Threat Hunting

Threat Intelligence

1

What Is Cyber Threat Intelligence?

In order to perform threat hunting, it is especially important to have at least a basic understanding of the main cyber threat intelligence concepts.

In this chapter, we are going to cover the following topics:

- **Cyber threat intelligence**
- **The intelligence cycle**
- **Defining your intelligence requirements**
- **The collection process**
- **Processing and exploitation**
- **Bias and analysis**

Cyber threat intelligence

Cyber Threat Intelligence (**CTI**) is a cybersecurity discipline that attempts to be a **proactive** measure of computer and network security, which nourishes itself from the traditional intelligence theory.

CTI focuses on **data collection** and **information analysis** so that we can gain a better understanding of the **threats facing an organization.**

intelligence only has value if it is **relevant**, **accurate**, and, most importantly, if it is **delivered on time**.

Cyber threat intelligence

Cyber Threat Intelligence (**CTI**) is a cybersecurity discipline that attempts to be a **proactive** measure of computer and network security, which nourishes itself from the traditional intelligence theory.

CTI focuses on **data collection** and **information analysis** so that we can gain a better understanding of the **threats facing an organization.**

intelligence only has value if it is **relevant**, **accurate**, and, most importantly, if it is **delivered on time**.

we can classify intelligence according to its form; that is, **strategic**, **tactical**, or **operational** intelligence.

Strategic level

Strategic intelligence informs the top decision makers – usually called the CSuite: **CEO**, **CFO**, **COO**, **CIO**, **CSO**, **CISO** – and any other chief executive to whom the information could be relevant.

Operational level

Operational intelligence is given to those making day-to-day decisions; that is, those who are in charge of defining priorities and allocating resources. To complete these tasks more efficiently, the intelligence team should provide them with information regarding which groups may target the organization and which ones have been the most recently active.

Tactical level

Tactical intelligence should be delivered to those in need of instantaneous information. In this case, the deliverable may include **IP addresses**, **domains** and **URLs**, **hashes**, **registry keys**, **email artifacts**, and more. For example, these could be used to provide context to an alert and evaluate if it is worth involving the **incident response (IR) team.**

Threats

A threat is any circumstance or event that has the potential to **exploit vulnerabilities** and negatively impact operations, assets (including information and information systems), individuals, and other organizations or societies of an entity.

Threats

The main areas of interest for cyber threat intelligence are ***cybercrime***, ***cyberterrorism***, ***hacktivism***, and ***cyberespionage***. All of these can be roughly defined as organized groups that use technology to infiltrate public and private organizations and governments to steal proprietary information or cause damage to their assets.

However, this doesn't mean that other types of threats, such as **criminals** or **insiders**, are outside the scope of interest.

Structured Threat Information Expression

MITRE Corporation has developed the Structured Threat Information Expression (STIX) in order to facilitate the standardization and sharing of threat intelligence.

