GATEWATCHER

CTI_ FEED

Data sheet

Improving detection through cyber threat intelligence

Your company faces a number of challenges:

A long detection time for threats, particularly advanced persistent threats (APT).

A lack of in-depth, contextualised knowledge of certain threats and/or groups of actors.

A difficult evaluation and prioritisation of the criticality of alerts reported by analysts, slowing down their decision-making.

A complex cybersecurity protection that need to be adapted to a highly sophisticated and evolving threat environment.

47%

of companies are only using threat intelligence solutions.

207

number average of days for a company to detect a security breach in its network.

53%

of successful intrusions are not detected by the cyber detection tools already in place.

12+ million

of IoCs referenced by Gatewatcher CTI with 5000 new markers identified per day.

CTI: Key information to *optimise* your cyber investigations

Analysis

Automated sourcing of cyber intelligence from over 3,000 different sources.

Rapidity

Consolidated information on an open platform.

Contextualisation

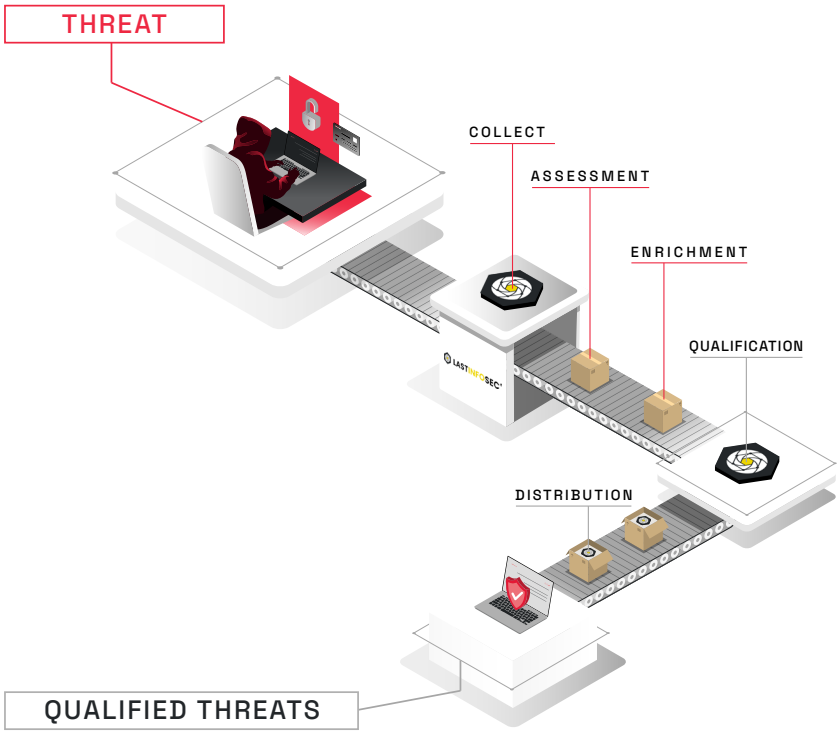
Information that is available, relevant and tailored to your context, thanks to the simplicity of importing it into your existing solutions.

Subscription-based information feed:

The aim ?

Strengthen your existing solutions through direct use in a complete cyber ecosystem.

- Threat blocking (IP and Domain blacklist)
- Contextualisation and enrichment of IoCs
- Automatic creation of rules (Yara rules)



User benefits

Increasing your knowledge and *understanding* of the evolution of threats

Collect the latest compromise indicators, enriched and contextualised to your activity.
Reduce the time you spend analysing a threat when it is detected, thanks to the continuous inventory and evaluation of data sources accessible via multiple channels: social networks, specialist sites, the darknet and the deep web.

Reducing cyber risks

Get information on the latest threats and techniques used, on average 24 hours before the competition, thanks to its automated collection, analysis and correlation engines. Our CTI has a library of several million indicators of compromise (IoCs), and over 5,500 new markers validated and enhanced every day.

Time-saving for your SOC analysts

Beyond simple deployment and integration in your ecosystem, make decision-making easier for your operational security teams. Dramatically reduce their analysis and response time in the event of an incident, without having to modify their internal processes. The time saved means you can increase the quality of alert coverage.

Strengthening existing threat detection solutions

Get only the significant alerts, with all the information you need to understand them, thanks to our enriched and contextualised data.
False positives from your solutions or other Threat Intelligence sources are also reduced by correlation with our CTI flow.

Features

Structuring cyber information_

Give your SOC experts greater speed in the implementation and day-to-day use of standards such as OpenCTI.

Automatic qualification of indicators for rapid contextualisation and remediation_

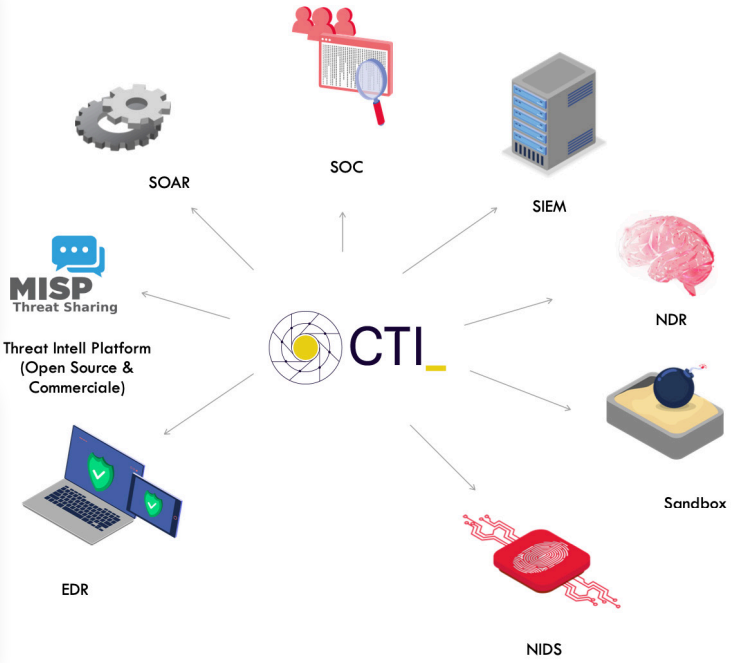
By submitting indicators from your detection solutions (IDS, EDR, SIEM, SOAR, SandBox, NGFW), contextualise precisely threats so that you can remedy them quickly.

Exhaustiveness and correlation of threats covered_

Ensure relevant monitoring of threat trends (APT) by collecting raw information across a broad spectrum.

Automatic creation of signatures_

Protect yourself as early as possible against the latest attack techniques (CVE) thanks to the industrialisation of detection rules.



ABOUT US_

Leader in cyber threat detection, Gatewatcher has been protecting the critical networks of major companies and public institutions around the world since 2015. Our Network Detection and Response (NDR) and Cyber Threat Intelligence (CTI) solutions detect intrusions and respond quickly to all attack techniques. By combining AI with dynamic analysis techniques, Gatewatcher provides a 360°, real-time view of cyber threats across the entire network, in the cloud and on premise.

Contact us

contact@gatewatcher.com
gatewatcher.com