GATEWATCHER

REAL-TIME DETECTION OF ADVANCED THREATS

Based on a next-generation technology, Trackwatch® Full Edition detection system, published by Gatewatcher, efficiently protects organisations against intrusions and breaches.

SECURITY VISA

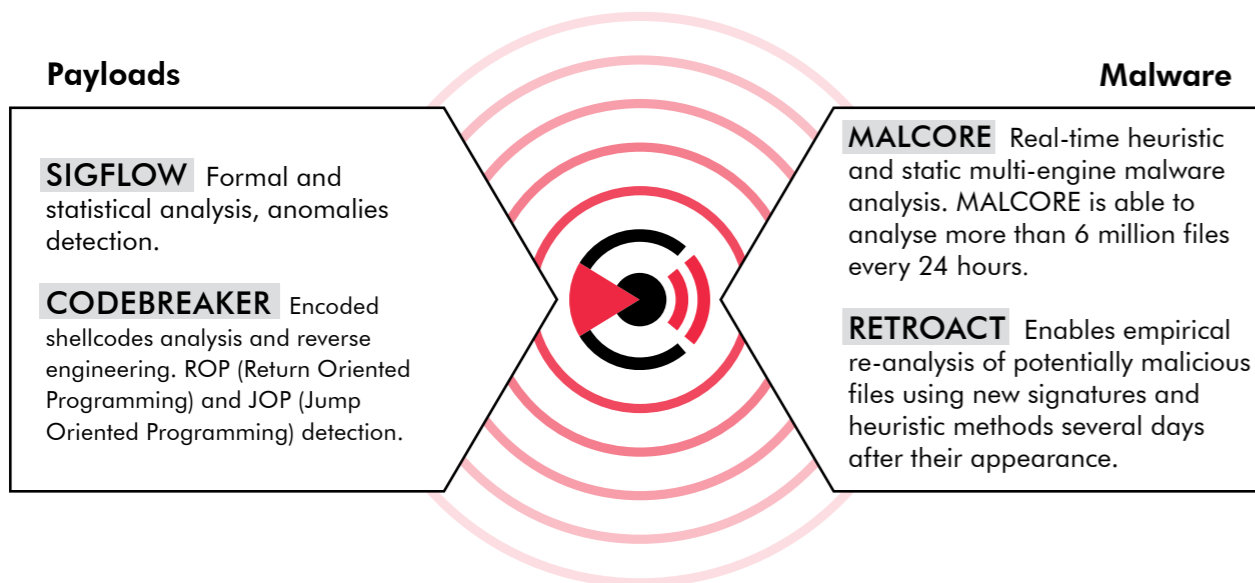AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI ·

