



# Cyber Threat Intelligence Management in Technical Cybersecurity Operations

Sampsa Suominen

Master's thesis

May 2024

Information technology

Master's Degree Programme in Information Technology, Cyber Security

**Suominen, Sampsa**

### **Cyber Threat Intelligence Management in Technical Cybersecurity Operations**

Jyväskylä: Jamk University of Applied Sciences, May 2024, 68 pages.

Degree Programme in Information Technology, Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

#### **Abstract**

Over the past years, cybercriminals and other adversaries exploiting information systems have continuously developed their capabilities to breach systems in an attempt to gain access to the confidential information of organizations. The practicality of threat intelligence is that, based on this information, threat events can be predicted, and the organization's information security capabilities can be adapted to prevent such attacks.

The continuous increase in the amount of threat information has led to a situation where successful utilization of threat intelligence requires consistency and structure. There is no single correct method for developing a successful threat intelligence management model. A threat intelligence program should support the organizations business requirement for it to be useful. In order to achieve this, sufficient maturity and willingness are required from the organization.

As a result of the research, a threat intelligence management model was developed utilizing tools, framework and processes. In order to test and evaluate the concept, a threat hypothesis was carried out, combined with existing processes and tools of the organization. The concept provides a basis for technical cybersecurity functions for processing threat intelligence and for the continuous development of threat intelligence management. Interview with the stakeholders of the commissioning organization was utilized in assessing the suitability of the concept.

#### **Keywords/tags (subjects)**

Cyber Threat Intelligence, Cybersecurity, CSIRT, CSOC

#### **Miscellaneous (Confidential information)**

N/A

Suominen, Sampsa

### Uhkatiedon Hallinta Teknisissä Kyberturvallisuuden Toiminteissa

Jyväskylä: Jyväskylän ammattikorkeakoulu, toukokuu 2024, 68 sivua.

Degree Programme in Information Technology, Cyber Security. Master's thesis.

Verkkojulkaisulupa myönnetty: Kyllä

Julkaisun kieli: Englanti

### Tiivistelmä

Kyberrikolliset sekä muut tietojärjestelmiä hyväksikäyttävät tahot ovat viimeisten vuosien aikana jatkuvasti kehittäneet kyvykkyyksiään murtautuakseen organisaatioiden järjestelmiin ja saadakseen pääsyn luottamuksellisiin tietoihin. Uhkatiedon käytännöllisyys esiintyy sillä, että näiden tietojen pohjalta uhkatapahtumia pystytään ennakoimaan ja mukauttaa organisaation tietoturvakyvykkyyksiä hyökkäysten estämiseksi.

Uhkatiedon määrän jatkuva lisääntyminen on johtanut siihen, että sen onnistunut hyödyntäminen vaatii johdonmukaisuutta ja rakenteellisuutta. Hyödyllisen uhkatiedon hallinnan mallin kehittämiseksi ei ole yhtä oikeaa menetelmää, vaan se on määriteltävä vastaamaan liiketoiminnan tietoturvan tarpeita. Tämän saavuttamiseksi organisaatiolta vaaditaan riittävää kypsyyttä sekä tahtotilaa.

Tutkimuksen tuloksena kehitettiin uhkatiedon hallinnan malli hyödyntäen työkaluja, viitekehystä sekä prosesseja. Konseptin testaamiseksi ja arvioimiseksi suoritettiin uhkahypoteesi, johon liitettiin organisaation olemassa olevia prosesseja ja työkaluja. Konsepti antaa teknisille tietoturvatointeille pohjan uhkatiedon käsittelemiseksi sekä uhkatiedon hallinnan jatkuvalla kehittämiselle. Konseptin sopivuutta toimeksi antavaan organisaatioon arviointiin sidosryhmän haastattelun avulla.

### Avainsanat (asiasanat)

Kyberuhkatieto, Kyberturvallisuus, CSIRT, CSOC

### Muut tiedot (salassa pidettävät liitteet)

N/A

<b>Terminology.....</b>	<b>4</b>
<b>1 Introduction .....</b>	<b>6</b>
1.1 Thesis background and objectives .....	7
1.2 Research design and methods .....	8
1.3 ISF Standard of Good Practice.....	10
<b>2 Threat intelligence.....</b>	<b>11</b>
2.1 Levels of Threat Intelligence .....	11
2.1.1 Strategic threat intelligence .....	11
2.1.2 Tactical threat intelligence .....	12
2.1.3 Operational threat intelligence .....	12
2.2 Cyber threat actors.....	12
2.3 Threat intelligence cycle .....	15
2.4 Implementing threat intelligence .....	16
2.4.1 Threat intelligence feeds .....	17
2.4.2 News Reports, blogs, and social media .....	18
2.4.3 Data breach, patch, and vulnerability notifications .....	18
2.5 Threat information sharing .....	19
2.6 Applying threat intelligence .....	27
2.6.1 Security Tools.....	27
2.6.2 Threat Intelligence platforms .....	29
2.6.3 Threat hunting .....	30
2.7 Attack frameworks .....	31
<b>3 Development plan .....</b>	<b>36</b>
3.1 Focus-group workshop 1. Defining business requirements.....	37
3.2 Focus-group workshop 2. Current state analysis and key development targets .....	38
<b>4 Implementation.....</b>	<b>40</b>
4.1 TIP Installation.....	41
4.2 Integrating MITRE ATT&CK.....	43
4.3 Integrating Threat Feeds .....	46
4.4 Enriching Indicators.....	47
4.5 Framework-based assessment.....	49
4.6 Evaluation via Threat Hypothesis.....	51
4.6.1 Threat Enrichment and Analysis .....	52
4.6.2 Updating capabilities .....	57
4.6.3 Reporting .....	58

<b>5</b>	<b>Evaluating implementation results</b> .....	<b>59</b>
5.1	Comparing results to key development targets.....	59
5.2	Demonstration session and feedback survey .....	60
<b>6</b>	<b>Research results</b> .....	<b>63</b>
6.1	Evaluating research results .....	63
6.2	Feedback survey results .....	64
<b>7</b>	<b>Conclusion</b> .....	<b>65</b>
7.1	Reflections.....	65
7.2	Research ethics and reliability .....	66
7.3	Further research.....	67
	<b>References</b> .....	<b>69</b>
	<b>Appendices</b> .....	<b>75</b>
	Appendix 1. Installing Portainer and OpenCTI stack.....	75
	Appendix 2. docker.compose.yml & sample.env.....	76
	Appendix 3. Demonstration feedback survey.....	79

## Figures

Figure 1.	Design & Development research framework (Ellis and Levy, 2010).....	9
Figure 2.	Threat actors and general motivations (Canadian Centre for Cyber Security, 2022). 13	
Figure 3.	Six phases of threat intelligence cycle (Kirschner, 2021).....	15
Figure 4.	Banking industry threat intelligence sources (McGowan, 2018).....	17
Figure 5.	Threat information sharing process (Homeland Security, 2016) .....	20
Figure 6.	The Pyramid of Pain (DavidJBianco, 2014). .....	25
Figure 7.	SIEM, threat intelligence and incident response (Karasev, 2019) .....	28
Figure 8.	MITRE ATT&CK Enterprise Matrix (The MITRE Corporation, n.d.) .....	32
Figure 9.	Red Team Assessment (Harrington, 2022) .....	35
Figure 10.	Development plan.....	36
Figure 11.	OpenCTI Architecture (Filigran, n.d.) .....	42
Figure 12.	Running containers in Portainer .....	43
Figure 13.	MITRE Datasets connector configuration .....	44
Figure 14.	APT29 Description.....	45
Figure 15.	APT29 Relationships.....	45

Figure 16. OTX Indicators of Compromise .....	46
Figure 17. Indicator attack-patterns .....	47
Figure 18. Enrichment connectors .....	48
Figure 19. Virustotal relationships .....	48
Figure 20. VirusTotal note .....	49
Figure 21. Cyber security capability map .....	50
Figure 22. Capability map principle .....	51
Figure 23. Threat intelligence process .....	52
Figure 24. Malicious IP-address relationships .....	52
Figure 25. Malicious IP-address enrichment.....	53
Figure 26. UAC-0184 threat report .....	53
Figure 27. Remcos RAT indicators.....	54
Figure 28. Defender advanced hunting indicator search from DeviceNetworkEvents .....	55
Figure 29. Defender advanced hunting indicator search from EmailUrlInfo.....	55
Figure 30. Defender advanced hunting indicator search from DeviceFileEvents .....	56
Figure 31. Adding hash indicator in defender XDR .....	57
Figure 32. APT18 Global kill chain.....	58
Figure 33. Feedback survey question 1.....	61
Figure 34. Feedback survey question 2.....	61
Figure 35. Feedback survey question 3.....	62
Figure 36. Feedback survey question 4.....	63

## Tables

Table 1. STIX 2.1 format malware indicator attributes (OASIS, 2021).....	23
Table 2. Threat intelligence sources and context .....	38
Table 3. Threat intelligence maturity assessment .....	39
Table 4. TIP evaluation .....	41
Table 5. Test machine specifications .....	42

## Terminology

API	Application Programming Interface
APT	Advanced Persistent Threat
AV	Antivirus
SIEM	Security Information and Event Management
CERT	Computer Emergency Response Team
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CSOC	Cyber Security Operations Center
CTA	Cyber Threat Actor
CTI	Cyber Threat Intelligence
DNS	Domain Name System
DoS	Denial of Service
DSRM	Desing Science Research Methodology
EDR	Endpoint Detection and Response
GDPR	General Data Protection Regulation
HTTP	Hyper Text Translation Protocol
IoC	Indicator of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Centre
IoT	Internet of Things
ISF	Information Security Forum
JSON	JavaScript Object Notation
MISP	Malware Inspection and Sharing Platform
MS	Microsoft
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
OTX	Open Threat Exchange
PII	Personally Identifiable Information
PSIRT	Product Security Incident Response Teams
RSS	Really Simple Syndication
SCO	STIX Cyber-observable Object
SDO	STIX Domain Object

SOC	Security Operations Center
SOGP	Standard of Good Practice
SRO	STIX Relationship Object
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information
TI	Threat Intelligence
TIP	Threat Intelligence Platform
TTP	Tactics Techniques and Procedures
URL	Uniform Resource Locator
XDR	Extended Detection and Response
YARA	Yet Another Recursive Acronym or Yet Another Ridiculous Acronym



## 1 Introduction

The transformation to digital connectivity has made cybercrime a profitable business for criminals. Several types of cyber-attacks, ranging from phishing attacks, frauds, and blackmailing money using ransomware attacks, are present threats in today's world. This criminal activity evolves rapidly, becoming more organized and sophisticated (Interpol, n.d.). The Europol SOCTA 2017 report on organized crime presents that the cybercriminal economy is driven by technological innovation and internet connectivity. The expansion of digital surfaces via developments like the Internet of Things (IoT) and other connected devices allows cybercriminals to conduct criminal activities remotely and even anonymously. This activity is made further accessible with the availability of attacking tools and Cybercrime as a Service. These attacks target not only public and private sector organizations but also individual citizens (Europol, 2017).

However, organized crime is not the only threat actor capitalizing on the continuing connectivity. The digital landscape allows various groups of threat actors with malicious intent to exploit weaknesses and vulnerabilities in connected devices, to gain access or otherwise disrupt the systems of their victims. These threat actors have distinct goals, methods, and motivations behind their actions (Canadian Centre for Cyber Security, 2022).

It is not possible to defend against threats if there is no information about their existence. The utility of threat intelligence comes from the fact that it enables the description of phenomena that have the potential to cause harm. By itself, this information is not necessarily beneficial, but by enriching it with sufficient context, the decision-makers should understand the threats and take the necessary actions to protect against them. The dynamics between attackers and defenders constantly change over time, along with the development of their capabilities. With this development, it has become clear that the attackers' abilities have become more sophisticated than before. As technology has become more integrated with critical functions of society, threat intelligence aims to inform us how to protect these functions from being abused by these increasingly capable adversaries (Lee, 2023).

A Cyber Threat Intelligence survey from 2016 conducted by SANS Institute presents that only 25,9 percent of respondents affirm that they have either a mature or fully mature Cyber Threat Intelligence (CTI) program in place, 40,5 percent claim that their CTI program is still immature but developing, 27,7 percent admit that their CTI program is immature or just starting, and 5,9 percent do not have a CTI program at all. The survey concludes that threat intelligence is seen as an increasingly valuable tool within the field of information security (Bromiley & SANS, 2016).

Even if executives see threat intelligence as an increasingly valuable tool, Bussa (2023) summarizes the key pitfalls of successfully implementing threat intelligence from Gartner's 2023 Market Guide for Security Threat Intelligence Products and Services report:

- Incomplete formalization of the threat intelligence program resulting in inadequate definition of requirements, lack of actionability and viability of a long-term intelligence program.
- Being overwhelmed with data caused by a lack of defining the key focus areas. Priority intelligence requirements should be defined and used to identify the tools and resources required to develop a thriving threat intelligence program.
- Acting based on threat intelligence remains the key goal of security managers, as having knowledge and understanding is not enough if priority intelligence requirements are not met.

## **1.1 Thesis background and objectives**

The thesis subject came up in discussions with the authors' team manager and team members.

The employer is a cooperative where the author is part of the Cyber Security team. The topic was part of Cyber Security operations development where it was speculated that threat intelligence is currently underutilized in the Cyber Security Operations Center (CSOC) and Computer Security Incident Response (CSIRT) operations.

The primary objective of the research was to investigate methods for building a security operations management model for threat information and its processing. The main purpose of the management model was to enhance and streamline the capability of the centralized CSOC and the CSIRT team to understand, detect, respond to, and prevent threats in the organization's digital environment. Part of developing the management model was to assess the organization's current and target maturity level concerning the handling of threat information.

The initial chapters of this research delve into the core concepts of 'what,' 'why,' and 'how' of threat intelligence. The objective was to build a comprehensive understanding of multiple facets of threat intelligence, thereby strengthening the knowledge base. With this understanding, suitable reference frameworks, best practices, and tools for managing threat intelligence were researched and evaluated for the best fit to support demonstration of the research.

The target result of the research was to create a solid base on which the cyber security team can begin further development of the necessary tools and processes for utilizing threat information and for the continuous development of the management model. The management model should also assist the cyber security functions with creating various metrics and statistics for distinct stakeholders to aid the business in preparing for emerging threats and improving its overall cyber security resilience.

## **1.2 Research design and methods**

Cyber threat intelligence as an independent practice has been around for about a decade since the first threat reports by security researchers started to emerge, according to Roberts (2021) this was marked by Mandiant's report on APT1. While literature about threat intelligence has gained some traction in recent years, a lot of research concentrates on the phenomenon and guiding principles of threat intelligence, rather than the practicality of it. Even if many entities in the cyber security field have published directional guidelines in recent years, the implementation of profound threat intelligence practices remains a complicated matter. The thesis aims to establish answers to the following research questions:

1. How to use threat intelligence efficiently in organizations' security operations to assist with preventing security breaches?
2. What frameworks and tools can be used to develop suitable threat intelligence practices to meet the target organization's security related needs?
3. How can threat intelligence practices be established as a part of technical cyber security operations?
4. How to generate threat-related metrics and statistics to assist in defining security related business needs?

Design science research methodology (DSRM) is well applicable in research where the goal is to enhance organizational capabilities by designing new and innovative methods and models. Design science research is fundamentally a problem-solving paradigm and the method is used to study dilemmas in real-world environments. An essential component to DSRM is the objective of generating knowledge about the subject of research, including elements such as technology, business processes and how to align the subject of research with organizational strategy (Brocke et al., 2020).

The DSRM was chosen as the methodology in this research as the objective is to demonstrate a solution implemented to a pre-existing environment. The project follows a framework for design and development research presented by Ellis and Levy (2010) in Figure 1.

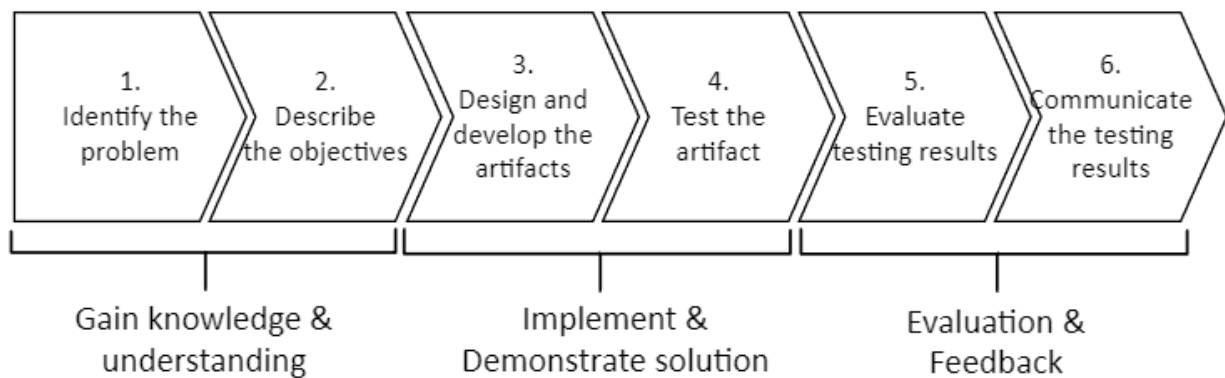


Figure 1. Design & Development research framework (Ellis and Levy, 2010)

Qualitative research requires interpretation of information collected using different methods to gain knowledge about a subject or phenomenon (Merriam & Tisdell, 2015, p. 105). The research process utilizes qualitative methods such as data mining from various literature sources and group interview to gather feedback. The research topic was commissioned by the authors organization, and as such includes focus-group workshops consisting of professionals from the organizations cyber security team.

While the research topic itself is not remarkably unique, the nature of it is highly subjective depending on multiple factors, such as organization structure, maturity of security operations, business needs and resources. A one-size-fits-all solution does not seem to exist, but organizations must develop their capabilities based on these factors. The target organization is a relatively large cooperative with multi-industry businesses including logistics, finance, retail, and hospitality businesses, making the threat landscape vast, and emphasizing the necessity of threat intelligence.

### 1.3 ISF Standard of Good Practice

The Information Security Forum (ISF) Standard Of Good Practice (SOGP) is a guide that assists organizations in managing their information security risks, by introducing various guidelines covering multiple current and emerging topics, regarding the threats and risks an organization may face (Haken et al., 2022). Threat intelligence related controls are covered in section TM1.4. The principle of threat intelligence presented in SOGP is that *“A threat intelligence capability should be established and supported by an intelligence cycle and analytical tools”* (Haken et al., 2022, p. 354). Additionally, the objective presented by SOGP is *“To provide information and situational awareness about past, present and predicted attacks, supporting information risk related decision and actions”* (Haken et al., 2022, p. 354).

