GATEWATCHER

Product Overview

REFLEX_

Boost your cyber reactivity_

Your *business value*_

Following multi-vector detection and prioritised processing of alerts within our NDR interface, response is the **essential step** in remedying **all types of cyber-attack**.

Consolidate your cyber resilience strategy and :

Target
your response to prioritised threats.

Tailor
your response to your specific context.

Complete
your response with a defensive, reactive, forensic or preventive component.

Reflex is a *platform* :

> OPERATIONAL
It is a truly intuitive tool that guarantees an agile response tailored to your environment.

> FLEXIBLE
It can be adapted to all types of organisation, whether in connected or fully disconnected mode, and is interoperable with a wide range of solutions.

> INTELLIGENT
It makes it easier to prioritise your remedial actions according to the players involved (ReBaC).

> COMPREHENSIVE
It orchestrates your response across all your assets in a coherent way.

> AUTOMATED
It simplifies the remediation work undertaken by your cyber experts by means of functional, customisable playbooks.

Key *benefits*_

Strenghten your defence arsenal

Improve the efficiency and coordination of your response thanks to the multiple standardised integrations offered within REFLEX.

Benefit from high visibility and consistent communication between all your tools.

Optimise your SOC's activities

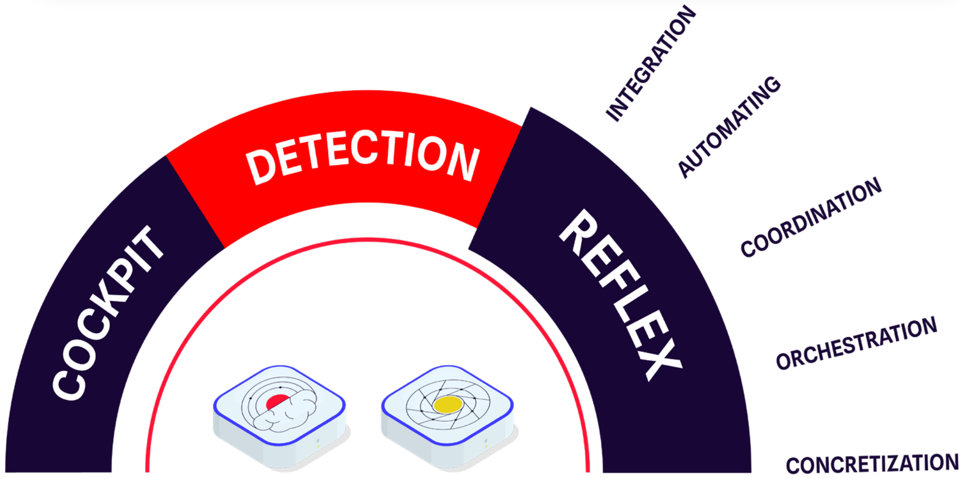
Following an accelerated and targeted analysis by your cyber experts on our NDR interface (COCKPIT), simplify their remediation through automated actions.

The analyst remains at the heart of the remediation and prioritises his or her efforts according to the level of risk of the threats identified.

Develop a response tailored to your specific environment

With 100% automated remediation, you benefit from a consistent end-to-end response tailored to your context, security policies and SLAs.

You can easily orchestrate your response across all your assets (endpoint, firewall, Active Directory, etc.) or on a specific asset, by blocking, disconnecting or deactivating its account.



Use *case*_

- ✓ Asset insulation
- ✓ Sessions blocking and IP addresses
- ✓ Deactivating user accounts
- ✓ Specific accesses blocking - blacklist
- ✓ Stopping communication sessions
- ✓ Disconnection from public networks (Internet)
- ✓ Enrichment of NDR incidents
- ✓ Closing ports
- ✓ User notifications
- ✓ Blocking malicious flows on the network

Features_

Flexible operation

Whichever way you choose to deploy our NDR and CTI solution, you'll benefit from continuous detection and response across your entire spectrum, operating in connected mode (SaaS) or completely disconnected (on prem), particularly for your sensitive infrastructures.

Automated and personalised playbooks

Initiate remediation of your assets automatically or manually via functional playbooks. Customisable and/or predefined by Gatewatcher's cyber experts, they enable you to easily orchestrate your tasks and enrich the context of a security incident in order to refine your response.

A global response

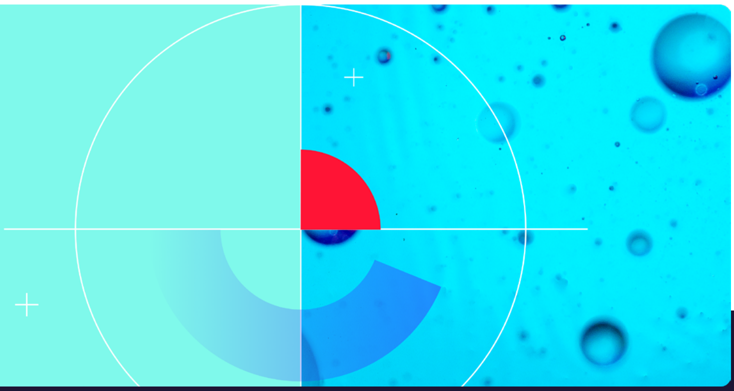
All the information gathered by our NDR and CTI solutions is available on a single SaaS platform. Improve
your analysis and handling of security incidents, and strengthen your response in a 100% automatic and integrated way thanks to REFLEX.

Enhanced integration

Enhance your interoperability with your entire ecosystem thanks to native integration of SaaS solutions from the various manufacturers and publishers on the market - NGFW, EDR, XDR including Office 365, Fortinet, Palo Alto,

5 min to discover
REFLEX_

Demander une démo →



About us_

> Leader in advanced threat detection
> Innovative NDR technology with cutting-edge AI
> 360° detection enhanced by our CTI
> A large network of international partners, CISOs and analysts who place their trust in us - MEA, APAC, Europe
> Recognised for our expertise by ANSSI, French Tec

Nous contacter

contact@gatewatcher.com
gatewatcher.com