

Understanding Cyber Threat Intelligence

Reading

1h



Status

Incomplete

Introduction

This reading introduces you to the fundamentals of cyber threat intelligence (CTI) and helps you learn about different steps of the CTI lifecycle. You will also learn about different types of CTI in this reading.

Reading

CTI Fundamentals

An organization can protect itself against cyberattacks by using CTI, which provides information about current or potential cyber threats. According to [ECCouncil](#), threat intelligence is the analysis of data using tools and techniques to generate meaningful information about existing or emerging cyber threats targeting the organization that helps mitigate risks. Threat intelligence helps organizations make faster, more informed security decisions and change their behavior from reactive to proactive to combat the attacks.



Information on the motivations, tactics, and goals of cyber adversaries is included in CTI, along with vulnerable systems and specific threats. Also, CTI can be provided by a variety of sources, including government agencies, private security firms, and open-source information.

CTI Lifecycle

The process of transforming raw threat data into final information that can be used for decision making and action is known as the CTI lifecycle. During the course of your study, you will come across different variations of the intelligence cycle. However, the purpose of these cycles remains the same: to direct a Cyber Security team through the process of developing and executing an efficient threat intelligence program.

Intelligence pertaining to risks is difficult to get due to the fact that dangers are always changing, necessitating rapid adaptation and prompt action on the part of enterprises. The intelligence cycle offers a structure that enables teams to successfully respond to the changing nature of new threats while also optimizing the use of their resources. The following six processes make up this cycle, which ultimately results in a feedback loop to stimulate continual improvement, as shown in the diagram below:



Figure 1: Key Steps of the Cyber Threat Intelligence Lifecycle. Source: SOCRadar

Here is a look at these steps one by one:

1. Planning and Requirements

The stage of gathering requirements is an essential part of the lifecycle for threat intelligence since it determines the course of action for a particular threat intelligence operation. The team will reach a consensus on the objectives and procedures for their intelligence program during this stage of the planning process. These decisions will be based on the requirements posed by the various stakeholders. The team could go off on an adventure to find the motivation of the attackers, their attack surface, and what particular steps need to be made for strong cyber defense.

2. Information Collection

After the criteria have been identified, the team moves on to the next step, which is to collect the information that is necessary to achieve those goals. The team will often search out traffic logs, publicly available data sources, relevant forums, social media, and industry or subject matter experts, although this may vary depending on the aims.

3. Processing

Following the collection of the raw data, it will be necessary to transform the data into a format that is appropriate for analysis. The majority of the time, this requires arranging data points into spreadsheets, decrypting files, translating information from foreign sources, and reviewing the data to determine its relevance and dependability.

4. Analysis

Following the completion of the processing of the data set, the group will need to carry out an exhaustive analysis in order to identify responses to the questions that were given during the requirements phase. During the period of analysis, the team will also endeavor to translate the data set into relevant suggestions and action items for the stakeholders.

5. Dissemination

In order to complete the dissemination phase, the threat intelligence team must first transform their analysis into a format that can be easily consumed, and then they must convey the results to the stakeholders. The analysis is provided in a manner that is appropriate for the audience. In the majority of instances, the suggestions have to be provided in a manner that is clear and succinct, free from complex technical jargon, and can take the form of either a one-page report or a brief slide presentation.

Types of CTI

Threat intelligence data is the data that identifies threats and helps businesses to make decisions on strategies to deal with them. It comes from a huge number of different sources and data needs to be broken up into different types so that information gathered from different sources can be better managed.

This subdivision was done to help the intelligence's customers and goals. It helps people use threat intelligence and is split into four different types.

This subdivision helps businesses better organize threat intelligence plans ensuring that they can respond according to the scale and impact of these threats to various parts of the security ecosystem. Therefore, CTI helps with planning, resourcing, budgeting, and prioritizing actionable plans in an organization.

CTI can be divided into three categories: strategic threat intelligence, operational threat intelligence, and tactical threat intelligence; below is each category in more detail:

Strategic Intelligence

The purpose of strategic CTI is to help organizations make informed strategic decisions about how to protect their assets by collecting and analyzing long-term threat landscape information. The study focuses on trends, patterns, and threats that could affect an organization over the long term.

