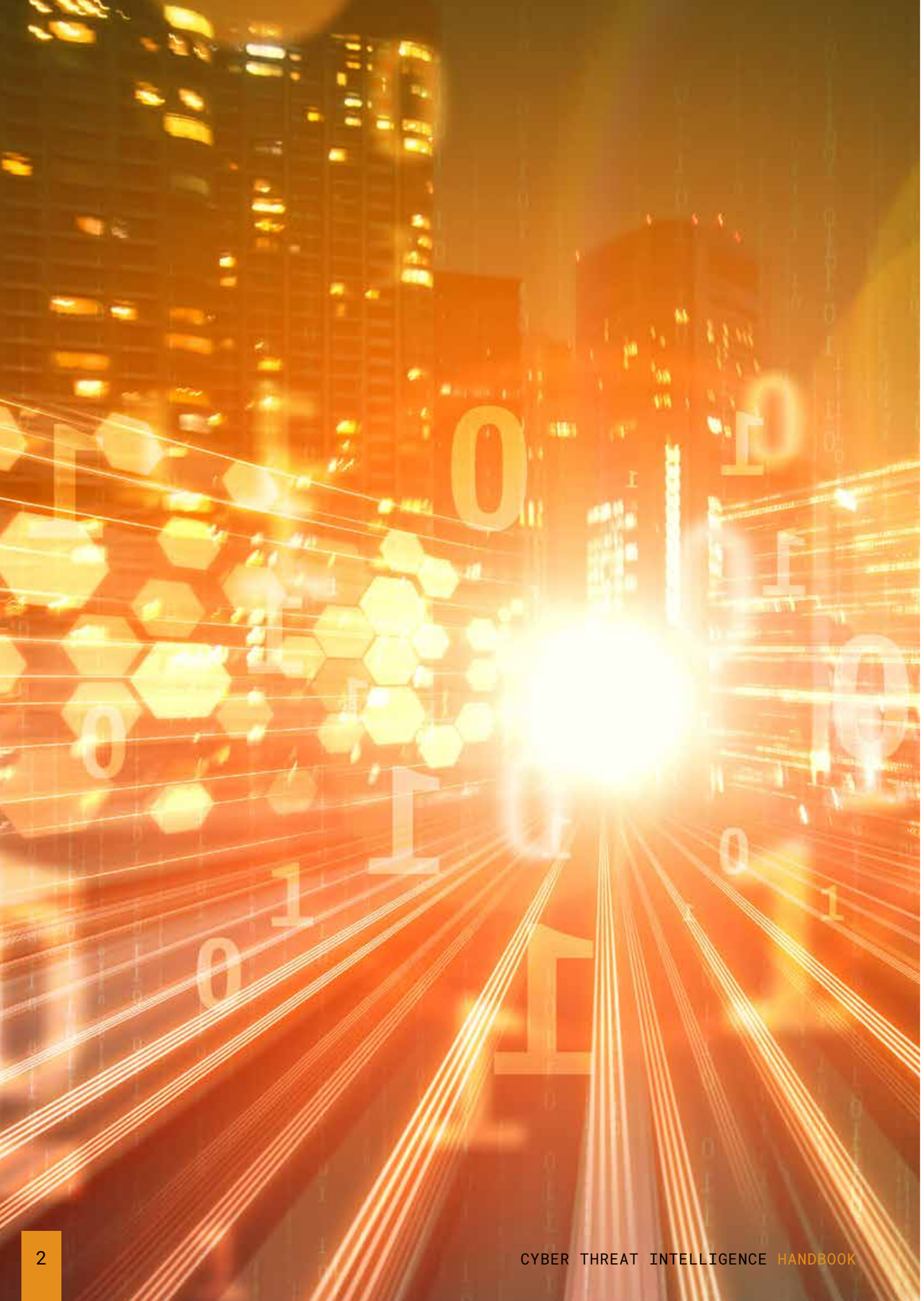
Cyberwatch Finland

DNV CYBER

CYBER THREAT INTELLIGENCE HANDBOOK



FOREWORD

Cyber threats are constantly changing and evolving, and organisations are increasingly expected to be able to understand and make use of information relating to cyber threats. This is highlighted not only by current practical needs but also by legislative requirements. Although the EU's Network and Information Security Directive (NIS2 Directive, EU2022/2555) and its nationally applicable versions (the Cybersecurity Act, the Act on Information Management in Public Administration and the Act on Electronic Communications Services) do not directly mandate the acquisition or utilisation of cyber threat intelligence, they do require organisations to assess and manage cyber threats, to establish an operational model for cyber risk management based on these assessments, and to report significant deviations to the supervisory authority. In practice, implementing this requires cyber threat intelligence. Similarly, the ISO/IEC 27000 series of information security standards, which is in use in many companies, requires the collection and analysis of threat intelligence in the form of control measures. For example, control measure 5.7 (threat intelligence) of the ISO 27001:2022 standard requires organisations to collect, analyse and produce information on information security threats.

With the new Cyber Security Act, company management now has a more binding role, and the new obligations emphasise the increased personal responsibility of management in implementing – and failing to implement – risk management measures. In practice, it is virtually impossible to implement cyber risk management measures without real-time threat intelligence, meaning that visibility of the threat landscape remains limited and often unreliable. The broader and more comprehensive a company's cyber threat intelligence is, the more time it has to prepare.

The aim of this handbook is to explain in more detail what cyber threat intelligence might entail, where it can be obtained, and to provide various methods – that is, practical tools – for organisations planning or developing its use of the cyber threat intelligence. The book is divided into an introduction, followed by the cyber threat intelligence utilisation process, which is divided into four stages (steering; collection/processing; analysis; and distribution). Each phase separately outlines the responsibilities of the organisation's management, the practical steps to be taken (operational measures) and the specific tools that can be utilised at this stage of the work.

The handbook is Intended for operators in critical infrastructure and other cyber-dependent sectors in the Nordics, with national examples from Finland. Its content can also be utilised more broadly, regardless of an organisation's sector or size.

This handbook has been produced in collaboration with Cyberwatch Finland and DNV Cyber. It has been developed as part of the SOW275 Knowledge Mining for Intelligence project, a collaboration between Finnish organisations in critical sectors. The aim of this handbook is to enhance the understanding and ability of organisations in critical sectors in Finland to utilise cyber threat intelligence. The sources used include relevant international publications, in particular the 4th edition of the Threat Intelligence Handbook published by Recorded Future. The guidelines in this handbook aim to take into account the Finnish operating environment and the requirements and needs of critical sectors.

Editorial Board of the Handbook,
Helsinki 2026

CONTENTS

TO THE READER

The cyber threat landscape has changed fundamentally. It is no longer enough to address vulnerabilities within weeks or months – the real measure is time. In several recent cases, we have seen the same pattern: a vulnerability becomes publicly known, exploits appear within hours or days, and mass scanning and opportunistic exploits begin almost immediately. Attackers exploit vulnerabilities before organizations even realize they are exposed to them. Internet-facing services and legacy systems in particular pose a persistent risk.

Cyber threat intelligence means anticipating what can be exploited — not just what is theoretically vulnerable. This is a core part of operational risk management. The role of cyber threat intelligence is to move organizations from reactive defense to proactive — and right now, in a race against time, this is critically important.

The handbook provides a comprehensive and accessible overview of Cyber Threat Intelligence (CTI) and prepares organizations for a structured and systematic approach to fulfilling their obligations and improving their operational capabilities.

Niko Candelin, Chairman, Board of Directors,
Finnish Information Security Cluster, FISC

Finnish Information Security Cluster - FISC ry (in Finnish Kyberala ry) represents the cyber security sector operating in Finland. The purpose of the association is to promote the risk management of digital technologies, digital security and the prerequisites of the industry in Finland and the EU in cooperation with public administration, companies and civil society. The FISC recommends the Cyber Threat Intelligence Handbook for Organizations (2026) for all organizations looking to strengthen their cybersecurity and meet the growing regulatory and risk management requirements. The handbook provides a practical overview of the utilisation of cyber threat intelligence (CTI) from management decision-making to operational implementation, adapted to the Finnish operating environment. In particular, the handbook supports the knowledge-driven principle of the EU's NIS2 and DORA regulations and the ISO/IEC 27001 standard, and helps organizations develop their maturity level in a controlled manner. The guide is suitable for both critical actors and more broadly for anyone seeking a better situational picture, foresight and effective measures in the changing cyber threat environment.

Peter Sund, CEO,
Finnish Information Security Cluster, FISC

1 INTRODUCTION

1.1 The need for cyber threat intelligence

In the modern information society, every organisation must prepare for cyber threats – either directly or indirectly. A cyber threat is a potential situation, event or action that may damage or disrupt communication networks and information systems, the users of such systems and other individuals, or otherwise adversely affect them.[1] Threats are both unique to a specific organisation or sector and general in nature, regardless of the organisation's size or operating models. It is essential to prepare for and respond to these threats. All too often, organisations' level of preparedness is not sufficient to treat the materialisation of a cyber threat with the seriousness it deserves. Furthermore, operating models still emphasise a reactive rather than a proactive approach, and measures are only implemented once the cyber threat has materialised, reputational damage has already occurred, and the authorities have taken an interest in the incident. Timely and relevant threat intelligence aims to bring predictability and efficiency to measures, whilst minimising the costs of damage. Cyber threat intelligence aims to provide the time and background information needed for decision-making. For threat intelligence to be of benefit to an organisation, the organisation's management must also have adequate ability to make decisions based on it in order to steer the organisation in the right direction. Cyber threat intelligence alone is of no use if it is not used correctly.

Cyber threat intelligence refers to information obtained from or relating to the operating environment regarding which or what types of threats are most likely and how to protect against them. In practice, it is information that guides an organisation's decisions regarding investments in cybersecurity, operating models or technical solutions. It is entirely possible to make these decisions and implement these solutions without threat intelligence, but in such cases one is effectively operating blind, and the risk of making the wrong decisions – or, worse still, overlooking the most significant threats – increases significantly. Cyber threat intelligence is therefore a prerequisite for more advanced and precise intelligence-led management when planning and implementing cyber security.

Cyber threat intelligence, and the process of producing it, is very similar to intelligence and the intelligence process. The traditional intelligence process is a continuous, phased operational model used to collect, analyse and disseminate information to support decision-making. The intelligence process is divided into four stages: 1) steering, 2) information gathering/processing, 3) Analysis, and 4) distribution. The production of cyber threat intelligence involves the same stages and has a similar objective: to produce information to support decision-making. In the case of cyber threat intelligence, the specific aim is to buy time for decision-making and to shift from reactive to proactive, or anticipatory, action. In practice, the aim is to detect and respond to threats before they materialise, making defence easier and preventing damage from occurring.

Cyber threat intelligence is a broad concept. It encompasses, for example, an understanding of threat actors' motives, the most common and popular forms of attack, information on identified malware, or a list of IP addresses linked to criminal activity. It is precisely the diversity of this information and, on the other hand, its abundance that makes handling it challenging. Many organisations do not know what information they should be collecting, where to obtain it, or what to do with it. For the most part, there is also a lack of capability and understanding of how cyber threat intelligence can be analysed and used as a tool for management and foresight.

