**Cyber Threat Intelligence**

Cyber threat intelligence (CTI) refers to the process of collecting, analyzing, and interpreting data and information about potential or actual cyber threats to identify their nature, scope, and potential impact.

According to Gartner, Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications, and action-oriented advice) about existing or emerging menaces or hazards to assets.

**Who Needs CTI?**

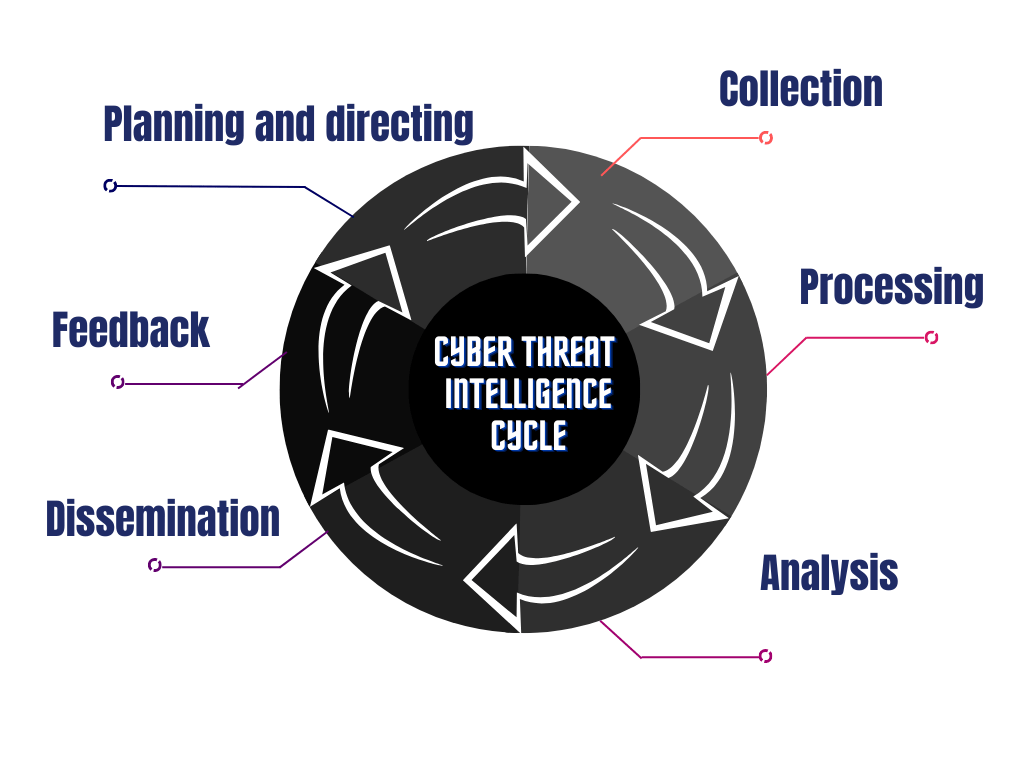
Organizations of all sizes and in all sectors, including the military, government, financial, healthcare, and retail sectors, use CTI. It is a crucial component of any contemporary[cybersecurity](https://www.geeksforgeeks.org/cyber-security-types-and-importance/) program, assisting firms in protecting their important assets and data and helping them stay one step ahead of thieves.

The following particular groups can gain from using cyber threat intelligence techniques: –

* **Government agencies:** Federal, state, and municipal governments must keep ahead of cyber threats because they are managing sensitive data and vital infrastructure. So, they require cyber threat intelligence to identify potential attacks, evaluate the risk, and take the proper action.
* **Businesses:** Cyber-attacks impact businesses of all sizes and in all sectors. Businesses can find weaknesses and defend themselves from potential cyber threats by implementing cyber threat intelligence methods.
* **Nonprofit institutions:** Nonprofit organizations frequently handle sensitive data regarding their funders, volunteers, and beneficiaries. To safeguard this data and the privacy and security of its stakeholders, these businesses must establish cyber threat intelligence practices.
* **Individuals:** People are also vulnerable to cyberattacks like financial fraud and identity theft.

**What is Cyber Threat Intelligence?**

A continual procedure called the cyber threat intelligence cycle aids firms in staying ahead of potential online attacks. The following steps are often included in the cycle:



**Planning and Directing**

This is the starting point of intelligence scope and identifying the main stakeholders’ needs and expectations. e.g.-if suppose a company demands information on System vulnerabilities/Loopholes in their servers then we will plan the whole flow of investigation on the demand of stakeholders.  
Some common investigation questions:

1. Who is attacking whom?
2. The purpose of the attacker
3. The attacking surface is what.
4. What specific steps will be made to defend against upcoming attacks?

**Collection**

Data is collected in this step from various sources, including open-source information, human intelligence, and technical intelligence.It is possible to gather data from:

* Blog, posts and news articles from the surface web and deep web
* Threat database from external sources
* Social media handles
* Online communications with cyber criminals, etc.

**Processing**

Data processing involves removing redundant or irrelevant information from the data gathered in the first stage and looking for patterns or trends.

**Analysis**

Potential threats are identified, and their likelihood and potential impact are measured on the organization’s systems and employees. After that, the Analyzed data is evaluated using the processed data to get a clear picture of potential threats.

**Dissemination**

The findings of the analysis report are communicated and distributed to the respective parties of the organization/stakeholders, including top management, IT workers, and other personnel.

**Feedback**

Stakeholder feedback is gathered to assess the intelligence program’s success and pinpoint areas for development.

Lastly, based on the intelligence gathered and assessed, the organization takes action and makes safety policies and procedures. For example, an organization may put security measures in place (e.g.-Data centers, Administration controls, employee login) to reduce possible threats or respond to an ongoing attack.