Operational Threat Intelligence

Operational CTI is information that is collected and analyzed to help organizations understand the immediate threat landscape and make informed decisions about how to protect their assets. As part of the process of developing and implementing security policies and procedures, this type of assessment uses specific threats and vulnerabilities that could affect an organization in the short term.

Tactical Threat Intelligence

Tactical CTI is information that is collected and analyzed to help organizations understand the threat landscape in real-time and make informed decisions about how to protect their assets. It is often focused on particular vulnerabilities and threats that are currently being exploited, and it is used to influence the implementation of security measures and the response to ongoing assaults.

The overall significance of these three degrees of CTI lies in the fact that they provide firms with the data they want in order to comprehend the dangers posed by cyber threats and develop strategies to counteract those dangers. Organizations are able to acquire a more full and accurate picture of the dangers they face if they collect and analyze data from a number of sources. This enables them to take the required actions to safeguard their assets and ensure their safety.

The illustration given here depicts how four different types of threat intelligence align with the short-term and long-term goals of an organization, along with specific examples of each type of threat intelligence. This approach helps us get an understanding of our threat landscape which is important when it comes to making business decisions as well as understanding the type of threat we could be facing or may face in the future.

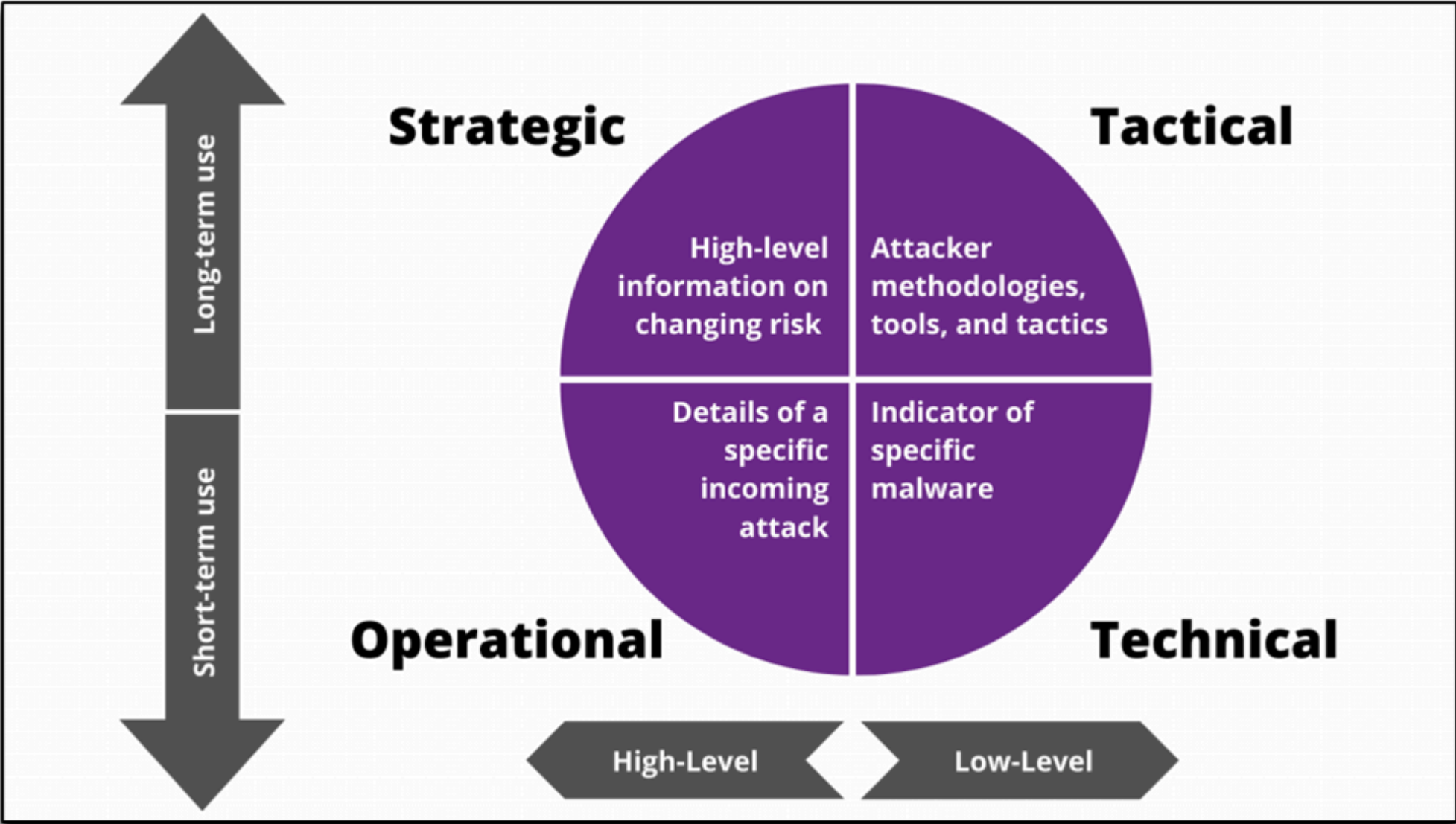


Figure 2: Alignment of Threat Intelligence with Organizational Goals. Source: Balbix



Read what actionable intelligence is and how it helps Blue Team members in day-to-day security operations.

Actionable intelligence is a term that is commonly used to refer to information or **indicators of compromise (IOCs)** that were acquired after doing analysis on intelligence that was supplied to you by the CTI team. According to TechTarget, IOCs are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity in a system or network. Examples of an IOC include unusual network traffic, unusual privileged user account activity, login anomalies, increases in database read volume, suspicious registry or system file changes, etc. Actionable intelligence has two major components that set it apart from raw threat data; it has to be actionable and more contextual. You will learn more about actionable intelligence later in the course.

Open-Source Threat Intelligence (OSINT) vs. Commercial Threat Intelligence

There are a plethora of threat intelligence sources available, but knowing which ones to use is important. If you choose to go for OSINT sources, you will find information which is legitimately gathered from a wide variety of free and publicly available sources, such as discussion boards, vlogs, online communities, websites, books, conferences, public speeches, etc.