New international and national laws, such as the aforementioned NIS2, as well as, for example, the DORA (Digital Operational Resilience Act) and the Cyber Resilience Act , require the creation of a more rigorously monitored cyber risk management model, which must be based on an assessment of the likelihood and impact of cyber risks. A structured cyber threat intelligence process has been developed to address this issue. It helps organisations understand how to derive the maximum benefit from cyber threat intelligence and how to avoid wasting resources on acquiring or processing irrelevant or non-relevant information. It is also iterative and self-improving in nature. This should make starting up easy, yet at the same time it naturally develops itself and the organisation implementing it towards a higher level of maturity and a better ability to identify, prepare for and respond to cyber threats. At its best, a good cyber threat intelligence process also enables its use in marketing or external communications. An organisation's detailed and up-to-date picture of the cyber threats affecting itself and its own sector can serve as an advantage in competitive situations, as well as in gaining and maintaining a reputation as a trustworthy operator.

[1] Finland's Cybersecurity Strategy 2024–2035, Concepts and Definitions, pp. 48–49.

1.2 Levels of threat intelligence

It is important for organisations, and particularly senior management, to understand the different types of threat intelligence available. Cyber threat intelligence is often divided into three levels to aid understanding (Figure 1).

These levels are strategic threat intelligence, operational threat intelligence and technical (sometimes also tactical) threat intelligence.

Figure 1. Levels of cyber threat intelligence.

STRATEGIC THREAT INTELLIGENCE

General information on cyber threat actors, their modus operandi, changes and prevailing trends. For example, overviews of cyber phenomena or the activities of identified threat actors. Recipients include the organisation's senior management or the body responsible for business risks. Produced at longer intervals, for example monthly or quarterly.

OPERATIONAL THREAT INTELLIGENCE

Information that is of direct relevance to the organisation itself and requires exceptional, non-automated measures. For example, an indication of a threat directed at the organisation itself or a subcontractor. Operational threat intelligence analyses, among other things, the attacker's motives. It affects day-to-day work. Information is collected continuously, but information likely to trigger measures is gathered a few times a month.

TECHNICAL/ TACTICAL THREAT INTELLIGENCE

Technical data that can be used to identify or block threat actors, malware or ongoing operations. For example, lists of malicious IP addresses, CVE vulnerabilities or other potential IoC data (i.e. Indicators of Compromise). Daily and continuous data collection and updating of security systems. Often machine-readable. Threat intelligence is referred to as tactical when technical threat intelligence is converted into daily active technical defence measures by searching for concrete threat indicators.

Although classification by level is useful and aids in process planning, organisations should not become too fixated on it when preparing practical processes. It is more worthwhile to consider what kind of information is needed and from which sources, rather than simply thinking about whether strategic information is needed and how much. The most important criterion that can be applied to threat intelligence is its usability. This means that the threat intelligence produced or acquired by an organisation is, in terms of its nature and content, such that it meets needs, leads to direct action, or confirms the validity of measures already taken. In this context, the level of threat intelligence is irrelevant, but considering the different levels nevertheless helps to understand the various sources of information and information needs.

Once the threat intelligence process is underway, the data or information produced can also be classified according to its severity. Classification based on severity refers to how significant the threat or indication of a threat is, and influences how the information is handled and how quickly a response is mounted.

1.3 Development and evaluation of the threat intelligence process

Cyber threat intelligence can be produced and utilised at many different levels, but the minimum requirement level, i.e. the basic level, is often not sufficient in the long term. The different levels of the threat intelligence process and their dimensions are outlined in the table below (Table 1). The table serves as a roadmap for organisations developing a threat intelligence process, but it should not be understood as a direct instruction on what to aim for. Each organisation has its own resources and objectives, which determine the scope of the threat intelligence process it aims for, and the extent to which it utilises its own operations and those of its partners. Threat intelligence levels are divided here into four tiers: 1) minimum level, 2) developing process, 3) effective user of cyber threat intelligence, and 4) thought leader/innovator. It is worth noting that not everyone needs to become a thought leader or innovator in this regard; often, a good basic level is sufficient. However, it is possible to develop and improve everyone's activities.

The scope and quality of the cyber threat intelligence process can also be assessed through the organisation's maturity level – or cyber maturity – which is measured using other tools. The maturity level indicates the extent of an organisation's cyber capabilities to protect itself against cyber threats and ensure business continuity in the event of disruptions. Maturity levels can be determined using various tools (such as the Cyber Security Centre's Cyber Meter), and the levels are either benchmarked against the organisation's own sector or defined as organisation-specific target levels. However, rather than directly comparing itself to others, it is important for an organisation to understand what level is appropriate and sufficient for it specifically; nevertheless, comparison can still be useful in many ways. Maturity levels can be compared with peers in the same sector to determine a general benchmark and maintain a competitive advantage. It is often easier to justify investment in cybersecurity or threat intelligence by looking at what others are

	LEVEL 1: Basic	**LEVEL 2: Developing process**	**LEVEL 3: Effective Implementer**	**LEVEL 4: Thought leader /innovator**
Decision: What decisions is cyber threat intelligence be used	Threat intelligence remains at the level of experts	Threat intelligence is shared within the organisation, but its utilisation is inconsistent and unplanned	Threat intelligence guides decision-making and procurement and is utilised extensively across the organisation's functions	The organisation is recognised as a thought leader in its own sector through the cyber threat intelligence it produces
Operating models: The ability to achieve information	Threat intelligence collection is limited and sources are one-sided; collection may be outsourced	Threat intelligence gathering is targeted, and sources vary	The collection and sharing is diverse and active, and is supported through networks	The collection and sharing is organised and managed; networks are actively utilised
Tools: Technological maturity	The ability to use various tools is limited: for example, sending threat intelligence directly to the device's block list	The ability to utilize the best tools and new technology is in the hands of a few employees, and resources are limited	The value of new innovations is recognised and efforts are made to utilise them, but operations are ad hoc, i.e. case-by-case or unplanned	The utilization of new technologies is planned and prioritised, the organisation tests and is a pioneer in utilising innovations
Objective: Continuous improvement	Cyber threat intelligence is collected; guides and best practices are utilised as advised	The cyber threat intelligence process has evolved in line with the organisation's own identified needs and objectives	The cyber threat intelligence process is unique and constantly evolving based on lessons learnt within networks	The organisation is a pioneer in cyber threat intelligence and, together with its partners, produces and shares new methods, information and operating practices, i.e. teaches others

Table 1: The different levels and dimensions of the threat intelligence process.

doing, rather than by focusing on the benefits it yields, which can be difficult to grasp at first. This may be particularly necessary in the early stages of the threat intelligence process, when the concrete benefits it yields have not yet been realised.

Similarly, measuring one's own maturity level may be necessary when selecting suppliers and other partners, such as alliances, information-sharing networks or non-commercial partners. There are several ways to approach measurement, but the most commonly used methods include various self-assessment forms, official standards, or metrics based on the operational benefit of cyber threat intelligence (i.e. how often decisions are made based on threat intelligence). Particularly in the case of subcontractors, it is often useful to assess their technological capabilities, i.e. what systems they use or what types of data sources they have access to. When selecting measurement methods, it is important to remember that results obtained from different metrics are rarely comparable with one another. When selecting partners, an organisation should focus more specifically on meeting its own needs and risk assessments, rather than on the results of metrics that are of minor significance to it. Furthermore, it is possible and advisable to require a certain level or specific functions from subcontractors, even if no concrete maturity metric is used.

The primary objective of measuring maturity levels is to assess an organisation's maturity and, through this, to develop it. Measuring the level of the threat intelligence process is also useful as the process evolves, in identifying the organisation's next steps and in ensuring its own reliability. Once the baseline has been mapped out and documented, it is easier to see progress later on. Comparisons with other competitors in the same sector and the resulting competitive advantage help to justify the necessity and usefulness of investments. Indeed, the development of the process and how well it meets the set objectives and identified needs can be considered one of the most important metrics related to the cyber threat intelligence process.

Increasing an organisation's cyber maturity is a process in which the organisation moves from haphazard information security towards a more systematic, risk-based and proactive approach that combines people, processes and technology. An organisation's cyber maturity can be enhanced by first assessing its current situation, i.e. the baseline, using various methods (such as the gap analysis described later). Following this, key risks are identified and control measures defined for them, for which management draws up an action plan and allocates resources. Increasing maturity begins with getting the basics right, one of the most crucial aspects of which is creating a cyber-secure organisational culture by training staff. Another key measure is the implementation of technical measures that improve day-to-day information security operations. Cyber maturity increases as working methods and processes are developed in line with continuous feedback and the evolving cyber operating environment.

1.4 Outsourcing and the reliability of partners

The cyber threat intelligence process is almost always based, to a greater or lesser extent, on information sharing and cooperation. It is such a broad and multifaceted undertaking that even the best-resourced organisation would be ill-advised to attempt to produce and do everything itself; rather, an important part of a successful process is also securing the right partners. Nor is it cost-effective to do everything in-house these days: if a company's own cyber expertise and capabilities are lacking, investing in a reliable cybersecurity partner is often more than justified. Partnerships can take the form of equal knowledge-sharing networks or subcontractor or supplier relationships, through which information or expertise is acquired to support the cyber threat intelligence process. The best partnership is one in which both parties can give and receive information. This enables mutual growth and development.

When selecting partners, it is important to assess what they can deliver and how they meet the organisation's needs. It rarely makes sense to acquire a partner that produces exactly the same things; instead, it is usually advisable to focus on filling one's own information or expertise gaps. This is achieved by acquiring partners specialising in a specific type of cyber threat intelligence or the process of producing it. Certain stages of the threat intelligence process also require experience and expertise, and it is often easier, particularly in the early stages, to acquire this externally rather than develop it in-house. Partnerships, whether they involve subcontracting or information exchange, should not, however, be viewed as static. They are intended to evolve and, above all, to develop both parties. In an ideal scenario, the expertise purchased from a subcontractor is transferred to the organisation's own staff, and knowledge-sharing agreements evolve as the various parties become better at utilising the information provided by their partners and understanding what kind of data is required. A well-chosen partner helps to increase the organisation's maturity: if the organisation is still in the early stages of its maturity, the best partner is one that grows the organisation's own capabilities as the collaboration progresses.

Another key aspect of the assessment is the reliability of the partner. When it comes to partners used in cyber threat intelligence, there are two types of trust: trust in the service provider itself and trust in the reliability of the information it produces. Both are critical to a successful threat intelligence process. Trust in the service provider itself means the same audit obligation that an organisation has with regard to any IT service provider. Cyberattacks are increasingly targeting subcontractors and, as subcontractors producing cyber threat intelligence often have access to the systems of multiple organisations, they are an attractive target for cyberattacks.

