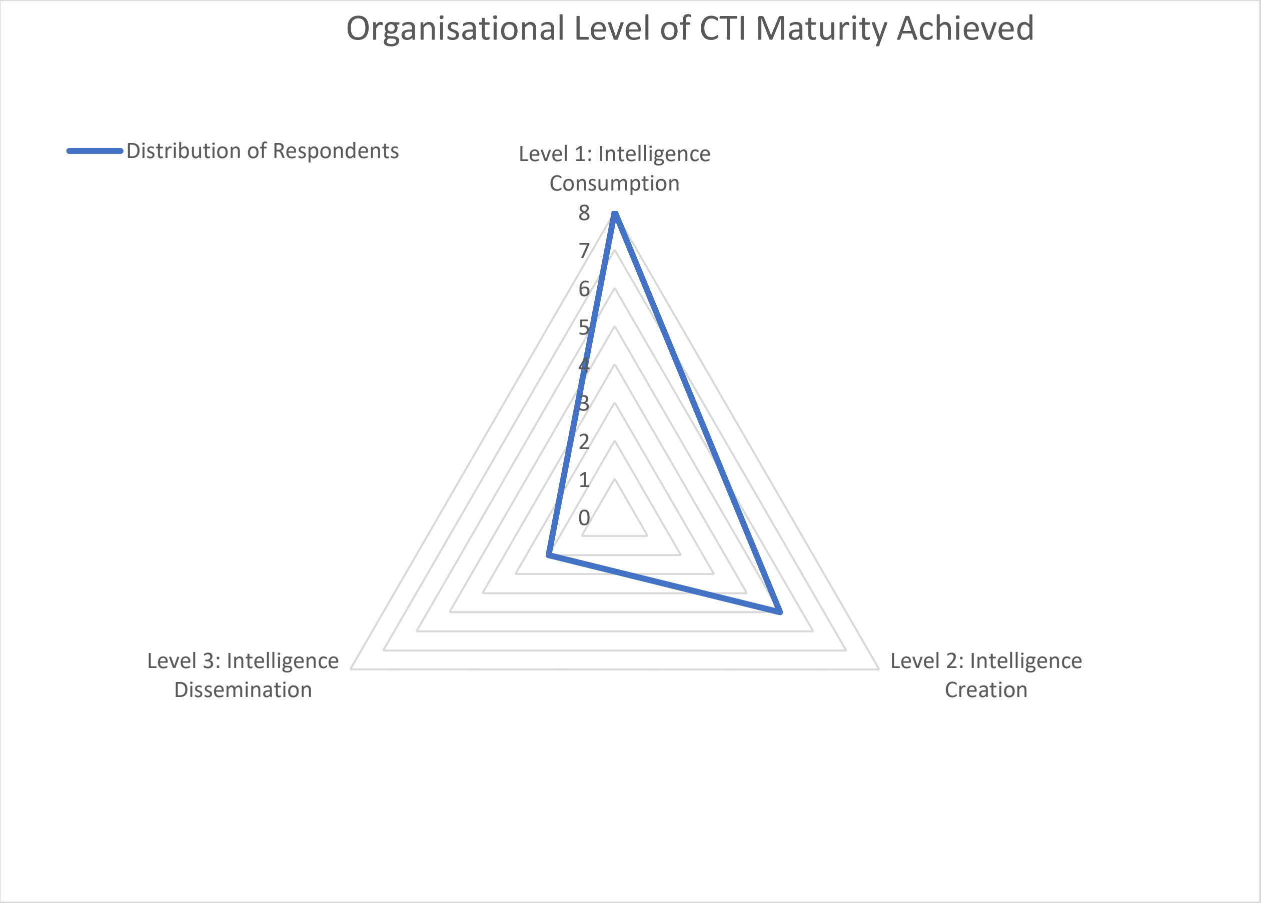


Figure 19 Organisational Level of CTI Maturity Achieved

Chapter 5

Analysis of Interview Findings and Potential Improvements

Contents:

5.1 Section One: People
5.1.1 Staffing issues - Considering Fusion Teams or Dual Hat Analysts
5.1.2. Analytical Cohesion Between Analyst - Introducing Structured Analytics
5.2 Section Two: Processes
5.2.1 Structuring the Intelligence Collection Process
5.2.2 Structuring the Analysis Process
5.3 Section Three: Technology
5.3.1 MISP
5.3.2 Dutch National Cert Resources: The National Detection Network and ISIDOOR
5.3.3 OpenCTI
5.4 Section Four: Information
5.4.1 MITRE ATT&CK Framework
5.4.2 Open-Source Threat Intelligence Libraries
5.4.3 Helping Stakeholders Understand Uncertainty in Intelligence

Chapter four presented the high-level interview findings and compared these between the respondents. This chapter aims to take a more comprehensive look at some specific findings, elaborate on them, and suggest improvements where possible.

These findings will be enriched by leveraging traditional intelligence literature, academic research, or open-source threat intelligence community developments. Specific emphasis will be placed on the open-source tooling that saw significant use by the interview audience. These are primarily novel technologies currently receiving limited exposure in academic research. The subjects will be separated into high-level categories of People, Processes, Technology and Information.

An aggregation of the best practices identified in this chapter is presented in diagram form in chapter 6.3 Closing Remarks and Diagram of Findings. This overview can be considered an alternative strategy to augment current programs or as a starting point for new CTI adoptions based on the interview respondent's best practices.

5.1 Section One: People

This section will elaborate on interview insights relating to human-centric processes. This will describe respondents staffing considerations and how they adopted structured analytical methods.

Respondents were asked about their approach to staffing in the interview questions relating to 4.2.2 Initial Objectives and 4.3.2 Complications Relating to People Factors. This identified that two organisations positioned their CTI analysts in a novel dual-hat position. The usage of Structured Analytics was surveyed in question 4.2.11 Usage of Structured Analytics. This identified ACH as the primary method leveraged by the majority of respondents. ACH will be introduced and applied to the CTI discipline in this section. Lastly, two information structuring methods, MindMap and BowTie, each in use with an individual respondent, will be presented.

5.1.1 Staffing Issues - Considering Fusion Teams or Dual Hat Analysts

Three respondents identified issues recruiting experienced CTI *staff. Two respondents leveraged a novel approach to staffing their CTI team, which will be described here.*

The cybersecurity market is thriving, leading to a shortage of experienced staff, specifically in the more specialized cybersecurity fields such as CTI [96] [97]. This dissertation does not aim to comprehensively analyse or resolve this issue; however, the approach taken by two interview respondents was interesting because they leveraged dual-hat positions for the CTI team or foregone distinguishing the CTI position altogether.

- One respondent had assigned two analysts with a dual hat position to the CTI team. These analysts originated from the SOC, where they work as senior analysts. However, they would alternate between working for the SOC and the CTI team. This team identified their CTI operations as successful. The dual hat position was identified as a benefit for cross-training and integrating between the two teams, which aligned with their primary objective of CTI serving the SOC as the main stakeholder.

- Another respondent had foregone the distinction of CTI analysts altogether and instead trained all the analysts that were part of their CERT (a total of 12 full-time employees) in the CTI process. All CERT and forensic staff were expected to participate in CTI activities and leverage the CTI methodologies when performing their investigations. This approach was deemed to be very successful for this organization. This synergy was also described in a conference talk for ENISA by Ing. Selene Giupponi. She described the synergy that can be achieved involving forensic expertise and cross-training forensic analysts into the CTI discipline [98].

The above is provided as a novel insight, and more analysis is required to verify these observations. However, there does appear to be a conceptual overlap between the forensic disciplines and CTI. Additionally, the dual hat and merged solutions above are similar to the concept of intelligence fusion and may help smaller organizations staff their CTI team appropriately.

Based on this insight, it appears beneficial for CTI organisations that struggle with staffing to consider the above two approaches. They may also benefit from consulting specific intelligence literature on Intelligence Fusion to further solidify this integrated approach [99].

5.1.2. Analytical Cohesion Between Analysts – Introducing Structured Analytics

Structured analytics are processes and methodologies to perform repeatable, unbiased intelligence analysis. A heuristic for this is "**Thinking about thinking**". It is meant to provide the analyst with a framework to distance their personal bias from the factual observation and provide a more neutral analysis assessment. Having structured analytical processes embedded in a CTI team can help promote objective analysis amongst multiple analysts from different backgrounds and lead to analytically rigorous and repeatable analysis. We will first introduce the traditional ACH method, developed by Richard Heuer [99]. After this traditional interpretation, we will reinterpret this methodology to make it feasible for application in the CTI domain. Lastly, we will describe two additional analytical methods mentioned by two respondents.

Traditional ACH usage

Seven respondents were aware of the structured analytical technique of 'analysis of competing hypotheses' (further abbreviated to ACH)[14], [26]. However, only three organizations have leveraged ACH in their program, and all three are no longer using ACH actively due to the time-intensive nature of this method.

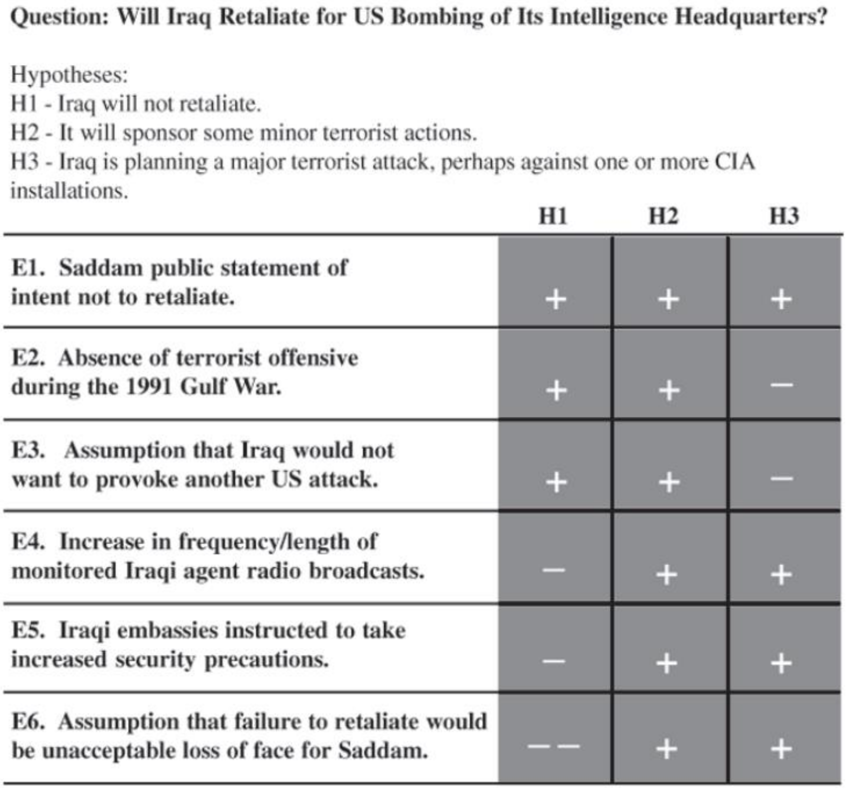
The complexity of producing consistent analysis in teams involving a variety of analytical backgrounds was also identified by Richard 'Dick' J. Heuer. Heuer developed several structured analytical techniques to help reduce personal bias and objectively compare intelligence hypotheses originating from different domains or backgrounds. These techniques were presented in his book 'The Psychology of Intelligence Analysis'[26]. This book is now available in the public domain through the library of the United States Defense Tactical Information Center; [100].

ACH follows an 8-step process. The following is an ad verbatim citation from Psychology of Intelligence by Richard J. Heuer [26] (page 95).

1. *Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.*
2. *Make a list of significant evidence and arguments for and against each hypothesis.*
3. *Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence and arguments- that is, identify which items are most helpful in judging the relative likelihood of the hypotheses.*
4. *Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.*
5. *Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove the hypotheses rather than prove them.*
6. *Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.*
7. *Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.*
8. *Identify milestones for future observations that may indicate events on taking a different course than expected.*

Following the above process can create a competition between the plausible hypotheses to see which ones stand up to analytical scrutiny and most likely align with the available information. The remaining hypotheses that have not been disproven can be further assessed and graded to assess the most likely candidate. On ACH, Heuer concedes, *"It will not always yield the right answer, but it can help analysts overcome cognitive limitations"* [26].

In his book 'The Psychology of Intelligence Analysis', Heuer provided the table below as an example of how the ACH process would assess foreign intelligence relating to the Iraq war [26].



Question: Will Iraq Retaliate for US Bombing of Its Intelligence Headquarters?

Hypotheses:
H1 - Iraq will not retaliate.
H2 - It will sponsor some minor terrorist actions.
H3 - Iraq is planning a major terrorist attack, perhaps against one or more CIA installations.

	H1	H2	H3
E1. Saddam public statement of intent not to retaliate.	+	+	+
E2. Absence of terrorist offensive during the 1991 Gulf War.	+	+	−
E3. Assumption that Iraq would not want to provoke another US attack.	+	+	−
E4. Increase in frequency/length of monitored Iraqi agent radio broadcasts.	−	+	+
E5. Iraqi embassies instructed to take increased security precautions.	−	+	+
E6. Assumption that failure to retaliate would be unacceptable loss of face for Saddam.	− −	+	+

Figure 20 ACH Example Richard J Heuer, Psychology of Analysis [26]

Lightweight ACH Usage

Incident driven tactical CTI is often performed under time pressure. The compilation of several hypotheses and their comparison is an activity that is likely to take several hours. Because of this ACH was discounted by the interview respondents when used for tactical CTI activities.

Traditional ACH is an extensive process that does not restrict itself to specific questions. Applying ACH to a technically constrained operational environment such as tactical level CTI will likely see the re-use of many hypotheses and variables. Because of this, it may be considered to compile pre-filled hypotheses for likely scenarios before they manifest themselves.

