GATEWATCHER

AIONIQ_

Product Overview

Detecting advanced persistent threats at early stages
NDR, cornerstone of your *cybersecurity strategy*

Your company faces a number of challenges:

A long time to detect threats, and particularly advanced persistent threats (APT).

A difficult evaluation and prioritisation of the criticality of alerts raised by analysts.

A recurring overload of cyber experts teams in the face of the number of false positives.

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

1,8
average number of successful attacks per year affecting organisations.

207
days on average 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.

AIONIQ: a *unique* NDR solution

Visibility

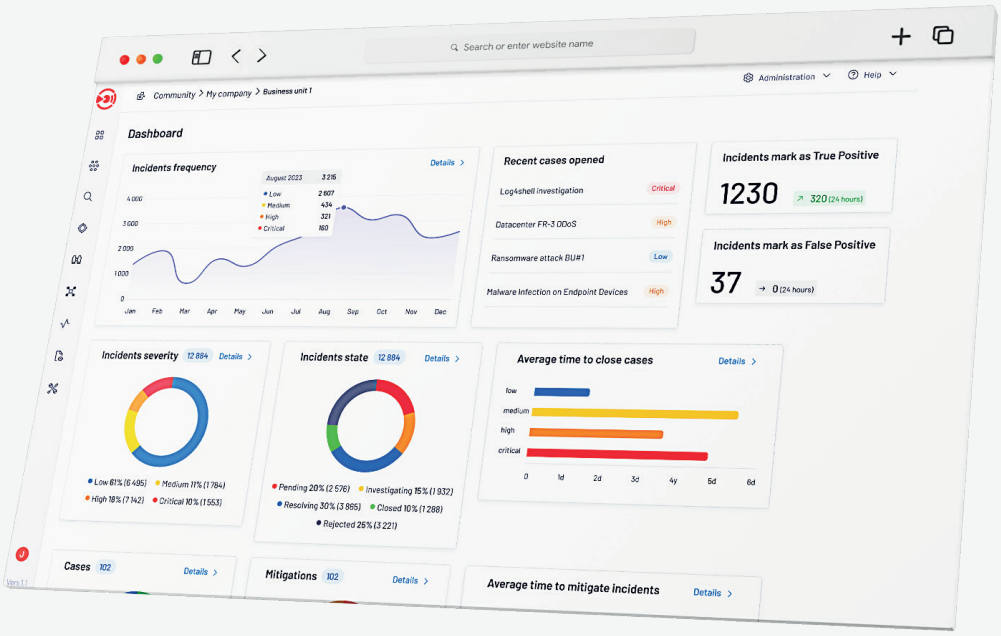
Immediate 360° visibility of the assets and users present on the network, to facilitate investigations and speed up the search of 0-Day exploits.

Rapidity

Multi-vector detection for the earliest possible remediation of intrusion attempts, thanks to intelligent analysis of the first weak signals.

Control

A solution that integrates seamlessly into your existing ecosystem, maximising the efficiency of your SOC teams without impact on your business.



*easy as*_

N
D
R

User benefits

Threat detection including encrypted flows

Gain visibility of known, unknown and hidden threats based on all available metadata.

Automatic *control and knowledge* of your network

Discover and map all your assets and user behaviours passively and using different models.

Operating *flexibility*

Deploy an NDR without constraints, available in on-premise mode or within your cloud instances, in line with your current security policies.

Consolidation and aggregation of threats

Simplify investigations and remediations based on the MITRE ATT&CK framework to optimise the efficiency of your SOC.

Integration with your existing ecosystem

Get a flexible, open solution with native or API integrations, interoperable with most tools on the market.

Global threat *remediation*

Benefit from response capabilities for endpoints, users and your perimeter protection.

Features

Plug-and-detect protection_

Benefit from effective, customised protection that is immediately operational, without disrupting your production environment, thanks to AIONIQ's easily configurable multi-vector detection.

Prioritising threats_

Based on a risk score that changes according to your environnement, quickly sort aggregated alerts and speed up decision-making by your SOC experts.

Research and anticipation of vulnerability exploitations_

Make it easier for your SOC experts to proactively search for intrusions and deal with security incidents. With AIONIQ, they have access to all the data and metadata resulting from the analysis of network communications.

Flexible interconnection with the ecosystem_

Through specific developments based on AIONIQ APIs, or through standardised connectors (EDR, XDR, SIEM, SOAR, NGFW), you can be sure of being interconnected with the entire ecosystem thanks to AIONIQ.

Software platform resilient to cyber attacks_

Increase your resistance to corruption attempts and reduce your attack surface with AIONIQ's hardened OS, developed using a "Secure by design" approach.

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