An assessment of an organisation's reliability may be based, for example, on certificates, questionnaires completed by subcontractors, or general reputation. In the case of cyber threat intelligence providers, it is worth remembering that not all of them necessarily need to meet the same audit criteria as, for example, IT service providers. If, for example, an external party merely procures threat intelligence and never connects its own systems or otherwise gains access to the organisation's information systems, the requirements need not be as stringent. Even in these cases, however, the level of reliability affects, for example, what kind of information and how sensitive the information is that the organisation itself can share with this supplier. In many cases, threat intelligence that has passed through the process may contain direct references to the organisation itself or reveal something about its security and identification capabilities. This information may also be valuable to malicious actors. The reliability of external suppliers must determine not only the depth of cooperation that can be entered into with various parties, but also the level of sensitivity of the information that can be shared with them.

Another important aspect of reliability is the level of certainty of the threat intelligence produced by external actors. This refers to how accurate, up-to-date and correct the information they produce is. At its worst, poor threat intelligence can lead not only to threats being overlooked, but also to a false sense of security, which is when the most serious damage usually occurs. From the outside, without prior knowledge, it can be difficult to assess how reliable the information produced by a particular provider is. The quality of information is easiest to assess only after it has been obtained from the source for a while and, generally, compared with other sources producing information on the same subject. Nor is trust divided into an either/or (reliable/unreliable) assessment scale; rather, reliability is often guided by motives and shared interests. When selecting partners, however, one often has to rely on the supplier's reputation or the number and quality of its existing customers. Data produced by a company that has long supplied information to key stakeholders is likely to be fairly reliable, whereas information from lesser-known sources should be treated with caution.

Depending on how much data an organisation is capable of processing, collecting data with a lower level of reliability may still be useful. A data source that no one else in the sector uses can prove highly valuable if its reliability can be verified through long-term monitoring. A single critical signal from a completely new source may be precisely what enables the early detection of a threat that would otherwise go undetected, and thus often proves to be the most significant source of information. However, the use of often unreliable information sources is usually only sensible for organisations specialising in threat intelligence gathering, though it is naturally possible for anyone willing to invest sufficient resources in it. An organisation must understand the value of information at different levels of confidence and, based on its own resources and needs, determine the type and calibre of partners from whom it should obtain information.

2 THE CYBER THREAT INTELLIGENCE PROCESS

The use of cyber threat intelligence is referred to as the cyber threat intelligence process (CTI process). Through a cyclical threat intelligence process, it is possible to develop and guide management's ability to understand cyber threat intelligence. It encompasses all stages, from the initial plan through to the collection and utilisation of information, as well as the implementation of development needs identified during operations for the next collection cycle. The raw data collected during the process is transformed into information and ultimately into intelligence that supports or guides decision-making. It is cyclical and continuous in nature, and can be easily illustrated using the intelligence cycle familiar from the intelligence community. The intelligence cycle is a description of the process of collecting, analysing and utilising intelligence, and is divided into four or five stages. In the case of cyber threat intelligence, the four-stage cycle is the most useful (Figure 2). In this handbook, the cycle is divided into the stages of Steering, information gathering, analysis and distribution. The cycle should not be understood as a process diagram where one moves in a straight line from the first stage to the next. In reality, each stage of the cycle runs simultaneously alongside the others, and several CTI processes may be running at the same time. The 'circle' essentially illustrates what happens to threat intelligence at each stage and how it is refined from raw data into insights that support decision-making.

In this chapter of the handbook, the various stages of the CTI process are discussed individually, divided into three different perspectives. At the start of each stage, the responsibilities and measures of the organisation's management are addressed. This is followed by a discussion of operational-level measures and the duties of operational management. Finally, the practical and technical tools that can be utilised at that stage are discussed. The aim is for representatives of each perspective to derive concrete benefit from the handbook's content, so that the whole provides as broad and comprehensive an overview as possible of the entire cyber threat intelligence process.

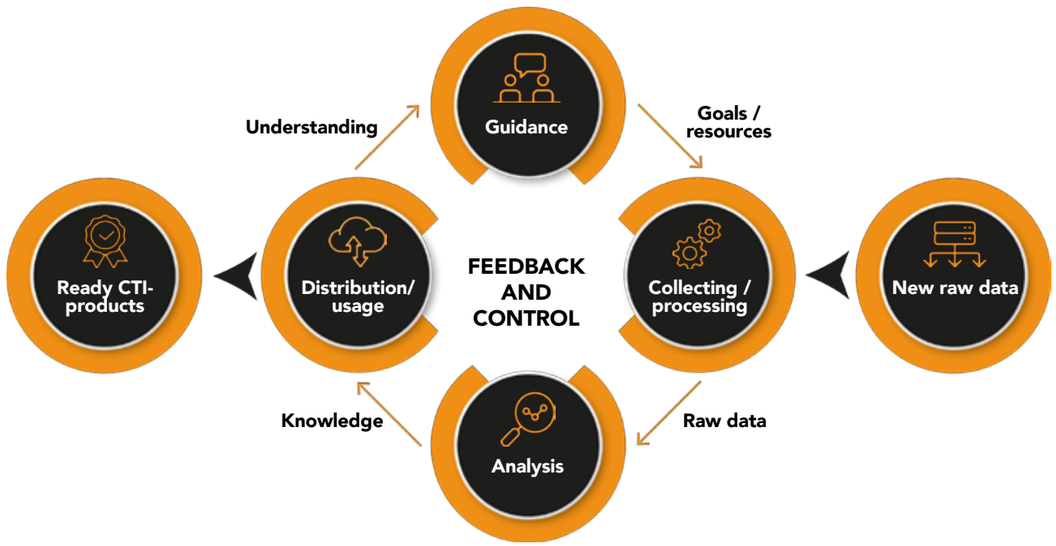


Figure 2: An individual process within the cyber threat intelligence circle.

2.1 Steering

Steering of the CTI process is often the most critical step in ensuring the process's success. This involves defining the process objectives, as well as the resources and mandate required to achieve them. Without careful steering, it is likely that resources will be wasted on collecting or processing the wrong kind of data, or that not all available and necessary data will be collected or utilised. It is therefore the responsibility of management to ensure well-executed steering to protect the company's IT assets from various threat actors, as even a single oversight can lead to a significant information security incident. Put simply, the steering phase involves planning the collection and utilisation of threat intelligence, as well as preparing for the practical implementation of these plans. Ultimately, the CTI process is about investing in security, such as protecting IT assets, and if you want a return on that investment, it needs to be carefully planned and prepared.

2.1.1 Management's responsibility

During the steering phase, the organisation's management bears significant responsibility. Management defines the objectives, threat intelligence requirements and available resources. Management also makes decisions, for example, on the use of partners at different stages of the process. The extent to which strategic management implements this and the proportion that falls to those responsible for operational activities varies from organisation to organisation. Ideally, both parties are closely involved in the process. The process also involves and consults other parts of the organisation, namely all those who may come to utilise the collected cyber threat intelligence. It is natural that if the CTI process is launched from scratch, this task may seem challenging. At this stage, it is even advisable to consult external experts if there is insufficient experience in the field.

In practice, there are two tasks involved in steering the CTI process:

1. Identifying the assets to be protected and mapping the threat vectors targeting them.
2. Determining the necessary information and its level (strategic, operational, technical) to ensure that the information required for decision-making is available.

The first involves not only identifying assets but also assessing the impact of attacks or disruptions targeting them, as well as prioritising the assets to be protected. The latter involves questions such as 'what kind of threat intelligence is needed', 'who can produce it' and 'in what format can the collected information be best utilised'. It is important to understand who within the organisation needs cyber threat intelligence, in what format and to what extent it is required, and what the organisation's capabilities are for acquiring and processing the information. Based on these and other questions, the organisation's management determines the information requirements and the resources available to meet them (in practice, often personnel and capital). A good outcome at this stage is a set of specific questions, the answers to which will be addressed in the final phase of the process. The aim is to select the questions for which answers are sought and to identify the threats for which advance warning is required.

Not all organisations necessarily require information at every level, and the number of questions can range from a few to several dozen. What is actually needed – that is, the types of questions for which answers are sought – is unique to each organisation. It is also worth noting that information requests are not free, so for this reason too, it is essential to be able to list and define the questions that correspond to the organisation's current information needs, and to weed out the so-called unnecessary, but 'good to know' questions. It is precisely this mapping out that is the most important task of the steering phase for senior management.

In addition to the above, a prerequisite for successful steering is the definition of early warning criteria. This means that management must define the issues on which it wants the CTI process to provide the organisation with early warning. This also makes it easier for the organisation to define the triggers that will set off an alert or other immediate response to which to react.

EXAMPLE QUESTIONS IN THE CTI PROCESS, DEPENDING ON THE ORGANISATION AND ITS UNIQUE CONTEXT

Strategic-level questions:

"How will the cyber threat landscape develop over the next year?",

"How will geopolitics affect the operations of threat actors targeting us?",

"On which issues or developments do we want to receive early warning?",

"Which shift in trends could significantly hamper the organisation's operations in the future?"

Operational-level questions:

"What types of attacks are currently most prevalent in the operations of known threat actors?",

"Where is information relating to cyber attacks shared?"

Technical-level questions:

"What methods can be used to identify and limit the spread of malware or its infection of our own devices?",

"Which IP addresses have been identified as belonging to specific threat actors, and where can this information be obtained?"

2.1.2 Operational measures

Once management has defined the strategic objectives, issues and requirements for cyber threat intelligence, it is the responsibility of the operational level to decide how these will be achieved in practice and what tools and support are needed to meet these objectives. This involves decisions regarding personnel, partners, investments, methods and tools to be used. In a sense, this is an investment project for managing cyber risks – if the investment is not backed by the right resources, the results, and consequently the benefits, may well remain modest. Typically, at this stage, there are still extensive discussions with senior management regarding the objectives and possible approaches.

Once the final plan is in place, operational management determines the measures that must be implemented before the data collection phase begins. This may include, for example, hiring new staff, procuring tools, or entering into cooperation agreements with partners and subcontractors. At this stage, practical measures still mainly involve mapping and drawing up plans. However, the aim is to produce concrete, feasible plans, rather than high-level lists of objectives or questions that require answers.

Mapping of expertise and personnel

An important part of the concrete measures in the steering phase is mapping the necessary expertise. At a strategic level, cyber threat intelligence can sometimes be better produced by a geopolitics or international relations professional rather than a cyber expert. It is essential to ensure that staff are available not only to collect and process threat intelligence, but also to share it. A person who collects and analyses technical-level threat intelligence is not necessarily the best person to communicate findings to non-technical staff or to liaise with external parties for the purpose of sharing information. The size of the organisation and the scope of the process, in turn, determine how much staff each stage of the work requires, and whether the same staff are used at different stages of the process. During the planning phase, the organisation must determine, based on the agreed data collection questions, what kind of expertise and which staff are required to implement the process.

Selection of partners

It is natural that hardly any organisation is able or feels it necessary to carry out the entire CTI process using only its own staff. It must be remembered that cyber threat intelligence is part of a broader, interconnected threat intelligence ecosystem and should not be understood or viewed as a separate entity from, for example, surrounding geopolitical events or other threat intelligence affecting the organisation's own business operations. Sharing and receiving threat intelligence across organisational boundaries is, in fact, a crucial part of the CTI process. Participation in information-sharing networks, the use of subcontractors in certain stages of the CTI process, and the sharing of threat intelligence are effective ways of improving outcomes, particularly if an organisation's own capacity for processing or collecting information is limited. For example, national ISACs (Information Sharing and Analysis Centres) are cybersecurity cooperation bodies established for different sectors, which address various sector-specific cyber threats and best practices for protecting against them. It is therefore important to understand that the sharing of information regarding cyber threats is almost always reciprocal. Rather than simply seeking benefits, organisations should consider how they themselves can add value to any given network, as this often leads to an improvement in the quality of the information received.

