

CYBER THREAT INTELLIGENCE · BROCHURE

The service that keeps you one step ahead of hackers.

**Spot threats before
they become problems.**

Cyber Threat Intelligence



What is Cyber Threat Intelligence?

Cyber Threat Intelligence is the knowledge of a **threat or risk to your assets.**

The service starts from the assumption that a **threat is already present**, even before there's proof. This proactive approach lets you intercept attacks at the source, rather than defending only when they're already in motion.

The goal is to turn the raw data available on the web into **actionable** information that security teams can base operational decisions on.

The benefits are many

+34%

Greater team efficiency

Time saved on drafting reports and on priority management.

10×

Faster threat localisation

Faster at identifying a threat than a traditional approach.



Timely mitigation

Detected threats are suppressed much more quickly, reducing their impact.

The Cyber Threat Intelligence cycle

CTI is the finished product of a **six-part cycle** that includes data collection, processing and analysis.

The process is a cycle because new questions and gaps are identified as the intelligence develops, leading to new collection requirements. An effective intelligence programme is iterative — it becomes more **refined and efficient** over time.



1. Planning & Direction

The first step is asking the **right question** to drive the creation of actionable information about potential threats.

2. Collection

Gather **raw data** that meets the requirements set in the first phase.

3. Processing

Collected data is organised with metadata, filtering out redundant information, false positives and false negatives.

4. Analysis

Look for potential **security issues** and notify the relevant teams in the way defined during the planning phase.

5. Dissemination

For threat *intelligence* to be usable, it has to reach the **right people**.

6. Feedback

The original requester reviews the finished intelligence product and determines whether their questions have been answered.

The secret? Think like a hacker

The **continuous analysis** of data found on the *Deep Web* and the *Dark Web* provides crucial clues about what hackers' **new attack techniques** might be.

We also monitor the **fraudulent sources** traceable below the surface of the mainstream web.

Starting from the assumption that you might be under attack **unknowingly**, the research is bias-free. Continuous verifications and checks make sure the intelligence collected doesn't already apply to your company.

We continuously monitor

20B+

stolen credentials

250+

threat-intelligence sources

100M+

domain names

50+

official legal sources

Surface Web

Everything indexed by public search engines.

Deep Web

Non-indexed content: corporate portals, private databases, restricted areas.

Dark Web

Networks accessible only with dedicated software, where stolen data often circulates.

What the service includes in practice

Thanks to **OSINT** (*Open Source Intelligence*) techniques, we can **scour the entire web** in search of information and data that may have been stolen.

It's not uncommon for corporate data to be exfiltrated and used to plan an attack, for example a *ransomware*. This data is often shared in the areas of the web known as the **Deep Web** and **Dark Web**.

Thanks to our **Cyber Threat Hunters** we can search for and recover that information. Knowing what's been stolen makes it far easier to organise a **targeted defence**.

What might already be in the wrong hands

- **Stolen credentials**

- **Exposed documents**

- **Source code leaks**

- Systems that have suffered a **Data Breach**

- **Phishing** sites tied to the company name

- Fake accounts on **Social Networks**

- Unsolicited **vulnerability** reports

- **Brand** violations

- Squatted **domain** names

Since **2011** we've been working in Cloud technology and cybersecurity — rely on experienced professionals.



**Choose
security for
your business**

Discover the service on our website



For more information, our contact details are:

*Via Statuto 3,
42121 Reggio Emilia (RE), Italy
www.cyberfero.com*

*Phone: +39 0522 1685330
E-mail: info@cyberfero.com
PEC: cyberfero@pec.it
VAT ID: 03058120357*