The ISF SOGP Security healthcheck assessment summarizes the threat intelligence related principles into four questions that can be used by organizations to assess their current maturity level in threat intelligence. In context of this research the questions are rephrased to the following four:

- Does a capability to create and manage threat intelligence exist with sufficient analytical tools and an intelligence cycle supporting it?
- Is the range of external and internal sources for information about threats and other supporting details sufficient?
- Does the capability to perform specialized activity leveraging threat intelligence exist to identify activity that may lead to a security breach?
- Does a process exist for regular review and improvement of intelligence capabilities?

As part of threat intelligence maturity assessment, this research aims to answer these questions by assigning a quantitative value to each question to assess the starting level of the development process.

## **2 Threat intelligence**

Threat intelligence (TI) is information and data about various threats that has been analyzed, enriched, or otherwise processed adding context to the information for further utilization (Johnson et al., 2016). This data may then be used to understand various threat actors' rationale, objective, and behaviors (Baker, 2022). Sources for threat information may be found both in open source and commercial solutions. Common technical forms of threat intelligence are IP addresses, domain names, malicious URLs, hashes of files or malware and other similar identifiers (Chapple & Seidl, 2020, p. 36). However, just being aware of the threats is not enough. Threat intelligence should be relevant, current, and actionable (Kirschner, 2021). This is where threat intelligence management processes help in turning the overwhelming amount of available intelligence, to information making cyber security operations more efficient.

### **2.1 Levels of Threat Intelligence**

Threat intelligence comes in different forms and various threat intelligence have distinct stakeholders, depending on their priorities and threat intelligence use cases (Kirschner, 2021). Threat intelligence can be divided into three levels of intelligence: tactical-, operational-, and strategic threat intelligence (Baker, 2022).

#### **2.1.1 Strategic threat intelligence**

Strategic threat intelligence helps the higher management personnel with decision making capabilities to direct resources and investments in alignment with strategic priorities. Strategic intelligence is often produced via human data collection and enriched with analysis that requires intimate knowledge of cybersecurity and the influence and consequences of geopolitical incidents. The most generic form of strategic threat intelligence is reports (Baker, 2022). Strategic threat intelligence may give insight into the company's security posture, risk profile, and broader security strategy. The stakeholders of strategic threat intelligence should include higher management, executives, and chief information security officers (CISOs) (Snyk, n.d.).

### **2.1.2 Tactical threat intelligence**

Tactical threat intelligence comes in the form of indicators of compromise (IOCs), is technical in essence, and focuses on the instant future. The most usual forms of tactical threat intelligence are IP addresses, domains, and file hashes that have been deemed malicious by some entity. Tactical threat intelligence can be acquired via various data feeds and is often automated. A technical threat intelligence characteristic is that it often has a short lifespan, as malicious domains and IP addresses regularly become obsolete in days or even hours (Baker, 2022).

### **2.1.3 Operational threat intelligence**

Operational threat intelligence is a combination of highly detailed knowledge on the adversary, its capabilities and the specialized threats connected to this specific actor. Operational threat intelligence aims to answer the motivations, threat actors and the methods, or tactics, techniques, and procedures (TTPs) employed by the threat actor. The main goal of operational intelligence is to provide insight into the operations of adversaries. Operational intelligence may be useful for security personnel working in technical positions that require deeper analysis into security incidents, like people who work in a security operations center (SOC) (Baker, 2022).

## **2.2 Cyber threat actors**

A cyber threat actor (CTA) is an individual or a group of personnel with malicious intent, using computers, networks, or other systems. The motivations, relevance and techniques vary between the threat actors, and it is important to identify the incentive behind various threat actors. The Center for Internet Security (CIS) is a non-profit organization intending to support individuals and organizations to secure against cyber threats. While naming conventions vary between different cyber security entities, CIS classifies the most prevalent CTAs in five groups: Cybercriminals, Insider Threats, Nation-State actors, Hacktivists and Terrorist Organizations (Center for Internet Security [CIS], n.d.). A general summarization of CTAs and their motivations is illustrated in Figure 2 below:

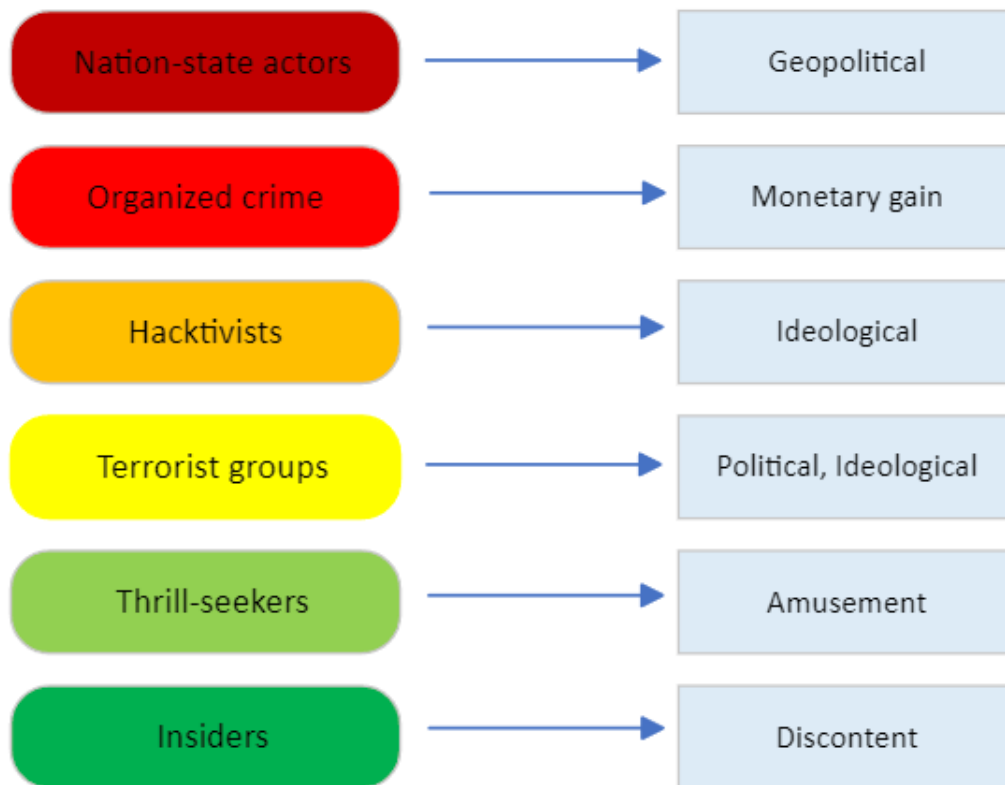


Figure 2. Threat actors and general motivations (Canadian Centre for Cyber Security, 2022).

**Cybercriminals** are opportunistic, often profit-driven threat actors who pose a global threat to multiple organizations and individuals. They work as individuals or organize in groups to achieve their goals. Cybercriminals are either financially motivated, or to enhance their reputation (Center for Internet Security [CIS], n.d.). Cybercriminals vary widely in their capabilities and sophistication. Their methods often include attacks that affect a wide population, and they may have supporting functions and planning involved in their activities. The spreading of illegal markets for easily deployable tools and services has made organized crime more accessible and profitable for criminals (Canadian Centre for Cyber Security, 2022).

**Insider threats** or insiders are malicious actors inside an organization. They may be current or former employees, or otherwise affiliated with the organization. Insiders may abuse their access to systems in a way that compromises the confidentiality, integrity, or availability of the systems (Center for Internet Security [CIS], n.d.). Insider threats may be particularly dangerous as they can have legitimate access to internal data and processes. Insiders are often motivated by dissatisfac-



tion with the organization or may be otherwise associated with other threat actors (Canadian Centre for Cyber Security, 2022). It is also essential to distinguish unwitting insiders from malicious insiders, as they may compromise systems due to carelessness rather than malicious intent.

**Nation-state actors** target organizations' assets for persistent access to their infrastructure in public and private sectors alike. A hacking organization funded by nations may be called Advanced Persistent Threat (APT). Nation-state actors are primarily motivated by espionage, or gaining influence in political, economic, or military objectives. While APT and Nation-state actors are sometimes used interchangeably, it is important to understand that APT can also refer to other CTAs, like highly sophisticated criminal organizations utilizing cyber threat activity. Nation-state actors are sometimes directed, funded, or otherwise technically assisted by a nation-state (Center for Internet Security [CIS], n.d.).

**A hacktivist** is a type of attacker who is ideologically, politically, or otherwise philosophically motivated threat actor. The motivation behind an individual or hacktivist group may be publicity for their cause. An example of a hacktivist group is the widely known Anonymous (Chapple & Seidl, 2020, p. 45). Hacktivists' methods usually include the usage of readily available tools requiring relatively low skill to deploy and operate. Attacks organized by them are usually geared towards causing damage and disorder to their target (Canadian Centre for Cyber Security, 2022).

**Terrorist organizations** are groups, designated by the U.S. Department of State. The goal of terrorist groups may vary between spying activities and spreading propaganda motivated by political or ideological ambitions. The nature of offensive activities can also include harassment and disruptive methods, like denial of service and defacement. Terrorist organizations often employ methods similar to those of hacktivist groups (Center for Internet Security [CIS], n.d.).

While CIS does not classify Thrill seekers as their own CTA category, many security operators like the Canadian Centre for Cyber Security have a definition for CTAs primarily driven by satisfaction in hacking activities (Canadian Centre for Cyber Security, 2022). Thrill seekers can also include the low-ability, typically inexperienced individuals called script-kiddies. Script kiddies may engage in various hacking activities to have fun or evaluate their skills (Sophos, n.d.)

## 2.3 Threat intelligence cycle

Organizations may adopt a threat intelligence life cycle to assist with its management. Many professionals in the field of cyber security describe the intelligence cycle as consisting of either five or six distinct phases. While the operatives may deviate from the exact number and naming of these phases, the content and subject matter are practically the same. The Zerofox (Kirschner, 2021) organization describes this cyclical process as illustrated in Figure 3. chart below:



Figure 3, Six phases of threat intelligence cycle (Kirschner, 2021)

1. Direction – What are the assets that require protection, the impact or interruption caused by a service disruption? What kind of TI is required and how is it processed to best prevent the impact caused by an attack?
2. Collection – After the requirements are agreed on, the intelligence must be collected. In this phase, the different available sources are utilized, for example threat intelligence feeds, dark web data and others.
3. Processing – The data collected must be processed into an understandable and usable format. Various sources contain data in different schemes, which might require transformations to a usable form.

4. Analysis & Production – After the data is in a usable format, it should be used to achieve the goals set in the first phase. Common techniques may include log correlation or other methods to identify anomalous activity in the environment.
5. Dissemination – This phase includes the distribution of threat data to different stakeholders. Based on this activity, the security personnel can act according to the information discovered, and new mitigation or prevention capabilities may be developed.
6. Feedback – The final phase includes analyzing the data from previous phases. Is the TI collected still actionable? Have the goals been met? This phase is important in improving the organization's TI capabilities.

## 2.4 Implementing threat intelligence

Referring to the threat intelligence cycle, the first phase direction assumes that a request or demand for threat intelligence has been established. Roberts (2021) proposes that every organization implementing a threat intelligence program should have in place a process to identify a process for developing threat intelligence requirements. As each organization has its own challenges, the intelligence requirements depend on multiple circumstances, such as available resources, tools, prevalent threat actors, IT-environment, and many other dependencies. A good starting point is to consider the character and digital footprint of the organization. For example, a small private company is less likely to be targeted by a nation-state threat actor, and threats like espionage are less likely to occur in such an organization. While all kinds of organizations can be targeted by various threat actors with varying levels of sophistication, the trend indicates that a ransomware attack by a threat actor with high level of sophistication is more likely to occur in a company that will have the funds to pay out significant amount of ransom.

Geographical location can also play a role in determining threat intelligence needs. The political climate can influence politically motivated threat actors, and territorial data handling legislations such as the General Data Protection Regulation (GDPR) can cause hindrance to the ability of intelligence sharing between multiple territories. One of the subjects contributing to an organization's digital footprint is the technological solutions in use for the organization. A fully cloud-hosted IT environment has different demands than on-premises devices. An understanding of the organization's critical systems and networks is important from a threat intelligence perspective, as it can assist with prioritizing and resource allocation. The profile of the company attracts different threats and threat actors, an organization only doing business in finance will face different threats from a company that only does business in retail (Roberts, 2021).

When business requirements have been set according to the first phase of threat intelligence cycle, the second stage is the collection phase. Sources for threat intelligence will depend on the requirements, resources, tools, and expertise available. Requirements should indicate some direction for what reliable sources are to achieve them, the next steps are to identify the necessary intelligence sources (Roberts, 2021). A reference figure for banking industry threat intelligence sources as described by McGowan (2018) is illustrated in Figure 4 below.



Figure 4. Banking industry threat intelligence sources (McGowan, 2018).

#### 2.4.1 Threat intelligence feeds

Threat intelligence feeds can be commercial, sometimes integrated into the security service or tool provided. However, there are many crowd-sourced, or community driven threat intelligence feeds, such as AlienVault Open Threat Exchange freely available for anyone to use. Tactical threat intelligence feeds generally consist of Indicators of Compromise (IoCs) (Cooper, 2023).

While implementing IoC-based detection and prevention capabilities with available threat feeds and automation is important, this approach has disadvantages. Setting up a command & control or web domain that hosts phishing content is a trivial task for the adversaries and the number of IoCs is constantly increasing, making it an impossible task to manage and prevent attacks solely based

on them. Analyzing hundreds of thousands of IoCs is not a realistically achievable task and leads to overload of information. Also, most IoCs will not likely be relevant to the target organization. However, with adequate analysis IoCs can be used to identify trends and campaigns and connect them to different threat actors and the TTPs used by them (Roberts, 2021).

#### **2.4.2 News Reports, blogs, and social media**

There exist numerous sources for news reports and blogs concentrating on technology and cyber security related topics. The level of reliability of these open sources should be considered when consuming intelligence from them however, as they can considerably vary in quality. Blog posts from security researchers can be valuable information when researching vulnerabilities and proof-of-concepts from exploits generated by information security professionals. Many social media platforms offer the ability to follow feeds and keywords related to cyber security. This can be a valuable method of keeping track of emerging threats and news about vulnerabilities, as plenty of security professionals and cyber security services providers participate in these platforms. Even threat actors have been known to use social media platforms to promote their attacks (Roberts, 2021).

#### **2.4.3 Data breach, patch, and vulnerability notifications**

Data breach is sometimes used interchangeably with the term cyber-attack but cyberattacks do not always lead to a data breach and not all data breaches are caused by cyberattacks. A data breach is an event where an unauthorized party gains access to information without the permission of the system owner. A data breach can lead to the loss of proprietary and confidential information, such as personally identifiable information (PII), credit card information or other sensitive data. An example of an attack that doesn't imply data breach is a distributed denial of service (DoS) attack (IBM, n.d.).

Organizations can be indirectly impacted by the exposure of login credentials used by their employees or suppliers. The risk of affected users utilizing the same login details across both the breached service and the organization's systems is a possibility. Data breaches can give insight on how the attackers compromised the victim systems and thus give information on the adversary

methods of operation. If the same technologies are used in another organization, this information can be beneficial to mitigate the attack techniques used by the adversary (Roberts, 2021).

Knowing when the environment has vulnerabilities and patching requirements is of high importance for preventing cyberattacks. Vulnerability and patch notifications, when used with threat intelligence, help with prioritizing critical vulnerabilities within the environment. CTI can help with raising urgency by adding necessary context to the vulnerabilities for immediate actions to mitigate the exposure (Roberts, 2021).

## **2.5 Threat information sharing**

Threat information in context to sharing refers to any specific information connected to a threat or attacker characteristics that can be utilized by the defender to protect against a cyberattack (Johnson et al., 2016).

Threat information can be obtained by various methods and numerous sources. Often intelligence is shared within an industry, or between nationwide actors. Benefits behind threat information sharing include access for an organization to threat intelligence otherwise unavailable to them (Johnson et al., 2016). Co-operation between organizations allows them to share resources and capabilities with their partners and affiliates in the industry, to leverage their knowledge and experiences proactively. The threat intelligence sharing process as described by Homeland Security in their publication for Critical Infrastructure Threat Information Sharing Framework is illustrated in Figure 5 below.

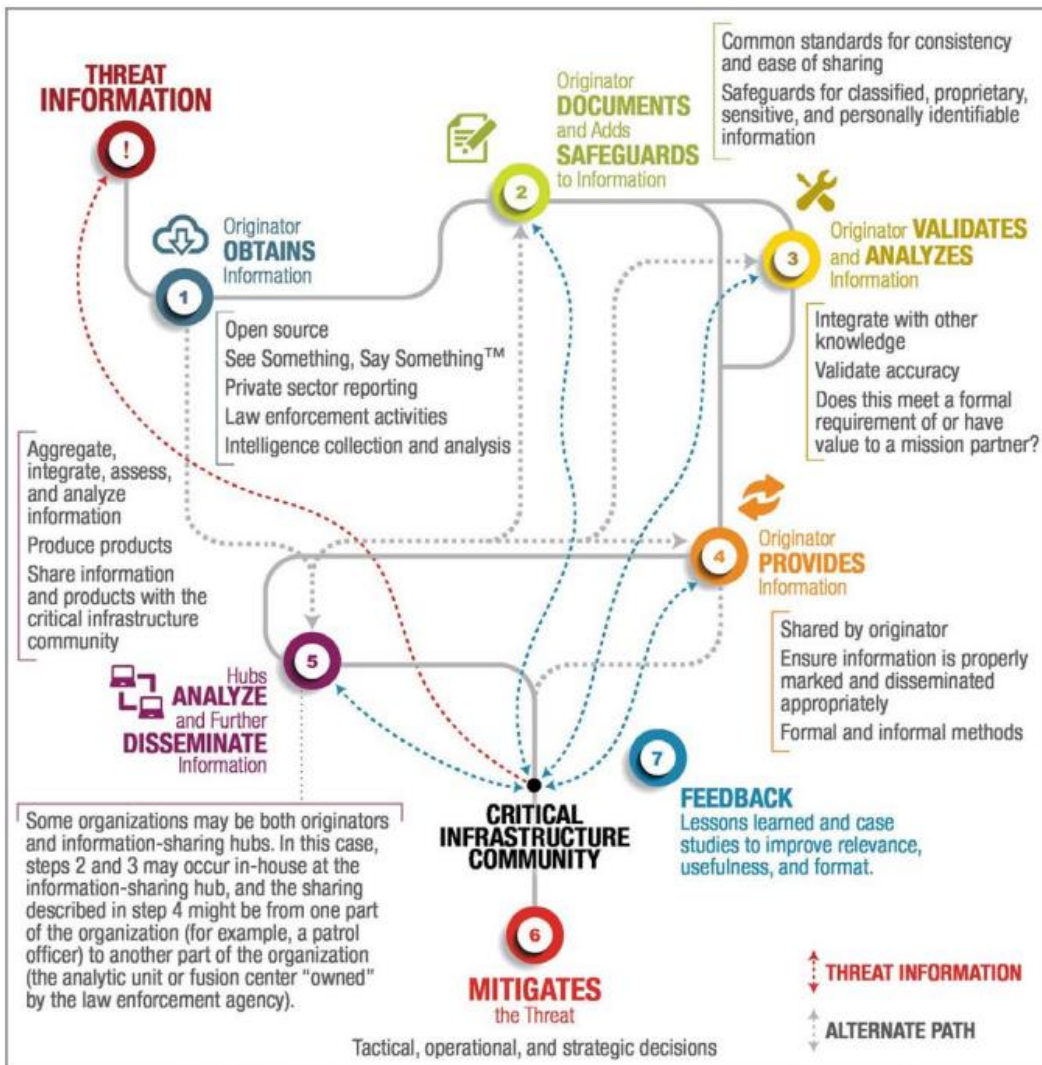


Figure 5. Threat information sharing process (Homeland Security, 2016)

Indicators are technical observables and artifacts, which might suggest an attack being underway or imminent in the target organization. Indicators are utilized in technical controls to make defending against threats and detection of compromise easier. Examples of indicators include Internet Protocol (IP) addresses that may be used for malicious purposes, Domain Name System (DNS) domain names, Uniform Resource Locators (URL) hosting potentially harmful content, or file hashes indicating a virus or otherwise malicious executables (Johnson et al., 2016).