The selection and auditing of partners are discussed in more detail in section 2.4, but if no partners have yet been selected, it is natural to do so at this stage of the process. Once the partners have been identified, a decision is made at this stage of the process on how they will be utilised. For example, will part of the data collection or analysis be outsourced entirely? To what extent is the data obtained from different partners or networks trusted? Does the organisation itself do anything other than receive information and share it internally with the relevant parties? How is the collaboration carried out in practice, i.e. what equipment and networks are used? These are some of the questions we aim to answer at this stage of the process.

Tools for operational measures

During the steering phase, a plan must be drawn up for the tools to be used in the CTI process and for which there are sufficient resources. Although in practice, what work is done and how it is done often evolves during the process, it is advisable to identify potential application or tool purchases during the planning phase. Once you know what you want to achieve, it is often easy to determine what kind of tools are required for implementation, how many of these solutions already exist, and what still needs to be acquired. The tools used determine to some extent the format and nature of the threat intelligence produced. When selecting tools, it is therefore advisable to consider what other industry players or partners are using, and to guide choices to facilitate compatibility and information sharing. It is important to bear in mind the organisation's own context and available resources, , and to assess the necessity of each tool individually. One should not automatically choose the most popular or most widely used solution in the sector, but rather understand what one's own organisation needs. It is therefore important to understand both the specific requirements of one's own sector and those arising from one's specific field of activity, and to select tools and partners accordingly. It is also worth noting that larger organisations have the opportunity to use more optimised and advanced tools than medium-sized or small organisations.

If subcontractors are used in the CTI process, it is advisable to ascertain what technical solutions or other tools they have at their disposal. This should be done not only to assess reliability and cyber maturity, but also because the tools used by subcontractors should be compatible with the organisation's own tools. When selecting subcontractors, it is also worth noting that the data they produce should be readable and understandable using the methods and systems in place within the organisation.

Planning for utilisation

Throughout the planning phase, it is important to bear in mind the end result and the final product that the CTI process aims to achieve. When making choices regarding personnel or tools, these must be based on the type of information that is ultimately to be produced and how it can best be utilised. In terms of utilisation, it is critical, for example, that the information obtained is in an understandable format and accessible to all those individuals and bodies who need it. The aim is to use CTI to make decisions that support the company's core business, either directly or indirectly. In practice, this involves an internal assessment of which entities can utilise threat intelligence and in what format. Whether the threat intelligence obtained as a result of the process is a list of IP addresses belonging to identified threat actors or a multi-page analysis of how quantum technology will affect existing encryption systems within five years, it must be clear what will be done with the end product.

Cyber threat intelligence is being utilised more extensively and for a wider range of purposes (Figure 3). Tailored customer needs guide the type of cyber threat intelligence an organisation should collect. In addition to the intended uses of the direct cyber threat intelligence obtained (such as information being passed on to management to support decision-making and as a guiding factor for technical measures) , the information, expertise or material produced can also be utilised, for example, in the organisation's own marketing or publications, which establishes the organisation as a pioneer or thought leader. In fact, it is possible to derive other by-products from the end products of cyber threat intelligence, in addition to the actual intended benefit. In the future, it is likely that the range of applications will become even more diverse. However, not all organisations need to plan creative or surprising uses straight away. It is natural that, in the early stages, the uses will be quite straightforward. As experience in acquiring and utilising threat intelligence accumulates, it becomes easier to adapt and develop the process to produce products that can be utilised more widely.

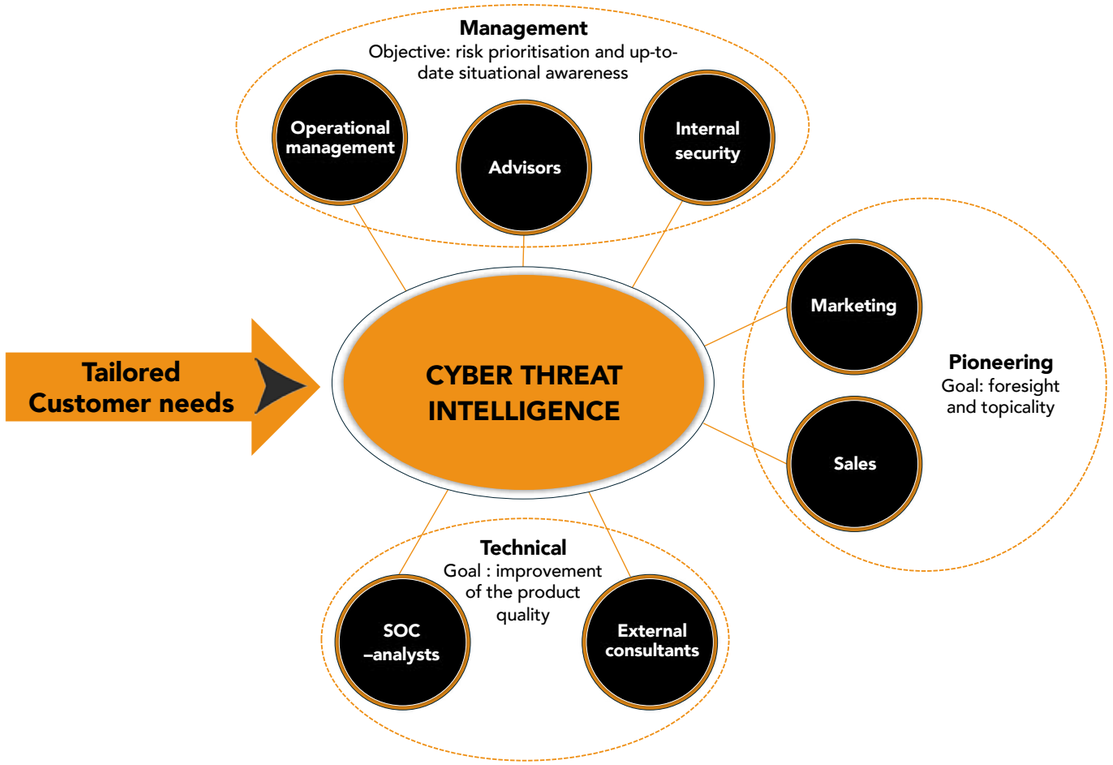


Figure 3: The diverse uses of cyber threat intelligence.
Source: image based on a sketch by Pietari Sarjakivi (2025).

2.1.3 Practical tools

Of all the stages of the CTI process, steering is the one for which the fewest clear, concrete tools or methods are available. 'Tools' at this stage refer more to discussion- and list-based activities. Planning usually takes the form of brainstorming or group discussions, which can be quite informal. However, there are also researched, structured methods available that can streamline the process, improve its reliability and facilitate development. Furthermore, a wide range of scanners or technical tools for mapping network assets can be used to identify the assets to be protected and the threat vectors targeting them. The CTI process produces more valuable information the better the organisation's IT assets and the threats targeting them have been identified. At its best, a successful CTI process can provide advance warning of who will strike, where and when the attack will occur, and how it might be prevented. Below are two different tools, the GAP analysis and the asset mapping model, which are examples of methods for implementing the control phase activities in a structured manner. However, these are not the only methods, nor are they necessarily the most suitable for every situation.

GAP analysis

A popular approach to the CTI process is the GAP analysis. A GAP analysis is a method that compares the current state with the target state and identifies the gap between them. It enables the organisation to see what is missing, what needs to be developed, and what resources or processes are required to achieve the target state. The aim is to link information needs to the company's strategy and business operations. As an analytical method, it is versatile, and there are several different models available. Below is an example of how a GAP analysis can be used in the steering phase of the CTI process.

Mapping the current state:
- What threat intelligence sources are already in use?
- How is the data collected, analysed and shared?
- Are standards used (e.g. STIX/TAXII industry standards for describing and sharing cyber threat intelligence)?
  - STIX (Structured Threat Information eXpression): A standardised language used to describe threats, such as malware, actors, attack methods and indicators, making the data machine-readable
  - TAXII (Trusted Automated eXchange of Intelligence Information): A protocol that defines how STIX-formatted information is shared automatically, making sharing efficient and secure
- What are the staff's skills and technical capabilities?

Defining the target state:
- Do we want to automate threat intelligence collection?
- Are integrations with SIEM, SOC or other systems required?
- What kind of threat intelligence utilisation process should the organisation have (e.g. response, analysis, sharing)?

Identifying gaps:
- Which tools, processes, data sources or expertise are missing?
- Are there any legislative, contractual or data protection challenges or requirements?
- Is current capability insufficient for a specific threat model (e.g. ransomware actors, vulnerability alerts)?

A GAP analysis can be used to draw up a concrete development plan:
- What to procure, what to develop in-house, what to automate
- Which processes require guidelines
- What training or skills are required

Measuring capabilities and continuous improvement:
- Once the baseline and target are known, progress can be measured and threat intelligence management can be turned into a continuous process

A GAP analysis is most effective when it involves a broad range of staff from different parts of the organisation. In addition to senior management, it is important to include those responsible for day-to-day operations and technical experts. External experts may also be involved, particularly if parts of the process are to be outsourced or if there is no experience of the CTI process within the organisation. The example above can serve as a template for the organisation to build its own GAP analysis, but it should not be viewed as a rigid or unchangeable model to which one cannot add their own questions or points for consideration.

Model for mapping assets to be protected

During the steering phase, another use for concrete tools is the mapping of assets to be protected, which is also part of the GAP analysis. Various ready-made tools and models are available for this purpose, which can be utilised to map industry-specific assets. The model refers to the identification of one's own assets to be protected, but often also to prioritisation and the mapping of potential threat vectors. The larger the organisation, the more difficult this process becomes. IT assets are constantly changing, so maintaining an up-to-date picture is almost impossible, and the number of assets requiring protection is so vast that it is simply not possible to map all the threats affecting them. In these situations, it is important to identify the assets that are most critical to operations and to prioritise their protection. One method for mapping assets to be protected and the threats they face is presented below.

Asset inventory:
- Ready-made lists of your own IT infrastructure
- Automatic scanners for assets visible both internally and externally

Identification of key assets:
- Which systems or devices are critical to business continuity, and are there alternatives or backups for them?
- Where is the most critical or sensitive data stored, and who has access to it?