As a case study, a pre-filled ACH matrix for the investigation of malware detection is provided on the next page. Organizations could augment this by creating similar ACH matrixes for most incident types they are likely to encounter. This will place the majority workload of performing ACH analysis beforehand and require only a modification or update when a suitable situation arises.

Suggestions for the ACH matrixes to be developed pro-actively could be:

- Insider Threat Scenario
- Data Leakage
- Inappropriate transfer of financial funds
- DDOS on organisation assets

Alternatively, any other threat that is deemed relevant to the respective organisations.

Lightweight ACH for CTI Investigations on Malware Infection

The below example can be considered a starting template to perform an ACH exercise for a common malware-related incident response scenario. It is inspired by the CTI tailored ACH method described by Caitlyn Huey at the FIRST CTI Conference in 2019 [101].

In this example, C2 is the Command-and-Control channel (IP or DNS) communicating with the potential malware sample.

ACH for Malware Infection on the internal environment

	H1	H2	H3
C2 IP of origin has multiple simultaneous users, including legitimate traffic	-		+
C2 IP is identified as active botnet traffic	-	-	++
C2 IP was historically botnet traffic			+
The malware encountered is in common use, readily available		+	
The malware is novel or unique	++	-	--
The malware is simplistic	-		++
The malware and tools were sophisticated	++	-	--
Initial targeted asset is perimeter facing and opportune	-	+	++
Initial targeted asset is High Value (due to data or positioning)	+	++	
The targeted user is generic (no significant value)	-	+	++
The targeted user is opportune (high rights individual, VIP)	++	+	
Subsequent activities such as lateral movement were identified post-infection	+		-
Activities happened at a rapid pace (scripted)	+	-	+

Table 3 Proactive ACH Table for Malware Infection

Hypotheses

H1: Incident was targeted

H2: Incident was opportunistic but manual

H3: Incident was opportunistic and automated

Scoring

--	Very Inconsistent
-	Inconsistent
'	Neither consistent nor inconsistent
+	Consistent
++	Very Consistent

Alternative Structured Analytical Techniques

Individual respondents identified two additional analytical techniques. These are the MindMap, and the Bowtie Method described briefly here.

Mind Mapping

Mind mapping is a method for graphing the relations between subjects in a diagram. Though not strictly a structured analytical technique, it does serve to organize information and could be a valuable method for some teams or analysts [98], [99]. The aim is to visualize and organise the information to make it easier to understand and remember.

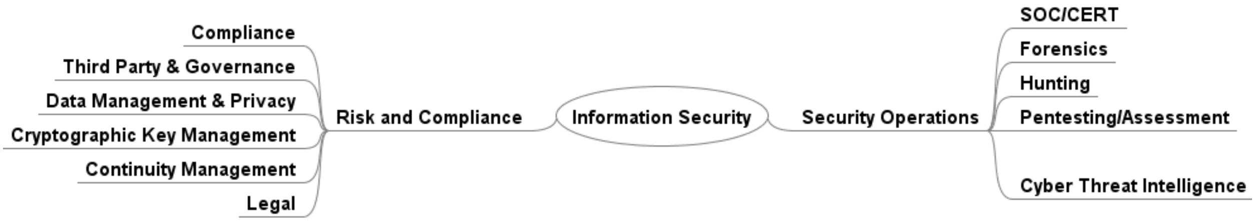


Figure 21 Mind Map Example for the CTI Domain

Bow Tie Method

Like Mind Mapping, the Bow Tie Method is a diagram that helps order information. The respondent leveraged it to state several iterative questions on whether a piece of information was appropriate for their collection plan.

The respondent that leveraged the Bow Tie Model described their process as the following. "*When we identify something in the public domain/media, we find sources, but we want to distil the initial article and event that originated this. To help our collection process, we re-interpreted the Bow-Tie Model. Our intelligence team helped define eight iterative questions that our collection analyst can apply to filter the incoming information and define the actual value. For example, questions like: Are we dealing with recent activity, is this targeting our country, is this targeting a peer organization? In other cases, we defined technical questions such as 'Can this be remotely exploited, does this operate on root or administrative level access, can this propagate automatically (like a worm)'.*

The process described by the respondent broadly aligned with the conceptual steps of the Bow-Tie method but was more practically driven.   The Bow tie is known for several usages, including risk management, as it helps identify relations between events and outcomes [94], [102].

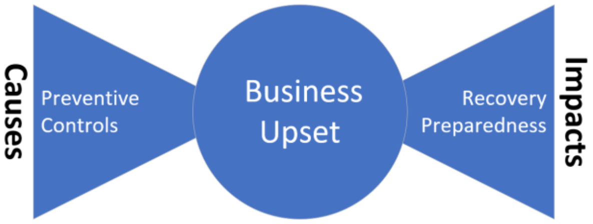


Figure 22 Bow Tie Example On Risk Management.

5.2 Section Two: Processes

This section will elaborate on interview responses that related to processes. Respondents were asked about their internal processes in question 4.3.3 Complications Relating to Process Factors. The interviewed organisations' approaches to processes varied. Only one of the organisations adhered to the traditional intelligence approach to designate separate teams for the Collection and Analysis phases. The other organisations had a less strict designation of these phases but did incorporate processes such as a four-eyes approach to intelligence creation (with internal peer reviews) and a workflow distinguishing Raw and Finished Intelligence deliverables as separate products. Additionally, two respondents leveraged the Intel471 CU-GHIR framework to structure their intelligence creation which will also be presented here.

5.2.1 Structuring the Intelligence Collection Process

- One of the respondents had a dedicated collection analyst assigned to the collection process. By leveraging the bow-tie model, this analyst had a structured approach to filter the incoming information.
- Two respondents identified that the collection process was a natural part of the analysis process for their analysts within their operations. As such, they did not distinguish a separate phase for this.
- Two respondents referred to Intel 471's CU-GHIR framework as the basis for their collection requirements, presented here [81], [103].

As introduced in chapter 2.3, The Intelligence Lenses of Collection, Processing and Analysis, In the traditional process of intelligence collection, the first step is to develop a collection plan. [30], [34]. Two respondents leveraged Intel471's CU-GHIR framework to structure their collection process, which will be described on the following page.

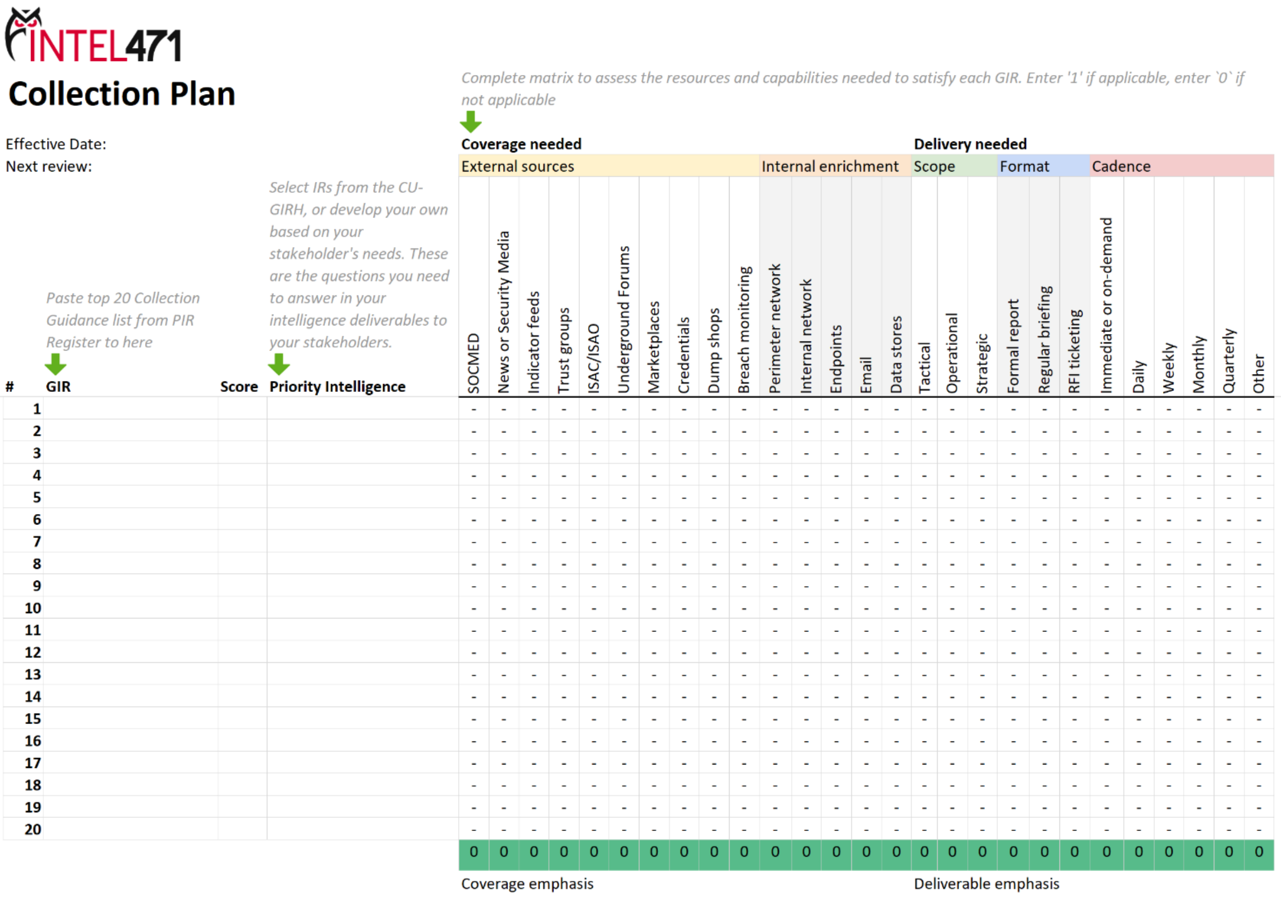
Intel471 – Criminal Underground General Intelligence Requirements Handbook

Intel 471 is a premium cyber threat intelligence provider with a specific emphasis on threat actor intelligence (intelligence specialized in the attribution of actors and their malware [103].

The Intel 471 Cyber Underground General Intelligence Requirement Handbook (CU-GHIR) is a framework specifically developed to provide organizations with a comprehensive methodology to perform CTI collection and analysis.

This involves a collection matrix that can help structure the collection process and select reliable sources for inclusion. The framework also provides specific worksheets that can support the initial phases of identifying stakeholders and setting PIR's and SIR's that will lead to the collection process [81].

The GHIR framework is available for free, but only by specific request. Approval was provided by Intel471 to cite the GHIR framework and include the below example of the Sample Collection Plan. The free CU-GHIR framework can be requested here.



INTEL471

Collection Plan

Effective Date:
Next review:

Complete matrix to assess the resources and capabilities needed to satisfy each GIR. Enter '1' if applicable, enter `0` if not applicable

Paste top 20 Collection Guidance list from PIR Register to here

Select IRs from the CU-GIRH, or develop your own based on your stakeholder's needs. These are the questions you need to answer in your intelligence deliverables to your stakeholders.

				Coverage needed															Delivery needed											
				External sources										Internal enrichment					Scope			Format			Cadence					
#	GIR	Score	Priority Intelligence	SOCMED	News or Security Media	Indicator feeds	Trust groups	ISAC/ISAO	Underground Forums	Marketplaces	Credentials	Dump shops	Breach monitoring	Perimeter network	Internal network	Endpoints	Email	Data stores	Tactical	Operational	Strategic	Formal report	Regular briefing	RFI ticketing	Immediate or on-demand	Daily	Weekly	Monthly	Quarterly	Other
1				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
2				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
5				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
7				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
8				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
9				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
10				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
12				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
14				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
15				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
17				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
18				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
19				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
20				-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
				0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
				Coverage emphasis															Deliverable emphasis											

Figure 23 Intel471 GHIR Collection Plan [81]

5.2.2 Structuring the Analysis Process

Distinguishing Raw Intelligence and Finished Intelligence

None of the respondents leveraged a formal process to finalize their CTI intelligence products. The discipline of traditional intelligence does specify a distinction regarding the finalization of intelligence deliverables. The phrases ‘Raw Intelligence’ and ‘Finished Intelligence’ are commonly used to distinguish between intermediate analysis products and finalized intelligence[34]. Clark and Lowenthal defined the following definitions for these categories, which also apply to our purposes.
“Raw Intelligence is the end product of intelligence collection.”
“Finished Intelligence is the term customarily applied to the product of all-source analysis.” [104].

The above definition hinges on applying all-source analysis, including multiple analytical disciplines. At this moment, with the identified average CTI team sizes being less than seven, it is unrealistic to expect the concept of multi-disciplinary all-source intelligence cells to be feasible for CTI teams that are primarily set up for tactical-technical level intelligence. However, I assert that the concept is still valid and can be applied to small scale CTI teams in another way.

To develop an analytically rigorous repeatable process, it may be recommended to require the assessments of a minimum of two analysts to align before an intelligence deliverable should be deemed ‘Finished Intelligence’. This requirement also translates to a ‘Four Eyes’ principle, commonly used in other fields, often relating to delegation responsibilities.

Introducing the Four-Eyes Principle to CTI Analysis

The Four-Eyes principle is a simple fundamental concept whereby the validation of at least two people is required before a decision is made [105]. The Four-Eyes principle is found in many different applications, including processes where a high degree of responsibility is taken. For example, financial institutions leverage this to transfer a certain amount of money, requiring supervisory approval after exceeding a certain threshold. A similar quality requirement and second validation can also be implemented to distinguish between raw and finished intelligence in the following way.

Raw Intelligence: The initial stage of any intelligence deliverable, when it is analysed and compiled by a single analyst. Raw intelligence can help serve investigations that are low in complexity or time-sensitive. In these examples, a superficial analysis may be sufficient to serve the stakeholder. An example can be the technical enrichment of an indicator of compromise for internal distribution to the SOC.