Tactics, techniques, and procedures (TTPs) are a description of methods and behaviors applied by threat actors (Johnson et al., 2016). Tactics describe the highest level of behavior in the distinct stages of cyberattack kill chain. Examples of these stages may include reconnaissance, delivery,

and exploitation, and acting on the objectives (Raza, 2023). Techniques are more specific descriptions of actions committed within the context of a tactic (Johnson et al., 2016). Techniques are often described as generic activity applicable to any cyberattack. Techniques do not specify the tools and technology employed in an attack, but rather the methods and patterns involved (Raza, 2023). Procedures are the lowest level, specific operations committed within the context of techniques by threat actors. Procedures can be used to identify different threat actors' tendency to use specific order of operations, tools, and distinct malware variants deployed in a cyberattack (Johnson et al., 2016).

Security alerts include several types of advisories, bulletins, and notes often about vulnerabilities, exploits, and security issues. These are most often human-readable, technical documentation regarding current pertinent security-related observations. Sources for this information often originate from commercial security service providers, Product Security Incident Response Teams (PSIRTs), researchers, and national or governmental entities such as CERTS and ISACs (Johnson et al., 2016).

Threat intelligence reports are documentation about active threat actors, TTPs, technologies, and products actively targeted. Threat intelligence reports contain information that has been readily enriched with added context (Johnson et al., 2016). Threat intelligence reports can be important contributors to organizations' situational awareness.

Tool configurations offer information about setting up and utilizing tools that support necessary features for threat information processing, such as analysis, sharing capabilities and ingestion of threat information. This information could include context for how to set up malware detection and response capabilities, access control lists (ACLs) or firewall rules for network perimeter security devices (Johnson et al., 2016).

## **CERT**

National Computer Emergency Readiness Teams (CERTs) have been established by many countries nowadays. In Finland, the national CERTs (CERT-FI) purpose is to investigate data security breaches



in services, communication, and other services, and disseminate and communicate security related information (Kyberturvallisuuskeskus, 2022).

### **Information sharing and analysis centers**

Information sharing and analysis centers (ISACs) are information-sharing networks for different sectors, specifically for those that have a significant role in ensuring the functioning of critical services of a society. ISACs handle various cyber security-related information, like best practices and industry-specific threats (Kyberturvallisuuskeskus, 2022). The Finnish National Cyber Security Center manages various ISACs in Finland.

### **STIX / TAXII**

For organizations to be able to process and use threat intelligence in any tooling, standardization is needed for threat intelligence management and sharing purposes. Structured Threat Information Expression (STIX) is a format for exchanging Cyber Threat intelligence (Chapple & Seidl, 2020, p. 41). STIX allows security functions to contribute to and ingest CTI. STIX can be stored in a machine-readable format in JavaScript Object Notation (JSON) or be visually represented to security personnel as the format is human-readable. The latest version of STIX 2.1 defines up to 18 different STIX Domain Objects (SDOs). SDOs define the profile of various cyber threat intelligence. Examples of SDOs are Indicators, Malwares, Threat Actors and Tools (OASIS, 2023).

STIX Cyber-observable objects (SCOs) describe network and host-based information about various artifacts observed, like files, IP-addresses, and domain names (OASIS, 2023). STIX objects are defined via a set of properties describing the characteristics of the object. Properties can include common properties that provide core information about the object, and object specific properties depending on the type of object. An example of properties usable by malware SDO is illustrated in Table 1. below.

Table 1. STIX 2.1 format malware indicator attributes (OASIS, 2021)

Property	Type	Example value	Property type	Required?
type	string	malware	Common	Yes
spec_version	string	2.1	Common	Yes
id	string	malware-- 0a9c0h87-opf6- 5a1k-ao3g- mar328jd1031	Common	Yes
created	timestamp	2022-06- 11T09:11:24.000Z	Malware Specific	No
modified	Timestamp	2022-06- 11T09:11:24.000Z	Malware Specific	No
name	string	Keylogger	Malware Specific	No
description	string	Keystroke steal- ing software	Malware Specific	No
malware_types	list (open- vocab)	keylogger	Malware Specific	No
is_family	boolean	false	Malware Specific	Yes

Same malware properties in the table above, presented in JSON:

```
{
  "type": "malware",
  "spec_version": "2.1",
  "id": "malware--0a9c0h87-opf6-5a1k-ao3g-mar328jd1031",
  "created": "2022-06-11T09:11:24.000Z",
  "modified": "2022-06-11T09:11:24.000Z",
  "name": "Keylogger",
  "description": "Keystroke stealing software ",
  "malware_types": ["keylogger"],
  "is_family": false
}
```

Some SDOs and SCOs may have a relationship with another, that can be defined with STIX Relationship Objects (SROs). An example of relationship between two SCOs is a domain name that resolves to IPv4 IP-Address. An SRO can be used to link these two objects to one another (OASIS, 2021).

Some properties on STIX encourage the usage of open vocabularies, like in the previous example the malware type property. Using values from open vocabularies ensures that same definitions are used across all entities sharing CTI, for example one entity using “keylogger” and another using “keylogging-virus” (OASIS, 2021).

Trusted Automated Exchange of Intelligence Information (TAXII) is a protocol specifically designed for CTI exchange between various actors over HTTPS. TAXII's key concepts are collection, allowing an entity to maintain a repository of STIX data and keep it readily available for consumers of the data, and channel allowing the distribution of the data. These concepts allow organizing and distributing the data, for example, to specific groups based on trust (OASIS, 2023b).

### **3.2.5 The Pyramid Of Pain**

As stated before, indicators of compromise are observables and artifacts linked to malicious activity, like IP addresses, domains, and URLs. While these are examples of straightforward technical artifacts, an IoC might also include behaviors and tools that indicate unusual activity in the Environment. A Cyber Security Professional David J Bianco came up with the concept of the pyramid of pain, following a report on APT group called CommonCrew, released by a security services provider Mandiant. The Pyramid of Pain demonstrates the effectiveness of denying attackers from using certain indicators when commencing Cyber Attacks. Bianco produced the idea of the concept when realizing that defenders are not using indicators effectively when responding to them. The perception is that by responding quickly to the indicators, the defender denies the adversaries their methods of attack. However, not all indicators are equal when denying their usage. The higher up we move in the pyramid of pain, the harder it is for the adversaries to attack their target, essentially making attacking more painful for the attackers (DavidJBianco, 2014). The hierarchy of the Pyramid of Pain is illustrated in Figure 6 below:

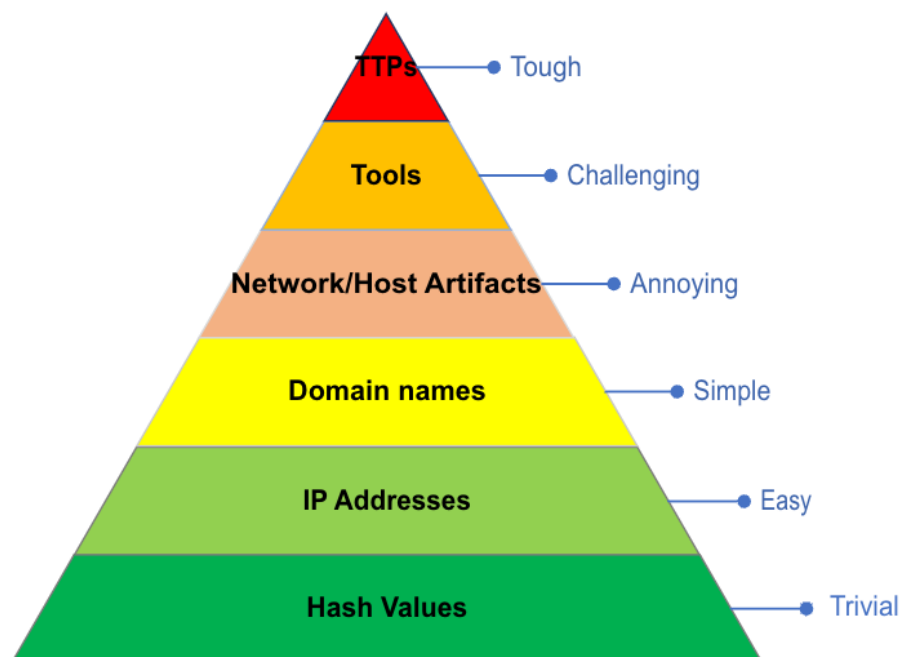


Figure 6, The Pyramid of Pain (DavidJBianco, 2014).

Hash values are the most rudimentary form of indicators. Most hash algorithms are based on computing a digest from an input. This input is transformed into a fixed length output, generally different for each input file. Common hash algorithms include MD5, SHA1 and SHA256. While hashes are extremely accurate, tracking them may prove difficult as even the tiniest modification to the input data changes the hash value (DavidJBianco, 2014). Hash indicators are commonly used to detect and prevent various types of malicious files or malware on devices. Challenges with hash indicators are that they are often not feasible to prevent fileless attacks, and the sheer amount of them existing makes managing them hard.

IP-addresses or netblocks are the second to least trivial indicator for the attackers. While restricting access from IP-addresses may provide momentary protection, switching IP-addresses is an effortless task for the attackers. This effect is amplified with the usage of anonymization services like Tor that allow rapid changing of IP-addresses (DavidJBianco, 2014). Common use cases for IP-addresses are detecting malicious network connections in the environment. Examples of malicious connections are command & control traffic, and user login events from tor and anonymizing proxy services.

Next up on the hierarchy are domain names. While the availability of free domain registration services with lenient standards for registration is high, it still requires more effort for the attackers to change domain names in comparison to IP-addresses. Domains require registration, may require a fee, and often take some time to be functional (DavidJBianco, 2014). Domain name IoCs are useful in identifying network connections to malicious web services, like phishing sites.

The third most painful form of indicators are network and host artifacts, which is the first stage where the actual noticeable impact on the adversary actions should be impacted. An example of such an indicator is reconnaissance tools using HTTP protocol where distinct user agents can be observed. Successfully intercepting such tools would require more thoughtful actions from the attackers, like reconfiguring their tools, forcing them to spend time on developing new methods. While this is not likely to completely thwart the attack, it forces the attackers to spend resources in overcoming an obstacle (DavidJBianco, 2014).

Second to the top are tools, referring to the technical accessories available to adversaries. Responding on this level would mean that the capability to detect various artifacts has developed to the level that adjustments to the tooling made by the adversaries are no longer able to bypass detection. For the attackers to continue, they would be required to either find or create new tools to achieve the same objective, requiring time invested in developing new capabilities and training to use them. YARA signatures are an example of tools that can be able to recognize slight to moderate changes in malware, in contrast to detection capability based solely on individual file hashes (DavidJBianco, 2014).

On the top of the pyramid are TTPs. As opposed to reacting based on adversary tools, on this level the defenders are operating directly against attacker behaviors. This would mean that in case for example in a pass-the-hash attack, the defenders would detect the actual occurrence of pass-the-hash activity, by discovering anomalies and patterns in logs, rather than observing the attackers' tools used to execute such attack. Successfully denying the adversaries their behaviors would require them to either reinvent new behaviors or give up on their operation. As creating new behaviors would often require excessive time and resources, the latter may often be what attackers opt to (DavidJBianco, 2014).

## 2.6 Applying threat intelligence

A comprehensive threat intelligence framework requires co-operation between multiple segments of an organization. Threat intelligence may be utilized by various security functions, like vulnerability management, risk management and incident response (Chapple & Seidl, 2020, p. 53-54). Common use cases for threat intelligence include improving the efficiency of security solutions by enriching information processed by them. Threat intelligence may assist by enhancing decision-making and detection capabilities when working with security incidents, in tools like SIEM, Firewalls, Intrusion detection (IDS) and prevention (IPS) systems (The Recorded Future Team, 2018).

Threat intelligence can aid organizations in vulnerability management by providing information and statistics relevant to prioritizing vulnerabilities. While the traditional approach to fixing vulnerabilities might be that “everything should be patched all the time” leads to often impossible standards, accurate threat intelligence assists in identifying the most likely exploited vulnerabilities and weaknesses (The Recorded Future Team, 2018).

### 2.6.1 Security Tools

When combining security tools and IoCs, the threat intelligence used is on the tactical level, focusing on the ‘how’ and ‘what’ rather than the long-term effects. In this form, threat intelligence can be taken advantage of to rapidly stop network communications with infected systems or detect security breaches within the company network (Lee, 2023). Many traditional security tools can take advantage of threat intelligence, especially in the form of indicators of compromise. IoCs can enhance detection and response capabilities to various cyber-attacks.

### SIEM

Security Information and Event management (SIEM) systems collect data and telemetry, analyzing and transforming the data ingested into alerts, reports, and dashboards. SIEM can be used for continuous security monitoring and threat hunting. SIEM acts as the central point for log management and correlation from various sources and can collect information like logs and events from IT devices and systems, providing a holistic view of the environment to security personnel. These log

sources can include network devices like firewalls and routers, endpoint devices like laptops, servers, and business-critical applications. A SIEM solution can also help some organizations meet requirements introduced by regulations and compliance (Elastic, n.d.). An illustration of a SIEM system correlating internal data with external threat intelligence, including the incident response function is illustrated in Figure 7 below.

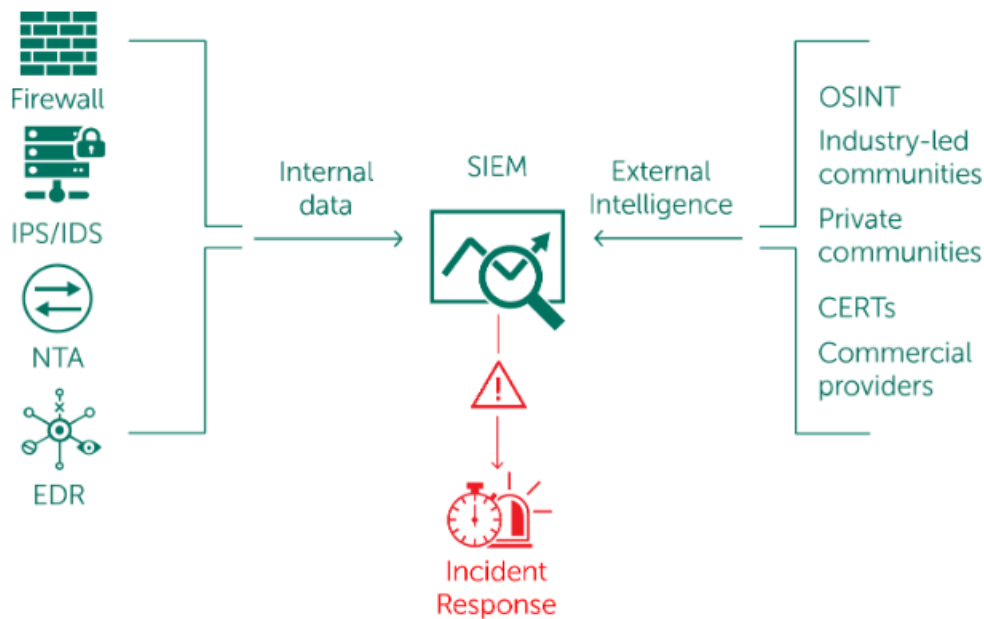


Figure 7. SIEM, threat intelligence and incident response (Karasev, 2019)

Microsoft Sentinel is an example of a cloud-native security solution, with SIEM capabilities. Most generic forms of threat intelligence utilized in SIEM solutions are IOCs, like IP addresses, domain names URLs, and file hashes. Sentinel supports STIX/TAXII feeds and can be integrated with multiple threat intelligence platform solutions like MISP. Sentinel supports rule-based alert correlation, where security rules compare threat intelligence indicators created in sentinel to raw data from integrated data sources. While it is possible to produce these analytic rules from scratch, Microsoft Sentinel provides capabilities for threat intelligence-based analytic rules out-of-the-box (austinmccollum et al., 2023).

## Endpoint security

Antivirus or AV has been a traditional tool for enterprises to prevent known malicious files, by comparing signatures from files to a database of known malicious files of the Antivirus scanner. If a match is established between a file and a signature, the AV tool would block the computer from executing the file. The signatures of the database would consist of file hashes, or potentially describe a set of attributes typical for malware, that matches with malware like file type, file size, or human-readable strings. The drawback of traditional antivirus includes the evolving threat landscape and sophistication of cyber-attacks. The constantly increasing number of signatures and attackers' ability to modify and obfuscate characteristics of their malware make maintaining a satisfactory database of signatures difficult. Additionally, the sophistication of TTPs has led to some actors utilizing fileless attacks bypassing signature-based antivirus tools. (SentinelOne, 2021).