Mapping threats and risk factors:
- Mapping the attack surface: How could the most important identified assets be attacked: an open network port, a vulnerable server, a poorly configured cloud environment?
- Vulnerability management: How could an attacker move from one system to another? What are the internal connections through which the most critical assets could be accessed?
- Threat modelling: How likely are various threat scenarios or forms of attack? What is the likelihood of state-sponsored influence operations targeting your organisation? How attractive is the target from a ransomware operator's perspective?
- The information produced by this assessment phase is an essential part of the company's overall information security processes

These questions are used to produce a prioritised or categorised list of assets to be protected, dividing them, for example, into critical, important and non-critical assets. This list is compared with the identified threats and their probabilities. For the most critical assets, more detailed scenarios can be developed to illustrate how

various threats might specifically affect them. Finally, practical measures are listed to mitigate these risks. The assessment should also be repeated and updated regularly; in some respects, it may even be an ongoing process.

From the perspective of the CTI process, it is important to identify what kind of information is needed to maintain security and what level of capability or motivation threat actors are most likely to have when attacking the organisation.

2.2 Collection/processing

The next stage following guidance is the collection and processing of information. This chapter covers both functions, with the focus on the collection phase. Collection refers to the acquisition of information at various stages of processing (raw data or pre-analysed data) in accordance with the plans made in the previous phase. Processing refers to the conversion of collected data into coherent, usable and contextual threat intelligence for subsequent analysis and utilisation. In other words, in order for data to be utilised, it must first be identified and collected. Only once this collected data has been processed is it usable.

This stage is just as critical as the previous one, and errors made here have a significant impact on the final result. Particularly when launching a new cyber threat intelligence process, a common mistake is made during the collection phase where data is simply gathered in as large a volume as possible from as many sources as possible. Although a large volume of data is, in principle, a good thing, this approach generally leads to a situation where there is too much input to process, and security teams become paralysed by unnecessary alerts and a mass of data requiring manual review. During the collection phase, it is therefore important to bear in mind the specific needs defined in the previous phase and to guide operations accordingly. An excessive amount of data can lead to errors just as easily as an incomplete collection. Only the most advanced organisations and those that have invested the most resources in the cyber threat intelligence process should collect all available information.

2.2.1 Management's responsibility

During the collection phase, the organisation's management has less responsibility than during the steering phase. An important management responsibility related to the collection phase is the creation and maintenance of partnerships. Nowadays, a significant proportion of threat intelligence is obtained from partners or through networks, and it is management's task to maintain and strengthen these relationships. No single organisation can collect or produce all possible information on its own, so this plays a particularly important role in a successful CTI process.

During the collection phase, the plans established in the previous stage are implemented, and senior management is primarily responsible for monitoring operations and receiving reports, or requesting them where necessary. At this stage, the reports are not intended to contain actual threat intelligence; rather, the focus is on monitoring how well the set objectives can be achieved in practice, and whether any new, previously overlooked sources of information or information needs come to light during the collection process. Taking these into account is primarily the responsibility of those implementing the work, but the organisation's management should stay informed about what is being done and how the process is progressing, so that, for example, any shortcomings or challenges that have now come to light can be taken into account during the steering phase of the next iteration. At its simplest, this monitoring may involve requesting feedback or interim reports; at its best, everything proceeds according to plan and the reports are very brief.
It is the responsibility of management to keep themselves informed of the costs associated with data collection and the efficiency of operations. When carrying out collection, it is easy to become somewhat 'blinded by speed' when there is an almost endless amount of data and information available, but gathering too much of it without the ability or intention to utilise it mainly drains the efficiency of the process. Crucially, this also involves identifying and managing potential biases: sometimes preconceptions can steer the collection process in the wrong direction from the outset. Management must ensure that the organisation's objective is clear and that activities are carried out in accordance with plans and within reasonable limits, taking into account the organisation's capabilities and needs.

2.2.2 Operational measures

The practical measures in the collection and processing phase are divided into the acquisition of raw data via selected data collection channels and its processing

EXTERNAL NON-TECHNICAL SOURCES
Broader contextual information that influences the threat picture.

OSINT sources (Open-Source Intelligence):
- News, blogs, security research
- GitHub / Pastebin (leaks, tools)
- Social media
- Academic papers
- MITRE ATT&CK database (TTP data)

Communities and networks:
- ISAC networks (e.g. finance or healthcare)
- CERT/CSIRT communities
- National cyber security centres
- Closed Slack/Discord/Telegram security groups

Off-the-shelf security products:
- Trend analyses (e.g. Gartner, Forrester)
- Threat analyses from security firms
- Service provider bulletins (Microsoft, Checkpoint)

Dark web and criminal forums:
- Tor forums
- Marketplaces
- Data dump services
- Ransomware groups' leak pages

INTERNAL NON-TECHNICAL SOURCES
Non-technical information that may reveal vulnerabilities or risk areas.

- Internal security reports
- Risk analyses
- Red team / penetration test reports
- Incident response reports
- Staff observations (e.g. phishing reports)

EXTERNAL TECHNICAL SOURCES
Data obtained from technical feeds.

Threat feeds:
- IOC feeds (IPs, hashes, domains)
- Paid curated feeds (Recorded Future,
- Mandiant, CrowdStrike, Anomali, etc.)
- Free feeds (Abuse.ch, Spamhaus, CERTs)

Vulnerability databases:
- NVD, CVE databases
- CERT/CC publications
- Vendor bulletins (Microsoft, Cisco, Adobe…)

Malware databases:
- VirusTotal
- Hybrid Analysis
- Joe Sandbox
- URL and domain reputation systems

INTERNAL TECHNICAL SOURCES
These are based on the organisation's own infrastructure.

Log data:
- Firewall logs
- IDS/IPS and NDR logs
- Proxy and DNS logs
- VPN and authentication logs
- Endpoint logs (EDR/XDR)

Network traffic metrics:
- NetFlow / sFlow
- Packet capture data

Server and application logs:
- Web servers (Apache, Nginx)
- Databases
- Cloud service audit logs (Azure, AWS, GCP)

Security systems:
- SIEM
- DLP systems
- Honeypots and honeynets (collection of indicators of compromise)

for further analysis. Depending on the organisation and the scope of its operations, there may be anywhere from a few to hundreds of data sources, ranging in nature from news media to internal log data. Some of the most typical data sources are presented below, but in practical work it is worth remembering that any source that appears to produce information corresponding to the information needs defined in the guidance can be utilised.

Collection

Raw data collection can be targeted at a diverse range of data sources. Similarly, it can be focused on generating information about attacks on the organisation that are potential, years away, or already underway. It is precisely the easy accessibility and diverse range of data that many new organisations collecting cyber threat intelligence fall into the trap of. It is just as important to understand what information is not needed or cannot be processed within one's own process as it is to know what kind of information is required. The collection phase evolves with each iteration of the process and may change significantly with the introduction of new data sources.

In practice, the collection phase can be outsourced in its entirety. In this case, the service provider handles the collection, processing and the next stage of work, namely analysis. It is more typical, however, to combine in-house data collection with external sources. The importance of networks is particularly emphasised during the collection phase. Particularly in terms of the development of the threat intelligence process, it is important for an organisation to identify what kinds of networks exist within its own sector or region and what is required to join them. When combining external sources with the organisation's own data collection, it is of the utmost importance to ensure that the data is channelled by the various collectors to a single location for processing and subsequent analysis. Whether the processing is carried out by a subcontractor or the organisation itself, it must be ensured that all collected information ends up in the organisation's possession, and that information obtained from network-organised information-sharing meetings does not remain solely with the person who attended the meeting.

If the organisation's objective is to develop its own threat intelligence process or improve its maturity, it is recommended that not all threat intelligence collection, and certainly not the processing, be outsourced. It is natural to rely heavily on external experts, particularly in the early stages. This may also be the best way to understand how and from where to obtain information from a wide range of sources. Developing in-house expertise with the support of an external service provider makes sense in the long term and is often cost-effective.

Processing

Before the collected raw data can be analysed, it must be converted into a format suitable for processing. This is known as raw data processing. Different types of raw data require varying degrees of processing to become usable. Sometimes the collected data may be ready to use almost as it is, for example, the signatures of a new piece of malware or a list of malicious IP addresses, both of which can, in practice, be fed directly into firewalls or SIEM systems. Other times, the collected data requires a great deal of processing and adjustment of the level of abstraction to ensure that its analysis is not only effective but also possible. In practice, processing may involve converting data into a common format, removing extraneous 'noise' and duplicates, as well as clarifying the data and standardising the language. It often involves creating metadata to improve the traceability of the process or enriching the data by combining inputs from several different sources. What this entails in practice depends on the objectives and intelligence targets set by the organisation itself. Processing is a stage that benefits from experience and expertise; when done successfully, it reduces the workload in subsequent stages. On the other hand, failure at this stage can result in important information being overlooked.

In addition to data collected in-house, processing often involves data generated externally, for example by the aforementioned networks or partners. It is very common for this data to require some modification so that it can be harmonised with the data collected by the organisation itself or fed into analysis software or a database. Particularly for organisations with a very extensive threat intelligence process, where a large amount of data is received from external sources, processing capacity must be high. The ability to receive data in virtually any format and utilise different file formats is both useful and critical for organisations operating in this type of environment. At the very least, all organisations running threat intelligence processes should be prepared to receive the simplest and most common data formats. However, the burden of processing can be reduced by considering in advance what format the data is likely to be received in and how it can be handled most simply. If the analysis tools have been selected with the type of data to be collected in mind, there may not be a need for as much data manipulation.

In any case, processing is at least as important a stage as the collection of the raw data itself. Without it, resources are wasted in the analysis on sifting through irrelevant duplicates, and important connections may go unnoticed. Whether the analyst is an automated tool or a human, both benefit from the data being processed more effectively at the collection stage.

2.2.3 Practical tools

The tools used for collection vary considerably depending on the type of data and the source from which it is collected. Collection can be carried out manually by individual analysts, and this remains very popular. For example, when searching for raw data for strategic analysis. However, there are an ever-increasing number of better automated collection tools available, which can be utilised to gather many different types of data. Nowadays, most automated search engines utilise artificial intelligence, most commonly large language models, and, in addition to mere collection or scraping, also perform some processing, such as removing duplicates or formatting the results to a specific type or language.

DATA COLLECTION TOOLS

- Automated search engines/aggregated feeds – for example, Google Alerts, Talkwalker and Feedly
  - Enable automated monitoring of specific search terms or criteria and generate notifications
- Data extraction and scraping tools – for example, Python-based BeautifulSoup and Scrapy
  - Perform automated web scraping
- Dark web monitoring tools – As part of other application suites, such as CrowdStrike's X Recon, or specialised platforms, such as Cyber Intelligence House
  - Generate raw data from the dark and deep web, either for direct use or for further analysis
- Indexing tools – for example, Splunk and Elasticsearch
  - Collect and process machine-generated data from numerous sources, enabling its storage and searches within data repositories
  - Offer opportunities for visualising the collected data and can serve as analysis platforms

Popular information-sharing platforms, through which an organisation can both receive and share threat intelligence, can also be considered collection tools. One such example is MISP (Malware Information Sharing Platform), a free, open-source platform used by numerous authorities around the world to compile and share threat intelligence. MISP offers the opportunity to join networks where standardised and often verified threat intelligence is shared in an easily usable format. In addition, the free and open-source OpenCTI tool is often used; it offers some of the same functions but acts more as a tool to support the analysis process. OpenCTI is also a newer tool and, partly due to overlapping features, acts as a challenger, but the tools work best in parallel.