Finished Intelligence: An extensive analysis such as a peer-reviewed report after having passed four-eye approval. Examples can be a threat landscape or a quarterly overview of trends. This will, at the minimum, involve two analysts and a formal review process before it is deemed publishable.

The specific organisational preference can decide how to implement the four-eyes principle. For some organizations, this may become an informal validation by another analyst. In some more rigorously structured workflow-based organisations, it may be a technical process whereby the raw intelligence products are sent to a review queue for review and approval. Some CTI Threat Intel Platforms (MISP, for example) are already set up with internal workflows that help facilitate this process[86].

5.3 Section Three: Technology

The interviews identified several preferences relating to CTI technology. Specifically, interview question 4.2.10 CTI Tooling Known and Leveraged by Respondents identified the technological solutions leveraged by our respondents. This identified three technologies in significant use.

All eight respondents leveraged MISP. All three government respondents leveraged the 'National Detectie Network', and two of the respondents had used OpenCTI. All three of these technologies are non-commercial, and any organization can use both MISP and OpenCTI without requiring significant investment. To describe the purpose of these solutions, a brief description of these technologies will be described in this section. Some technologies received only individual mentions, and these will be presented in Appendix B: Additional CTI Capabilities Mentioned by Individual Respondents.

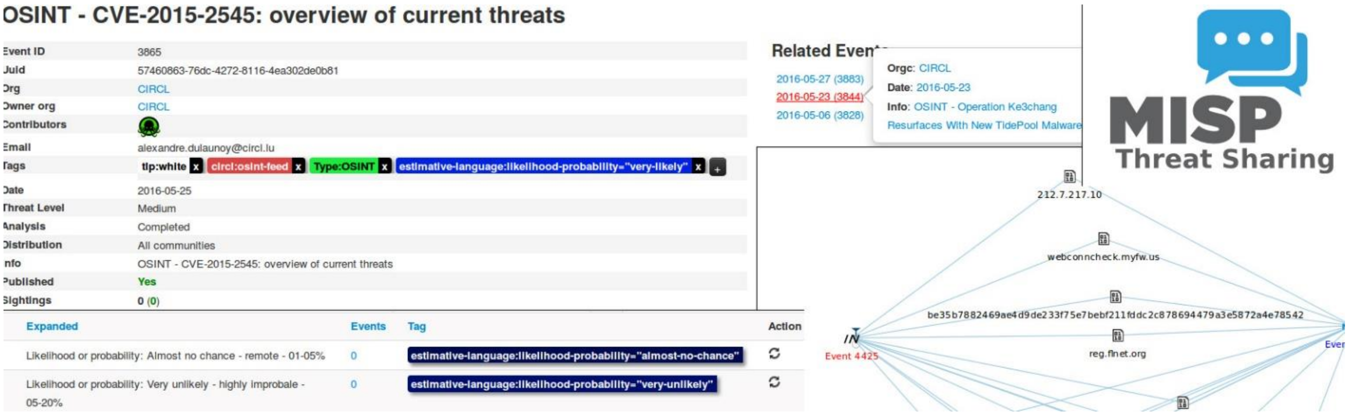
5.3.1 MISP

All identified respondents leveraged the MISP platform, with three of them defining it as the primary CTI tool with which they started their initiative. This chapter is meant as a high-level introduction to the platform and its capabilities.

The Malware Information Sharing Platform (hereafter referred to as MISP) is an open-source (GNU Licensed) threat intelligence platform developed by the Luxembourg Cert, CIRCL.LU [106]. The program was set up to be open to other contributors, and notable contributors are the NATO cert NCIRC [107] and the European Union cert CERT-EU [108]. The MISP program is co-financed by the European Union.

The MISP project was started in 2012 to provide an open and accessible sharing platform for both public and private actors. Access is provided to subgroups, and information is classified and distributed according to the Traffic Light Protocol [56].

Information in MISP is distributed by subscribing to threat intelligence feeds which contain STIX formatted data containing technical indicators related to intrusions. Some feeds are open source and free of use. Other (more sensitive feeds) are restricted and require invitations. The platform has several graphing options that can aid in correlating event data. Information can also be enriched with third-party datasets, further increasing the fidelity of the data.



OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Uuid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability="very-likely" x +
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbale - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	

Related Events

2016-05-27 (3883)
2016-05-23 (3844)
2016-05-06 (3828)

Orgc: CIRCL
Date: 2016-05-23
Info: OSINT - Operation Ke3chang Resurfaces With New TidePool Malware

Figure 24 MISP Overview screen [106]

MISP integrations

There is a sizable development community building integration with MISP. MISP threat data can be manually exported or automatically fed to other systems, including signature formats such as Suricata, Snort, Bro, OpenIOC and several XML and JSON formats. This eases integration of threat intelligence data into perimeter network logging devices, which can aid in detecting compromises or even serve to automatically fill detection or block lists of perimeter devices.

MISP Communities

There is a vibrant community of MISP sharing circles. MISP states that they have more than 1200 MISP communities, which serve a total of more than 4000 active users [86].

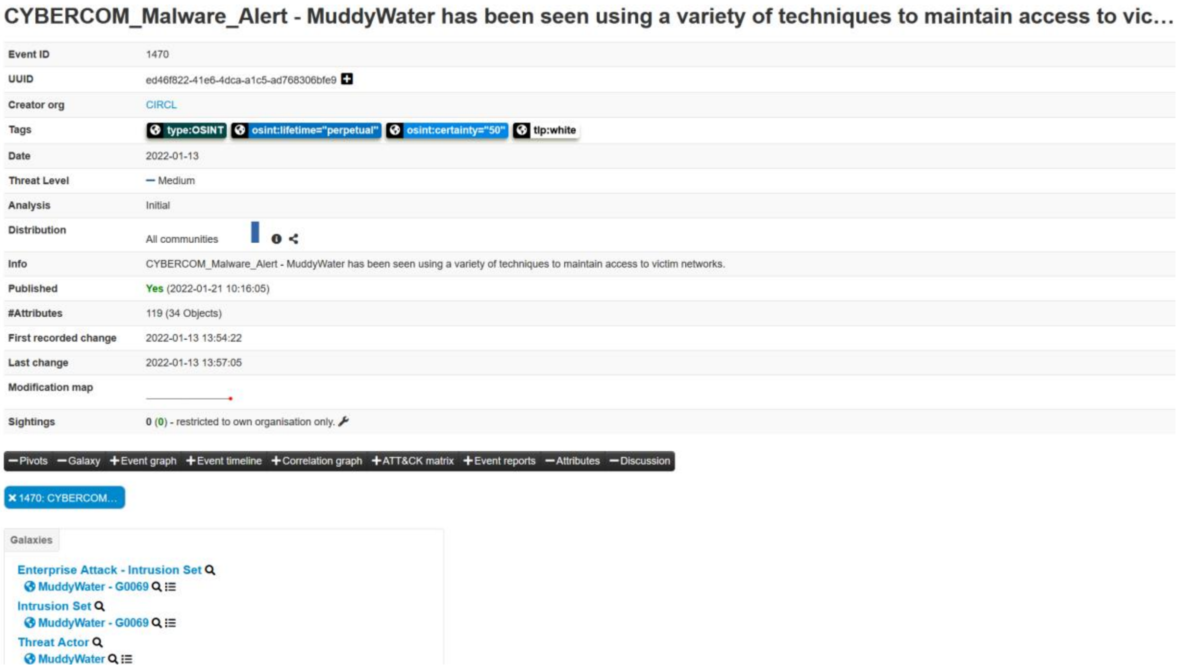
Setting up and operating a MISP environment is a zero-cost initiative that can yield significant returns. The value can increase exponentially if the organization also pro-actively networks with peer organizations and each participant integrates their sightings into a centralized community feed.

Large scale MISP communities are present for many sectors, for example:

- Financial services
- Law Enforcement / military communities
- International organizations and non-profits
- Trusted groups of researchers

To stimulate development on MISP CIRCL.LU organizes MISP Hackathons where participants work on the MISP platform and offer improvement suggestions [87].

Due to the open-source nature and lack of licensing fees, any organization can start using MISP. There are also many options to set up advanced integrations using third-party tooling such as Maltego, which is set up for MISP data integration or connecting to Suricata or Zeek to generate detection rules automatically.



CYBERCOM_Malware_Alert - MuddyWater has been seen using a variety of techniques to maintain access to vic…

Event ID	1470
UUID	ed46f822-41e6-4dca-a1c5-ad768306bfe9
Creator org	CIRCL
Tags	type:OSINT osint:lifetime="perpetual" osint:certainty="50" tlp:white
Date	2022-01-13
Threat Level	— Medium
Analysis	Initial
Distribution	All communities
Info	CYBERCOM_Malware_Alert - MuddyWater has been seen using a variety of techniques to maintain access to victim networks.
Published	Yes (2022-01-21 10:16:05)
#Attributes	119 (34 Objects)
First recorded change	2022-01-13 13:54:22
Last change	2022-01-13 13:57:05
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Enterprise Attack - Intrusion Set
MuddyWater - G0069
Intrusion Set
MuddyWater - G0069
Threat Actor
MuddyWater

Figure 25 MISP Event Entity Example [106]

5.3.2 Dutch National Cert Resources: The National Detection Network and ISIDOOR

All three Dutch Government respondents identified the 'Nationale Detectie Netwerk' as one of their objectives and a primary stakeholder to their CTI program. Four respondents participated in the bi-annual ISIDOOR exercise organized by the Dutch NCSC, and the remaining four respondents were aware of this exercise.

The NDN, which stands for 'National Detection Network' [80], is an information-sharing collaborative operated by the Dutch National Cert NCSC[53]. The project collaborates with the Dutch General Intelligence organizations AIVD [109] and the Military Intelligence Service MIVD [110]**.** The NDN has been in operation since 2011, and its customers are the Dutch government and selected organizations which are deemed to be part of the Dutch critical infrastructure [15].

The NDN is also a technical sensor network, whereby sensors are deployed across the networks of its government members so that centralized threat detection can take place. Due to non-competition laws, the sensors cannot be distributed to the critical sector partners. However, they can receive the threat intelligence data separately and implement detection capabilities themselves.

Through this integration, members can choose to share the sightings with the NDN so that centralized correlation and analysis can occur. In some cases, this can lead to an incident response activity from the NCSC's National CERT team [111].

Outside of the sensor platform itself, the NCSC also leveraged the NDN as a community to reach out to the participants and organize meetings to collaborate on best practices, lessons learned and discuss their experience in a confidential environment.

Though the NCSC is a Dutch initiative and only open to selected participants, it can serve as an example for a higher-level sharing initiative within organizations and governments.

Exercise ISIDOOR [112]
ISIDOOR is a bi-annual cybersecurity exercise facilitated by the Dutch National Cert, which in 2021 involved 1500 individuals from 96 organizations. It also involved the members of the NDN. Four interview respondents had participated in the ISIDOOR exercises. These are all three government respondents and one respondent who was part of the Dutch critical infrastructure, thus in scope for ISIDOOR participation. Despite not participating directly, the other four respondents were also aware of ISIDOOR. The objective of ISIDOOR is to provide a cyber security scenario that tests not only technical response capabilities but also involves strategic level objectives for policymakers and emphasizes the moment collaboration should overreach the organization and can become coordinated through the NCSC.

An English language keynote presentation from the National Cert is found here titled 'CTI for CERT's, the Dutch Approach '. It details how the Dutch government leverages CTI [113].

5.3.3 OpenCTI

Two respondents had tested the OpenCTI platform, and one respondent still has OpenCTI in active use. Because of this, a description of this Open-Source Threat Intelligence will be provided.

The OpenCTI project [114]was started in 2018 in collaboration with The French National Cert, ANSSI [115] and the EU Computer Emergency Response Team EU-CERT [108]. Its objective was to help develop and facilitate the ANSSI's collaboration with its constituents and partners.

To promote this technical collaboration, ANSSI (in collaboration with EU-CERT) developed a threat intelligence platform that operates as an open-source knowledge management database to create and share threat intelligence data. Once the platform was past initial conception the tool was also released to the public domain, in collaboration with the non-profit Luatix organization [116].

OpenCTI provides a graphical web-based interface that presents the underlying data. The datasets can be provided by subscribing to community shared threat intelligence feeds, including feeds originating from MITRE or MISP. The platform also has a graphing engine to identify correlations of data points.

There is a wide range of data feed integrations supported, most notably MISP, MITRE ATT&CK, The CVE (vulnerability) database and several more, which can be found here.

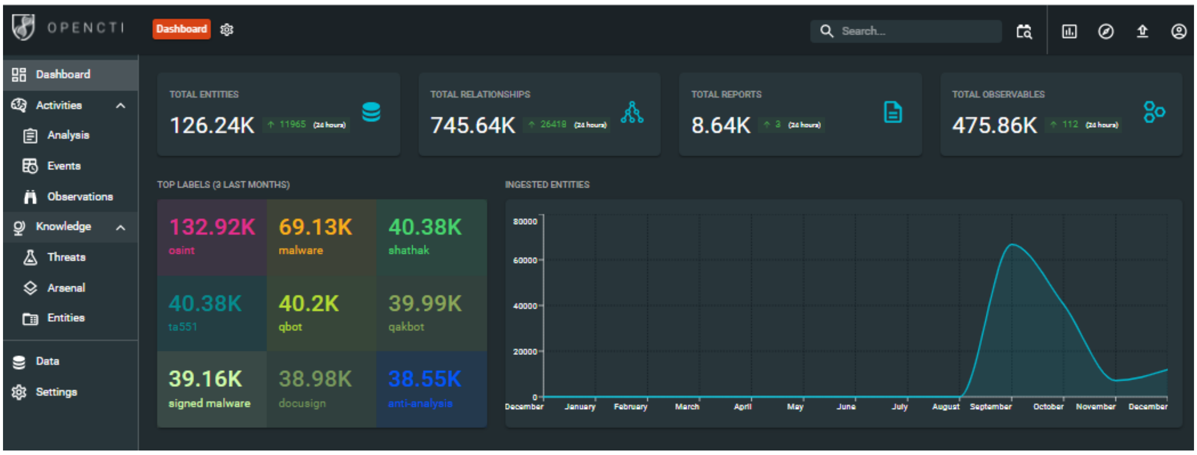


Figure 26 OpenCTI Graphical Dashboard [117]

A test instance of OpenCTI is available here; the development team provides this to allow visitors to try the platform. The Github for OpenCTI provides all the code required to run an OpenCTI instance. https://github.com/OpenCTI-Platform

OpenCTI offers some similar capabilities as MISP. However, MISP has seen extended development and invested more in the technical threat feed environment and sharing community. OpenCTI has more modern graphing technology, and its graphical user interface looks more modern and intuitive. Due to OpenCTI supporting data ingestion from MISP and both platforms being open source and free to use, they can be considered complementary. Integrating MISP data in OpenCTI combines the best of both platforms.