On the other hand, commercial threat intelligence sources offer a variety of advantages that are missing in OSINT. For example, commercial threat intelligence providers are responsible for all aspects of collecting, processing, evaluating, and validating active threats. This information is then condensed into a consumable format that can be readily incorporated into a variety of security systems.

Open-source threat information is frequently combined with a number of other commercial feeds and integrated into various security tools. Commercial feeds typically leverage a combination of OSINT and a variety of commercial feeds.



Read the article [OSINT vs Commercial Threat Intelligence](#) to learn more on how commercial threat intelligence is preferred over OSINT.

Key Takeaways

- Threat intelligence is the analysis of data using tools and techniques to generate meaningful and actionable information about potential cyber threats.
- CTI lifecycle allows for the transformation of raw threat data into final information that can be used for decision making and actions.
- CTI can be divided into three categories: strategic threat intelligence, operational threat intelligence, and tactical threat intelligence.
- Categorizing CTI helps with planning, resourcing, budgeting, and prioritizing actionable plans in an organization.
- Actionable intelligence helps us to identify IOCs.
- IOCs are pieces of forensic data that identify potentially malicious activity in a system or network.
- OSINT feeds are generalized whereas commercial threat intelligence feeds are customized enough to meet the specific needs of your business.

Conclusion

In this reading, you learned what CTI is, how it is divided into different categories, and how the CTI lifecycle helps Blue Team members acquire the necessary threat intelligence to take required actions. Next, you will understand what tools and platforms Blue Team members use to process threat data and information in order to create threat intelligence.

Further Readings

- Read the following resource to deepen your understanding of CTI: <https://www.eccouncil.org/cyber-threat-intelligence/>
- Typically, tactical intelligence brings more actionable intelligence. To deep dive into understanding tactical intelligence, the following could be a good source: <https://www.recordedfuture.com/tactical-threat-intelligence>

✓ Mark Completed

←

Previous

Overview - Threat Defense Operations

Next

Threat Intelligence Platforms and Their Usage

→

How well did this activity help you to understand the content?

Let us know how we're doing




W07D4

Thu Aug 8

> Lectures (1)

✓ Work (7)

7 hrs

 Project: Encryption

 Course Reflection

 Overview - Threat Defense Operations

 Understanding Cyber Threat Intelligence

 Threat Intelligence Platforms and Their Usage

 Threat Actors and Their Tactics

 Cyber Kill Chain & Intrusion Analysis

> Other (1)

W07D4 Schedule »