The tools used for processing raw data consist of standards for data modelling and applications designed for indexing or organisation. Standards such as STIX and TAXII enable the sharing of threat intelligence by providing a structured way to store information. Depending on the source or type of raw data, converting it to these standards may require some effort, but in principle, both can be used to process threat intelligence that is significantly different or at different levels. In the future, artificial intelligence will also play an increasingly significant role in the further processing of raw data in cyber threat intelligence processes of this kind. AI can be utilised, for example, particularly in the data pre-processing and structuring stages, in enriching the data, and in removing excess noise. Customised AI solutions will further ease the processing burden on analysts or data handlers and often enable near-complete automation in the processing of data from routine data sources.

2.3 Analysis

The third stage is analysis. In the analysis stage, raw data is transformed into threat intelligence through the analysis process. Depending on the quality of the collected data, this can be simple or require a great deal of work. The aim is to add meaning to the raw data, combine information from different sources to draw conclusions, and ultimately produce comprehensible information to support decision-making and thus lead to concrete measures. Crucial to the final outcome are clearly defined intelligence questions and information needs established at the early stages of the process. In cyber threat intelligence, analysis can be carried out just as effectively by a human as by a system. Automation and the use of artificial intelligence, particularly in the analysis of technical data, are constantly evolving, but human analysts still play a significant role, particularly in strategic-level analysis.

2.3.1 Management's responsibility

During the analysis phase, management's responsibility lies in oversight, deepening the context, providing guidance where necessary, and preparing for the utilisation of the final product. Management must ensure that the resources and tools required for the analysis are available and that emerging needs can be met. Most of the actual guidance has, in principle, already been provided during the steering phase dedicated to this, but in practice, new needs or opportunities often emerge at this stage. The individuals or systems carrying out the actual analysis may not have been involved in the steering phase, and they may not have precise knowledge of the nature of the information produced or the purpose for which it was intended. It is the management's task to remain involved in the process and steer it in the direction of the objectives, so that it yields the greatest benefit in subsequent decision-making.

An important part of the analysis phase is reporting findings. It is the analysts' responsibility to produce reports in a format that is easy to understand and whose content can be utilised by the recipient. This is often the organisation's management. Particularly when working with new types of data or new sources, analysts may initially find it difficult to understand the format in which the data should be presented. In such cases, it is management's role to provide feedback and demand more from the reporting. If the reports produced by the threat intelligence process do not lead to practical measures, the process must be developed. Although the reporting format and other details should already have been agreed upon during the steering phase, providing continuous feedback and striving to develop the process is also important during the analysis phase. Dialogue between analysts and the parties utilising the reports must be open, and both parties must understand what kind of information is required and in what format.

However, management should not interfere with the actual analytical work. Although it is desirable for management to know what analysts are doing and what the practical work entails, it should not participate in or direct the process too intensively but rather ensure that the analysis is carried out as objectively as possible. Excessive involvement can restrict analysts' freedom or influence conclusions, particularly in strategic-level analysis. Therefore, whilst guidance and understanding are important, management should not interfere too much in the process itself.

In practice, management's responsibility during the analysis phase is to ensure that the work is heading in the right direction. Cyber threat intelligence, or its production, must not become 'politicised', i.e. it must not be guided by the organisation's (or its leaders') objectives, wishes or preferences. If the organisation's management is too heavily involved in the process, there is an increased risk that those conducting the analysis may, perhaps subconsciously, seek to produce information that would please the manager would like to see, or to conceal findings that are not believed to please the manager. This can easily lead to cognitive biases in the process. This, too, is an evolving and iterative process. When the threat intelligence process is carried out for the first few times, management's involvement is likely to be greater. This is often a good thing, but ideally, their role at this stage of the work diminishes as best practices become clear and issues are resolved through repetition.

2.3.2 Operational measures

There are countless options for practical measures during the analysis phase. How the data is analysed depends on the type of data the organisation has collected and what the objectives or defined information needs are. The aim of the analysis phase is to distinguish the significance of events from noise and random occurrences. Generally, analysis involves determining the meaning of the data, validating it (i.e. establishing its reliability) and prioritising it (i.e. determining its level of urgency). The most common steps in the cyber threat intelligence analysis process are outlined below. This list should not be regarded as exhaustive or universally applicable. In practice, it is important for an organisation to understand how to derive the maximum practical benefit from the raw data collected. External experts can often be utilised in the analysis process.

Anomaly detection

Anomaly detection is an extremely important part of technical threat intelligence analysis. It can be carried out by human analysts, but more and more aspects of this process can be automated. In anomaly detection, massive amounts of log data are often searched to detect anomalies in order to identify potential intrusion attempts or to identify threat actors who have already gained access to systems. Log data is collected either as part of normal security monitoring or as part of the threat intelligence process during the data collection phase. The analysis looks for either any anomalies or pre-defined indicators of threat activity. Furthermore, the analysis looks for technical similarities between campaigns, such as similar malware, command-and-control channels, infrastructure solutions or attack chains, which can be used to combine individual observations into a broader picture of threat actors' modus operandi.

Threat modelling and attribution

Threat modelling and attribution involve identifying observed external activity, often intrusion attempts, and understanding cause-and-effect relationships. Threat modelling and attribution aim to use raw data to understand who is behind the observed activity and what the actors' possible motives might be. Threat modelling involves drawing conclusions about the objectives of the activity based on observed indicators, i.e. how the threat actor, for example, seeks to infiltrate the most critical assets. Threat modelling is intended to be carried out continuously and proactively, and its purpose is to be proactive. Even before the cyber threat intelligence process begins, the organisation's primary objective is to identify assets and, in particular, systems critical to its operations, and to map potential attack vectors (discussed in section 3.1.3). The analysis phase is therefore more about using the collected data to determine at what stage of the attack an external actor is and whether the operation follows the identified threat vectors. Whatever the answer to this question, it immediately guides the countermeasures to be taken, which may be either pre-planned (identified threat vectors) or entirely new.

In attribution, observations of external activity are combined with prior knowledge of the operations of various threat actors or types of threat actors, with the aim of identifying who is behind the activity. The aim of attribution is not necessarily to identify, at the threat actor level, which group is involved; rather, it is often sufficient to understand whether the activity is, for example, opportunistic, automated or targeted. This information alone can help in responding to an ongoing threat and in preparing for similar operations in the future.

Impact and risk analysis

If the aim of threat modelling is to determine how an attacker might gain access to critical assets, the purpose of an impact analysis is to identify what kind of damage would be caused if this were to happen. If, on the other hand, it is found that the intruder is not following any identified threat vector or targeting the most critical assets, the role of the impact analysis is to identify what the attacker might be seeking. Similarly, as the name suggests, the aim is to understand what kind of damage the threat actor could cause from the foothold they have already gained, or what data they may already have compromised.

It is particularly important to carry out an impact analysis in the event of an acute threat. This is facilitated by having as detailed and up to date a picture as possible of one's own IT assets, connections and what data is stored where. An impact analysis can be carried out in advance, and this is certainly the recommended approach for critical assets. Often, an attack is in some way different from what was anticipated, or it may, for example, be limited to only a specific part of the network. In such cases, the importance of impact analysis is emphasised. It helps to respond to the threat, facilitates crisis communication, for example, and may even prevent reputational damage. It is easy to find examples of cases where an organisation targeted by a cyber attack has communicated unclearly or incorrectly based on a poorly executed impact analysis. This has often resulted in a significant blow to credibility. Organisations may have given the impression that partners' or customers' data was not compromised in the attack. When it later transpires that this was not the case, the public perception is often one of dishonesty, even though the underlying cause may have been an error in the impact analysis.

Strategic analysis

The functions presented earlier focus largely on the analysis of technical threat data. The analysis of strategic and operational data is significantly different and often slower in its cycle. The aim of this form of analysis may be, for example, to understand the operating environment, anticipate future changes to it, or assess the likelihood and impact of new emerging threats. Structured analysis tools, which are a family of methods originally developed for intelligence analysis, can be used in the analysis of strategic and operational threat data. Structured analysis tools include, for example, various scenario tools, analysis of competing hypotheses (ACH), and force field analysis. Of these, the ACH is presented later in this chapter. The purpose of using structured analysis tools is to reduce errors in analysis by preventing intuitive pitfalls and cognitive biases. Using them forces one to approach the phenomena under consideration from multiple perspectives and to critically examine preconceptions.

The use of structured analysis tools, like other forms of strategic-level analysis, often requires experience and skilled analysts. It is not worthwhile for nearly every organisation to invest in the production of strategic analysis, but the value of the understanding it provides is worth recognising. An understanding of changes in the operating environment aids in proactive investment decisions. Identifying threats before they become serious is always more cost-effective than responding to them reactively. Furthermore, a 'general understanding' of cyber threats can be valuable information when building relationships and in informal discussions with partners. It is worthwhile to utilise and acquire strategic threat intelligence and ready-made reports, even if it is not always sensible or feasible to invest in producing them in-house. An understanding of strategic cyber threats is part of the situational awareness that management must maintain in one way or another.

Documentation and reporting of the analysis

The final and perhaps most important operational stage is the dissemination of the conclusions reached in the analysis, i.e. sharing the ready-made information with those who need it. The analysed information can take any form, from a text-based report to a verbal statement, or a list of IP addresses identified as definitely malicious, fed directly into a firewall.

Reports must be produced in a format suitable for different target audiences:

- The C-level needs a clear summary of the implications and recommendations.
- The SOC team needs technical artefacts, indicators and descriptions of the attack chain.
- The architecture team benefits from longer-term TTP (Tactics, Techniques and Procedures) trends and recommendations.

A high-quality report clearly distinguishes between observations, conclusions and recommended actions, and includes the analyst's confidence scale. In some situations, citing the source of the original raw data may also be appropriate, but this is not always necessary. A rule of thumb is that analysis products, particularly those in report format, should be delivered to the end user in as concise a form as possible and in the smallest possible volume. Reporting unnecessary information that does not lead to action increases the workload and generally yields no useful results. Those responsible for cybersecurity already have to contend with a daily flood of information, so analysis that produces only relevant and genuinely meaningful information is extremely valuable. Superfluous or overly long reports, especially when they are repetitive, often diminish the recipient's interest, meaning that on the one occasion when a report does contain valuable information or information requiring a response, it goes unnoticed.

In the final stage of the analysis, it is important to document the work carried out. This involves recording information about what kind of data has been analysed and what conclusions have been drawn from it. Documentation makes it easier to repeat similar analytical work, but is particularly valuable in situations where it becomes apparent that the analysis has led to an incorrect result. Well-documented analysis makes it easy to trace where the error occurred and avoid it in the future. Documentation is valuable when assessing the reliability of data obtained from various sources or partners. Although the end product of the analysis process, be it a report or an indicator fed into a SIEM, does not contain the source of the original data, it is important for traceability that the data is stored somewhere. If data from a particular source is consistently incorrect or incomplete, it can be difficult to detect or distinguish it from the final product. Careful documentation is therefore essential.