5.4 Section Four: Information

Identifying how organizations leverage information and intelligence was a by-product of the overall interview process, with insights identified in several interview questions and summarized in 4.2.1 Summary of the Interview Responses. Respondents identified several public methodologies and data sources that were of value to their programs, these will be presented here.

Multiple respondents identified difficulties in positioning and promoting their intelligence initiative within the organisation, and this was primarily identified in question 4.4 Interview Findings after CTI Adoption. Similarly, the degree to which designated stakeholders were unaware of what intelligence meant was identified in question 4.3.2 Complications Relating to People Factors; because of this, an introduction will be provided on conveying the uncertainty factor of intelligence to a new audience.

5.4.1 MITRE ATT&CK Framework

The MITRE ATTC&CK Framework (Adversarial Tactics, Techniques, and Common Knowledge) was actively used by five respondents, and two other respondents were also well aware of this framework.

The non-profit research organization MITRE is the custodian of the ATT&CK Framework [61], [91]. The framework is created as a collaborative initiative with quality control being provided by MITRE. This cyber security taxonomy describes the phases and activities of a cyber compromise in specifically defined categories.

The framework has several matrixes, with the Enterprise Matrix being the most popular (and extensive). Other matrixes are specific to Mobile device threats and Industrial Control System environments.

The ATT&CK matrix has designated several distinct phases, which are identified on the top row of the model. These phases are called 'tactics' but can be interpreted as a specific phase in a cyber-attack. From a practical perspective, the framework broadly follows the progression of the Lockheed Martin Kill Chain described in chapter 3.3, The Lockheed Martin – Cyber Kill Chain, the notable difference being that the ATT&CK framework presents this progression horizontally. MITRE added more granularity and defined additional intermediate phases that do not exist in the simplified Kill Chain Model. Defenders can use this taxonomy in many ways.

ATT&CK as a Knowledgebase

MITRE has created a threat intelligence library based on the activities observed in past compromises. This provides an extensive and well-referenced overview of open-source threat intelligence sources. The library is kept up to date through community participation.

The framework's core is based on the specific ATT&CK techniques. The underlying articles also refer to potential mitigating activities that help defenders resolve potential vulnerabilities for each described technique. The library also provides a threat actor section to identify specific techniques leveraged by the identified actors, which helps organisations perform analysis based on their specific adversaries of interest. Additionally, the library has an extensive chapter on specific attack tools and malware, which are also mapped to their corresponding techniques and capabilities.

ATT&CK Navigator to identify exposure to actor capabilities, and defensive potential

One popular use case for the ATT&CK is for defenders to identify their primary threat actors of concern (This can be derived from intelligence PIR's and SIR's). For each identified technique leveraged by the threat actor, an analyst can mark or colour one of the boxes. This creates a heatmap of the actor's tools, techniques, and capabilities to aid overall analysis and comparison.

MITRE created the ATT&CK Navigator tool that allows users to generate these overlays and store them in several data formats to aid in its operation.

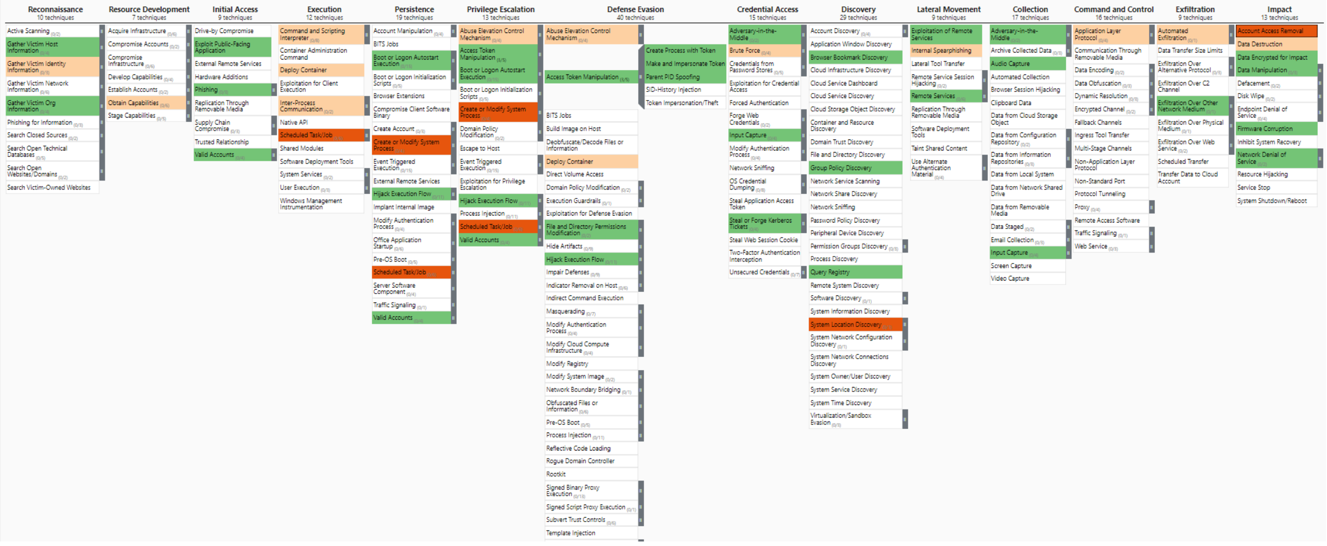


Figure 27 Navigator view of the MITRE ATT&CK model [118]

Rabobank DeTTECT |Framework Enhancement on Navigator

The Rabobank Cyber Defence Center developed the DetTTECt platform, an open-source initiative aimed to enhance the usability of the MITRE ATT&CK Navigator. The resulting product can be interpreted as a 'heatmap' on potential areas of high risk where mitigations are necessary. Unlike the navigator tool, the DeTTECT tool can derive metrics from third-party data to operate as a real-time heatmap fed with relevant telemetry originating from other systems. In this operation, it can even serve as a real-time dashboard to identify the current security status of defensive capabilities [119].

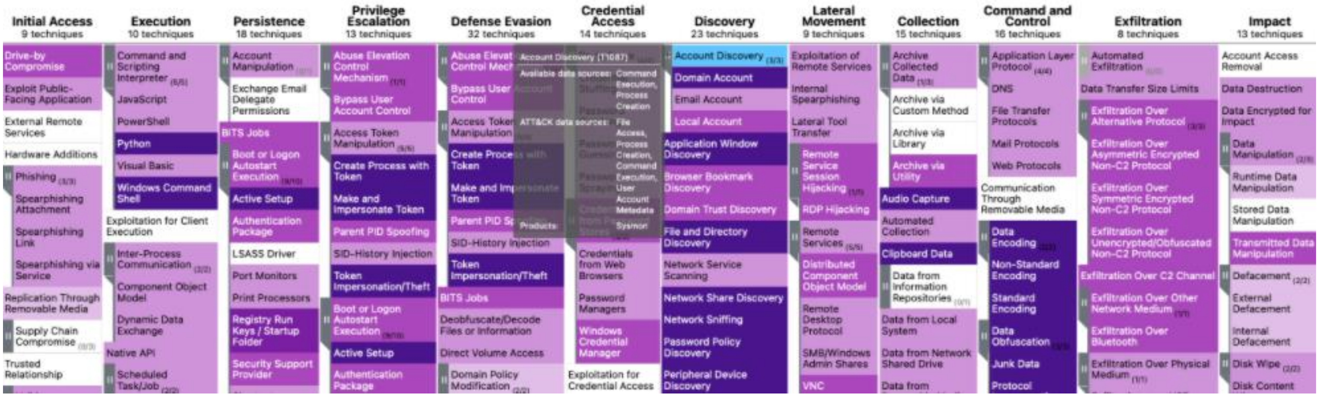


Figure 28 DeTTECT Framework [119]

5.4.2 Open-Source Threat Intelligence Libraries

Several respondents identified public data repositories as valuable sources of open-source intelligence content that fed into their CTI program. Since these sources are freely accessible in the public domain, they will likely benefit other organisations interested in CTI.

ThaiCert Threat Group Cards: A Threat Actor Encyclopedia

The Taiwanese Cert has published an extensive library with threat actor groups known through open source references. This is one of the more comprehensive public threat actor libraries [120]. Each actor has a specific profile describing its origins and observed activities.

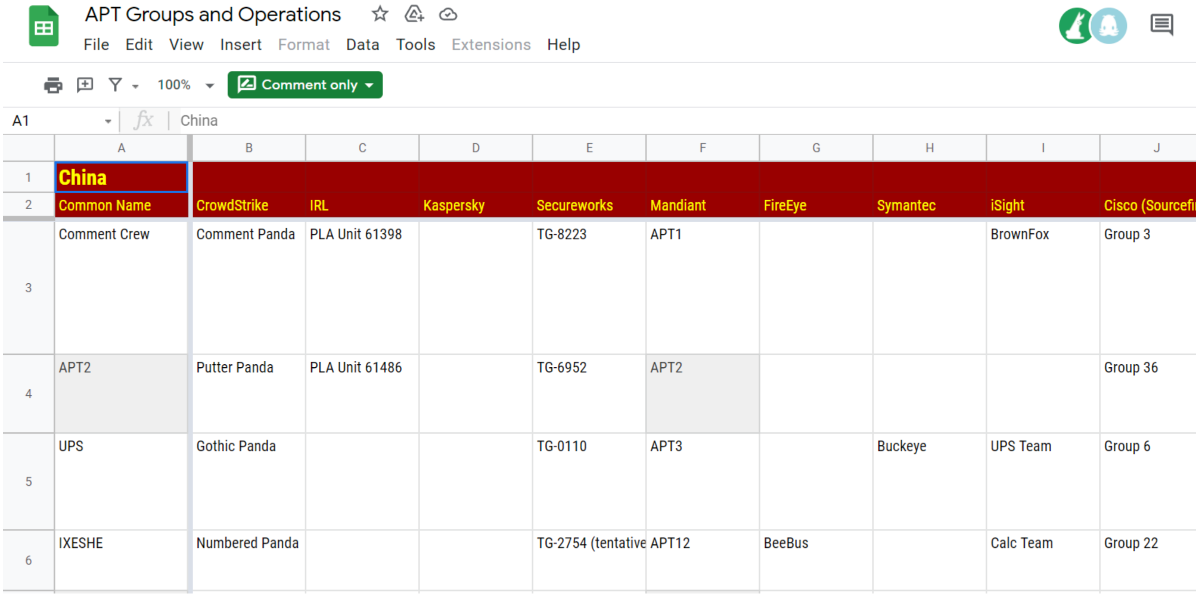
MITRE websites

As stated in the previous chapter, the MITRE ATT&CK library also holds a significant amount of context on threat actors. One significant capability of the ATT&CK library is that content is cross-referenced within the platform and sorted by malware or malicious actors.

APT Groups and Operations

This online 'Threat Tracking' spreadsheet is an open-source community initiative to collaborate on a single overview to identify the different pseudonyms used for the various threat actors. In doing so, it briefly identifies recent observations of operations, identified tools, techniques and procedures and, where possible, victimology.

It is highly recommended not to access this sheet with a browser session with an authenticated Google account signed in. It will identify your Google account to other viewers of the document. The collaborative spreadsheet can be found here: https://apt.threattracking.com/



	A	B	C	D	E	F	G	H	I	J
1	China									
2	Common Name	CrowdStrike	IRL	Kaspersky	Secureworks	Mandiant	FireEye	Symantec	iSight	Cisco (Sourcefi
3	Comment Crew	Comment Panda	PLA Unit 61398		TG-8223	APT1			BrownFox	Group 3
4	APT2	Putter Panda	PLA Unit 61486		TG-6952	APT2				Group 36
5	UPS	Gothic Panda			TG-0110	APT3		Buckeye	UPS Team	Group 6
6	IXESHE	Numbered Panda			TG-2754 (tentative	APT12	BeeBus		Calc Team	Group 22

Figure 29 APT Groups and Operations Spreadsheet [121]

5.4.3 Helping Stakeholders Understand Uncertainty in Intelligence

Two stakeholders identified complications in creating visibility for their team in an organization that was not used to the intelligence process. To support intelligence adoption, a method will be described to communicate the uncertainty of intelligence to stakeholders that are new to this domain.

Intelligence intends to predict potential future events. In doing so, analysts work by defining several hypotheses. Some of these hypotheses may appear likely, as they can describe the long-term continuation of an ongoing event. However, some events may seem very unlikely, but their occurrence may severely negatively impact our stakeholders. This follows the lines of the information security risk analysis process, which works by the premise of 'Risk = Likelihood * Impact'. When considering the resulting risk value, it is our organisational or personal risk appetite that decides whether these risks are acted on or not.

Extreme outliers in intelligence, Black Swan Events

The extreme rare outliers can be very significant for our stakeholders but are almost impossible to predict effectively. These events are often coined 'black swan event' due to their rarity but extreme impact [122].

Notable historic black swan events were the United States terrorist bombings on 9-11. While the occurrence could not be accurately predicted and was at the time considered extremely unlikely, the impact was extremely severe on the following 20 years of geopolitical developments.