Trackwatch® Full Edition is the first advanced threats detection system qualified by the French National Cybersecurity Agency (ANSSI).
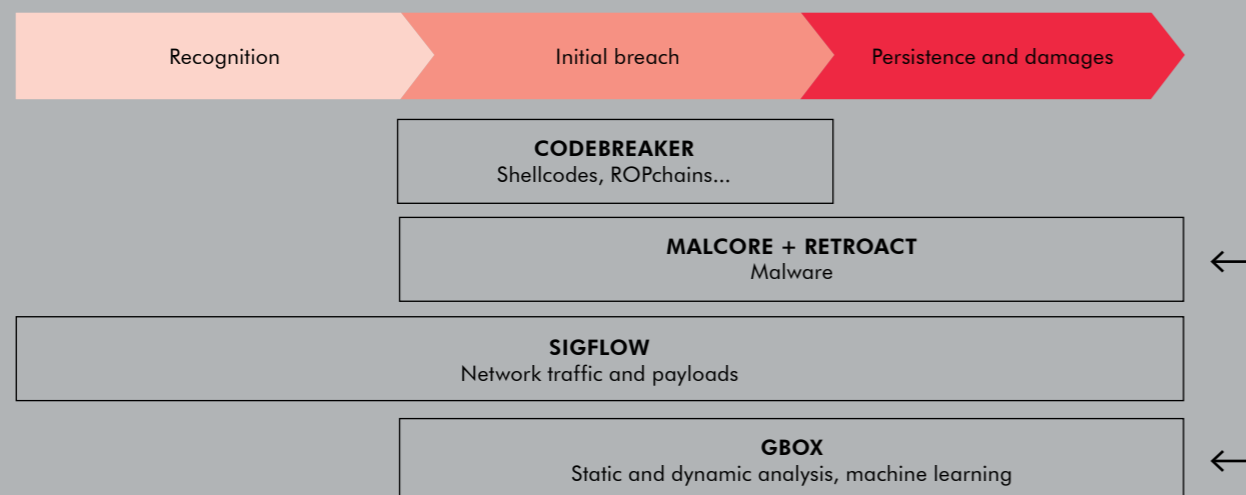
The solution detects abnormal behaviour and weak signals within network flows. Trackwatch® is composed of one or several detection probes (GCAP) and a management appliance (GCENTER).
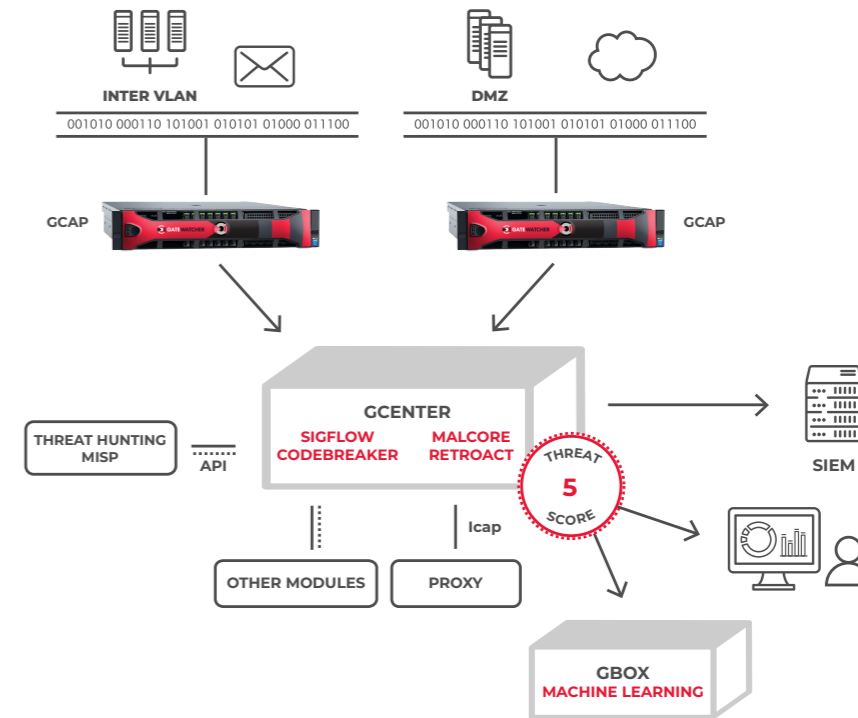
TRACKWATCH® DETECTION ENGINES

▸ Unrivalled breach detection thanks to its **dual approach to the threat** in the exploration phase.

▸ **4 next-generation engines**.

Payloads

SIGFLOW Formal and statistical analysis, anomalies detection.

CODEBREAKER Encoded shellcodes analysis and reverse engineering. ROP (Return Oriented Programming) and JOP (Jump Oriented Programming) detection.

Malware

MALCORE Real-time heuristic and static multi-engine malware analysis. MALCORE is able to analyse more than 6 million files every 24 hours.

RETROACT Enables empirical re-analysis of potentially malicious files using new signatures and heuristic methods several days after their appearance.

TIMELINE OF AN APT DETECTED BY TRACKWATCH®

Recognition	Initial breach	Persistence and damages

CODEBREAKER
Shellcodes, ROPchains...