https://oasis-open.github.io/cti-documentation/stix/intro

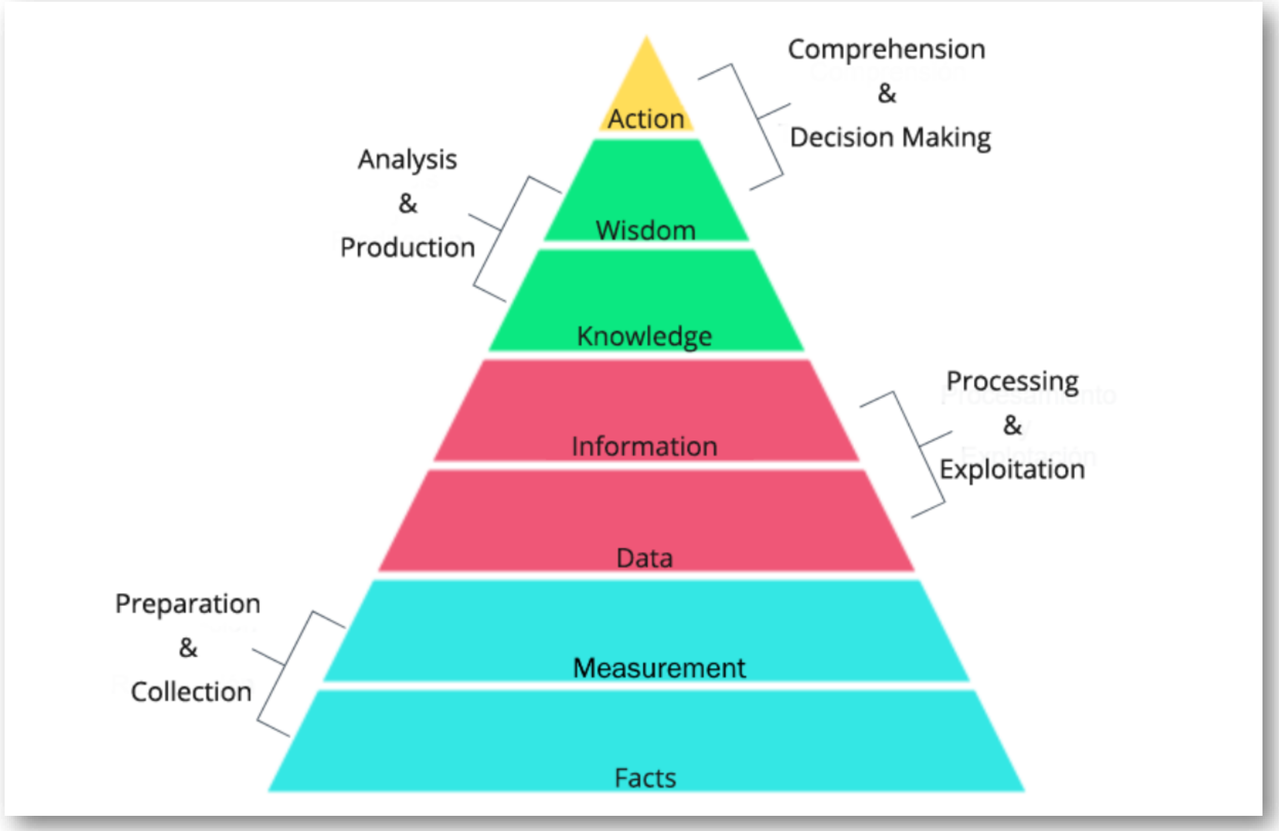
If we follow the STIX definition (https://stixproject.github.io/data-model/), threat actors are "**actual individuals, groups, or organizations believed to be operating with malicious intent**."

The intelligence cycle

it is worth showing the relationship between data, knowledge, and intelligence practice through what is known as a **knowledge pyramid**

- **facts**, through **measurement**, are transformed into **data**
- **Information** can extract from data when it processing
- When analyzed, it can be transformed into **knowledge**
- This knowledge interacts with our own experience and forms the basis of what we call **wisdom**
- It is this ultimate wisdom that we rely on for **decision-making**

The intelligence cycle



An intelligence analyst must process data to transform it into wisdom (intelligence), which in the last instance will lead to an action (decision).

The intelligence cycle

The intelligence process is understood as a six-phase cycle:

- **planning and targeting**
- **preparation and collection**
- **processing and exploitation**
- **analysis and production**
- **dissemination and integration**
- **valuation and feedback**

Planning and targeting

The first step is to identify the **intelligence requirements (IRs)**. Any information that the decision makers need and don't know enough about falls under this category. In this stage of the process, it is important to identify the following:

- The mission of the organization
- The key assets of the organization
- Why the organization might be an interesting target
- what the security concerns of those in charge of making decisions are
- Potential threats that exist and what mitigations can be prioritized (through a process known as **threat modeling**)

Preparation and collection

This stage refers to defining and developing collection methods to obtain information regarding the requirements that were established in the previous phase

Processing and exploitation

Once the planned data has been collected, the next step is to process it to generate information.

Analysis and production

The information that's been gathered so far must be analyzed in order to generate intelligence. There are several techniques that are used for intelligence analysis and to prevent the analyst's bias.