Sherman Kent's scale of probability (and estimative language)

Most intelligence stakeholders require intelligence products that are dense and actionable. This means that intelligence analysts cannot present all the underlying hypotheses that led to its creation. However, the analyst may still want the intelligence deliverable to represent the appropriate degree of uncertainty.

Another significant contribution Sherman Kent made to the intelligence field was formalising analytical language to define degrees of uncertainty. To mitigate any confusion between the meaning of estimative language, Sherman Kent came up with an initial scale to provide a quantitative metric for using estimative language [123].

Charles Weiss published a paper on words of estimative probability that compared both Kent's scale and other common analytical assessments from other fields. This is an interesting comparison as it involved Kent's perspective, The DNI (Director of National Intelligence), the IPCC (Inter-Governmental Panel on Climate Change) and jargon in common usage within legal environments. The resulting comparison is provided below [123].

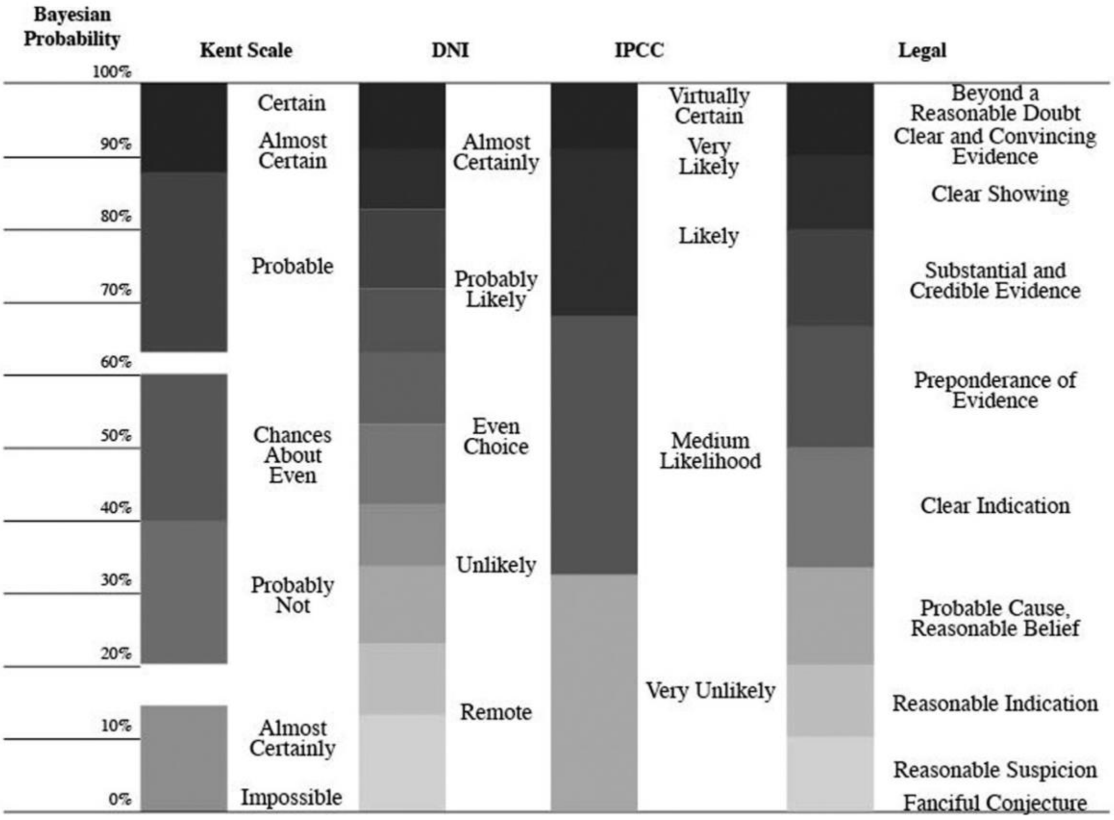


Figure 30 Scales of Uncertainty – Weiss [124]

The above graph is provided as a suggestion; regardless of the scale used, both the intelligence stakeholders and the intelligence analysts must agree about using similar meanings for their words of estimative language. It is recommended to explicitly mention the specific scale used to compile an intelligence deliverable.

The NATO Admiralty standard

The NATO Admiralty standard is a system used to describe the reliability of a source and the level of confidence in the specific piece of intelligence. It does this by designating an alphabetic character to grade the overall reliability of the source. It pairs this character with a number that signifies the degree of confidence our CTI team has in this specific piece of intelligence. For example, an intelligence deliverable can be graded with a rating of A1, implying the source was of the highest level of reliability and that our analysis was able to confirm the truthfulness of the product with completeness. Similarly, an assessment of F6 implies that our analysis has found no basis for evaluating the source's reliability and that our analysis process could not evaluate the validity of the information.

This is a valuable metric because it allows analysts additional granularity to distinguish low-quality information originating from sources deemed highly reliable in the past.

The following two tables are a reproduction of the Source and Information Reliability Matrix, which originates from the United States Army FM2022.3 handbook [125] *in Human Intelligence Collector Operations (Appendix B).*

The description of the table suggests analytical assessments that can be used to assess the appropriate grade for either overall source or specific information reliability.

A	**Reliable**	**No doubt** on the authenticity, trustworthiness or competency; has a history of complete reliability
B	**Usually Reliable**	**Minor doubt** about authenticity, trustworthiness or competency; has a history of valid information most of the time.
C	**Fairly Reliable**	**Doubt** of authenticity, trustworthiness, or competency but has provided valid information in the past.
D	**Not Usually Reliable**	**Significant doubt** about authenticity, trustworthiness or competency but has provided valid information in the past.
E	**Unreliable**	**Lacking** in authenticity, trustworthiness and competency, history of invalid information
F	**Cannot be Judged**	**No basis** exists for evaluating the reliability of the source

Table 4 Evaluation of Source Reliability [125]

1	**Confirmed**	**Confirmed** by other independent sources; **logical** in itself, **Consistent** with other information on the subject.
2	**Probably True**	Not confirmed**; Logical** in itself**; consistent** with other information on the subject.
3	**Possibly True**	Not confirmed; **reasonably logical** in itself, **agrees with some** other information on the subject.
4	**Doubtfully True**	Not confirmed, possible but **not logical** in itself. Agrees with some other information on the subject.
5	**Improbable**	Not confirmed, **not logical** in itself, **contradicted** by other information on the subject.
6	**Cannot Be Judged**	**No basis** exists for evaluating the validity of the information.

Table 5 Evaluation of Information Content [125]

Chapter 6

Conclusion

Contents:

6.1 Conclusion
6.2 Further Research
6.3 Closing Remarks and Diagram of Findings

This chapter will present the conclusion of this dissertation. It will summarise the overall findings and insights identified from the interview audience's CTI implementation experiences. A brief future outlook on the developing domain of CTI will also be provided.

Lastly, the shared lessons learned from our interview audience will be presented in a diagram that presents these findings in a logical implementation order. Organisations considering CTI adoption or wishing to enhance ongoing programs can leverage this to repurpose the best practices identified by the interview respondents.

6.1 Conclusion

The main objective of this dissertation was to explore the experiences of eight Dutch organisations that set up CTI initiatives independently from each other within the last ten years. The motivation for this dissertation came from the initial perception that the field of CTI is still in development and that limited resources are available that describe the implementation of an overall tactical level program. Despite the CTI discipline itself being in fluent development, the teams appeared to have found common ground in leveraging similar strategies to adopt CTI successfully.

- All teams had the primary objective of the CTI initiative serving the SOC/CERT team with tactical/technical level CTI (technical indicator-based intelligence).
- Three organisations also planned for strategic level intelligence ambitions, but tactical level intelligence remained their primary interest.
- There was a significant influence from the Dutch National Cert (NCSC[53]), as all respondents were aware of several of its initiatives. All respondents knew the ISIDOOR bi-yearly NCSC cyber exercise [112].
- All three government respondents were part of the Dutch National Detection Network [80].
- All respondents leveraged the Malware Information Sharing Platform, a free and open-source EU funded CTI platform to disseminate tactical/technical threat intelligence data making it a primary contributor to the CTI programs for these teams [106].
- All respondents were aware of the SANS FOR 578 CTI training course; seven respondents used this to train their analysts; it was the dominant training method [83].

Several complicating factors were identified during the adoption of the program.

- Programs overall did encounter delays in seven cases. Most delays originated from technical integrations such as infrastructure or data (log) source integrations.
- Staffing issues arose due to a shortage of experienced CTI staff. Two organisations that either staffed the CTI team with (forensic) CERT specialists or placed experienced SOC analysts in a dual-hat position partially mitigated this problem.

Regardless of these complications, all eight respondents described their program as successfully meeting their organisational requirements; their (self-assessed) maturity also identified this success.

- All eight respondents' CTI programs were capable of ingesting external Intelligence.
- Five respondents can self-create intelligence.
- Two organisations were able to disseminate their self-generated intelligence at a large (automated) scale to government peers or customers; these were the two longest-running teams (more than five years) with the highest analyst headcount (nine and twelve, respectively).

The processes, methodologies and tools identified in this dissertation are presented in a logical implementation order in chapter 6.3 Closing Remarks and Diagram of Findings. This can help draft a roadmap for organisations considering open-source CTI adoption based on the best practices identified by the interview respondents.

6.2 Further Research

This dissertation aimed to identify how eight Dutch organisations adopted Cyber Threat Intelligence and their successes and complications. This can be considered a mere tip of the iceberg on how CTI can be approached, and many approaches and CTI specific subjects remain unexplored, which could be investigated in future analysis. A few examples will be stated.

Identified Biases and Research Gaps for Further Research

Western Bias in Intelligence in this Dissertation

This document relied on the traditional intelligence discipline, but this was written with a Western intelligence bias. Non-Western cultures have developed threat intelligence initiatives. I consider it likely that there is a potential for future learning by investigating foreign cultural intelligence practices and identifying novel insights or potential synergy between these practices.

Industry-Specific Adoption of CTI

This dissertation and the interviews were scoped to involve a wide array of respondents; it is likely that future research with a more constrained scope of respondents, for instance, a particular industry, organisation size, or other groups, would identify more unique observations. It may also be interesting to do a broader analysis with the same question set to compare European or global organisations comprehensively.

Quantitative Analysis of CTI Teams Through High-Level Survey

This dissertation intended to narrow down on a limited group of respondents through semi-structured open interviews. An alternative approach with a fixed survey for a larger group of respondents may help identify other trends and outliers.

Comparison of Public National Cert Initiatives

Future research could compare national cert initiatives or provide a comprehensive overview. This analysis identified three significant National Cert projects, the Dutch NDN, the French OpenCTI, and Luxembourg’s MISP. Likely, many more initiatives were not yet identified in this dissertation deserving of academic interest.

Inventory and Comparison of Significant Open-Source Information Security Tools

This analysis described CTI tools and projects that the respondents were aware of. It is not intended as a representative description of the tooling publicly available. It could be interesting to perform research to identify and compare the publicly available Information security tools for a specific area of interest.

Future Outlook on the Field of CTI

Shortage of Cybersecurity Staff Affecting the CTI Field Likely to Remain for Several Years

In our research, three respondents identified staffing as one of their main impediments in developing their CTI programs to full maturity. Staffing as a complicating factor to mature CTI teams was also identified by two other papers on CTI maturity by Veeresamy [126] and Berndt and Ophoff [127]. Though European educational programs are being developed to help fill the gap of cyber security skilled workers [127], this shortage will likely remain in the upcoming years. This shortage can be expected to affect new CTI teams. It may be recommended to consider staffing an early priority for organisations with ambitions to set up CTI teams.

Future Automation of CTI – Integration in Orchestration Processes (SOAR)
One respondent identified that their future development plan would rely on adopting security orchestration processes and the automated integration of CTI processes. This concept is known as Security Orchestration and Automated Response (SOAR). As some of the technical implementations of CTI are based on retrieving external information and applying it to internal logging, further process integration can likely be achieved in the future.

New Standards on the Horizon
The open-source CTI community is actively developing new standards to address identified issues the community faces. Within the last two years, several new standards were identified and developed.

A few notable examples include the OASIS CACAO standard [128] to automate the generation of Intelligence Courses of Actions playbooks, OASIS OpenC2 [129], a standard to identify malicious command and control channels, and the RE&CT Framework [130], a MITRE ATT&CK inspired standard to serve incident response activities with a specific ontology. These standards are now being adopted, and future tools and methodologies are already being worked on. The frequent publication of new CTI tools and methodologies by itself could be a subject for recurring future research, and it appears that the pace of development is only increasing.