ACH method (Analysis of Competing Hypotheses)

ACH is a structured analysis method in which competing hypotheses are systematically evaluated against available information. Its key benefit is the reduction of cognitive biases and the improvement of analytical transparency. The method is used particularly in strategic and operational threat assessment, for example when assessing the perpetrator, motive or likely future developments of an attack based on uncertain or conflicting information.

Red Team / Blue Team cross-check

The Red Team / Blue Team approach is used to ensure the quality of analysis and to identify alternative interpretations. The Red Team challenges the assumptions and conclusions of the analysis from the attacker's perspective, whilst the Blue Team represents a defensive interpretation grounded in the organisation's reality. The method improves the reliability of the analysis and helps to identify gaps or erroneous conclusions, particularly in operational and tactical-level CTI.

Modelling a timeline of the attacker's likely progression

A timeline is used to organise the events of an attack into a logical and chronological order. This supports an understanding of how the attack has progressed, at what stage the attacker is currently at, and what the likely next steps are. The method also helps to identify inconsistencies. Timelines are utilised in particular for case-by-case analysis, incident response support and proactive threat assessment.

Cyber Kill Chain

The Kill Chain model provides a framework for identifying the stages of an attack, from reconnaissance to achieving impact. It enables analysts to pinpoint at which stage an attack has been detected and where defensive measures should be targeted. The model is commonly used in tactical and operational-level analysis to identify gaps in defences and develop detection capabilities.

Attacker TTP modelling (MITRE ATT&CK)

MITRE ATT&CK provides a standardised framework for describing attackers' tactics, techniques and procedures (TTP). Its key benefit is a common language between analysts, SOC teams and management, as well as the comparability of analysis across different incidents and threat actors. The model is applied to support tactical analysis and to profile threat detections and threat actors.

Diamond Model structure

The Diamond Model structures cyber threats through four key elements: threat actor, infrastructure, capability/activity, and motive or victim. The model helps to understand the overall picture of the threat and the relationships between the different elements. It is utilised particularly in operational and strategic CTI when seeking to link technical detection data to a broader context and the threat actor's objectives.

Scenario exercises and workshops

Strategic-level scenario exercises help to visualise the impact of threats on an organisation's core functions and may reveal previously overlooked weaknesses in preparedness. Operational-level exercises train and develop preparedness through concrete contingency measures.

2.3.3 Practical tools

There is a wide variety of analysis tools available for use in cyber threat intelligence. Their use depends significantly on the quality of the data being analysed and the objective of the analysis process. Below are a few tools used in the analysis of strategic and operational cyber threat intelligence.

2.4 Distribution

Whilst the previous stages have been crucial to ensuring that the CTI process is as successful as possible, the final stage of distribution and utilisation is essential for the work to yield any practical benefits. As noted in the steering phase, the most important criterion for the type of threat intelligence an organisation should seek to acquire is its usability, and it is precisely the realisation of this usability that is at stake in this phase. Whether the final recipient of the threat intelligence is a system, an individual or a department within the organisation, the task of this stage is to ensure that the collected and analysed information reaches its destination and that the recipient knows what they are receiving and what to do with it.

The distribution of cyber threat intelligence concerns both the organisation itself and external partners. The functioning of networks is based on all parties both producing and receiving information, so organisations working with cyber threat intelligence must also be prepared to share the threat intelligence they have acquired and processed with others. In this regard, particular attention must be paid to the type of information to be shared and to ensuring that the shared information is reliable and useful. Sharing incorrect information not only undermines the overall level of security in the field but can also cause reputational damage to the organisation. In particular, there must be complete certainty regarding the quality of the threat intelligence to be shared; alternatively, any uncertainty must be clearly stated. The uncertainty assessment methods defined by the Finnish Security Intelligence Service (SuPo) can be used here to determine the reliability of the information source and content. By definition, uncertainty assessment essentially consists of two key areas: assessing the reliability of the information source (the source's history, competence and past accuracy) and assessing the reliability of the information content (the integrity, verifiability and context of the information). The assessment of reliability is also influenced by the classification of information according to its security classification and confidentiality requirements: document-specific security and reliability classifications are often determined on the basis of risk management and consequences (TL I–IV).

An important consideration is therefore what kind of information the organisation is able to share and with whom. The criticality of threat intelligence must be defined internally within the organisation, and different information-sharing networks or partners classified according to their (level of access), specifying to whom information of which level may be shared. Data processors, i.e. analysts, rarely know where and when the information will actually be used after it has been shared.

In principle, the distribution and utilisation of cyber threat intelligence should be planned at the early stages of a project, but, as with any project, the plan is a good starting point that often changes in practice. New data sources or data formats are discovered during the project, or unexpected and rapidly emerging collaboration yields new types of information that prove useful. The most important task during the distribution and utilisation phase is to ensure that plans are implemented, to modify them where necessary, and to ensure that external threat intelligence is also utilised as effectively as possible.

2.4.1 Management responsibilities

In the final phase of the cyber threat intelligence process, management's responsibilities are twofold. The first responsibility, which has already been touched upon, is to ensure that threat intelligence reaches all areas where it is needed. The second, and perhaps more significant, is to ensure that the information is utilised and used to make decisions about the future or to develop current operations. The aim of the threat intelligence process is not to produce information for its own sake, but specifically to support or guide decision-making. It is the responsibility of management to enable the transformation of raw data into information, the development of that information into understanding, and ultimately into actions that lead to the mitigation of various cyber threat risks. Even the best threat intelligence process will not yield concrete benefits unless the understanding it provides can be effectively implemented. It is the responsibility of management both to make decisions based on threat intelligence and to ensure that other parts of the organisation to which the information is shared utilise it correctly.

In practice, these actions may involve reallocating resources, making new investments or managing exceptional situations. Indeed, another key responsibility of management is to prepare, implement, assign responsibility for and ensure that these measures are carried out. The best approach is to lead by example and demonstrate that cyber threats are treated as business risks rather than merely IT issues. It is useful to gather and request feedback from different parts of the organisation on the usefulness of cyber threat intelligence. If shortcomings are identified in the quality or format of the information, these can be used to steer future collection and analysis. Whether it concerns technical threat intelligence or strategic reports, it is the responsibility of management to ensure that the process in which the organisation has invested has a real impact on its operations. Without active leadership, cyber threat intelligence often remains merely reports and data. It is the responsibility of management to translate cyber threat intelligence into action and risk management.

Management is also responsible for organising and allocating resources for the sharing of threat intelligence with external stakeholders. In practice, this may be handled at analyst level, but management is generally responsible for drawing up information-sharing agreements, the resources allocated to them and the maintenance of the agreements. A proactive approach is important, and agreements and practices must be effective. If the sharing of certain information or types of information is hampered by bureaucracy or uncertainty about the scope of existing agreements, this significantly undermines the effectiveness of the networks. This often affects the willingness of external actors to share their own information.

2.4.2 Operational measures

While it is the responsibility of an organisation's senior management to ensure that threat intelligence leads to concrete measures, it is the responsibility of operational management to select, prioritise and implement them in practice. Measures can be quite simple (for example, adding new IOCs or identified malicious IP addresses to a firewall or SIEM) or complex long-term changes (modifying processes or procuring new systems). It is generally the responsibility of operational management to understand what these measures are and who will carry them out in practice. For example, it is possible that the threat intelligence relates to a system used by the organisation but produced and maintained entirely by an external service provider, in which case operational management is responsible for communication and coordination with the subcontractor. Coordination is also important within the organisation itself, as practical measures often require input from several different areas of operation or departments within the organisation.

CONCRETE MEASURES TRIGGERED BY THREAT INTELLIGENCE

- Patching and hardening measures
- Updates to monitoring policies
- Reviews of access rights
- Deployment of new systems
- Informing and/or training staff
- Temporary heightened alert and stricter security measures

Once the necessary measures have been selected, the next task is to prioritise them. The severity rating of threats or vulnerabilities produced during the analysis phase usually helps with this, but it should not be the sole guideline when deciding the order of measures. A serious vulnerability in an insignificant target is not necessarily as urgent to fix as a potential attack targeting the most critical assets. Tasks must be prioritised taking into account the criticality of different functions, available resources and other urgent tasks. Information security teams are almost always plagued by constant overwork, and prioritisation is often driven by necessity. It is therefore important that the party responsible for prioritisation understands the resources at its disposal and the order of priority for protecting targets.

Monitoring and reporting

Simply initiating measures is not enough. Particularly when working with new types of threat intelligence, it is extremely important to monitor that the measures are progressing and are both feasible and beneficial. Any deviations, difficulties or delays should be highlighted as quickly as possible so that they can be addressed and, if necessary, either the ongoing process can be adjusted or lessons learned for the future. Status reports must be required for all projects in which one cannot participate directly or whose progress cannot be monitored. This applies to both in-house measures and those delegated to subcontractors and partners. Furthermore, it is generally the responsibility of operational management to report upwards on the progress of operations.

All of this requires maintaining a good and accurate overview of ongoing activities. Maintaining this overview also involves, where necessary, communicating it to the relevant units so that they understand what the priorities are and why certain threats are assessed as more critical than others.

Providing feedback and updating operational models

Whilst maintaining situational awareness and monitoring the progress of measures, it is important to provide feedback to threat intelligence providers. Feedback should be provided on the content and format of the threat intelligence, but particularly also on its timing. It is extremely important to note if any threat intelligence arrives too late and should have been received earlier due to a lengthy implementation process. In such cases, it is justified to consider streamlining the analysis phase or utilising raw data directly.

It is important for cyber threat intelligence to be relevant, reliable and actionable. Although this is the aim at every stage of the process, some redundant information inevitably finds its way through. In such cases, it is worth assessing how many resources were used to produce the excess information and whether it was generated as a 'by-product' of necessary information, in which case it is difficult to avoid its creation. To clarify this, documented analysis and dialogue between the implementing units and operational management are essential.

The aim of providing feedback should be to improve operations. The cyber threat intelligence process is continuous, and in practice, a single organisation often carries out all its stages simultaneously. In such cases, the continuous collection and provision of feedback is important so that operations can be developed and remain effective. The CTI process must have a clear objective and goal, so that the process does not simply run in the background as if automatically: ultimately producing little information relevant to decision-making. In such cases, there is a risk that the CTI process will become little more than a self-perpetuating cycle with no real practical value.

In real life, it is not usually possible to organise a specific 'feedback session', so issues must be raised as and when shortcomings or opportunities for improvement are identified. Updating work instructions and procedures is particularly common in the early stages of the threat intelligence process, and one must be prepared for this. It is important to ensure that the lessons learned on an ongoing basis are utilised in such a way that they become permanent operating practices, rather than merely one-off changes to operations. It is important that the cyber threat intelligence process has an owner who collects feedback and is responsible for the continuous development of the process.

2.4.3 Practical tools

There are relatively few concrete tools available at the distribution stage. Depending on the quality and type of threat intelligence, distribution and utilisation may be carried out using individual technical cyber threat intelligence distribution platforms, such as Splunk or MISP (Malware Information Sharing Platform). It may just as well involve forwarding reports within the organisation as email attachments. The same distribution methods also apply to sharing information outside the organisation. The tools used for this are largely the same as the information-sharing channels and threat intelligence standards presented in the collection phase of this handbook, which help to ensure the transmission of harmonised information.

INFORMATION SHARING CHANNELS AND TOOLS

MISP/OpenCTI applications designed for the sharing and processing of threat intelligence, which enable the rapid and standardised sharing of data.

Standards such as STIX and TAXII are used on sharing platforms but also allow data to be transferred outside these platforms and utilised by other tools that are not directly connected.

Internal information sharing within an organisation, such as information-sharing channels on internal networks, weekly meetings, threat briefings for the management team, regular threat and crisis management workshops, as well as board and other regular reporting.

Informal threat intelligence networks may include, for example, monthly information-sharing meetings where authorities or the sector's major players verbally share information on cyber threats they have recently encountered or prevailing trends. A good example of this is the National Cyber Security Centre, Traficom, ISAC information exchange groups, whose main purpose is to share sector-specific information and experiences and, through this, to enhance the ability of organisations and sectors to protect themselves against digital threats and manage incidents. (For further information on ISAC activities, please contact ktk-verkostot@traficom.fi.)

Nor are there any particularly comprehensive lists of specific tools available for utilising threat intelligence. The specific actions that threat intelligence guides are highly context-dependent. For example, the hardening measures or changes to monitoring policies presented in the previous section are based on the platforms and applications that the organisation already uses.

3 CTI - A CONTINUOUSLY EVOLVING PROCESS

The primary purpose of cyber threat intelligence is to provide time and information for decision-making, as already noted in the introduction to this handbook. The aim is to allow time for the early identification of threats and for responding to them before they materialise. This window is constantly shrinking, and obtaining advance warning is becoming increasingly difficult. Threat actors' operations have accelerated, and the time between the disclosure of new vulnerabilities and their exploitation has shortened. At present, we often speak of a matter of minutes between the disclosure of a vulnerability and attacks seeking to exploit it. Technological development favours attackers, and artificial intelligence has already provided a significant advantage to those carrying out cyberattacks. Although AI has also yielded defensive benefits and new innovations are constantly emerging as a result, attackers have a considerable head start, as they do not need to audit or verify that an AI-powered attack tool will work reliably in all situations. A single success is enough, and if the tool does not work, no harm is done.

In other words, as a result of cyber influence operations becoming increasingly intense, the need for up-to-date cyber threat intelligence has grown even further. Controls required to protect an organisation's most critical assets are needed faster than a human can implement them alone. This, in turn, has increased the importance of artificial intelligence in the collection, processing and analysis of threat intelligence. The growing need for information, coupled with the increasing volume of various types of threat intelligence, has forced organisations to adopt AI agents and tools that facilitate these processes at an ever-faster pace. However, ensuring the reliability of AI remains a challenge. In the future, human analysts leveraging AI tools working will be best placed to meet this growing need for relevant cyber threat intelligence.

In addition to acute information that needs to be utilised on a tight schedule. There is a greater need for strategic and operational intelligence as the general security situation deteriorates and state-sponsored cyber influence becomes more widespread. Organisations' need for cyber threat intelligence will increase, and with the trend towards greater regulation, it is likely that the resulting obligations to maintain situational awareness and threat intelligence will also grow. This will further increase the value of cyber threat intelligence in the future.

The need for cyber threat intelligence applies to every organisation, but not in the same way. The resources available to and the needs of each organisation determine the unique circumstances in which the organisation operates. It is virtually impossible to create universal guidelines that apply to everyone. This handbook aims to provide advice that is as widely and flexibly applicable as possible for the initiation, use and development of the cyber threat intelligence process.

The process of acquiring and utilising cyber threat intelligence is quite extensive and multifaceted, as well as constantly evolving and developing. Implementing it successfully requires motivation, resources and experience. The best way to develop the process is to expand it in line with your organisation's growing information needs. The continuous implementation of new information sources, processes or analysis tools is important not only for keeping pace with evolving threats, but also for developing operations. The cyber threat intelligence process must be understood as an ongoing and evolving activity. The cycle must keep turning, and feedback must be gathered on the implementation of the various stages. The most important factor in an evolving process is the interest in developing it. The cyber threat intelligence process should not be viewed merely as a mandatory measure, but as an investment that generates added value, capable of saving the organisation from crippling damage and providing a position as a market and thought leader.

Case studies for the different levels of cyber threat intelligence

The introduction to this handbook referred to the different levels of cyber threat intelligence (strategic, operational and technical), and the various chapters have touched upon how intelligence at different levels requires different measures and handling. These case studies present a few models illustrating the practical measures required at each stage for threat intelligence at different levels. The examples are intended to help illustrate how information at different levels requires different measures and what these might be.

S = STEERING **C = COLLECTION / PROCESSING** **A = ANALYSIS** **D = DISTRIBUTION / UTILISATION**

STRATEGIC THREAT INTELLIGENCE (EXAMPLE CASE 1):
An organisation in a critical sector is targeted by state-sponsored cyber influence operations

S An organisation operating in a critical sector is known to be of interest to foreign cyber threat actors .

S The need to acquire information on cyber threats affecting the sector and their global development is identified.

S The organisation assesses its own capabilities to gather this information but concludes that the most cost-effective approach is to engage a subcontractor with whom an agreement is reached regarding the procurement of threat intelligence.

C The organisation begins to receive threat intelligence concerning its own sector, collected and pre-analysed by the subcontractor and delivered at regular intervals, supplemented by separately commissioned reports on critical topics.

C The organisation stores the information received in its own systems and ensures that it is accessible and reliably stored.

A The organisation's information security team reviews the reports, compares them with its own understanding, and compiles a summary of the situational picture.

A A summary of a few sentences is written up from the situational overview for presentation to the management team. In addition, the reports and sources on which the situational overview is based are stored. A version of the summary is retained that clearly shows the origin of each piece of information.

D The situational picture is presented at the monthly management team meeting and shared at a joint situational picture meeting with organisations in the same sector.

D Based on the insights gained, preparations are made for spikes in threat actor activity, and responses are formulated to new forms of attack or emerging trends.

OPERATIONAL THREAT INTELLIGENCE (CASE STUDY 2):
Increased risk identified in the cyber risk analysis

S In the risk analysis, the organisation identifies the diverse cyber threats it faces and concludes that preparing for these requires proactive action and the acquisition of up-to-date threat intelligence.

S The need to obtain information on ongoing cyberattack campaigns, new malware and the development of threat actors' tools is identified.

S The available means of acquiring information are mapped out, and a decision is made to procure an external SOC service that generates, processes and analyses threat intelligence, as well as up-to-date IOC threat intelligence via networks.

S Determine what information is to be collected, by whom, and how the acquired data will be utilised.

S The organisation audits and compares different service providers and agrees with the supplier on the provision of SOC services. The agreement sets out how the supplier collects data from the organisation's network interface, how to respond to it, and to whom any anomalies are reported. At the same time, it is ensured that information sharing between the organisation and the SOC centre is smooth and works in both directions; for example, threat intelligence obtained from the network is forwarded to the SOC centre for processing, and new information requirements are presented to the SOC provider.

C The organisation joins the national ISAC network, where up-to-date information on cyber threats is shared.

A The organisation ensures that all relevant information received through various channels is analysed. In practice, this involves ensuring that the person attending information-sharing sessions is either able to assess what is relevant and pass this information on within the organisation (or to an external SOC provider), or alternatively, that all information is received and processed at a later stage.

A An outsourced SOC service analyses the threat intelligence it has collected and maintains defences to counter changing or evolving threats. The organisation's own staff, in turn, analyse the information received from ISAC groups, combining it with the SOC analysis. The organisation must remain aware of what is being done and why. Communication and information exchange with the SOC service provider must be actively maintained.

D The organisation receives information from the SOC service and ensures that, at the same time, threat intelligence obtained from other sources is made available for use by the centre (and the rest of the organisation).

D The organisation shares observations produced by the SOC service regarding thwarted attacks or intrusion attempts with other industry players known to use similar applications that have been targeted. The organisation also informs the authorities of any anomalies.

D When sharing information, the classification of the data and the type of information that can be shared externally must be taken into account. Information concerning the organisation's operations or monitoring capabilities is not shared with external parties without being 'cleaned' and transmitted via a secure channel.

TECHNICAL THREAT INTELLIGENCE (CASE STUDY 3):
Improving the organisation's technical information security

S The organisation notes in its risk assessments that the probability of becoming a target of a cyber attack is high and decides to improve its level of technical information security.

S Resources are allocated to improving security, and as part of this, a decision is made to increase the procurement of technical threat intelligence.

S The organisation identifies the most critical assets to be protected and maps out external and internal sources from which relevant threat intelligence relating to these applications can be obtained.

S It is determined what information is to be collected, by whom, and how the acquired data will be utilised.

C The organisation expands its technical threat intelligence gathering by adding new vulnerability databases and feeds to its sources. Data is collected and aggregated on the Splunk platform, to which information from existing MISP networks is also directed.

C In Splunk, the data is harmonised and the application is configured to trigger alerts upon the identification of threats related to the most critical targets.

A Raw data is continuously analysed using AI models specialising in anomaly detection and other similar tools. Alert thresholds are adjusted and customised to generate only relevant notifications that require actual action.

D Alerts are communicated within the organisation as necessary, and management is responsible for sharing information on anomaly situations with parties outside the organisation.

ABOUT DNV CYBER

DNV Cyber is a leading cybersecurity services provider. We empower businesses with complex needs to become safer and more resilient with tailored solutions. Our global team of more than 500 experts brings over 30 years of IT and industrial control system security experience to your business, helping you breathe easier and perform better.

We identify, prioritize, and communicate risk, guide you through regulations, and align your cybersecurity with your business goals. We bring you technology and threat insight, help you to secure cyber investments, and implement cost-effective security control measures. We detect and respond to threats, ensuring continuous improvement and quick recovery.

We ask questions and listen, speaking your industry's language. We collaborate and share insights, setting industry standards and delivering best practice. We safeguard your critical, enabling your business to thrive.

DNV Cyber was formed by merging Nixu, Applied Risk and DNV in 2024.

ABOUT DNV

DNV is an independent assurance and risk management provider, operating in more than 100 countries, with the purpose of safeguarding life, property, and the environment. As a trusted voice for many of the world's most successful organizations, we help seize opportunities and tackle the risks arising from global transformations. We use our broad experience and deep expertise to advance safety and sustainable performance, set industry standards, and inspire and invent solutions.

DNV Cyber Safeguards Your Critical.

CYBERWATCH FINLAND

The company was founded in February 2017.

Cyberwatch Finland became a part of Netum Group Plc 21st of April 2026.

Cyberwatch Finland serves companies and other organizations by strengthening and developing their cybersecurity culture and ability to prevent cyberattacks.

Our goal is to improve strategic cyber awareness and capabilities at all levels of operations, from individuals to the top management of organizations. We will tell you about the current cyber security phenomena and the factors affecting them.
Our team of experts consists of diverse expertise in strategic cybersecurity, complemented by extensive experience in management, comprehensive security and operations in an international business environment.

Our Aim is to Add Cyber Capabilities in the World.


AI