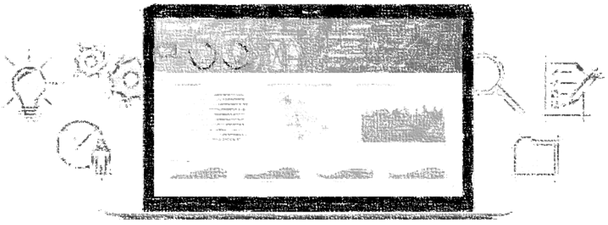
Dissemination and integration

In this stage, the intelligence that's been produced is distributed to the necessary sectors. An analysts have to consider a variety of things as following:

- What the most pressing issues are among the intelligence that's been collected
- Who should receive the report
- How urgent the intelligence is or how much detail the recipient needs
- Should the report include preventive recommendations?

Evaluation and feedback

This is the final stage of the process and probably the most difficult to achieve, mainly due to the usual **lack of feedback from intelligence recipients**. Establishing good mechanisms to get feedback helps intelligence producers evaluate the effectiveness of the intelligence that's been generated before they repeat the process over and over, without making the necessary adjustments that will make the intelligence that's produced more relevant to the recipients. As intelligence producers, we want our intelligence to be relevant – we want our intelligence to help the decision makers to make informed decisions. Without gathering the appropriate feedback, we won't know if we are achieving our goal, and we won't know which steps to take to improve our product.



Let's learn how to define and identify our intelligence requirements

Defining your intelligence requirements

The first stage in the intelligence cycle is to identify the information that the decision-maker needs. When working out your intelligence requirements, ask yourself the following questions:

- **What's the mission of my organization?**
- **What threat actors are interested in my organization's industry?**
- **What threat actors are known for targeting my area of operation?**
- **What threat actors could target my organization in order to reach another company I supply a service for?**
- **Had my organization been targeted previously?**
- **If so, what type of threat actor did it? What were its motivations?**
- **What asset does my organization need to protect?**
- **What type of exploits should my organization be looking out for?**

Defining your intelligence requirements

There are four criteria to keep in mind when validating a PIR:

- **Specificity** of the question
- **Necessity** of the question
- **The feasibility** of the collection
- **The timeliness** of the intelligence that would be generated from it

If the requirement meets all these criteria, we can start the collection process

The collection process

Once the intelligence requirements have been defined, we can proceed with collecting the raw data we need to fulfill them. There are two most significant sources for collection:

- **Internal sources** such as networks, infrastructure, endpoints, servers, and so on.
- **External sources** such as blogs, threat intelligence feeds, threat reports, public databases, forums, and so on.

The most effective way to carry on the collection process is to use a **collection management framework (CMF)**

Using CMF allows you to identify data sources and easily track the type of information you are gathering for each.

The collection process

Here's an example of CMF that we would like to show you:

Source \ Data Type	SHA256	URL	IPs	Who is	First Seen	[...]
Source 1						
Source 2						
Source 3						

The collection process - Indicators of compromise

An indicator of compromise (IOC), as the name suggests, is an artifact that's been observed in a network or in an operating system that, with high confidence, indicates that it has been compromised.

Typical IOCs may include the following:

- **hashes of malicious files**
- **URLs**
- **domains**
- **IPS**
- **Filenames**
- **Registry Keys**
- **files themselves**

The collection process - Using public sources for collection – OSINT

Open Source Intelligence (OSINT) is the process of collecting publicly available data. The most common sources that come to mind when talking about OSINT are **social media**, **blogs**, **news**, and the **dark web**.

https://www.virustotal.com/

https://www.ccssforum.org/malware-certificates.php

https://urlhaus.abuse.ch/

https://osintcurio.us/

Processing and exploitation

- Once the data has been collected, it must be processed and exploited so that it can be converted into intelligence.
- The IOCs must be provided with context, and their relevance and reliability must be assessed.
- One way to approach this is to break data into buckets and take advantage of the available frameworks in order to look for patterns.
- We are going to quickly review three of the most commonly used intelligence frameworks: the **Cyber Kill Chain®**, the **Diamond Model**, and the **MITRE ATT&CK™** Framework.