6.3 Closing Remarks and Diagram of Findings

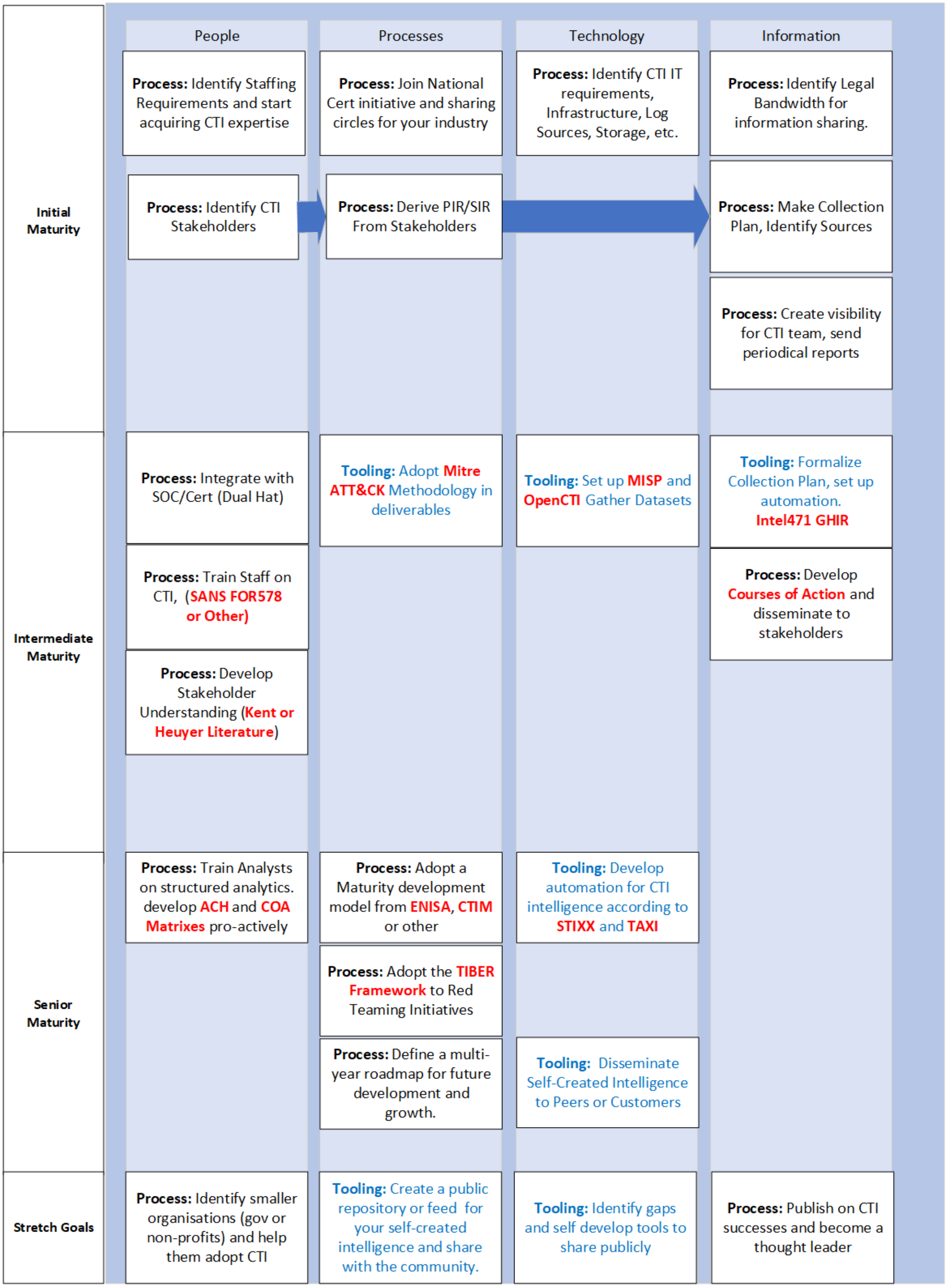
CTI is a discipline that came forth from the requirements of well-meaning defenders sharing intelligence and self-developing technical capabilities to enhance this process. Though CTI started from informal and experimental beginnings, it has now reached a level of maturity where it is being adopted into reputable information security frameworks such as the ISO 27002 standard and the NIST Framework [1], [2]. Its increasing visibility will likely entice more organisations into exploring the value CTI can bring to their organisation. It can be expected that CTI will become a future mandatory requirement for upcoming accreditations and regulations.

Initiatives like ENISA's CTI Maturity program and The German and Dutch University CTIM collaboration are great examples of academic collaboration in the developing field of CTI. France's CERT's OpenCTI, MITRE's ATT&CK Framework, NATO, and Luxembourg's CERT MISP project are examples of mature open-source CTI capabilities developed and shared with the public. These are powerful CTI capabilities that the interviewed respondents had eagerly adopted.

It can be expected that the interest by both the academic audience and the open-source community will remain key drivers in the future development of the CTI practice and its overall maturity. This will help make CTI feasible for small scale and limited budget organisations and make them more resilient to future threats, as long as they consider these open-source community-driven initiatives.

Diagram of Findings

This overview presents the processes, tools and techniques identified in this dissertation and groups them to a logical CTI adoption phase. These topics are based on the interview respondents' best practices and insights identified within their programs.



	People	Processes	Technology	Information
Initial Maturity	**Process:** Identify Staffing Requirements and start acquiring CTI expertise **Process:** Identify CTI Stakeholders	**Process:** Join National Cert initiative and sharing circles for your industry **Process:** Derive PIR/SIR From Stakeholders	**Process:** Identify CTI IT requirements, Infrastructure, Log Sources, Storage, etc.	**Process:** Identify Legal Bandwidth for information sharing. **Process:** Make Collection Plan, Identify Sources **Process:** Create visibility for CTI team, send periodical reports
Intermediate Maturity	**Process:** Integrate with SOC/Cert (Dual Hat) **Process:** Train Staff on CTI, (**SANS FOR578 or Other)** **Process:** Develop Stakeholder Understanding (**Kent or Heuyer Literature**)	**Tooling:** Adopt **Mitre ATT&CK** Methodology in deliverables	**Tooling:** Set up **MISP** and **OpenCTI** Gather Datasets	**Tooling:** Formalize Collection Plan, set up automation. **Intel471 GHIR** **Process:** Develop **Courses of Action** and disseminate to stakeholders
Senior Maturity	**Process:** Train Analysts on structured analytics. develop **ACH** and **COA Matrixes** pro-actively	**Process:** Adopt a Maturity development model from **ENISA**, **CTIM** or other **Process:** Adopt the **TIBER Framework** to Red Teaming Initiatives **Process:** Define a multi-year roadmap for future development and growth.	**Tooling:** Develop automation for CTI intelligence according to **STIXX** and **TAXI** **Tooling:** Disseminate Self-Created Intelligence to Peers or Customers	
Stretch Goals	**Process:** Identify smaller organisations (gov or non-profits) and help them adopt CTI	**Tooling:** Create a public repository or feed for your self-created intelligence and share with the community.	**Tooling:** Identify gaps and self develop tools to share publicly	**Process:** Publish on CTI successes and become a thought leader

Bibliography - References

[1] ISO, “ISO/IEC DIS 27002(en) Information security, cybersecurity and privacy protection — Information security controls,” *ISO Organisation - Online Browsing Platform*, 2020. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:dis:ed-3:v1:en:enhttps://quointelligence.eu/2021/07/factsheet-iso-changes-to-iso-27002-include-addition-of-threat-intelligence/. [Accessed: 12-Aug-2021].

[2] C. S. Johnson, L. Feldman, and G. A. Witte, “Cyber Threat Intelligence and Information Sharing,” 2017.

[3] Institute of Electrical and Electronics Engineers Transactions/Journals Department, “IEEE Reference guide,” *IEEE Periodicals*, 2018.

[4] J. C. Stadler, *The Battle of Waterloo, June 18th 1815. Depicting Arthur Wellesley, the Duke of Wellington. The defeat of the French forces of Napoleon Bonaparte. The last major battle of the Napoleonic wars*. British Library, 1819.

[5] H. B. de Jomini, *Précis de l’art de la guerre (Summary of the Art of War)*. 1838.

[6] K. Oosthoek and C. Doerr, “Cyber Threat Intelligence: A Product Without a Process?,” *Int. J. Intell. CounterIntelligence*, vol. 34, no. 2, pp. 300–315, Apr. 2021.

[7] D. Schlette, M. Vielberth, and G. Pernul, “CTI-SOC2M2 – The quest for mature, intelligence-driven security operations and incident response capabilities,” *Comput. Secur.*, vol. 111, no. 102482, p. 102482, Dec. 2021.

[8] D. Schlette, F. Böhm, M. Caselli, and G. Pernul, “Measuring and visualizing cyber threat intelligence quality,” *Int. J. Inf. Secur.*, vol. 20, no. 1, pp. 21–38, Feb. 2021.

[9] M. Lourenco, “ENISA CTI Capability Maturity Model,” in *CTI Capability Maturity Model*, https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cti-eu-cti-capability-maturity-model.pdf, 2018, p. 19.

[10] Royal Holloway-University of London, “Information Security Project Guide - Appendix B PDF Ethics,” Royal Holloway - University of London, 2021.

[11] J. Davis and Central Intelligence Agency Washington DC, “Sherman Kent and the profession of intelligence analysis,” Central Intelligence Agency, Nov. 2002.

[12] S. Kent, “The need for an intelligence literature,” *Studies in Intelligence*, vol. 1, no. 1, pp. 1–11, 1955.

[13] R. J. Heuer, “Limits of intelligence analysis,” *Orbis*, vol. 49, no. 1, pp. 75–94, 2005.

[14] R. J. Heuer, “The evolution of structured analytic techniques,” *National academy of science*, pp. 529–545, 2009.

[15] NCSC, “10 jaar Nationale Detectie Netwerk,” *Trots op tien jaar nationale detectie: Een toegankelijke geschiedenis van het Nationaal Detectie Netwerk*, 12-Feb-2021. [Online]. Available: https://www.ncsc.nl/actueel/weblog/weblog/2021/geschiedenis-van-het-ndn. [Accessed: 12-Jun-2021].

[16] CIRCL.LU, “CIRCL Mission Statement,” *CIRCL Mission Statement*, 2020. [Online]. Available: https://circl.lu/mission/. [Accessed: 18-Jan-2022].

[17] C. Luxembourg, “Sixth Annual MISP conference Youtube Recording,” *Sixth Annual MISP conference Youtube Recording*, 21-Oct-2021. [Online]. Available: https://youtu.be/zLX-ykn57uQ. [Accessed: 21-Oct-2021].

[18] S. T. Autor, Xunzi, Sunzi, S. Tzu, W. Sun, and S. C. Vu, *The Art of War*. Oxford University Press, 1971.

[19] United States Marine Corps, “United States Marine Corps Revisited - Commandants Revised Reading List,” 2013.

[20] Clausewitz, Carl, O.J. Matthijs Jolles (Translation to English), *On war*, vol. 20. Penguin UK, 1943.

[21] V. M. Rosello, “Clausewitz’s Contempt for Intelligence,” *ProQuest*, 1991.

[22] The Office of Strategic Services Society, “The Office of Strategic Services Society,” *The Office of Strategic Services Society*, 2022. [Online]. Available: https://www.osssociety.org/. [Accessed: 13-Feb-2022].

[23] S. Kent, “Strategic Intelligence for American World Policy,” in *Strategic Intelligence for American World Policy*, Princeton University Press, 2015.

[24] Z. T. Brown, “What if Sherman Kent was wrong, revisiting the intelligence debate of 1949,” *Warontherocks.com*, 10-Jan-2020. [Online]. Available: https://warontherocks.com/2020/10/what-if-sherman-kent-was-wrong-revisiting-the-intelligence-debate-of-1949/. [Accessed: 17-Aug-2021].

[25] EN-Academics-Academic DIctionaries sand Encyclopedias, “Richard Heuer Biography,” *Richard Heuer Biography*, 2021. [Online]. Available: https://en-academic.com/dic.nsf/enwiki/11641038. [Accessed: 13-Feb-2022].

[26] R. J. Heuer, *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, 1999.

[27] M. Warner, “Wanted: A Definition of ‘Intelligence,’” *CIA Studies in Intelligence*, 2003.

[28] S. Robert M Lee, “SANS FOR578 .1 CTI requirements.” 2017.

[29] R. Johnston, *Analytic Culture in the US Intelligence Community.pdf*. 2005.

[30] Department of Defense-Joint Chiefs of Staff, “Joint and National Intelligence Support to Military Operations 2_01.” 07-May-2017.

[31] M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, “Cyber Threat Intelligence – Issue and Challenges,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 1, pp. 371–379, Apr. 2018.

[32] C. V. Hallstensen, “Multisensor Fusion for Intrusion Detection and Situational Awareness.”

[33] J. King, “The Importance of Priority Intelligence Requirements to the Army Service Component Command (ASCC) and the Intelligence Apparatus,” *Small Wars Journal*, 02-May-2021. [Online]. Available: https://smallwarsjournal.com/jrnl/art/importance-priority-intelligence-requirements-army-service-component-command-ascc-and. [Accessed: 26-Aug-2021].

[34] Department of Defense-Joint Chiefs of Staff, “Joint Intelligence Paper JP 2_0.” 22-Oct-2013.

[35] Intel, “Cyber Underground General Intelligence Requirements Handbook (CU-GHIR),” Intel 471, 2021.

[36] NATO, “Allied Command Operations, Comprehensive Operations Planning Directive,” North Atlantic Treaty Organisation, https://sjms.nu/articles/10.31374/sjms.30/, 444.

[37] United States Information Security Oversight Office (ISOO), “Marking Classified National Security Information,” Archive.gov, https://www.archives.gov/files/isoo/training/marking-booklet.pdf, Executive Order 13526-Revision 2 January 2014, Jan. 2014.

[38] Los Alamos National Laboratory, “Uk-USA Classification Equivalency Table,” *Los Alamos National Laboratory Home*, Stored in the Internet Archive webcache on 10-05-2012. [Online]. Available: https://web.archive.org/web/20120510051228/http://badge.lanl.gov/uk-usa_classification.shtml. [Accessed: 10-Feb-2021].

[39] United States-Department of Energy, “Classification of Nuclear - Weapons Related Information,” United States - Office of Health Safety and Security, 1045.35-, 2012.

[40] Norwegian Ministry of Foreign Affairs, “Norway and the EU, Mission of Norway to the EU,” *norway.no*. [Online]. Available: https://www.norway.no/en/missions/eu/ten-facts-about-the-eea2/. [Accessed: 10-Feb-2021].

[41] M. J. Rogers, “H.R. 3523 - Cyber Threat Intelligence Sharing and Protection Act,” *congress.gov*, 30-Nov-2011. [Online]. Available: https://www.congress.gov/bill/112th-congress/house-bill/3523. [Accessed: 10-Mar-2021].

[42] FIRST, “FIRST Vision and Mission Statement,” *FIRST Vision and Mission Statement*, 07-Jan-2020. [Online]. Available: https://www.first.org/about/mission. [Accessed: 30-Oct-2021].

[43] ENISA organisation, “About ENISA - The European Union Agency for Cybersecurity,” *About ENISA*, 2022. [Online]. Available: https://www.enisa.europa.eu/about-enisa. [Accessed: 01-Jun-2021].

[44] J. L. Powell and II, “Utilizing cyber threat intelligence to enhance cybersecurity,” Utica College, Ann Arbor, United States, 2016.

[45] The Center for Internet Security Intel & Analysis Working Group, “What is Cyber Threat Intelligence,” *The Center for Internet Security (CIS)*. [Online]. Available: https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/. [Accessed: 10-Mar-2021].

[46] Lockheed-Martin, “The Cyber Kill Chain,” *lockheedmartin.com The Cyber Kill Chain*, 2021. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed: 30-Oct-2021].

[47] S. Robert M Lee, “SANS FOR578 .2 The Primary Collection Source, Intrusion Analysis.” 2017.

[48] D. J. Bianco, “The Pyamid of Pain,” *detect-respond blog*, 17-Jan-2014. [Online]. Available: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html. [Accessed: 30-Oct-2021].

[49] Intel, “Here’s who is powering the bulletproof hosting market,” *Intel471.com Blog*, 03-Mar-2021. [Online]. Available: https://intel471.com/blog/top-bulletproof-hosting-providers-yalishanda-ccweb-brazzzers-2021. [Accessed: 30-Oct-2021].

[50] V. M. Alvarez, “YARA,” *yara.readthedocs.io*, 2014. [Online]. Available: https://yara.readthedocs.io/en/stable/. [Accessed: 21-Nov-2021].

[51] S. Barnum, “Standardizing cyber threat intelligence information with the structured threat information expression (stix),” *Mitre Corporation*, 2012.

[52] S. E. Daniel Plohmann, “Malpedia,” *Malpedia*, 22-Nov-2021. [Online]. Available: https://malpedia.caad.fkie.fraunhofer.de/. [Accessed: 22-Nov-2021].

[53] N.-M. van Justitie en Veiligheid, “NCSC,” *Nationaal Cyber Security Centrum*, 11-Oct-2021. [Online]. Available: https://www.ncsc.nl/. [Accessed: 16-Nov-2021].

[54] GNU.org, “GNU.org,” *Gnu Free Software Foundation*, 2015. [Online]. Available: https://www.gnu.org/software/software.en.html. [Accessed: 30-Oct-2021].

[55] FIRST: Forum for Incident Responders and Response Teams, “Traffic Light Protocol,” *Traffic Light Protocol*, 2015. [Online]. Available: https://www.first.org/tlp/. [Accessed: 24-Aug-2021].

[56] Cybersecurity and Infrastructure Security Agency, “CISA Traffic Light Protocol,” *CISA Traffic Light Protocol (TLP) definitions and usage*. [Online]. Available: https://www.cisa.gov/tlp. [Accessed: 24-Aug-2021].

[57] ENISA, “ENISA on TLP,” *ENISA*, 2022. [Online]. Available: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol. [Accessed: 01-Jun-2022].

[58] Organisation Circl. LU, “Chatham House Rule (CHR)- Addition to TLP,” *Traffic Light Protocol (TLP) - Classification and Sharing of Sensitive Information*. [Online]. Available: https://www.circl.lu/pub/traffic-light-protocol/. [Accessed: 28-Sep-2021].

[59] P. Poputa-Clean, “Automated Defense, - Using Threat Intelligence to Augment,” SANS GIAC, Jan. 2015.

[60] B. I. Kim, N. Kim, S. Lee, H. Cho, and J. Park, “A Study on a Cyber Threat Intelligence Analysis (CTI) Platform for the Proactive Detection of Cyber Attacks Based on Automated Analysis,” in *2018 International Conference on Platform Technology and Service (PlatCon)*, 2018, pp. 1–6.

[61] MITRE, “MITRE organization - Corporate Overview,” *MITRE.org*, 2021. [Online]. Available: https://www.mitre.org/about/corporate-overview. [Accessed: 29-Nov-2021].

[62] D. H. S. Gov, “DHS.gov,” *United States Department of Homeland Security*, 12-Jul-2021. [Online]. Available: https://www.dhs.gov/. [Accessed: 12-Aug-2021].

[63] OASIS FOUNDATION, “STIX TAXII Interoperability,” *OASIS Foundation*, 16-Aug-2021. [Online]. Available: https://docs.oasis-open.org/cti/stix-taxii-2-interop-p1/v1.1/stix-taxii-2-interop-p1-v1.1.html. [Accessed: 12-Aug-2021].

[64] OASIS foundation, “Introduction to TAXII,” *oasis-open.github.io*, 10-May-2021. [Online]. Available: https://oasis-open.github.io/cti-documentation/taxii/intro.html. [Accessed: 12-Aug-2021].

[65] ENISA, “ENISA on ISAC’s,” *European Union Agency for Cyber Security on ISAC’s*, 2021. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing. [Accessed: 12-Aug-2021].

[66] NCSC, “Nationale Detectie Netwerk Infosheet,” *Nationale Detectie Netwerk Infosheet*, 05-Jan-2019. [Online]. Available: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/nationaal-detectie-netwerk-infosheet. [Accessed: 12-Feb-2021].

[67] OASIS Foundation, “Introduction to STIX,” *oasis-open.github.io*, 10-May-2021. [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro.html. [Accessed: 12-Aug-2021].

[68] Hasso Plattner Institut, TU Delft, “Cyber Threat Intelligence Maturity Platform,” *Cyber Threat Intelligence Maturity Platform*, 2021. [Online]. Available: https://www.ctim.eu/. [Accessed: 12-Dec-2021].

[69] Hasso Plattner Institut, “Hasso Plattner Institut,” *Hasso Plattner Institut*, 2022. [Online]. Available: https://hpi.de/en/index.html. [Accessed: 24-Jan-2022].

[70] T. U. Delft, “TU Delft Cyber Security,” *Technische Universiteit Delft - Cyber Security Faculteit*, 2022. [Online]. Available: https://www.tudelft.nl/tbm/cybersecurity. [Accessed: 24-Jan-2022].

[71] C. D. Mark Luchs, “Measuring Your Cyber Threat Intelligence Maturity - Whitepaper,” Hasso Plattner Institute, TU Delft, 2020.

[72] A. Persoonsgegevens, “Algemene verordening gegevensbescherming (AVG),” *Algemene verordening gegevensbescherming (AVG)*, 11-Dec-2021. [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten. [Accessed: 16-Nov-2021].

[73] European Commission, “GDPR,” *Data Protection in the EU - The General Data Protection Regulation (GDPR)*, 11-Jan-2021. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en. [Accessed: 16-Nov-2021].

[74] Various, “Elsevier Science Direct : Phenomenological Approach,” *Elsevier Science Direct*, 2022. [Online]. Available: https://www.sciencedirect.com/topics/psychology/phenomenological-approach. [Accessed: 01-Feb-2022].

[75] Various, *Encyclopedia of Creativity (Collection of Phenomenological Research)*. Academic Press (Elsevier), 2011.

[76] Nelson, “Research: Phenomenology,” in *Encyclopedia of Creativity: Chapter Research: Phenomenology*, S. R. P. Mark A. Runco, Ed. Science Direct (Elsevier), 2011, pp. 299–303.

[77] S. E. Hove and B. Anda, “Experiences from conducting semi-structured interviews in empirical software engineering research,” in *11th IEEE International Software Metrics Symposium (METRICS’05)*, 2005, pp. 10 pp. – 23.

[78] W. C. Adams, “Conducting Semi-Structured Interviews,” in *Handbook of Practical Program Evaluation*, Wiley.

[79] Jack Davis, “Sherman Kent and the Profession of Intelligence Analysis,” *Occasional Papers: Sherman Kent Center*, vol. 1, no. 5, Nov. 2002.

[80] NCSC, “NCSC NDN,” *NCSC: Nationale Detectie Netwerk*, 01-Jan-2021. [Online]. Available: https://www.ncsc.nl/onderwerpen/detectie. [Accessed: 12-Feb-2021].

[81] Intel, “Intel 471 Criminal Underground - General Intelligence Requirements Handbook,” *Intel471*, 2021. [Online]. Available: https://intel471.com/resources/cu-girh-download-request. [Accessed: 12-Jul-2021].

[82] Internet Engineering Task Force, “Key words for use in RFCs to Indicate Requirement Levels,” IETF, 2119, Jan. 1997.

[83] R. M. Lee, “SANS Cyber Threat Intelligence FOR578,” *SANS.org Cyber Threat Intelligence FOR578*, 01-Jan-2021. [Online]. Available: https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/. [Accessed: 26-Nov-2021].

[84] Treadstone, “Treadstone 71 - Cyber Threat Intelligence training,” *Treadstone 71 - Certified Threat Intelligence Analyst - Cyber Intelligence Tradecraft*, 01-Jan-2021. [Online]. Available:

https://www.treadstone71.com/index.php/cyber-intelligence-training/cyber-intelligence-tradecraft-certification. [Accessed: 26-Nov-2021].

[85] NICCS, “National Initiative for Cybersecurity Careers and Studies - United States Government,” *NICCS Cyber Intelligence Tradecraft Certification*, 01-Jan-2021. [Online]. Available: https://niccs.cisa.gov/training/search/treadstone-71/cyber-intelligence-tradecraft-certification. [Accessed: 26-Nov-2021].

[86] CIRCL, “MISP Training - CIRCL.Lu,” CIRCL, Oct. 2021.

[87] MISP, “MISP Hackathon,” *Github*, 14-Oct-2021. [Online]. Available: https://github.com/MISP/MISP/wiki/Hackathon. [Accessed: 30-Oct-2021].

[88] Security Academy, FoxIT, “Fox IT - CTI training,” *Cyber Threat Intelligence incompany training*, 01-Jan-2021. [Online]. Available: https://www.securityacademy.nl/opleidingen-overzicht/vendoren/fox-it/cyber-threat-intelligence/. [Accessed: 26-Nov-2021].

[89] ENISA, “ENISA CyberSecurity Certification Conference,” *enisa.europe.eu*, 01-Jan-2021. [Online]. Available: https://www.enisa.europa.eu/events/enisa-cybersecurity-certification-conference-2021/. [Accessed: 26-Nov-2021].

[90] CREST, “CREST Registered Threat Intelligence Analyst,” *crest-approved.org*, 01-Jan-2021. [Online]. Available: https://crest-approved.org/examination/crest-registered-threat-intelligence-analyst/index.html. [Accessed: 26-Nov-2021].

[91] MITRE, “MITRE ATT&CK Standard,” *MITRE ATT&CK Standard*, 25-Nov-2021. [Online]. Available: https://attack.mitre.org/. [Accessed: 27-Nov-2021].

[92] Paterva, “Maltego,” *Maltego.com*, 2021. [Online]. Available: https://www.maltego.com/. [Accessed: 27-Nov-2021].

[93] National Cyber Security Center, The Netherlands, “CSIRT Maturity Kit,” in *A step-by-step guide towards enhancing CSIRT Maturity*, 2015, p. 18.

[94] G. Book, “Lessons learned from real world application of the bow-tie method,” in *SPE Middle East Health, Safety, Security, and Environment Conference and Exhibition*, 2012.

[95] B. Holland, L. Holland, and J. Davies, “An investigation into the concept of mind mapping and the use of mind mapping software to support and improve student academic performance,” 2004.

[96] Department for Digital, Culture Media & Sport, United Kingdom, “Cyber Security skills in the UK labour market 2020,” Mar. 2020.

[97] J. DeCrosta, “Bridging the Gap: An exploration of the quantitative and qualitative factors influencing the cybersecurity workforce shortage,” MSc CyberSecurity, Utica College, 2021.

[98] I. S. Giupponi, “Current skills gap for capable CTI analysts: Training for forensics & analysis,” presented at the ENISA: Workshop CTI - EU, Link Campus University, Rome Italy, 31 October 2017.

[99] R. J. Heuer, “Strategic Deception and Counterdeception: A Cognitive Process Approach,” *Int. Stud. Q.*, vol. 25, no. 2, pp. 294–327, Jun. 1981.

[100] R. Heuer Jr, “Defense Technical Information Center,” *DTIC Library - Psychology of Intelligence Analysis*, 1999. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA500078. [Accessed: 27-Jan-2022].

[101] C. Huey, “A Place For Analysis Of Competing Hypotheses (ACH) In Cyber Threat Intelligence (CTI),” presented at the FIRST CTI Conference 2019, London, 18-Mar-2019.

[102] Per Håkon Melan, Karin Bernsmed, Christian Frøystad, Jingyue Li, Guttorm Sindre, “An experimental evaluation of bow-tie analysis for security,” *Information and Computer Security*, vol. 27, no. 4, p. 26, Jun. 2019.

[103] Intel, “Intel471 Main page,” *Intel471 Fight Cyber Threats - And win*, 01-Jan-2021. [Online]. Available: https://intel471.com/. [Accessed: 12-Jul-2021].

[104] M. M. Lowenthal and R. M. Clark, *The Five Disciplines of Intelligence Collection*, vol. 2. SAGE, 2015.

[105] European Commission, “The Four Eyes Principle,” *European Union - Four Eyes Principle*, 2021. [Online]. Available: https://ec.europa.eu/eurostat/cros/content/four-eyes-principle_en. [Accessed: 14-Dec-2021].

[106] CIRCL, “CIRCL MISP - Open Source Threat Intelligence Platform,” *Computer Incident Response Center Luxembourg*, 2020. [Online]. Available: https://www.circl.lu/services/misp-malware-information-sharing-platform/. [Accessed: 30-Oct-2021].

[107] NCIRC, “NCI Agency Cyber Security NCIRC,” *NCI Agency Cyber Security*, 2021. [Online]. Available: https://www.ncirc.nato.int/. [Accessed: 30-Oct-2021].

[108] CERT-EU, “CERT-EU,” *CERT-EU*, 29-Oct-2021. [Online]. Available: https://cert.europa.eu. [Accessed: 30-Oct-2021].

[109] AIVD, “AIVD,” *Algemene Inlichtingen en Veiligheids Dienst*, 11-Dec-2021. [Online]. Available: https://www.aivd.nl/. [Accessed: 12-Feb-2021].

[110] Ministerie van Defensie, “MIVD,” *MIVD*, 01-Jan-2021. [Online]. Available: https://www.defensie.nl/organisatie/bestuursstaf/eenheden/bijzondere-organisatie-eenheden/mivd. [Accessed: 12-Feb-2021].

[111] NCSC, “NCSC Forensic Response,” *NCSC, Incident Respons en Digitaal Forensisch onderzoek*, 03-Nov-2021. [Online]. Available: https://www.ncsc.nl/actueel/weblog/weblog/2021/incident-respons-en-digitaal-forensisch-onderzoek-voor-nederland. [Accessed: 12-Feb-2021].

[112] NCSC, “NCSC Exercise Isidoor,” *Cyberoefening ISIDOOR*, 01-Jan-2021. [Online]. Available: https://www.ncsc.nl/onderwerpen/isidoor2021. [Accessed: 12-Feb-2021].

[113] Noortje Henrichs, Head of CTI, NCSC, “CTI for CERT’s, the Dutch Approach,” presented at the NCSC One Conference 2021, Virtual event, 28-Sep-2021.

[114] ANSSI, “OPENCTI,” *OpenCTI – The open source solution for processing and sharing threat intelligence knowledge*, 01-Jan-2021. [Online]. Available: https://www.ssi.gouv.fr/en/actualite/opencti-the-open-source-solution-for-processing-and-sharing-threat-intelligence-knowledge/. [Accessed: 12-Feb-2021].

[115] ANSII, “ANSII - French National Cert,” *ANSSI*, 25-Nov-2021. [Online]. Available: https://www.ssi.gouv.fr/en/. [Accessed: 12-Feb-2021].

[116] L. Organizations, “Luatix,” *Luatix About*, 2021. [Online]. Available: https://www.luatix.org/en/about/. [Accessed: 12-Feb-2021].

[117] OpenCTI, “OPENCTI.IO,” *Open Cyber Threat Intelligence Platform*, 01-Jan-2021. [Online]. Available: https://www.opencti.io/en/. [Accessed: 12-Feb-2021].

[118] MITRE, “MITRE ATT&CK Navigator,” *MITRE ATT&CK Navigator*, 2022. [Online]. Available: https://mitre-attack.github.io/attack-navigator/. [Accessed: 22-Jan-2022].

[119] Rabobank, Marcus Bakker, Ruben Bouman, “Rabobank Github - DeTTECT,” *Rabobank Github - DeTTECT*, 11-Nov-2021. [Online]. Available: https://github.com/rabobank-cdc/DeTTECT. [Accessed: 11-Dec-2021].

[120] Thai Cert : Electronic Transactions Development Agency, “Thai Cert Actor Group Cards,” *Thai Cert Threat Group Cards*, 2022. [Online]. Available: https://apt.etda.or.th/cgi-bin/aptgroups.cgi. [Accessed: 21-Jan-2022].

[121] Public Community Project, “APT Groups and Operations,” *Google Docs: APT Groups and Operations*, 2022. [Online]. Available: https://apt.threattracking.com/. [Accessed: 18-Jan-2022].

[122] S. Coulthart, “[Bracketing] The Black Swan in Intelligence Analysis,” *Graduate School for Public and International Affairs, University of Pittsburg*, May 2014.

[123] S. Kent, “Words of estimative probability,” *Studies in intelligence*, vol. 8, no. 4, pp. 49–65, 1964.

[124] C. Weiss, “Communicating Uncertainty in Intelligence and Other Professions,” *Int. J. Intell. CounterIntelligence*, vol. 18, Jun. 2021.

[125] United States Army, “fm2-22-3.pdf Appendix B,” United States Army, FM 2-22.3 Human Intelligence Collector Operations-Appendix B, Sep. 2016.

[126] N. Veerasamy, “Cyber threat intelligence exchange: A growing requirement,” Jun. 2017.

[127] A. Berndt and J. Ophoff, “Exploring the Value of a Cyber Threat Intelligence Function in an Organization,” in *Information Security Education. Information Security in Action*, 2020, pp. 96–109.

[128] OASIS Open Foundation, “OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC,” *OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC*, 2020. [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao. [Accessed: 11-Dec-2021].

[129] ’OASIS Open’, “OASIS Open Command and Control (OpenC2),” *OASIS Open Command and Control (OpenC2)*, 2020. [Online]. Available: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2. [Accessed: 08-Jan-2022].

[130] RE&CT Project, “RE&CT Framework,” *RE&CT Framework*, 2021. [Online]. Available: https://atc-project.github.io/atc-react/. [Accessed: 08-Jan-2022].

[131] Open Source, various contributors, “Suricata .IO,” *Community Driven. Always Alert*, 2021. [Online]. Available: https://suricata.io/. [Accessed: 11-Dec-2021].

[132] Critical Path Security, “Zeek Intelligence Network,” *Zeek Intelligence Network*, 2021. [Online]. Available: https://www.criticalpathsecurity.com/services/managed-zeek-ids/zeek-intelligence-network/. [Accessed: 11-Dec-2021].

[133] Zeek Project, “Zeek Performance,” *Zeek Cluster Setup*, 2022. [Online]. Available: https://docs.zeek.org/en/master/cluster-setup.html#:~:text=Zeek%20is%20not%20multithreaded%2C%20so,or%20even%20many%20physical%20computers. [Accessed: 27-Jan-2022].

[134] B. V. OutFlank, “GitHub RedElk Siem tool,” *GitHub RedElk Siem tool - Tool for Red Teams for Tracking and Alarming on Blue team Activities*, 09-Jan-2021. [Online]. Available: https://github.com/outflanknl/RedELK. [Accessed: 11-Dec-2021].

[135] T. Hunt, “Have I been Powned Who, What and Why,” *Have I been Powned Who, What and Why*, 2021. [Online]. Available: https://haveibeenpwned.com/About. [Accessed: 01-Apr-2021].

[136] European Central Bank, “TIBER-EU Framework: How to Implement the European Framework for Threat Intelligence-based Ethical Red Teaming,” ECB, Jan. 2018.

[137] European Central Bank, “ecb.europe.eu TIBER-EU,” *ecb.europe.eu TIBER-EU*, 2021. [Online]. Available: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html. [Accessed: 16-Feb-2022].

[138] De Nederlandse Bank, “TIBER: working together against cybercrime,” *TIBER: working together against cybercrime*, 2021. [Online]. Available: https://www.dnb.nl/en/sector-information/payments/tiber-working-together-against-cybercrime/. [Accessed: 16-Feb-2022].

Appendix A: Interview Introduction and Questions

Dear sir/madam,

Thank you for your approval in participating in my Cyber Threat Intelligence maturity interview. I would first like to introduce myself and the purpose of this survey.

I am Sijmen Schenk, currently attending the MSc. Information Security program at the Royal Holloway University of London.

Purpose and scope
For my final dissertation project, I will be investigating Cyber Threat Intelligence maturity progression, with a specific emphasis on tactical/technical level intelligence.

The interview will be a semi/structured informal interview lasting approximately one hour. I will be asking several identical questions to all interview subjects—the answers can flow into a free form discussion to elaborate on more specific details.

- **Your anonymity**
  The dissertation project will not mention your identity and your organisation's identity. I will request your approval to identify you to my project supervisor; this will not be part of the dissertation but only for the methodological review of my interview process. I will identify you by a pseudonym, and your organizations will be roughly described as '(inter)national organization, sector, headcount'. No further information will be inferred from the questions or the answers provided.

- **Storage and destruction of data**
  The transcripts of the anonymous interviews will not be provided with the dissertation itself; they may only be kept as evidence for the review board and will be destroyed after the dissertation review is completed, which is expected to be around June 2022.

- **Data usage**
  The findings identified from the analysis of the interview transcripts will be used as a base to identify potential maturity solutions, for which I will perform further analysis to identify common problem areas and potential mitigating solutions.

- **Distribution of the final product**
  After final approval of the university's examination board, I will provide you with a copy of the dissertation if you please.

Why did I reach out to you as an interview respondent?

- Your organization invested significant efforts into developing a CTI program.
- Your position allows you to provide an overview of your organization's CTI program and the steps that led up to the current level of maturity and a potential future roadmap.

Interview Questions

1 Before CTI implementation

- 1.1 Were there pre-defined objectives before the program was initiated?
- 1.2 Did you specify the main stakeholders beforehand, if so, whom?
- 1.3 Did you involve external expertise to define the program?
- 1.4 Were there strategic, operational or tactical level objectives defined?
- 1.5 What were expectations regarding maturity development and timelines?
- 1.6 Did you collaborate with peers at this stage?
- 1.7 What was the planned size of the team (analysts)?
- 1.8 Were there any complications identified before the initiation of the program?
- 1.9 Did you adopt any formal structured analytical techniques at any stage of the CTI program?

2 During CTI implementation

- 2.1 Were there any unexpected complications in implementing the program in areas such as people, tools, collaboration, budgets.
- 2.2 Did the scope or outset of the CTI program ever change after being initiated?

3 After CTI implementation

- 3.1 Did the overall implementation match the set expectations?
- 3.2 Were you able to meet the pre-defined deadlines? If not, please specify why?
- 3.3 What would you identify as the most significant benefits achieved to date?
- 3.4 Were there significant delays or disappointments?
- 3.5 Are you aware of open-source and community-developed CTI capabilities? If so, which?
- 3.6 Did you leverage any open-source tools or standards in your implementation?

4 Open-end discussions

- 4.1 Did you formally adopt technical/tactical level intelligence processes, such as the enrichment, pivoting, sharing of intelligence?
- 4.2 Did you involve external training to train analysts? If so, please elaborate?
- 4.3 Was there a formal integration with the SOC/CERT processes? If so, please elaborate on the stakeholders involved?
- 4.4 Do you formalize working processes, and is there a (continual) improvement process part of your CTI team?

- 4.5 Is there a future outlook and improvement program defined? If so, what would be the most significant areas of improvement?
- 4.6 Is there anything you would have done differently afterwards?

5 Roundup

- 5.1 Do you have any remarks, suggestions or questions about this dissertation subject?
- 5.2 Do you have any other subjects to discuss?

Appendix B: Additional CTI Capabilities Mentioned by Individual Respondents

Several tools and methodologies were mentioned by respondents individually. The respondents considered these tools valuable, but they did not see prolific use amongst the respondent group. As they may be of future academic interest, they will be briefly described here.

Suricata https://suricata.io/ [131]
Suricata is an open-source detection engine that combines Intrusion Detection (IDS), Intrusion Prevention (IPS) and network security monitoring capabilities. Suricata's strength is its high-performance traffic inspection (partly due to its ability to multithread) and the abundance of publicly available Suricata rules. Defenders can set up Suricata to monitor their network and tailor specific Suricata detection rules. These rules are publicly shared within the CTI community. The Suricata team also hosts a repository to provide rules. Some commercial threat intelligence providers deliver their intelligence in the Suricata format. It is also possible to integrate MISP with Suricata so that Suricate creates detection rules from MISP data. An example of this usage is provided here.

Zeek (formerly known as the 'bro' project) https://zeek.org/ [132]
Bro was a popular network security monitoring tool that operates like a sensor. In its current incarnation, this project is called Zeek. It is a solution that can be deployed on hardware, software, virtualized assets or cloud solutions. The development of Zeek is community-driven and maintained on their GitHub site. Some capabilities of Suricata and Zeek overlap. However, where Suricate is driven by performance in its default configuration Zeek provides more customisation options and has a higher granularity in its ruleset, making it more applicable to advanced users. Zeek is CPU single-threaded, so it may lack performance in single-core processor systems[133].

Red Elk https://github.com/outflanknl/RedELK [134]
Red Elk is a red teaming framework developed by the organization OutFlank. It is described as a lightweight SIEM solution for Red Teams that can help them monitor and respond to Blue Team activities.

CACAO https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao [128]
CACAO stands for Collaborative Automated Course of Action Operations; it is an open-source project that aims to develop a Course of Action playbook model that can be used for cybersecurity. It generates these COA's in a machine-readable format and allows for its automated dissemination within organizations. When an organisation is sufficiently mature and has COA's in place, whenever a situation manifests itself related to a COA, the COA can be immediately presented to the respective stakeholder to support their decision-making. This project has started to receive interest and support from commercial organizations that support the CACAO public standard.

HaveIBeenPowned Project by Troy Hunt https://haveibeenpwned.com/ [135]
Troy Hunt is a journalist who receives sensitive insight into international data breaches due to his responsible disclosure approach. He often receives specific access to the affected parties' compromised datasets.

His website haveibeenpwned.com allows organisations to identify potential compromises of their organisation to breaches. We can query individual e-mail addresses from this website to identify their presence in a breach.

As an authenticated owner of a top-level domain, we can also perform this lookup on all e-mail addresses originating from this domain. This can help identify personal and organisational exposure and help to mitigate the potential risk.

TIBER-EU: Threat Intelligence Based Ethical Red Teaming [136]
TIBER is a framework developed by the European Central Bank[137]. It can be applied to perform cyber threat intelligence-led red-teaming. Its purpose is to mimic real threat actors' tactics, techniques, and procedures (TTP) to make the red-teaming engagement as realistic as possible.

TIBER engagements are also performed by the DNB (De Nederlandse Bank), which is the Dutch central banking authority that regulates financial institutions in the Netherlands. The DNB uses TIBER to test the national financial institutions [138]. The DNB produced a video presenting their TIBER initiative. This video provides a good representation of the overall process.

TIBER It also sees adoption by commercial organisations. Two of our interview respondents also provided ‘TIBER Testing’ services to their customers.