MALCORE + RETROACT
Malware

SIGFLOW
Network traffic and payloads

GBOX
Static and dynamic analysis, machine learning

TRACKWATCH® IS BASED ON UNIQUE TECHNOLOGIES IN WEAK SIGNALS ANALYSIS AND MACHINE LEARNING

INTER VLAN
001010 000110 101001 010101 01000 011100

DMZ
001010 000110 101001 010101 01000 011100

GCAP

GCAP

THREAT HUNTING MISP

API

GCENTER
SIGFLOW **MALCORE**
CODEBREAKER **RETROACT**

THREAT **5** SCORE

SIEM

OTHER MODULES

PROXY

Icap

GBOX
MACHINE LEARNING

DETECT WITH TRACKWATCH®

▸ « Network Behaviour » approach

▸ Daily updates of Threat Intelligence

▸ Decrease in false positives and recurring alerts

▸ Management of alert severity / criticity

▸ Easy to install and configure

▸ Connects with TAP or port mirroring

ANALYSE WITH GBOX

▸ Advanced analysis by machine learning

▸ In-depth analysis of threats and malware: how they work, where they come from.

▸ Can be used on its own or with the GCENTER

▸ Static analysis and multi anti-virus

▸ Dynamic analysis and anti-bypass techniques.

Trackwatch® CIE

Detection features for critical environments.

① SIGFLOW
② MALCORE (1 engine)
③ RETROACT

GBOX

Threats and malware analysis.

① 32 ENGINES
② SANDBOX
③ MACHINE LEARNING

Trackwatch® Full Edition

Optimal detection features for critical environments.

① SIGFLOW
② CODEBREAKER
③ MALCORE (16 engines)
④ RETROACT

Gatewatcher Foundation

Hardened and flexible OS.

① Random memory encryption (GRSEC)
② Securised boot
③ Dockerisation

Cyberattacks are getting more and more complex and targeted, causing important damages to various types of private and public organisations. They use discreet intrusions into the targeted information system.

Trackwatch® has been designed to protect various business sectors, such as transportation, telecommunications, hospitals, energy and banks. It allows strategic organisations to adress their cybersecurity needs by providing a cutting edge solution for detecting and analysing the most crafted threats.

The breach detection system Trackwatch® Full Edition published by Gatewatcher is qualified by the French National Cybersecurity Agency.
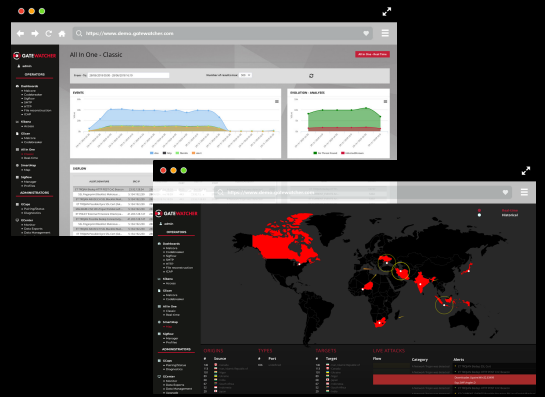
GATEWATCHER

42, rue Washington
75008 Paris, FRANCE

www.gatewatcher.com
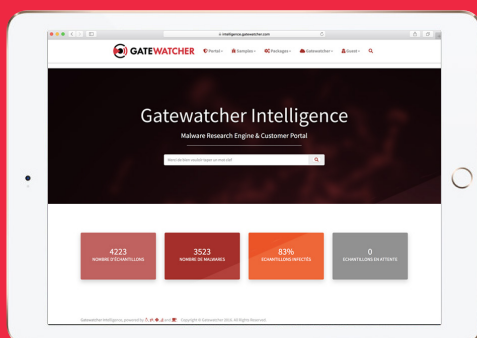
Discover and try our sample analysis platform:
intelligence.gatewatcher.com