Endpoint Detection and Response (EDR) is the successor of traditional antivirus. EDRs build on top of signature-based detection by introducing capabilities for deeper analysis based on data collected on the endpoints. EDRs can detect malicious activity based on patterns and telemetry and include means for responding to threats observed on the systems. (SentinelOne, 2021). Microsoft Defender for Endpoint allows defining lists of IoCs to enhance the detection and prevention of malicious activities. IP and URL indicators can be leveraged to manage site access to malicious content and file hash indicators can be used to block malicious or potentially unwanted applications. (diannegali et al., 2024)

### 2.6.2 Threat Intelligence platforms

Threat intelligence platform (TIP) is a tool used to organize and aggregate threat information from various sources. TIPs can help with contextualizing threat intelligence with enrichment and provide a holistic view of threat intelligence. As the amount of threat intelligence increases over time, TIPs can process this information in various formats, streamlining the process. TIPs also enable the cross-organization sharing of intelligence (Palo Alto Networks, n.d.).



## MISP

A commonly used tool is the Malware Information Sharing Platform (MISP) Threat Sharing platform. The platform is open source and allows an organization to leverage industry-wide threat intelligence by sharing, distributing, and collecting threat intelligence within their industry (Collins et al., 2021). MISP has achieved wide popularity as the project was adopted in to use in 2013 by the North Atlantic Treaty Organization (NATO) with the goal of expanding information-sharing capability to all NATO nations (NATO, 2013). While many other threat intelligence platforms exist, MISP is likely the most widely used freely available sharing platform in threat intelligence activities.

## OpenCTI

OpenCTI is an opensource TIP developed by Filigran in collaboration with national cyber security departments such as French National Cybersecurity agency (ANSSI) and the CERT of European Union CERT-EU. The product supports a wide variety of threat information schemas such as STIX2 and allows nested relationships between various threat objects and IoCs (Demir, 2023).

### 2.6.3 Threat hunting

Threat hunting is an approach for organizations to increase their cybersecurity resilience against adversaries. While a formal definition of threat hunting does not exist, the SANS institution definition of threat hunting is an *“analyst-driven process to search for attacker tactics, techniques, and procedures (TTP) within an environment”* (Gunter & Seitz, 2021. Abstract). The fundamental point of threat hunting is that attacker TTPs’ must be analyzed and understood to be able to find anomalies in data collection. Threat intelligence can add context to TTPs pertinent to attackers as information about IOCs, behaviors, and various signatures observed in organizations’ threat intelligence. This information should contain systems affected, target industries, and the kinds of vulnerabilities and protocols that are exploited. As threat hunting is attacker-focused, satisfactory threat intelligence should be acquired to ensure successful results. (Gunter & Seitz, 2021).

Whereas incident response and security monitoring are reactive processes, threat hunting may provide the organization with a proactive method of uncovering attackers present in an environment. A formal threat hunting process is required to ensure the integrity and success of hunting,

and to be able to handle such investigations rigorously. The methodology utilized by the adversaries is analogous, despite having variable levels of sophistication and techniques (Peiris et al., 2021, p. 6).

## **2.7 Attack frameworks**

Attack frameworks aim to describe attack methodologies to help defenders understand attacks and attacker methods and to help them appropriate their defenses. While an organization might employ its own threat assessment practices, some attack frameworks might assist in this task, especially when looking into the more technical side of defense. Three examples of the more widely known attack frameworks are MITRE's ATT&CK Framework, Lockheed Martin's Cyber Kill Chain and The Diamond Model of Intrusion Analysis (Chapple & Seidl, 2020, p. 48-51).

### **MITRE ATT&CK Framework**

MITRE ATT&CK Framework is an extensive library of advisory tactics, techniques, and procedures. The Abbreviation of ATT&CK stands for Adversary Tactics, Techniques, and Common Knowledge. The Framework was developed to record the various methods used by adversaries in a cyberattack in its numerous stages, recording the techniques used by adversaries in relation to their tactics (Buckbee, 2023).

The ATT&CK Framework was developed by MITRE initially in 2013. It has since been evolving and as new vectors of attack and vulnerabilities surface, they are included in the ATT&CK framework. The Framework has since been widely accepted as the industry standard regarding information about attacker behaviors, tools, and remediating actions. The knowledge from the ATT&CK framework can be used in various security functions, from red teaming to threat hunting, threat intelligence, and risk management (VMware, n.d.). As of writing this, the ATT&CK framework has gone through multiple iterations, and currently, the latest version of MITRE ATT&CK is v14 comprising of 14 tactics, 201 techniques and over 400 sub-techniques (The MITRE Corporation, n.d.).

The ATT&CK Framework is built on three foundational ideas. Tactics describe the short-term goals of the attackers, including initial access, reconnaissance, exfiltration, lateral movement, and other high-level descriptions. Techniques illustrate the lower-level methods used to achieve the higher-



The PRE-ATT&CK Matrix focuses on activities conducted by adversaries often outside of the organizations' visibility, making them hard to detect. Such activities might include gathering information available on the internet, knowledge about relationships between an already compromised organization and its partners, or other freely available intelligence and weak points. The PRE-ATT&CK Matrix can help organizations find solutions to monitor and understand such activities better (VMware, n.d.).

The Enterprise ATT&CK Matrix is the largest available matrix from the ATT&CK framework. The enterprise Matrix comprises of the various platforms used in an enterprise infrastructure. The tactics and techniques include information about adversary actions against operating systems like Windows, MacOS, and Linux, and various cloud services including Software as a Service (SaaS), Infrastructure as a Service (IaaS), containers and networks. The Mobile ATT&CK Matrix focuses on actions compromising the IOS and Android devices used in an organization. The matrix expands on the Mobile Threat Catalogue developed by NIST (VMware, n.d.). The ICS ATT&CK Matrix is the latest addition to MITRE's catalog. This matrix concentrates on Industrial Control Systems (ICS), like factories, power grids, and networks in an ICS environment.

The highest-level matrices can also be broken down into subsections. For example, if the organization wants to focus purely on its cloud security, the Enterprise matrix can be filtered to include only cloud-related tactics and techniques. The cloud matrix has considerably reduced attack surface compared to the full enterprise matrix, as things like malware are not related to cloud services, and the cloud environment itself is operated by cloud service providers. This subsection promotes adversary actions against cloud-native features (Trellix, n.d.).

MITRE ATT&CK Framework has multiple use cases depending on the needs of the organization. Authors from MITRE ATT&CK team have consolidated a Getting Started With MITRE ATT&CK eBook from their blog posts, discussing four different scenarios that the framework can be used for. Each use case is divided into three levels of sophistication, depending on the resources and maturity of the target organization (Applebaum et al., 2019).

## **Threat Intelligence**

Understanding pertinent APT's can be an important contributor to decision-making regarding defensive capabilities. A business that primarily works in pharmacy can focus on APT groups that MITRE has documented have been observed to target similar companies. Security analysts can then search for information about tactics and techniques utilized by the APT group in the past and shift their focus to developing mitigation actions directed at the specific methods used by the APT group. (Applebaum et al., 2019).

## **Detection and analytics**

ATT&CK framework-based development of detection capabilities are based on telemetry from organizations' environment, as opposed to the usual method of finding commonly known threats. ATT&CK techniques have listed data sources for the detection of each technique. Security personnel can then identify which data sources are required to detect each technique. Once the data sources have been identified, they can be processed with appropriate tools for further analysis. Many techniques are incorporated with pseudocode for what to look for to detect the adversary behavior in question, which can then be translated to the tools used for analysis (Applebaum et al., 2019).

## **Adversary Emulation and Red Teaming**

Red teaming is the act of emulating attackers to test the security within an organization, utilizing methods used by adversaries to gain access to the organization's data. The practice can include actual hacking activities too, also referred to as penetration testing. The purpose of red teaming is to discover security weaknesses and vulnerabilities within the assessed environment. With this information the target organization can apply fixes to their security posture before the occurrence of destructive cyberattack (Harrington, 2022). The precise process of red teaming is dependent on the assessment, but a general advancement of such assessment is described in Figure 9 below.

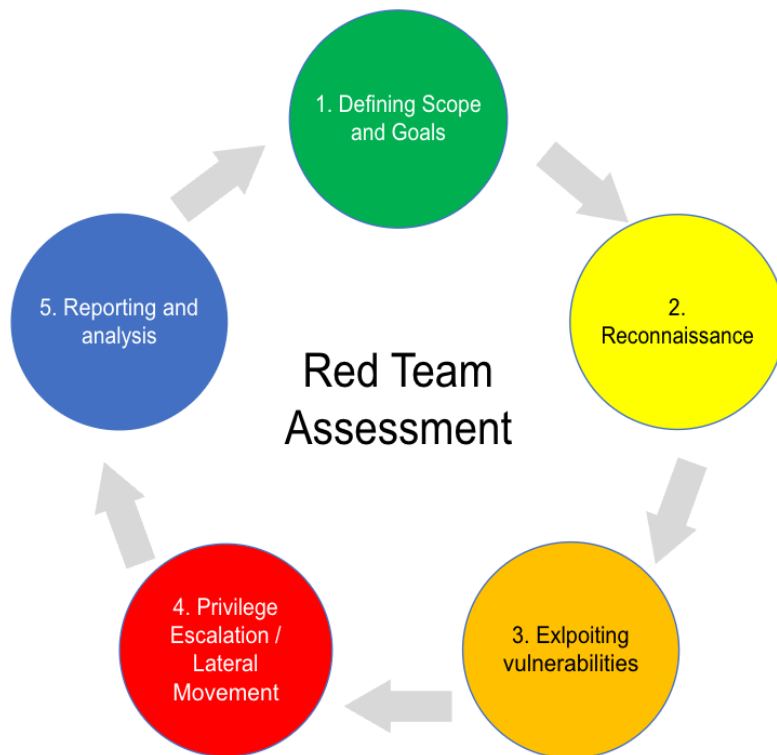


Figure 9. Red Team Assessment (Harrington, 2022)

ATT&CK can help red teamers and penetration testers in creating various attack scenarios based on the techniques introduced in ATT&CK. As ATT&CK comes with a large knowledge base of real-world adversary actions, it can support with creation of realistic scenarios applicable to the target organization. Adversary scenarios can help defenders focus on singular techniques and test their defensive capabilities (Applebaum et al., 2019).

### **Assessments and Engineering**

ATT&CK can be used to assess defensive capabilities to find gaps in organizations' security posture. One method of doing this is to map security tools and procedures to the tactics and techniques introduced in ATT&CK. By understanding the gaps in security posture, it is then possible to prioritize disparities in coverage and modify existing capabilities accordingly (Applebaum et al., 2019).

### 3 Development plan

This section covers the actions required to initiate the implementation of threat intelligence management program. Implementation of the system is based on previous chapters that cover the considerations required for successfully improving current threat intelligence capabilities, its management and continuous development, including tools, threat intelligence sources and processes.

As threat information management is already partially in place within the organization, a thorough analysis of the current situation is being conducted. This analysis will rely on business requirements and standards to identify areas of improvement within the existing model, which can be implemented to achieve the desired target state. A development plan is implemented to assist in the methodical development of threat intelligence management system as described in Figure 10 below.

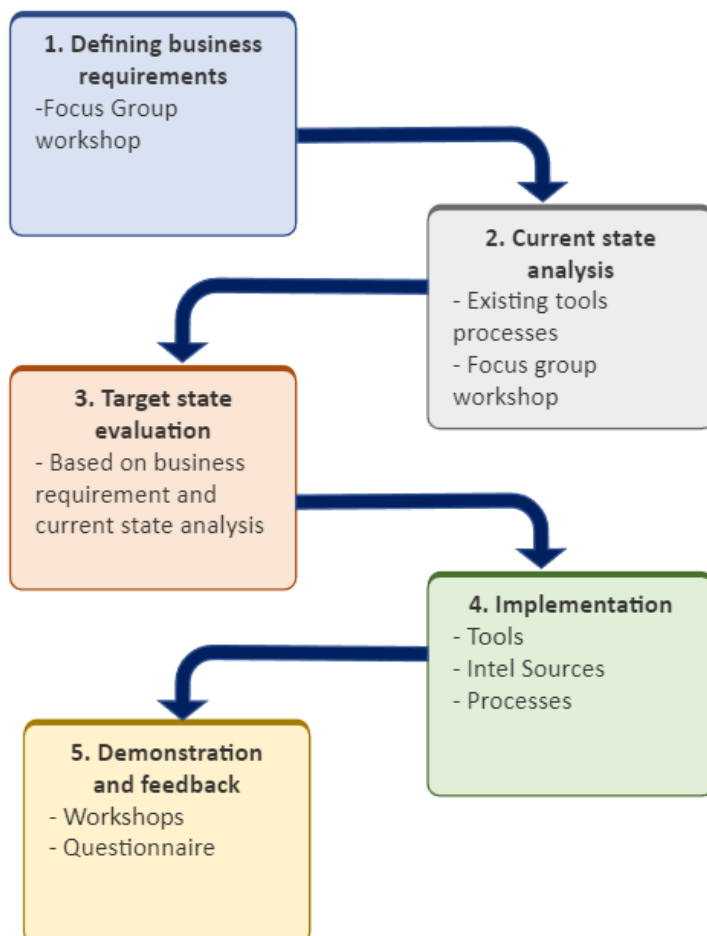


Figure 10. Development plan

1. Defining business requirements will be done in workshops within the cyber security team. This process will leverage the knowledge of the team members, their understanding of requirements for threat intelligence, and the standards used to assess the target use cases for threat intelligence.
2. Current state analysis will be evaluated via existing documentation, current utilization of threat intelligence, and the processes employed to process it.
3. Target state evaluation will combine the findings from the first and second phases to analyze the resources and direction of implementation to meet the requirements set in the first phase.
4. The implementation phase involves evaluating, testing, and improving current threat intelligence tools, sources, and processes. A test use case based on a constructed hypothesis will be used to test the implementation.
5. Demonstration and feedback questionnaire are conducted to communicate findings to stakeholders and receive feedback about the implementation.

### **3.1 Focus-group workshop 1. Defining business requirements**

To ensure that the direction of implementing threat intelligence is unanimous within the cyber security operations team, a workshop was arranged between the team members to define the business requirements for the implementation.

The question presented to the focus group was: *“In your opinion, what are the key short-term (3-6 months) goals that should be achieved with threat intelligence to enhance technical cyber security operations that contribute to security related business needs?”*. Based on the discussion the following requirements were selected as the primary goals:

1. Cyber Security functions can utilize threat intelligence tools and processes in monitoring systems to detect and prevent security breaches.
2. Cyber Security functions can use threat intelligence in evaluating and improving detection and prevention capabilities in their assessments.
3. Cyber Security functions can contextualize cyber threats in their reporting.
4. Threat intelligence is utilized in prioritizing the vulnerability management process by providing actionable context to vulnerabilities to support swift mitigating actions.

The scope of the initial development was limited to cover the top three requirements, as the fourth requirement regarding vulnerability management was estimated to be too laborious as a short-term goal.



### 3.2 Focus-group workshop 2. Current state analysis and key development targets

This section presents the groundwork required for starting the development segment of the research with the conducting of current state analysis on utilizing threat intelligence in CSOC and CSIRT operations and defining the target state for threat intelligence with the definition of business requirements. The question presented to the focus group was: *“What sources of threat intelligence are currently used in CSOC and CSIRT operations, how are they applied and what is the context?”* The discussion Identifying currently utilized threat intelligence sources and describing business context is documented in the Table 2 below.

Table 2. Threat intelligence sources and context

TI Source	Application	TI Context
External threat intelligence feeds	SIEM, Monitoring, Threat hunting	Tactical threat intelligence
National CERT Threat Reports	Threat hunting, Vulnerability management	Tactical threat intelligence, Operational threat intelligence
Partner and vendor advisories	Vulnerability management	Operational threat intelligence
Security and IT related News, blogs, and social media	Threat hunting, Vulnerability management, Situational Awareness	Tactical, Operational, Strategic threat intelligence
Vendor Advisories	Vulnerability management	Operational threat intelligence
National CERT Cyber Weather	Situational Awareness	Strategic Threat intelligence

1. Holistic view to threat intelligence does not exist. Currently management of threat intelligence is lacking as no systematic procedures have been defined.
2. While analysis on some forms of threat intelligence is conducted on operational and strategic level, it is lacking in the tactical level.
3. Contextualizing and enrichment of tactical threat intelligence is minimal. Currently enrichment is mostly manual.
4. Reporting and threat intelligence's contribution to situational awareness is not methodical.

As part of the current state analysis a maturity assessment was conducted based on ISF SOGP healthcheck questionnaire section TM1.4 introduced in chapter 1.3. The current state analysis was conducted to gain an understanding of targets for improvement in developing a higher maturity for threat intelligence management. Questionnaire for current and target state maturity assessments is documented in Table 3. The evaluation principle follows an assessment criterion of five levels from zero to four, zero meaning that the following question is in no case adhered to, two meaning the question is adhered to in about half of cases, and four meaning that the question is adhered to in all cases.

Table 3. Threat intelligence maturity assessment

Maturity Assessment question	Current state	Grading
1. Does a capability to create and manage threat intelligence exist with sufficient analytical tools and an intelligence cycle supporting it?	The capability to process threat intelligence exists with multiple security tools. Centralized management tools for threat intelligence do not exist. Intelligence cycle is loosely applied but a formal process is lacking	1
2. Is the range of external and internal sources for information about threats and other supporting details sufficient?	Some sources are acquired via unsystematic evaluation. No profound analysis has been performed to evaluate the sufficiency of current TI sources.	2
3. Does the capability to perform specialized activity leveraging threat intelligence exist to identify activity that may lead to a security breach?	Threat hunting and security monitoring capabilities exist, but threat intelligence is only loosely applied.	2
4. Does a process exist for regular review and improvement of intelligence capabilities and processes?	No formal process has been described for continuous threat hunting. Playbooks for limited use cases exist.	1

The target grading achievable via this evaluation will remain ambiguous as the grading is based on estimates rather than easily quantifiable values and should be reassessed sometime after development. However, the answers to the questionnaire provides some observations that can be used in determining points of improvement.

Conclusions for improving target state grading:

1. Implementing a centralized threat intelligence management tool for ingesting threat intelligence centrally will improve the capability for distributing threat intelligence for applications defined by business requirements. Procedures for managing the intelligence cycle should be created and enforced.
2. Evaluation on threat intelligence should be improved via analysis and enrichment of threat information. Evaluating the sufficiency of current threat intelligence sources is difficult as no intelligence tools are utilized.
3. Threat intelligence should be increasingly applied to security monitoring and threat hunting activities. Automation capabilities for processing threat intelligence with security tools should be improved.
4. Threat intelligence cycle should be applied to regularly review and improve threat intelligence capabilities.

The following proposals were deducted as the pivotal development targets for improving the threat intelligence management capability:

- **Threat intelligence platform** for centralized ingestion, analysis, distribution, and holistic view of threat information.
- **Threat intelligence cycle** for continuous evaluation and improvement of threat intelligence capabilities.
- **Automation** for processing threat information to improve CSOC and CSIRT capabilities for rapid detection and response to cyber threats.
- **Framework** for understanding threats and assessing the defensive capabilities of Cyber Security operations.