Processing and exploitation - The Cyber Kill Chain®

The **Cyber Kill Chain®** is a means to identify the steps the **threat actor** should follow in order to achieve their objective. There are seven different steps:

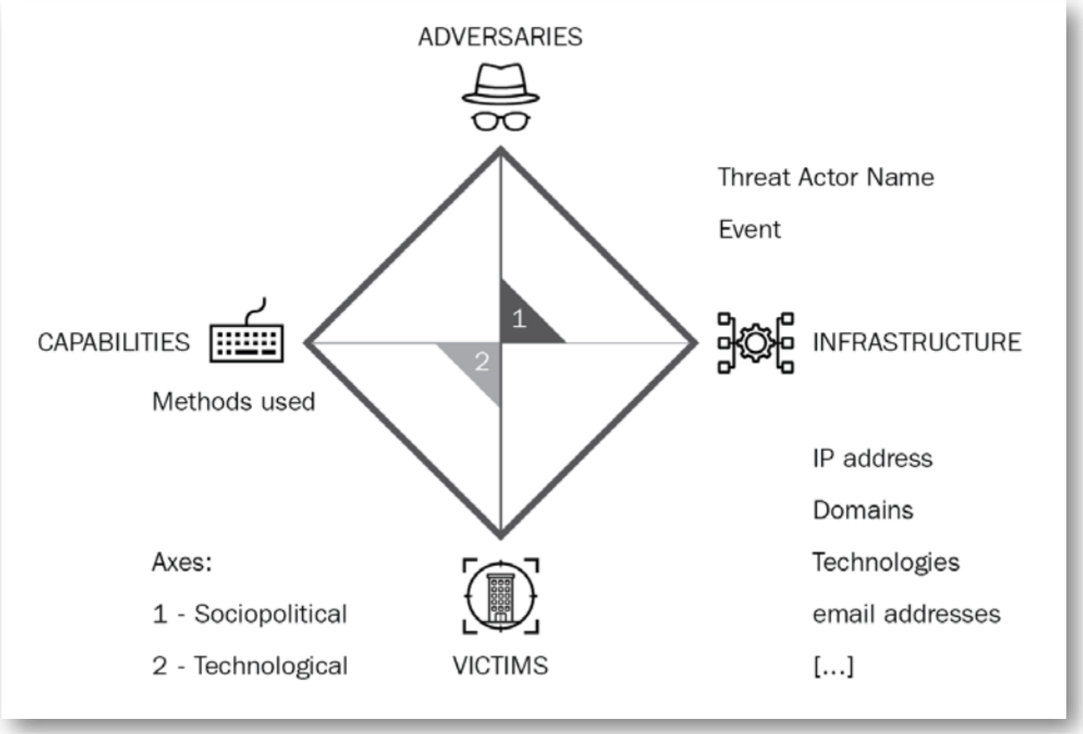
- **Reconnaissance**: Getting to know the victim using non-invasive techniques.
- **Weaponization**: Generating the malicious payload that is going to be delivered.
- **Delivery**: Delivering the weaponized artifact.
- **Exploitation**: Achieving code execution on the victim's system through the exploitation of a vulnerability.
- **Installation**: Installing the final malware piece.
- **Command and Control (C2)**: Establishing a channel to communicate with the malware on the victim's system.
- **Actions on objectives**: With full access and communication, the attacker achieves their goal.

Processing and exploitation - The Cyber Kill Chain®

Processing and exploitation - The Diamond Model

The Diamond Model provides us with a simple way to track breach intrusions since it helps us establish the atomic elements involved in them. It comprises four main features:

- **Adversary**
- **Infrastructure**
- **Capability**
- **Victim**



Processing and exploitation - MITRE ATT&CK™ Framework

- The MITRE ATT&CK™ Framework is a **descriptive model**
- ATT&CK™ Framework is that it provides a common taxonomy for the cybersecurity community to describe the adversary's behavior
- It works as a common language that both **offensive** and **defensive** researchers
- you can create your own set of **tactics**, **techniques** and **procedures (TTPs)**
- **12 tactics** are used to encompass different sets of techniques
- Each tactic represents a tactical goal
- Each of these tactics is composed of a set of techniques and **sub-techniques** that describe specific threat actor behaviors.

Processing and exploitation - MITRE ATT&CK™ Framework

Reference:

Practical Threat Intelligence and Data-Driven Threat Hunting

A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools