AIONIQ®

Behavorial & mapping analysis for Augmented Detection

GATEWATCHER

Detecting Advanced Cyber Threats : The New Challenge for Organizations

The financial consequences of a cyber attack can durably weaken your organization.

The growth in the volume of threats complicates the alert criticity assessment handled by your security analysts.

The persistence of an undetected targeted attack within your information system can increase the prejudice caused.

The stealth and complexity of the latest cyber attacks increase the risk of compromise for your IT infrastructure.

3,86M$

Is the average global cost of a data security breach in 2020. [1]

255%

growth in the number of ransomware attacks in France between 2019 and 2020. [2]

207 days

is the average time it takes for a company to detect a security breach. [3]

53%

of successful intrusions are not detected by the cyber detection tools already in place . [4]

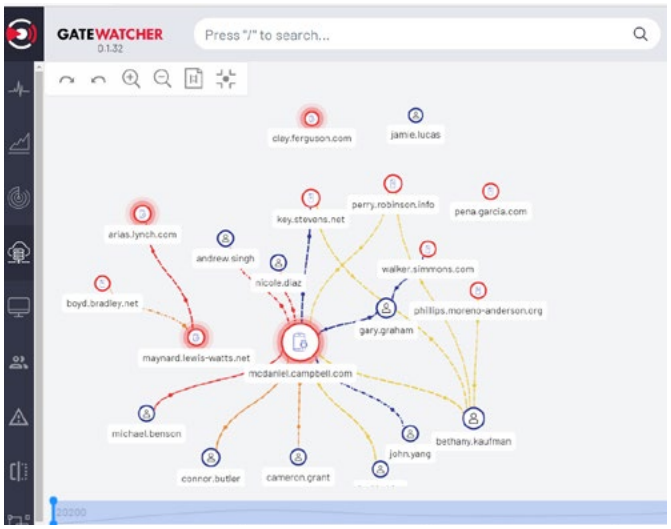
Aioniq®: Mapping and behavioral analysis of cyber threats for enhanced detection and new visibility into targeted attacks.

- **Threat detection, even with encrypted flows.** Aioniq® is an NDR platform capable of identifying, thanks to machine learning processing, all threats within your infrastructure, even if your network flows are encrypted.
- **Mapping of all the assets of the information system.** Aioniq® is the only NDR platform able to map all IT assets in a totally passive and agentless way in order to provide unseen level of detection of advanced attacks on east-west flows.
- **Better visibility into hidden threats.** Aioniq® is able to provide a metadata typology with a level of detail that is unique on the market, in order to optimize the time needed for your forensics analysis.
- **Risk modeling by asset and user.** Aioniq® is the only NDR platform capable of modeling the level of compromise associating event, asset and user, with a Mitre Att&ck view aggregated by risk of all alerts.

Aioniq® is a new detection and response platform (NDR) that enables to identify with certainty malicious actions and suspicious behaviors based on a mapping of all assets present on the information system.

Combining this capability with unprecedented performance analysis of malicious behavior, even in the case of encrypted network encrypted network flows, provides a 360-degree modelling of cyber risk associated with each and every connection between assets and users, for an unparalleled level of detection and visibility.

Granular and scalable, Aioniq® adapts continuously to provide a powerful and personalized response to known and unknown cyber threats as ransomwares, APTs, zero-day vulnerability exploits...



Sources : [1] Ponemon Institute, [2] ANSSI, [3] IBM, [4] FireEye Mandiant

User benefits

A SOFTWARE PLATFORM
RESILIENT TO CYBER ATTACKS

Developed with a "Security by design" approach, Aioniq® is powered by a hardened OS offering a strong resistance to corruption attempts and a minimized attack surface.

IMMEDIATE AND ACTIONNABLE
PROTECTION

Aioniq® does not involve additional equipment or hidden costs. The platform detects threats from the very beginning of the audit phase, without any impact on your production environment.

STRONG INTEROPERABILITY
WITH YOUR EXISTING ASSETS

Aioniq® is an open platform offering a strong reactivity against attacks thanks to its connection with most response and remediation tools on the market as EDR, SIEM & SOAR.

AN OFFER THAT COMBINES
PERFORMANCE AND SCALABILITY

Aioniq® adapts to the threats and specifics of your organization with a scalable system of detection engines and the ability to deploy on premise or in the cloud.

GRANULAR AND FLEXIBLE
PROTECTION

Aioniq® is available in various packages to perfectly match your protection infrastructure and technology choices in order to provide you with truly tailored protection.

OPTIMIZED EFFICIENCY FOR YOUR
SECURITY OPERATION CENTER

Aioniq® eases the investigation of analysts and their handling of alerts criticity by offering multiple metadata colection and detection mapping with chronological visualization compliant with MITRE ATT&CK framework.

Use cases

Detection: A rational use of machine learning.
Compared to a detection model that blindly uses AI, Aioniq® is characterized by a multifactorial approach composed of static, dynamic and algorithmic analysis in accordance with the typology of the threat in order to detect the TTPs specific to each cyber attack.

- Detection of Cobalt Strike beaconing in the context of a DGA attack
- Detection of network anomalies even with encrypted flows
- Detection of emerging obfuscation algorithms used in east-west lateral movement attacks

Hunting: React to the very first signs of a targeted attack.
Aioniq® is the only solution on the industry that can cover the entire Kill Chain of an advanced cyber attack and identify the exploit techniques used throughout the attack, leaving hackers with no place to hide.

- In-depth investigation of metadata types, sessions, protocols and user actions
- UEBA management of asset-user interactions allowing to concentrate only on the major cyber risks
- Post-mortem analysis of all metadata with next-generation indicators of compromise (IoC)

Incident response: A seamless connection to your tools for immediate remediation in the event of an attack.
Aioniq® is an agnostic and open solution allowing a quick and easy integration with most existing security stacks through a large APIs catalog for a zero-latency response in case of a cyber attack.

- Rapid ability to generate custom signature files to fit the customer's context
- SOAR playbook automation of incident response
- Extensive choice of APIs to EDRs for prompt and automated response

Forensics: Unique attack visibility for enhanced cyber resiliency. Aioniq®'s asset mapping capabilities and its ability to link them to each user to identify the level of risk provides unparalleled post mortem visibility into the modus operandi of each attack.

- Collection of multiple metadata allowing the precise contextualization of each attack
- Rapid enrichment thanks to interconnections with the various Threat Intelligence platforms on the market
- Interactive graphical investigation capability to determine the timing and propagation of each attack

About us

Gatewatcher is a leading European software vendor specialized in the detection of the most advanced cyberthreats and intrusions. Its unique model combines several technologies with A.I. to provide you an optimal protection.

Contact us

contact@gatewatcher.com
www.gatewatcher.com