## 4 Implementation

This section covers the implementation and testing phase of the development research. The implementation phase started with evaluating a Threat Intelligence Platform tool suitable for testing. I decided to evaluate two different TIP solutions, MISIP and OpenCTI. Based on the knowledge gained during the research I constructed a simple comparison table between the two solutions to

ensure that the requirements set in previous stages of the development plan are met, as seen in Table 4.

Table 4. TIP evaluation

Requirement	OpenCTI	MISP
1. Support for MITRE ATT&CK	x	x
2. Support for vulnerability notifications (at minimum RSS Feeds)	x	x
3. Integration with MS Sentinel	x	x
4. Support for the enrichment of indicators	x	x
5. Support for STIX Relationships	x	x
6. Support for visualization & reporting	x	x
7. Support for the top 2 levels of indicators of the Pyramid of Pain	x	x

While both the solutions meet the requirements set in the evaluation, I decided to use OpenCTI for the research. While MISP is considered the industry standard TIP, the rationale behind selecting OpenCTI is that a data connector is offered in the Azure Marketplace, providing an integration between Microsoft Sentinel SIEM and OpenCTI for two-way ingestion of indicators. While MISP does offer documentation on how to configure integration with Microsoft Sentinel, this integration seems more convoluted to implement and is not offered in the Azure Marketplace. The downside of choosing OpenCTI is that since it is a product with a shorter development time, the features are more limited compared to the MISP. Conversely, MISP has a lot of unnecessary features for the purpose of this demonstration, making the user interface more cluttered and difficult to navigate.

#### 4.1 TIP Installation

The installation of OpenCTI was done on a minimal install of Ubuntu 22.04LTS virtual machine on VMware Workstation Player with the following specifications seen in Table 5.

Table 5. Test machine specifications

Property	Value
Image	Ubuntu-22.04.3-desktop-amd64
Virtual machine name	opencti-testing-vm1
Memory	8192 MB
Storage	60 GB
CPU	4

Portainer, an open-source container management software was additionally chosen to manage the software stack, as OpenCTI offers the option to install it in a containerized environment using docker images. The diagram in Figure 11 below shows the reference to OpenCTI Architecture with its various components.

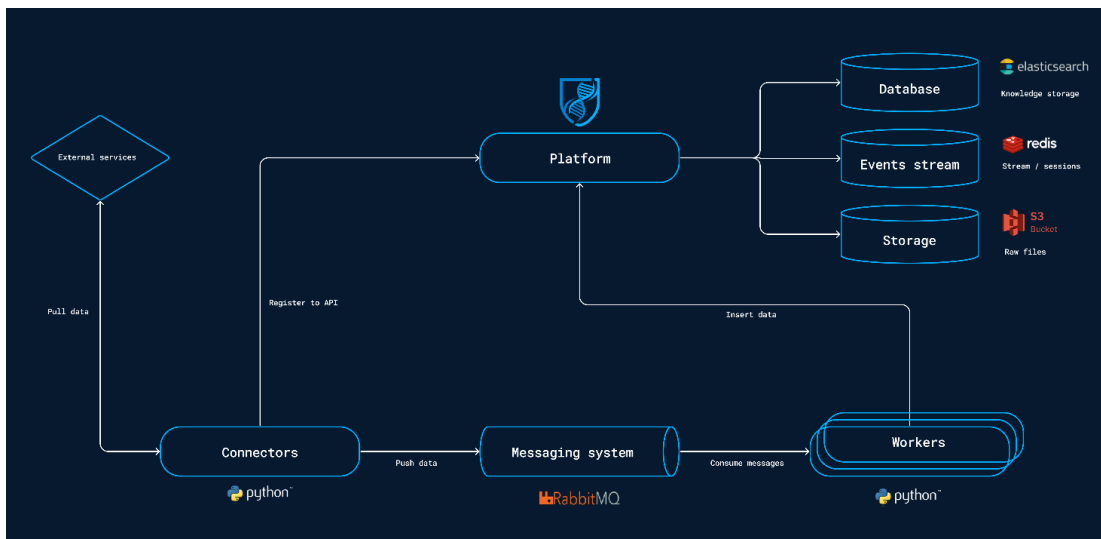


Figure 11. OpenCTI Architecture (Filigran, n.d.)

Portainer and OpenCTI stack installation was carried out following the official installation guide of OpenCTI and the installation guide by ZDS (2013), as seen in Appendix 1. To install OpenCTI con-

tainers, the **docker-compose.yml** file, and the **.env.sample** files (with minor modifications) available on the OpenCTI GitHub page were deployed, as shown in Appendix 2. After the installation was completed, the status of the newly created containers could be verified in the Portainer UI as shown in Figure 12.

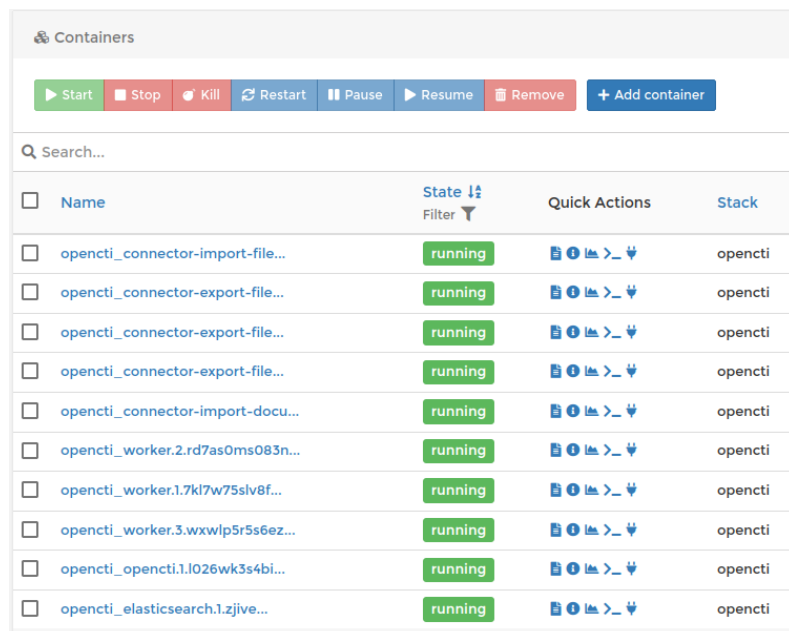


Figure 12. Running containers in Portainer

At this stage, the OpenCTI service is usable, and integration of data sources could be started.

OpenCTI Ecosystem is documented on the Filigrans OpenCTI Ecosystem website (accessible from the GitHub site <https://github.com/OpenCTI-Platform/connectors>). While many of these connectors are freely available to all OpenCTI users, some may require purchasing additional services to gain access to the data connector.

## 4.2 Integrating MITRE ATT&CK

The process of data collection was started with the MITRE Datasets external import connector to ingest information from the ATT&CK knowledge base. Creating data connectors is a fairly simple process, the connector parameters are described in the respective connectors **docker-compose.yml** file in the GitHub. Additionally, each connector must be given permission to access the

OpenCTI application programming interface (API), this can be achieved by creating a user associated to the “Connectors” group and using its access token in the configuration. The connector is then deployed by adding the configuration parameters in the stacks **docker-compose.yml** file and updating the stack in Portainer UI. Example configuration for the MITRE ATT&CK connector is shown in Figure 13.

```
connector-mitre:
  image: opencti/connector-mitre:5.12.33
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=f05cd3a0-09da-4e95-8b1e-29d9f90acd6b
    - CONNECTOR_ID=aa76cbd7-7ac4-4ce1-b7b0-6cc47689fc65
    - "CONNECTOR_NAME=MITRE_Datasets"
    - CONNECTOR_SCOPE=tool,report,malware,identity,campaign,intrusion-set,attack-pattern,course-of-action,x-mitre-data-source,x-mitre-data-component,x-mitre-matrix,x-mitre-tactic,x-mitre-collection
    - CONNECTOR_CONFIDENCE_LEVEL=75
    - CONNECTOR_UPDATE_EXISTING_DATA=false
    - CONNECTOR_RUN_AND_TERMINATE=false
    - CONNECTOR_LOG_LEVEL=error
    - MITRE_REMOVE_STATEMENT_MARKING=true
    - MITRE_INTERVAL=7 # In days
  restart: always
  depends_on:
    - opencti
```

Figure 13. MITRE Datasets connector configuration

With the MITRE Datasets connector, a total of 3709 entities were ingested into the platform with 21542 relationships between the entities, creating an extensive database of information about malware, intrusion sets and TTPs. Analysing the intrusion set APT29, in the description of the threat actor group and various information related to the threat actor can be seen in Figure 14 and 15 below.

**APT29** : IRON RITUAL X IRON HEMLOCK X NobleBaron X Dark Halo X StellarParticle X

OVERVIEW KNOWLEDGE ANALYSES DATA HISTORY

DETAILS

Description  
APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).(Citation: White House Imposing Costs RU Gov April 2021)(Citation: UK Gov Malign RIS Activity April 2021) They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.(Citation: F-Secure The Dukes)(Citation: GRIZZLY STEPPE JAR)(Citation:...

Resource level  
Unknown

Goals  
-

Originates from +  
-

First seen  
-

Last seen  
-

Primary motivation  
Unknown

Secondary motivations

Figure 14. APT29 Description

TIMELINE GLOBAL KILL CHAIN Add filter

Target Types = Attack-Pattern OR Campaign OR Incident X

June 7, 2019 at 11:41:15 PM [T1070] INDICATOR REMOVAL  
[APT29](https://attack.mitre.org/groups/G0016) used...

June 1, 2017 at 12:33:27 AM [T1064] SCRIPTING  
[APT29](https://attack.mitre.org/groups/G0016) has used encoded PowerShell scripts uploaded to...

January 30, 2019 at 4:19:17 PM COBALT STRIKE  
(Citation: FireEye APT29 Nov 2018)

January 30, 2019 at 4:19:17 PM [T1547.009] SHORTCUT MODIFICATION  
[APT29](https://attack.mitre.org/groups/G0016) drops a Windows shortcut file for...

January 30, 2019 at 4:19:17 PM [T1043] COMMONLY USED PORT  
[APT29](https://attack.mitre.org/groups/G0016) has used Port Number 443 for C2.(Citation: FireEye...

Figure 15. APT29 Relationships



### 4.3 Integrating Threat Feeds

At This point, a knowledgebase of threats has been created in the OpenCTI, but it lacks any actionable tactical level threat information that could be directly usable in CSOC and CSIRT operations. OpenCTI supports integrating a range of freely available IoC feeds to the platform. While following the process described in threat intelligence cycle, the quality and suitability of threat intelligence feeds should be evaluated, in the scope of this research it is not necessary as these feeds can be used to demonstrate the intelligence management process.

AlienVault Open Threat Exchange (OTX) feed is a free to use community driven threat exchange and collaboration service offering threat intelligence feeds (Alien Labs Open Threat Exchange, n.d.). The integration process was similar to the integration with MITRE Datasets but required an API access key to the OTX feed via registration to the service. Figure 16 below demonstrates the various types of indicators acquired from the OTX threat feed.

Entity type	TYPE	REPRESENTATION	AUTHOR	CREATORS	LABELS
AND Sighted by/in	DOMAIN NAME	thefinetreats.com	AlienVault	OTX	backdoor, chisel, cyber espionage
	DOMAIN NAME	jeepcarlease.com	AlienVault	OTX	backdoor, chisel, cyber espionage
	DOMAIN NAME	hanagram.jp	AlienVault	OTX	backdoor, chisel, cyber espionage
	DOMAIN NAME	carleasinguru.com	AlienVault	OTX	backdoor, chisel, cyber espionage
	DOMAIN NAME	caduff-sa.ch	AlienVault	OTX	backdoor, chisel, cyber espionage
	DOMAIN NAME	buy-new-car.com	AlienVault	OTX	backdoor, chisel, cyber espionage
	IPV4 ADDRESS	91.193.18.120	AlienVault	OTX	backdoor, chisel, cyber espionage
	FILE	ad4d196b3d85d982343132d52bffc6ebfec7bf30553fa441fd7c3ae495075fc	AlienVault	OTX	backdoor, chisel, cyber espionage
	FILE	b376a3abbae73840e70b2fa3df99d881def9250b42b6bb0458d0445ddfbc044	AlienVault	OTX	backdoor, chisel, cyber espionage
	FILE	267071d7f9927abd1e5710e924dd8a69e1c4ed74e7b69403cddcf6e6a453b	AlienVault	OTX	backdoor, chisel, cyber espionage
	HOSTNAME	yzrhk.kredit-money-fun202.buzz	AlienVault	OTX	disinformation, cyber espionage

Figure 16. OTX Indicators of Compromise

At this point, the capability to ingest actionable, technical threat information has been demonstrated. Taking a closer look to a STIX pattern indicator for IP-address 195.54.160.59, in the knowledge it is possible to see all the relationships to the various attack-patterns related to this IoC (Figure 17).

195.54.160.59

OVERVIEW **KNOWLEDGE** ANALYSES SIGHTINGS DATA HISTORY

Search these results...

RELATIONSHIP TYPE	ENTITY TYPE	NAME
INDICATES	ATTACK PATTE...	Spearphishing Link
BASED ON	IPV4 ADDRESS	195.54.160.59
INDICATES	ATTACK PATTE...	Domains
INDICATES	ATTACK PATTE...	Phishing
INDICATES	ATTACK PATTE...	Server
INDICATES	ATTACK PATTE...	Masquerading

Figure 17. Indicator attack-patterns

From this information it is possible to determine that this IP-address may have been used in a phishing attack. This level of information can directly be used in CSOC and CSIRT operations for monitoring, threat hunting and security configurations.

#### 4.4 Enriching Indicators

The internal-enrichment connectors include integrations to services with the capability to bring more context to the IoCs ingested in the TIP. VirusTotal and AbuseIPDB services offer limited free to use APIs to retrieve information related to indicators. After deploying the connectors, the enrichment option can be selected from the IP-address 195.54.160.59 as shown in Figure 18.

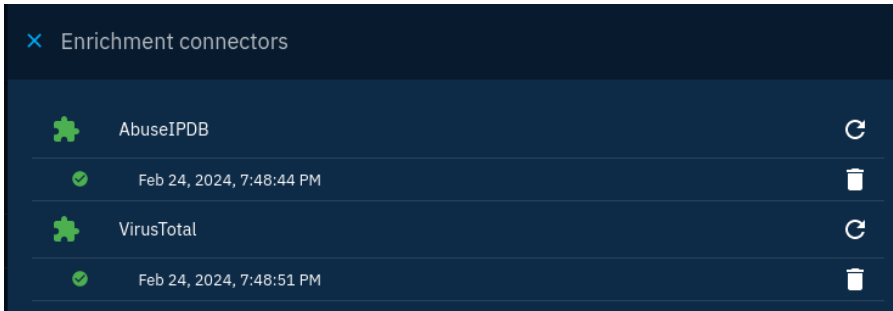


Figure 18. Enrichment connectors

Context regarding the geolocation and autonomous system is added in the form of labels to the indicator by the VirusTotal connector as seen in Figure 19. AbuseIPDB enrichment did not add context to this observable.

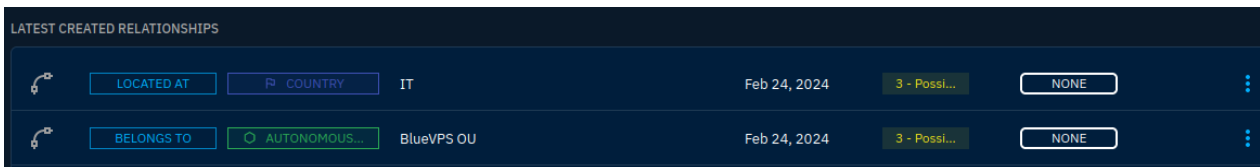


Figure 19. Virustotal relationships

Additionally, VirusTotal connector added a note to the indicator confirming its maliciousness as seen in Figure 20.

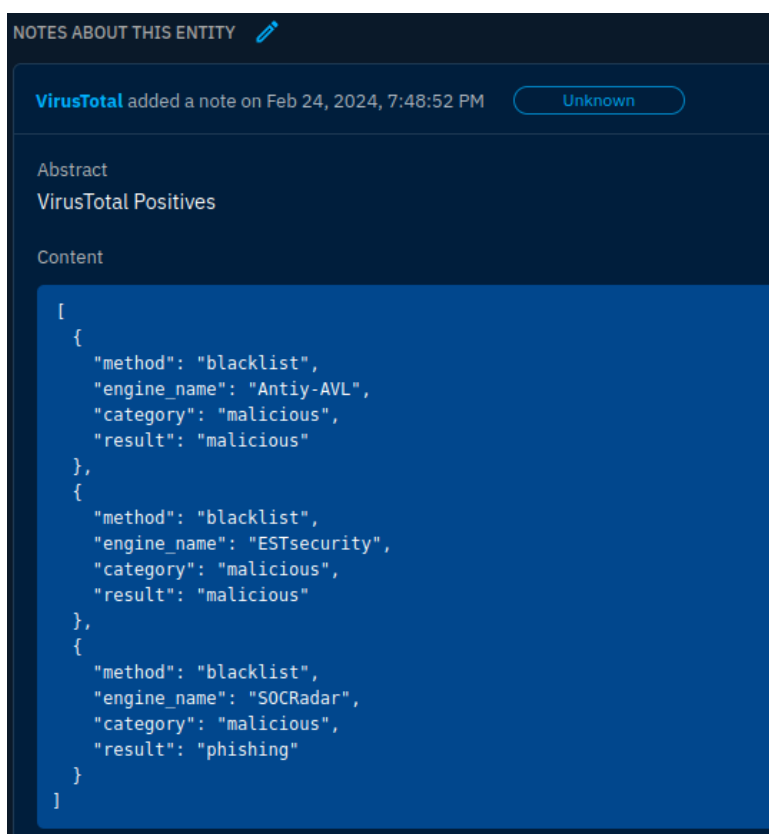


Figure 20. VirusTotal note

From this testing, the conclusion can be made that enrichment connectors are useful with adding a second opinion to indicators thus helping security operations with prioritizing indicators ingested from threat intelligence feeds.

## 4.5 Framework-based assessment

The idea for framework-based assessment came from the requirement for the cyber security operations team to measure its capability of detecting and preventing threats and being able to generate metrics for this capability, contributing to the security situational awareness of the organization. The MITRE ATT&CK Matrix tool is employed for this assessment, and it utilizes combination of methodologies described in Getting Started with MITRE ATT&CK sections **detection and analytics** and **assessment and engineering** (described in chapter 2.7.1). The process for Cybersecurity capability map is seen in Figure 21.

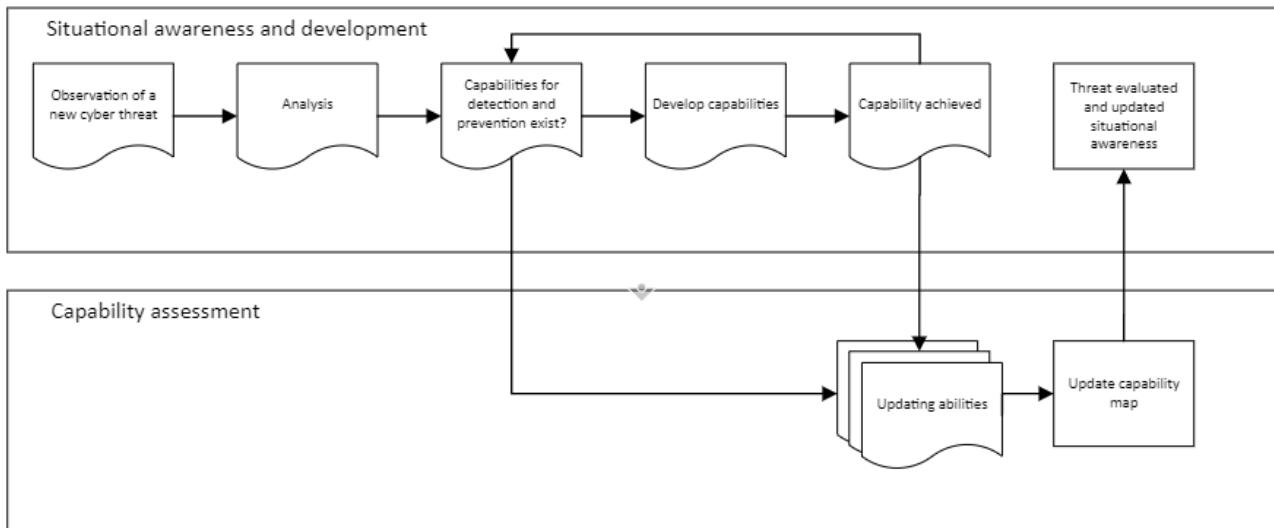


Figure 21. Cyber security capability map

The update process for the capability map includes an evaluation phase with five-stage scoring system for each technique and sub-technique:

- 0% No detection or prevention capability
- 25% Partial detection capability
- 50% Full detection capability
- 75% Full detection and partial prevention capability
- 100% Full detection and prevention capability

Implementation of this concept is seen in Figure 22, where this evaluation principle is demonstrated to two techniques and three sub-techniques from the execution tactic, in the MITRE ATT&CK Enterprise matrix. In this case, the team has conducted an assessment and determined that the current security capabilities have the full capability to detect and prevent malicious files, full capability to detect and a partial capability to prevent malicious images, and only partial capability to detect malicious links, granting the user execution technique an average score of 66.7%. The windows management instrumentation technique is not detected or prevented by security controls, thus having the score of 0%. Full assessment of the enterprise matrix presents an overview of the security operations capabilities compared to the TTPs presented in ATT&CK.

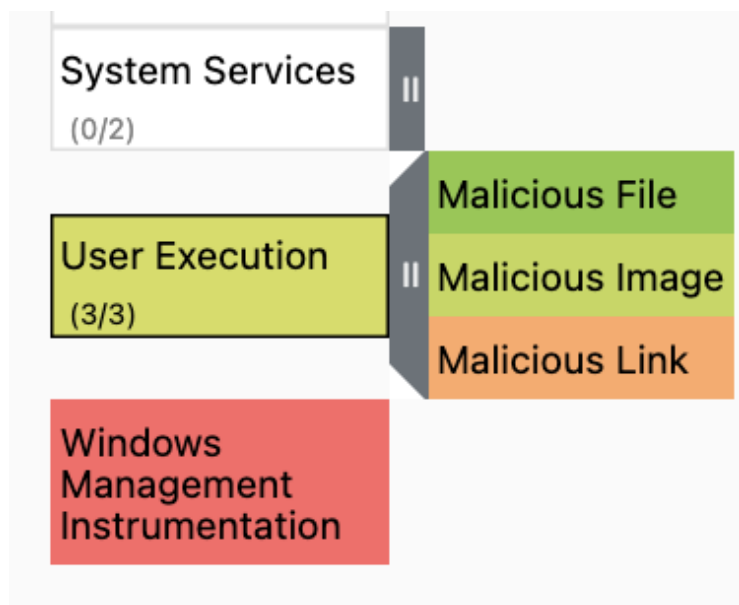


Figure 22. Capability map principle

The challenge with this concept is that as threats and TTPs evolve, the capability map should be updated to keep the view recent. Without proper threat intelligence management tools and procedures this has proven time consuming and difficult. To improve existing threat intelligence capabilities such as the capability map, the following threat intelligence process includes assessment of the capability map during threat investigation based on its results.

#### 4.6 Evaluation via Threat Hypothesis

Previous chapters in the implementation phase described methods of using tools and ATT&CK framework when managing threat information. In this chapter a threat hypothesis is constructed to demonstrate a threat intelligence management process and collect feedback from stakeholders to evaluate the success of this implementations design. Overview of the process is presented in Figure 23.

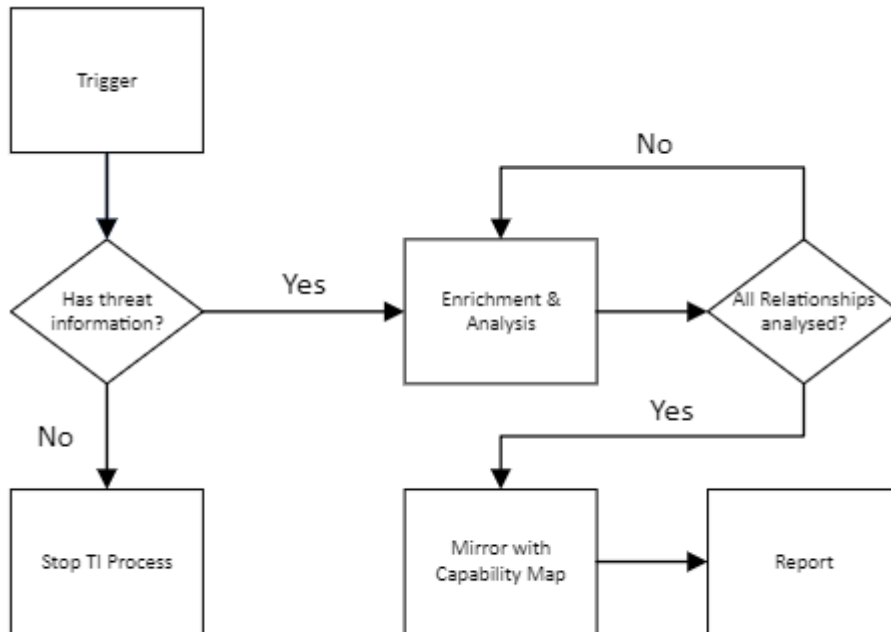


Figure 23. Threat intelligence process

#### 4.6.1 Threat Enrichment and Analysis

A trigger for a threat event could include any kind of information that indicates a threat actors' presence in the environment, such as security alert. Suppose that an alert is generated in the CSOC indicating that a device has connected to a potentially malicious IP-address **194.87.31.181**. Searching the IP-address from OpenCTI database it is possible to observe the relationships between the IP-Address, including steganography attack pattern, an intrusion set **UAC-0184** and the **Remcos RAT** malware as shown in Figure 24.

INDICATES	ATTACK P...	[T1001.002] Steganography	Mar 1, 2024	5 - Impr...	TLP:CLEAR	⋮
INDICATES	MALWARE	Remcos RAT	Mar 1, 2024	5 - Impr...	TLP:CLEAR	⋮
INDICATES	INTRUSIO...	UAC-0184	Mar 1, 2024	5 - Impr...	TLP:CLEAR	⋮
BASED ON	IPV4 ADD...	194.87.31.181	Mar 1, 2024	5 - Impr...	TLP:CLEAR	⋮

Figure 24. Malicious IP-address relationships

Enriching the indicator with VirusTotal connector provides more information about the IP-addresses origin country and the autonomous system as seen in Figure 25.

RELATIONSHIP	ENTITY TYPE	NAME	AUTHOR
LOCATED AT	COUNTRY	NL	VirusTotal
BASED ON	INDICATOR	194.87.31.181	AlienVault
BELONGS TO	AUTONOMOUS...	Global Internet Solutions LLC	VirusTotal

Figure 25. Malicious IP-address enrichment

Analysis on the threat actor can be observed in the report related to the indicator. From this information it is possible to deduce that the indicator is related to a Ukrainian entity operating in Finland, and the threat actor is utilizing obfuscation methods with the steganography technique to distribute malware, granting it with remote access capabilities as seen in Figure 26.

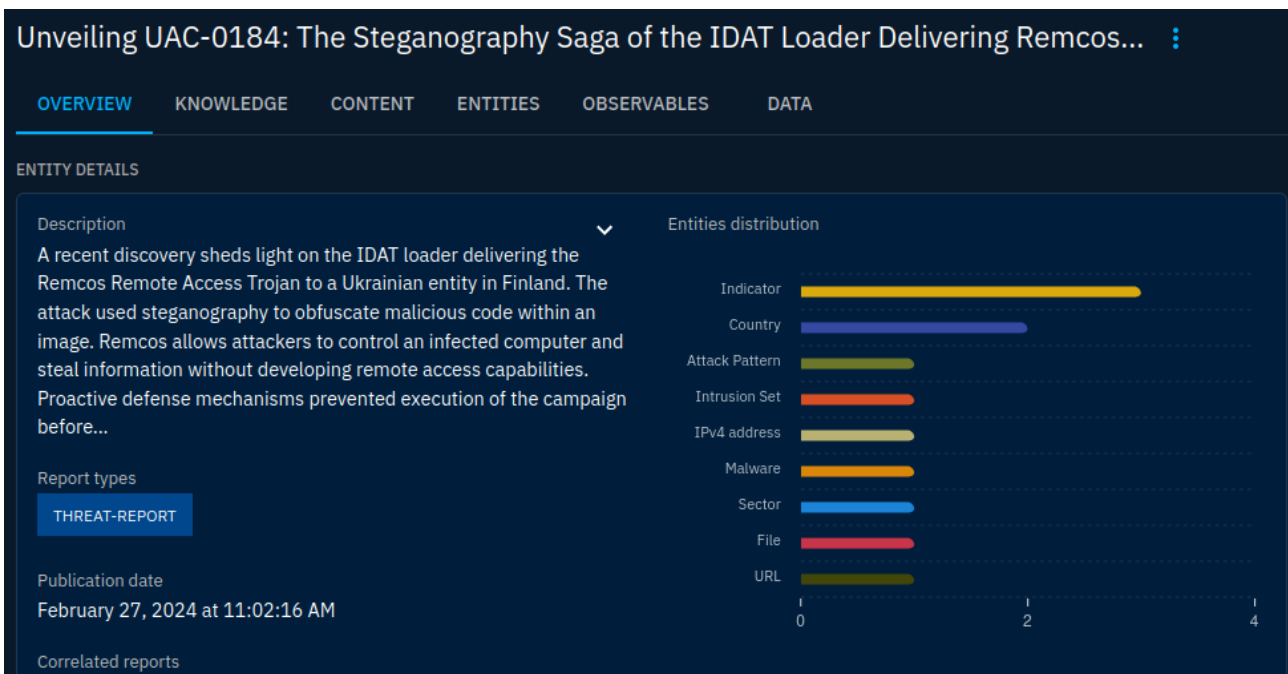
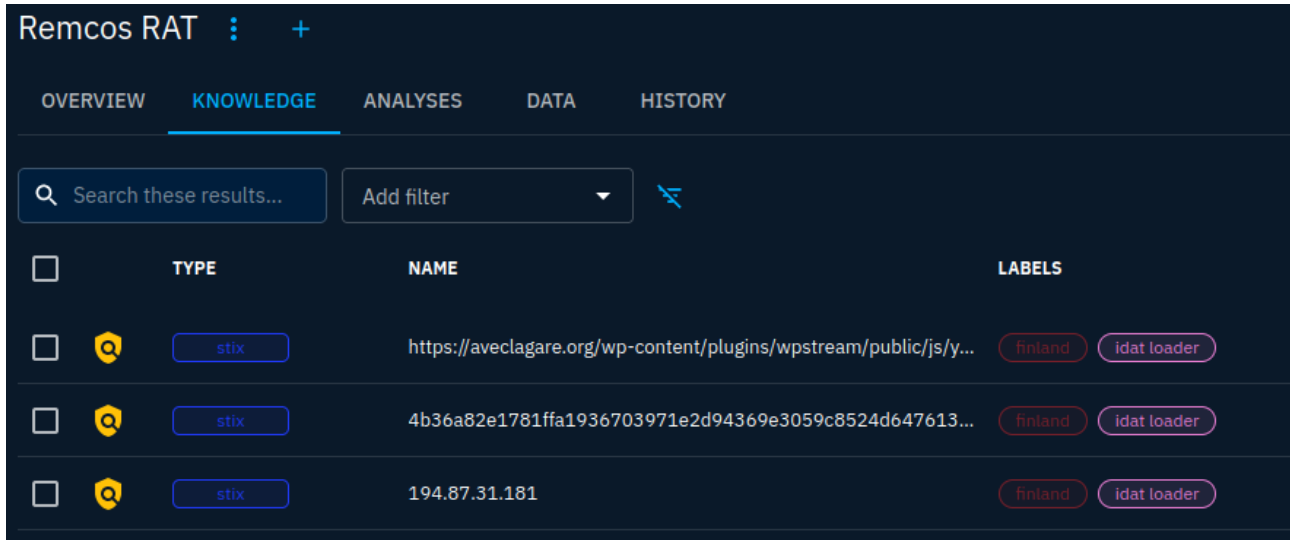


Figure 26. UAC-0184 threat report



Further analysis of the malware indicator provides information to two related indicators, an URL indicator and a SHA-256 hash indicator as seen in Figure 27. From this information it can be concluded that the related indicators might also be present in the environment.



	TYPE	NAME	LABELS
<input type="checkbox"/>	stix	https://aveclagare.org/wp-content/plugins/wpstream/public/js/y...	finland idat loader
<input type="checkbox"/>	stix	4b36a82e1781ffa1936703971e2d94369e3059c8524d647613...	finland idat loader
<input type="checkbox"/>	stix	194.87.31.181	finland idat loader

Figure 27. Remcos RAT indicators

Based on this information, a threat hunting scenario can be constructed to verify if devices in the environment are compromised by this attack. Microsoft defender extended detection and response (XDR) allows for users to generate queries with Kusto Query Language (KQL) to search threat indicators and events from devices onboarded to defender for endpoint (schmurky et al., 2023). The DeviceNetworkEvents table contains information related to network connections (schmurky et al., 2024). Running a query as shown in Figure 28, shows whether the onboarded devices have communicated to the threat indicators related to the Remcos RAT malware in the past seven days.

The screenshot shows a Kusto query editor with the following code:

```

1 DeviceNetworkEvents
2 | where Timestamp >= ago(7d)
3 | where RemoteUrl == "https://aveclagare.org/wp-content/plugins/wpstream/public/js/youtube.min.js"
4 or RemoteIP == "194.87.31.181"
5 | project Timestamp, DeviceName, RemoteIP, RemotePort
6

```

Below the query editor, the interface shows the 'Results' tab selected. The search bar contains '0 kohdetta' and 'Hae'. The execution time is 00:00.199 and the severity is Low. The table headers are Timestamp, DeviceName, RemoteIP, and RemotePort. The message 'No results found in the specified time frame.' is displayed at the bottom.

Figure 28. Defender advanced hunting indicator search from DeviceNetworkEvents

The EmailUrlInfo table contains information about Microsoft Defender for Office 365 processed emails and attachments containing URLs (schmurky et al., 2024). As email is a potential attack vector utilized by the attacker, a KQL query can be constructed to determine if recipients in the organization have received the malicious URL via email as demonstrated in Figure 29.

The screenshot shows a Kusto query editor with the following code:

```

1 EmailUrlInfo
2 | where Timestamp >= ago(7d)
3 | where Url == "https://aveclagare.org/wp-content/plugins/wpstream/public/js/youtube.min.js"
4 | project Timestamp, UrlDomain, Url, NetworkMessageId
5

```

Below the query editor, the interface shows the 'Results' tab selected. The search bar contains '0 kohdetta' and 'Hae'. The execution time is 00:00.331 and the severity is Low. The table headers are Timestamp, UrlDomain, Url, and NetworkMessageId. The message 'No results found in the specified time frame.' is displayed at the bottom.

Figure 29. Defender advanced hunting indicator search from EmailUrlInfo

While the threat hunt has not indicated a compromise so far, to rule out the possibility of the malware being distributed by other methods, it is possible to investigate files processed by the monitored devices. The DeviceFileEvents table contains information about files created and modified on the endpoint devices (schmurky et al., 2024). With the query illustrated in Figure 30, it is possible to determine whether the SHA256 file hash has been observed in the past seven days.

The screenshot shows a Kusto query editor with the following query:

```

1 DeviceFileEvents
2 | where Timestamp >= ago(7d)
3 | where SHA256 == "4b36a82e1781ffa1936703971e2d94369e3059c8524d647613244c6f9a92690b"
4 | project Timestamp, ActionType, DeviceId, FileName, FolderPath, InitiatingProcessFileName

```

Below the query editor, the interface shows the 'Results' tab selected. The search bar contains '0 kohdetta' (0 results) and a search icon. The table headers are: Timestamp, ActionType, DeviceId, FileName, and FolderPath. The message 'No results found in the specified time frame.' is displayed at the bottom of the results area.

Figure 30. Defender advanced hunting indicator search from DeviceFileEvents

At this stage, all the related indicators have been analysed and the possibility of malware infection can be ruled out. However, if it is determined that the threat actor poses a persistent threat, the Defender XDR allows for addition of indicator to ensure that the indicators are detected and prevented in their occurrence. The example addition of the hash indicator is illustrated in Figure 31. The process is repeatable for the IP-Address and URL indicators as well.

## Indicator

Indicator details

Specify the files and the expiration date. [Learn more](#)

File hash \*

Indicator type SHA256

Title \*

Description \*

Expires on (UTC)

Never

Custom

Figure 31. Adding hash indicator in defender XDR

#### 4.6.2 Updating capabilities

After sufficient enrichment and analysis of related indicators, it is possible to include the capability map process to the threat management process. Based on the information gained from the analysis it should be evaluated whether updates are required to the ATT&CK matrix. Assuming that the technique for steganography is graded at 100% percent based on previous assessments prior to the investigation, and no compromise related to the technique was uncovered from the analysis, it is sufficient to retain the score as is.

In events where multiple techniques are related to the threat activity, the same method of assessment can be applied to all related techniques. In an event where unprevented or undetected compromise has occurred by a threat actor using a certain technique, a more profound assessment should be engaged in to determine whether the threshold for detecting and preventing the attack has lowered and score the technique accordingly. To exemplify this, looking at the global kill chain

attributed to the threat actor APT18 in Figure 32, it is possible that the execution techniques are detected by the CSOC, but some or all the defense-evasion techniques go undetected. In this case the assessment would likely provide higher scores for the execution techniques, and lower scores for the defense-evasion techniques.

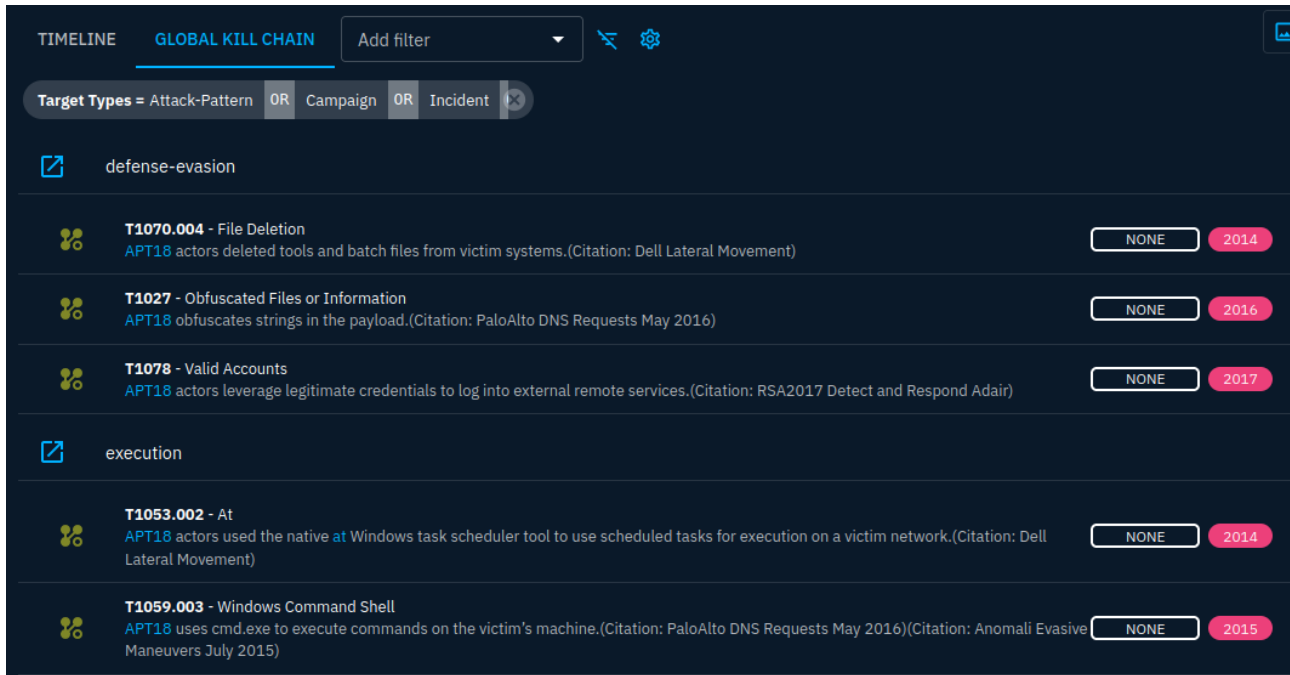


Figure 32. APT18 Global kill chain

### 4.6.3 Reporting

The last part of the process is to generate a report based on the threat event. The purpose of the report is to provide stakeholders with actionable information, recommendations, and context to threat events observed by cyber security operations team. Gathering data from the demonstration, it is possible to answer the following questions:

- 1. What happened? Why was this investigation started?** CSOC detected a network connection from a device to a potentially malicious IP-address.
- 2. Who was the threat actor?** The event indicates that an APT actor UAC-0184 is behind this event.
- 3. What is the threat actor's motive?** The threat actor has been observed targeting Ukrainian entities in Finland. The goal of the attacker is to deliver malware to victim devices in an attempt to gain remote access.
- 4. What techniques does the attacker use?** The attacker uses steganography technique to hide malicious code in images.

5. **What indicators are related to the attacker?** The attacker is related to one IP-address indicator, one URL indicator and one SHA256 file indicator. The malware used by the adversary is the Remcot RAT malware.
6. **Did compromise of data occur?** Based on threat hunting activities, there is no reason to suspect compromise.
7. **Were proactive methods employed?** The indicators have been added to the Defender XDR to prevent further attack attempts.
8. **Is capability map up to date?** Since the attack was unsuccessful, the detection and prevention capability for steganography remain at 100% based on previous assessments.

## 5 Evaluating implementation results

### 5.1 Comparing results to key development targets

The evaluation of the implementations results should be considered by comparing the key development targets recognized during the target state evaluation, and the test implementations capability to correspond to those.

**Implementation of TIP** solution provided a holistic view to threat information with a centralized repository. With this solution the ingestion, analysis and distribution of threat intelligence is less complicated. **The threat intelligence cycle** was not fully adhered to during the phases of development, however the TIP solution tested provides methods for future improvement, as many common formats and sources for threat intelligence are supported by it.

**Automation** is a key benefit of TIP's and was demonstrated during the implementation with enrichment, addition of context, and creating relationships between threat observables. To further increase the efficiency of the SOC and CSIRT operation, automation with security tools such as a SIEM system should be considered.

The addition of the **MITRE ATT&CK Framework** to the concept implemented supports the goal of structured threat information and provides knowledge about various TTP's used by adversaries. The benefit of the framework is further emphasized with the addition of the capability map process, as the MITRE ATT&CK matrix is already utilized in this assessment.

## 5.2 Demonstration session and feedback survey

To gain feedback and gather opinions and evaluate the success of the concept created in the research, a demonstration session was scheduled with the stakeholders (e.g. the organizations cyber security team). Seven team members participated in the session in addition to the author, the demonstration presentation was included following topics from the research:

- Background of the development research, research structure and research questions.
- General information about threat intelligence, definition, implementation, and application.
- Development plan structure and results from the focus group workshops (business requirements, current state analysis and target state evaluation).
- Information about tools and framework.
- Threat intelligence process including the capability map assessment.
- Threat hypothesis demonstrating the implementation.

The session was concluded with a feedback survey with four questions to gather impressions from the audience. The structure of the survey consisted of four multiple choice questions. Options for the response were strongly disagree, disagree, neutral, agree, and strongly agree. Questions from the feedback form are presented in appendix 3.

The first question *“I see threat intelligence as a valuable tool for cyber security operations”* was presented to gain a general sentiment from the audience towards the importance of threat intelligence in the organization’s security operations. Responses to the question are presented in Figure 33 below.

## 1. I see threat intelligence as a valuable tool for cyber security operations

### [Lisätietoja](#)

<span style="color: blue;">●</span> Strongly Disagree	0
<span style="color: orange;">●</span> Disagree	0
<span style="color: green;">●</span> Neutral	0
<span style="color: red;">●</span> Agree	0
<span style="color: purple;">●</span> Strongly Agree	7

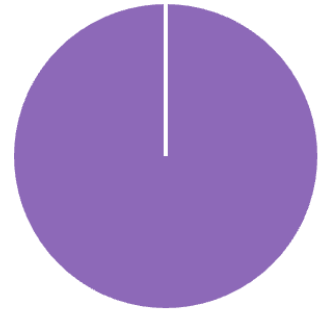


Figure 33. Feedback survey question 1.

Based on the results to the first question, all participants from the survey group answered “strongly agree”, indicating that among the survey group, threat intelligence is viewed as a valuable tool for cyber security operations. The second question presented was “*This demonstration provided solutions to the defined business requirements*” seen in Figure 34, to measure whether the concept demonstrated answered the requirements set in the focus group interview.

## 2. This demonstration provided solutions to the defined business requirements

### [Lisätietoja](#)

<span style="color: blue;">●</span> Strongly Disagree	0
<span style="color: orange;">●</span> Disagree	0
<span style="color: green;">●</span> Neutral	0
<span style="color: red;">●</span> Agree	4
<span style="color: purple;">●</span> Strongly Agree	3

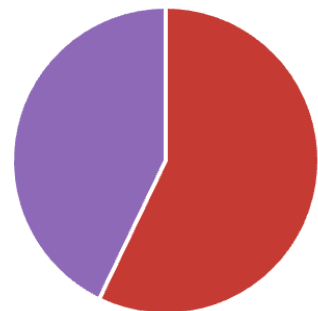


Figure 34. Feedback survey question 2.

Results for the second question included three participants responding, “Strongly Agree” and four participants answering “Agree”, indicating that the business requirements were not fully met with



the demonstrated concept. The third question presented (Figure 35) was “I believe that the tools, processes and frameworks introduced could improve our organizations maturity in threat intelligence”, to measure whether the participants feel that the concept presented would increase the organizations maturity in threat intelligence.

3. I believe that the tools, processes and frameworks introduced could improve our organizations maturity in threat intelligence

[Lisätietoja](#)

● Strongly disagree	0
● Disagree	0
● Neutral	0
● Agree	3
● Strongly agree	4

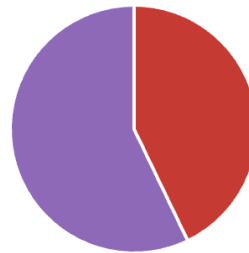


Figure 35. Feedback survey question 3.

Results to the third question included three participants responding “agree” and four participants responding “strongly agree”, indicating a positive effect to organizations threat intelligence maturity with the tools, processes and framework presented. The fourth question presented (Figure 36) “I believe that the concept demonstrated should be implemented for further development of threat intelligence capabilities” was inquired to measure the participants sentiment toward implementing the presented solution as part of the security team’s toolkit for further development.

4. I believe that the concept demonstrated should be implemented for further development of threat intelligence capabilities

[Lisätietoja](#)

● Strongly Disagree	0
● Disagree	0
● Neutral	0
● Agree	4
● Strongly Agree	3

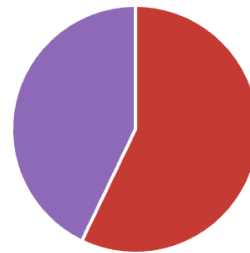


Figure 36. Feedback survey question 4.

Results for the fourth question included four participants responding “agree”, and three participants responding “strongly agree”, indicating that the concepts suitability for the organizations security operations was positively viewed among the participants.

## 6 Research results

The primary objective of the thesis was to investigate tools, methods, and frameworks to build a threat intelligence management model that supports the organization's technical cyber security operations. The concept implemented during the development phase includes a collection of mechanisms combined with the security team's existing tools and processes.

It should be specified that the design of the threat management process is largely independent of the tools used during the demonstration of the threat hypothesis. The tools of choice were only used during the development process to validate the concept's applicability in practice. The fundamental principles of this design could, to some extent, be adjusted to accommodate another organization's specific tools and requirements.

### 6.1 Evaluating research results

The validity of the research results can be inferred by comparing how the information collected during the research answer the research questions. To answer the first question “*How to use threat intelligence efficiently in organizations' security operations to assist with preventing security*”

*breaches?*”, the concept developed demonstrates method and process for security operations to identify threat related information and correlations between various identified artifacts. By demonstrating proactive defensive methods and application of threat intelligence collectively with security tools, the value supplemented by the concept can be validated.

The second question “*What frameworks and tools can be used to develop suitable threat intelligence practices to meet the target organization's security related needs?*”. This question is partly answered in the knowledge acquisition phase of the research. Gaining understanding in how to employ MITRE ATT&CK in threat intelligence processes in conjunction with security tools improves the ability to manage threat intelligence in a structured manner. The demonstration phase utilized this information by combining the threat intelligence process with the cyber security capability map updating process.

“*How can threat intelligence practices be established as a part of technical cyber security operations?*” The answer to this question is also demonstrated with the implemented demonstration by combining threat hunting and incident response activities together with the threat intelligence management process. While a general concept could be produced with a threat hypothesis, transition to production environment would likely require some amount of refinement.

“*How to generate threat-related metrics and statistics to assist in defining security related business needs?*”. Being able to distribute threat information in an understandable and actionable form requires enrichment and addition of context and relationships between various threat information. Without suitable tools and processes this seems to prove very difficult. Reflecting to the reporting generated with the information gained during the demonstration, all information related to the threat actors, it’s motives and methods would remain unknown without access to threat intelligence. This information can be used to proactively improve the organizations defensive capabilities, by allocating resources according to events and trends observed.

## **6.2 Feedback survey results**

Based on the result from the feedback survey, the importance of threat intelligence is recognized among the respondents, and the concept presented would produce value to cyber security opera-

tions in the target organization. The overall sentiment towards the presented solution was positive, and threat intelligence maturity in security operations will be improved to some capacity by including tools and methods from this research. However, room for improvement and further development remain.

Comparing the results from the feedback and result evaluation, it can be interpreted that the business requirements set in the definition phase were not fully met. This could implicate some lack of capability to automate the process due to the limitations of the demonstration environment. The threat intelligence cycle was another business requirement that was only partially addressed within this research.

One factor potentially influencing answers to the feedback questionnaire is explaining multifaceted concepts to the audience in a relatively short timeframe. Questions 3 and 4 especially require the ability to perceive the capabilities of the tools and processes to influence the current threat intelligence maturity in technical operations. All members of the audience may not have been fully acquainted with the specifics of such activities. This could also have been influenced by the presenter's imperfect delivery of the presentation.

## **7 Conclusion**

### **7.1 Reflections**

While some form of demonstration of a solution can be conducted in a testing environment such as in this research, the quality of the solution is not guaranteed until implemented in an actual production environment and evaluated after a sufficient period. The biggest problem is that threat intelligence requires actionable data, and without access to this data, the solution will, to some extent, rely on hypotheticals. This also presents the problem of not being able to quantifiably benchmark the concept in production environments, which might provide more information to evaluate the success of the concept.

Due to the limited scope of the research, the threat intelligence cycle could not be fully considered in all phases of implementation. For example, the direction and collection phases of the intelligence cycle should determine the sources for threat intelligence, but evaluating the quality of

threat intelligence sources, while important, would have been a huge undertaking. While every phase of the intelligence cycle was partly considered during the implementation, the process and methods would require more consideration to sufficiently support the management of threat intelligence. Implementing a TIP solution does support considerations brought by threat intelligence cycle, as many steps from collection to dissemination are supported by TIPs with ingestion, enrichment, automation, and dissemination capabilities.

Threat intelligence is a huge topic, and it has a number of practicality and applicability. Due to this, limiting the scope of the research to focus on small sample size of use-cases was essential. While the concept introduced provides a foundation on which to build on top of, threat intelligence is a constantly developing area of cybersecurity, and as such continuous development methods and procedures should also be constructed.

The design of the threat intelligence process doesn't necessitate the use of specific tools, such as those presented in this research during the evaluation of the threat hypothesis, for it to be efficient. However, it is clear that some level of operational cyber security capability must be in place before this concept can be adopted successfully, as utilizing threat intelligence in this fashion requires some expertise on the fundamentals of cyber security.

## **7.2 Research ethics and reliability**

Research requires rigor for it to influence the subject theory and practice. Results and conclusions should present information that measures up with the experiences and expectations of professionals and experts of the subject matter (Merriam & Tisdell, 2015, p. 237). It should be noted that this research incorporates processes and other elements potentially unique to the commissioning organization. The methodology used during this research ensures the repeatability of the research process but could potentially lead to distinct results due to its dependability on organization specific details.

The literature review process of this research incorporated the P.R.O.V.E.N methodology to evaluate the accuracy of source material (The University of Virginia, n.d.). The abbreviation P.R.O.V.E.N consists of the following themes:

- **Purpose:** What is the reason this information exists? Why was it published in the particular format and who is the information for?
- **Relevance:** Why is this information appropriate and how is it used? How does it compare to other sources?
- **Objective:** How is language in the source used? Does it have emotional or otherwise offensive language? Does the information present a fact or an opinion and is it biased?
- **Verifiability:** Does the information include sources and evidence? Is information misrepresented or otherwise verifiable from other sources?
- **Expertise:** Is the author an expert in the subject matter? Does the author have affiliations to institutions or organizations?
- **Newness:** When was the source published? Is the information in the source current and are there other sources more recent with the same information?

Triangulation is a method used in research to increase the reliability and credibility of the findings. Triangulation can be employed in different elements of the research, such as using multiple sources of data, using multiple data collection methods, or using several investigators to validate results (Merriam & Tisdell, 2015, p. 244). During the research process, data triangulation was employed where possible to increase accuracy of the information gathered and reduce bias. Methods triangulation was partially used by conducting a feedback survey and reflecting on the feedback data with researchers own conclusions.

The focus group work of this research was conducted with a relatively small number of participants, which makes it important to ensure quality of focus group work. The interviews were conducted in a structured format to minimize external effects to the accuracy of the research results. This is also important to minimize the influence of the presenter's delivery of the presentation content on the participants. The feedback survey was conducted anonymously so as not to discourage the participants from providing negative feedback.

### 7.3 Further research

The development section of the research included only a subset of business requirements defined in the focus group interview. Further development could include more security-related functions, such as utilizing threat intelligence in vulnerability management and risk management operations on top of the foundation developed during this research.

Further research could focus on how to adopt the principles of the threat intelligence cycle more profoundly in the development of this concept. Another topic that builds on top of this foundation could be how to use this basis to further increase the efficiency of managing threat intelligence with automation capabilities. One use case that was not discussed in this thesis is how this concept could better incorporate organizations' capability to generate and manage self-curated threat intelligence.

## References

Alien Labs Open Threat Exchange. (n.d.). <https://cybersecurity.att.com/open-threat-exchange>

Applebaum, A., Nickels, K., Schulz, T., Strom, B., & Wunder, J. (2019). <https://www.mitre.org/sites/default/files/2021-11/getting-started-with-attack-october-2019.pdf>

austinmccollum, prmerger-automator[bot], rod-trent, cwatson-cat, pritamso, dandye, rijutaka-poor2, yelevin, atikmapari, batamig, v-kents, & v-surgos. (2023, October 25). Threat intelligence integration in Microsoft Sentinel. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/sentinel/threat-intelligence-integration>

Baker, K. (2022, March 17). WHAT IS CYBER THREAT INTELLIGENCE? CrowdStrike. <https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/>

Buckbee, M. (2023, October 6). MITRE ATT&CK Framework: Everything You Need to Know. Varonis. <https://www.varonis.com/blog/mitre-attck-framework-complete-guide>

Bussa, T. (2023, December 19). Evolution of the threat intelligence Products and services market – our take on the latest Gartner® market guide. ThreatConnect. <https://threatconnect.com/blog/evolution-of-the-threat-intelligence-products-and-services-market-our-take-on-the-latest-gartner-market-guide/>

Brocke, J. V., Hevner, A. R., & Maedche, A. (2020). Introduction to Design Science Research. In Progress in IS (pp. 1–13). [https://doi.org/10.1007/978-3-030-46781-4\\_1](https://doi.org/10.1007/978-3-030-46781-4_1)

Bromiley, M. & SANS. (2016). Threat Intelligence: What It Is, and How to Use It Effectively. <https://nsfocusglobal.com/wp-content/uploads/2017/01/SANS-Whitepaper-Threat-Intelligence-What-It-Is-and-How-to-Use-It-Effectively.pdf>

Canadian Centre for Cyber Security. (2022). An introduction to the cyber threat environment. <https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment>



Center for Internet Security [CIS]. (n.d.). Cybersecurity Spotlight - Cyber Threat Actors. Retrieved December 30, 2023, from <https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors>

Chapple, M., & Seidl, D. (2020). CompTIA CySA+ Study Guide. John Wiley & Sons, Inc.

Collins, J., Contu, R., Schneider, M., & Lawson, C. (2021, December 10). Market Guide for Security Threat Intelligence Products and Service. <https://www.gartner.com/doc/reprints?id=1-28MP93JL&ct=220106&st=sb>

Cooper, S. (2023, June 1). The best threat intelligence feeds. Comparitech. <https://www.comparitech.com/net-admin/best-threat-intelligence-feeds/>

Crowdstrike (2022). CrowdStrike 2022 Global Threat Report. <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2022GTR.pdf>

DavidJBianco. (2014, January 17). The pyramid of pain. Retrieved February 3, 2024, from <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>

Demir, M. K. (2023, April 25). Open Cyber Threat Intelligence Platform (OPENCTI) - Mustafa Kaan Demir - Medium. Medium. <https://medium.com/@mkdemir1/open-cyber-threat-intelligence-platform-opencti-cb1986f06122>

diannegali, denisebmsft, American-Dipper, Dansimp, tdoucett-ms, v-mathavale, chrisda, bweston-8, alekyaj, sheshachary, msbemba, mjcaparas, & jweston-1. (2024, January 19). Create indicators. Microsoft Learn. <https://learn.microsoft.com/en-us/microsoft-365/security/defender-end-point/manage-indicators?view=o365-worldwide#indicator-of-compromise-ioc-overview>

Ellis, T., & Levy, Y. (2010). A Guide for Novice Researchers: Design and Development Research Methods. In ResearchGate. [https://www.researchgate.net/publication/228411189\\_A\\_Guide\\_for\\_Novice\\_Researchers\\_Design\\_and\\_Development\\_Research\\_Methods](https://www.researchgate.net/publication/228411189_A_Guide_for_Novice_Researchers_Design_and_Development_Research_Methods)

Europol. (2017). SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT. Retrieved February 3, 2024, from [https://www.europol.europa.eu/cms/sites/default/files/documents/report\\_socta2017\\_1.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/report_socta2017_1.pdf)

Filigran. (n.d.). Overview - OpenCTI documentation. <https://docs.opencti.io/5.8.X/deployment/overview/>

Gunter, D., & Seitz, M. (2021). A Practical Model for Conducting Cyber Threat Hunting. SANS Institute. <https://sansorg.egnyte.com/dl/hfu5PAbiPz>

Haken, G., Creasey, J., Thrower, E., Jordan, A., Palmer, A., Lord, J., ISF Members, & ISF Global Team (2022). Standard of Good Practice for Information Security 2022. Information Security Forum.

Harrington, D. (2022, July 1). What is Red Teaming? Methodology & Tools. Varonis. <https://www.varonis.com/blog/red-teaming#:~:text=Red%20teaming%20is%20a%20full,strategies%20to%20breach%20your%20defenses.>

Homeland Security. (2016, October). Critical Infrastructure Threat Information Sharing Framework. CISA. <https://www.cisa.gov/sites/default/files/publications/ci-threat-information-sharing-framework-508.pdf>

IBM. (n.d.). What is a Data Breach? | IBM. <https://www.ibm.com/topics/data-breach>

Interpol. (n.d.). *Cybercrimes cross borders and evolve rapidly*. Cybercrime. Retrieved February 3, 2024, from <https://www.interpol.int/en/Crimes/Cybercrime>

Johnson, C., Badger, L., Waltermire, D., Snyder, J., Skorupka, C., & National Institute of Standards and Technology [NIST]. (2016). Guide to Cyber Threat Information Sharing. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf>

Kirschner, M. (2021, November 2). Understanding the cyber Threat intelligence cycle. ZeroFox. <https://www.zerofox.com/blog/cyber-threat-intelligence-cycle/>

Lee, M. (2023). Cyber Threat intelligence. John Wiley & Sons.

McGowan, J. (2018, March 14). Stronger Together: The Bank Imperative for Cyberthreat intelligence sharing. Celent. <https://www.celent.com/insights/808409512>

Merriam, S. B., & Tisdell, E. J. (2015). Qualitative Research : A Guide to Design and Implementation. John Wiley & Sons, Incorporated.

The MITRE Corporation. (n.d.). Enterprise Techniques. MITRE ATT@CK. <https://attack.mitre.org/techniques/enterprise/>

OASIS. (2023, September 26). Introduction to STIX. <https://oasis-open.github.io/cti-documentation/stix/intro.html>

OASIS. (2023b, September 26). Introduction to TAXII. <https://oasis-open.github.io/cti-documentation/taxii/intro>

OASIS. (2021, June 10). STIX Version 2.1. <https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html>

Peiris, C., Pillai, B., & Kudrati, A. (2021). Threat hunting in the cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks. John Wiley & Sons.

Raza, M. (2023, May 30). What Are TTPs? Tactics, Techniques & Procedures Explained. Splunk. [https://www.splunk.com/en\\_us/blog/learn/ttp-tactics-techniques-procedures.html](https://www.splunk.com/en_us/blog/learn/ttp-tactics-techniques-procedures.html)

The Recorded Future Team. (2018, January 23). 5 Threat Intelligence Solution Use Cases. Recorded Future. <https://www.recordedfuture.com/blog/threat-intelligence-use-cases>

schmurky, ajaj-shaikh, samanthagy, American-Dipper, Dansimp, alekyaj, denisebmsft, v-samandalika, PatreciaPreetham, & Benzicald. (2024, March 7). EmailUrlInfo table in the advanced hunting schema. Microsoft Learn. <https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-emailurlinfo-table?view=o365-worldwide>

schmurky, American-Dipper, Dansimp, alekyaj, denisebmsft, v-stsavell, v-smandalika, Lovina-Saldanha, RatulaC, v-dihans, Benzicald, msbemba, & tiburd. (2023, November 15). Proactively hunt for threats with advanced hunting in Microsoft Defender XDR. Microsoft Learn. <https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-overview?view=o365-worldwide>

schmurky, samanthagy, American-Dipper, Dansimp, chrisda, alekyaj, denisebmsft, v-smandalika, PatreciaPreetham, & Benzicald. (2024, January 16). DeviceFileEvents. Microsoft Learn. <https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-device-fileevents-table?view=o365-worldwide>

schmurky, samanthagy, American-Dipper, Dansimp, msbemba, chrisda, alekyaj, denisebmsft, v-smandalika, PatreciaPreetham, & Benzicald. (2024, January 16). DeviceFileEvents. Microsoft Learn. <https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-devicenet-workevents-table?view=o365-worldwide>

SentinelOne. (2021, November 22). EDR vs Enterprise Antivirus: What's the Difference? SentinelOne. <https://www.sentinelone.com/blog/edr-vs-enterprise-antivirus-whats-the-difference/>

Snyk. (n.d.). A deep dive into cyber threat intelligence. Retrieved January 2, 2023, from <https://snyk.io/learn/threat-intelligence/>

Sophos. (n.d.). Threat Actors Explained: Motivations and Capabilities. SOPHOS. Retrieved January 3, 2023, from <https://www.sophos.com/en-us/cybersecurity-explained/threat-actors#:~:text=A%20threat%20actor%20can%20be,impact%20your%20company's%20security%20posture.>

Trellix. (n.d.). What is the MITRE ATT&CK Framework? <https://www.trellix.com/security-awareness/cybersecurity/what-is-mitre-attack-framework/>

The University of Virginia. (n.d.). P.R.O.V.E.N. Source Evaluation. UVA Library. <https://guides.lib.virginia.edu/c.php?g=1152471&p=8740721>

VMware. (n.d.). What is MITRE ATT&CK? <https://www.vmware.com/nordics/topics/glossary/content/mitre-attack.html>

ZDS. (2023, November 2). OpenCTI | Cyber Threat Intelligence Platform Installation Guide. Medium. <https://medium.com/@zdsecurity/opencti-all-in-one-installation-guide-8a9c159e5b28>

## Appendices

### Appendix 1. Installing Portainer and OpenCTI stack

```
tester@tester-virtual-machine:~/Documents$ cat config.txt
sudo apt-get update
sudo apt-get install apt-transport-https
sudo apt-get install ca-certificates
sudo apt-get install curl
sudo apt-get install gnupg-agent
sudo apt-get install software-properties-common
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu
$(lsb_release -cs) stable"
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io docker-compose
sudo usermod -aG docker $USER
sudo docker swarm init --advertise-addr 192.168.12.139
sudo sysctl -w vm.max_map_count=1048575
sudo /bin/su -c "echo "vm.max_map_count=1048575" >> /etc/sysctl.conf"
sudo docker stack deploy --compose-file=portainer-agent-stack.yml portainer
#Default Ports in ./portainer-agent-stack.yml were edited from 9000:9000 and 8000:
8000 to 29000:9000 and 18000:8000 to avoid conflicts.
```

## Appendix 2. docker.compose.yml & sample.env

### Docker.compose.yml part 1

```

tester@tester-virtual-machine:~/Documents$ cat docker.compose.yml
version: '3'
services:
  redis:
    image: redis:7.2.4
    restart: always
    volumes:
      - redisdata:/data
  elasticsearch:
    image: docker.elastic.co/elasticsearch/elasticsearch:8.12.1
    volumes:
      - esdata:/usr/share/elasticsearch/data
    environment:
      # Comment-out the line below for a cluster of multiple nodes
      - discovery.type=single-node
      # Uncomment the line below below for a cluster of multiple nodes
      # - cluster.name=docker-cluster
      - xpack.ml.enabled=false
      - xpack.security.enabled=false
      - thread_pool.search.queue_size=5000
      - logger.org.elasticsearch.discovery="ERROR"
      - "ES_JAVA_OPTS=-Xms${ELASTIC_MEMORY_SIZE} -Xmx${ELASTIC_MEMORY_SIZE}"
    restart: always
    ulimits:
      memlock:
        soft: -1
        hard: -1
      nofile:
        soft: 65536
        hard: 65536
  minio:
    image: minio/minio:RELEASE.2024-01-16T16-07-38Z
    volumes:
      - s3data:/data
    ports:
      - "9000:9000"
    environment:
      MINIO_ROOT_USER: ${MINIO_ROOT_USER}
      MINIO_ROOT_PASSWORD: ${MINIO_ROOT_PASSWORD}
    command: server /data
    restart: always
  rabbitmq:
    image: rabbitmq:3.12-management
    environment:
      - RABBITMQ_DEFAULT_USER=${RABBITMQ_DEFAULT_USER}
      - RABBITMQ_DEFAULT_PASS=${RABBITMQ_DEFAULT_PASS}
      - RABBITMQ_NODENAME=rabbit01@localhost
    volumes:
      - amqpdata:/var/lib/rabbitmq
    restart: always
  opentict:

```

## Docker.compose.yml part 2

```

connector-export-file-csv:
  image: opencti/connector-export-file-csv:5.12.33
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_CSV_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
    - CONNECTOR_NAME=ExportFileCsv
    - CONNECTOR_SCOPE=text/csv
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
connector-export-file-txt:
  image: opencti/connector-export-file-txt:5.12.33
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_TXT_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
    - CONNECTOR_NAME=ExportFileTxt
    - CONNECTOR_SCOPE=text/plain
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
connector-import-file-stix:
  image: opencti/connector-import-file-stix:5.12.33
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_IMPORT_FILE_STIX_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=INTERNAL_IMPORT_FILE
    - CONNECTOR_NAME=ImportFileStix
    - CONNECTOR_VALIDATE_BEFORE_IMPORT=true # Validate any bundle before import
    - CONNECTOR_SCOPE=application/json,text/xml
    - CONNECTOR_AUTO=true # Enable/disable auto-import of file
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
  restart: always
  depends_on:
    - opencti
connector-import-document:
  image: opencti/connector-import-document:5.12.33
  environment:
    - OPENCTI_URL=http://opencti:8080
    - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
    - CONNECTOR_ID=${CONNECTOR_IMPORT_DOCUMENT_ID} # Valid UUIDv4
    - CONNECTOR_TYPE=INTERNAL_IMPORT_FILE
    - CONNECTOR_NAME=ImportDocument
    - CONNECTOR_VALIDATE_BEFORE_IMPORT=true # Validate any bundle before import
    - CONNECTOR_SCOPE=application/pdf,text/plain,text/html
    - CONNECTOR_AUTO=true # Enable/disable auto-import of file
    - CONNECTOR_ONLY_CONTEXTUAL=false # Only extract data related to an entity (a report, a threat actor, etc.)
    - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
    - CONNECTOR_LOG_LEVEL=info
    - IMPORT_DOCUMENT_CREATE_INDICATOR=true
  restart: always
  depends_on:
    - opencti
volumes:
  esdata:
  s3data:
  redisdata:
  amqpdata:

```



## Docker.compose.yml part 3

```

image: opencti/platform:5.12.33
environment:
  - NODE_OPTIONS=--max-old-space-size=8096
  - APP__PORT=8080
  - APP__BASE_URL=${OPENCTI_BASE_URL}
  - APP__ADMIN__EMAIL=${OPENCTI_ADMIN_EMAIL}
  - APP__ADMIN__PASSWORD=${OPENCTI_ADMIN_PASSWORD}
  - APP__ADMIN__TOKEN=${OPENCTI_ADMIN_TOKEN}
  - APP__APP_LOGS__LOGS_LEVEL=error
  - REDIS__HOSTNAME=redis
  - REDIS__PORT=6379
  - ELASTICSEARCH__URL=http://elasticsearch:9200
  - MINIO__ENDPOINT=minio
  - MINIO__PORT=9000
  - MINIO__USE_SSL=false
  - MINIO__ACCESS_KEY=${MINIO_ROOT_USER}
  - MINIO__SECRET_KEY=${MINIO_ROOT_PASSWORD}
  - RABBITMQ__HOSTNAME=rabbitmq
  - RABBITMQ__PORT=5672
  - RABBITMQ__PORT_MANAGEMENT=15672
  - RABBITMQ__MANAGEMENT_SSL=false
  - RABBITMQ__USERNAME=${RABBITMQ_DEFAULT_USER}
  - RABBITMQ__PASSWORD=${RABBITMQ_DEFAULT_PASS}
  - SMTP__HOSTNAME=${SMTP_HOSTNAME}
  - SMTP__PORT=25
  - PROVIDERS__LOCAL__STRATEGY=LocalStrategy
ports:
  - "8080:8080"
depends_on:
  - redis
  - elasticsearch
  - minio
  - rabbitmq
restart: always
worker:
image: opencti/worker:5.12.33
environment:
  - OPENCTI_URL=http://opencti:8080
  - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
  - WORKER_LOG_LEVEL=info
depends_on:
  - opencti
deploy:
  mode: replicated
  replicas: 3
  restart: always
connector-export-file-stix:
image: opencti/connector-export-file-stix:5.12.33
environment:
  - OPENCTI_URL=http://opencti:8080
  - OPENCTI_TOKEN=${OPENCTI_ADMIN_TOKEN}
  - CONNECTOR_ID=${CONNECTOR_EXPORT_FILE_STIX_ID} # Valid UUIDv4
  - CONNECTOR_TYPE=INTERNAL_EXPORT_FILE
  - CONNECTOR_NAME=ExportFileStix2
  - CONNECTOR_SCOPE=application/json
  - CONNECTOR_CONFIDENCE_LEVEL=15 # From 0 (Unknown) to 100 (Fully trusted)
  - CONNECTOR_LOG_LEVEL=info
restart: always
depends_on:
  - opencti

```

## Sample.env

```
tester@tester-virtual-machine:~/Documents$ cat sample.env
OPENCTI_ADMIN_EMAIL=admin@opencti.io
OPENCTI_ADMIN_PASSWORD=Kissa123!
OPENCTI_ADMIN_TOKEN=b4775932-203d-4427-a721-5672ebe4ec17
OPENCTI_BASE_URL=http://localhost:8080
MINIO_ROOT_USER=opencti
MINIO_ROOT_PASSWORD=Kissa123!
RABBITMQ_DEFAULT_USER=opencti
RABBITMQ_DEFAULT_PASS=Kissa123!
CONNECTOR_EXPORT_FILE_STIX_ID=dd817c8b-abae-460a-9ebc-97b1551e70e6
CONNECTOR_EXPORT_FILE_CSV_ID=7ba187fb-fde8-4063-92b5-c3da34060dd7
CONNECTOR_EXPORT_FILE_TXT_ID=ca715d9c-bd64-4351-91db-33a8d728a58b
CONNECTOR_IMPORT_FILE_STIX_ID=72327164-0b35-482b-b5d6-a5a3f76b845f
CONNECTOR_IMPORT_DOCUMENT_ID=c3970f8a-ce4b-4497-a381-20b7256f56f0
SMTP_HOSTNAME=localhost
ELASTIC_MEMORY_SIZE=4G
```

## Appendix 3. Demonstration feedback survey

## Threat Intelligence Process Demonstration Feedback

1. I see threat intelligence as a valuable tool for cyber security operations \*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

2. This demonstration provided solutions to the defined business requirements \*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree

3. I believe that the tools, processes and frameworks introduced could improve our organizations maturity in threat intelligence \*

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree

4. I believe that the concept demonstrated should be implemented for further development of threat intelligence capabilities \*

- Strongly Disagree
- Disagree
- Neutral
- Agree
- Strongly Agree