LASTINFOSEC ®

Enriched streams analysis for Smarter 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 undetected targeted attack within your information system can raise the prejudice caused.

The sophistication and stealth of the latest cyberattacks increase the risk of compromise of your information system.

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]

Lastinfosec® : A Threat Intelligence feed that works with any cybersecurity solution and provides immediate improvements to your protection

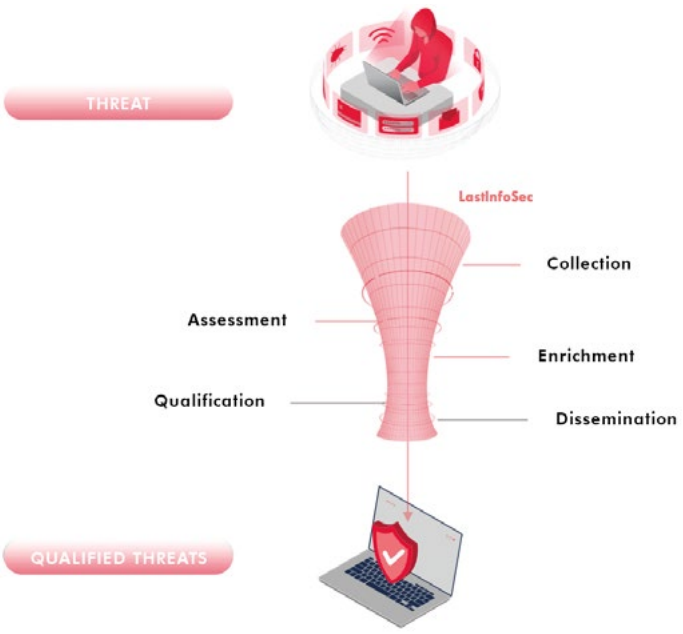
LastInfoSec® is a comprehensive Threat Intelligence platform that makes it easy to detect internal and external threats that are likely to target your information system. With a library of 6 million IoCs, over 5000 new qualified markers per day, and over 3000 different data sources, the LastInfoSec® infrastructure provides rich, contextualized threat intelligence to your business to reduce the time it spends analyzing a threat when it is detected.

LastInfoSec® makes it easier for your operational security teams to make decisions and dramatically reduces their analysis and incident response times without changing their internal processes.

LastInfoSec®'s automated collection, analysis, and correlation engines make threat information available an average of 24 hours before competition.

LastInfoSec® integration is quick and easy with standardized exports to the latest CTI standards (Stix v2, Stix v2.1, JSON, etc.) and available connectors to the leading analytics tools on the market (Splunk, OpenCTI, etc.)

LastInfoSec®'s platform continuously inventories and evaluates data sources accessible on multiple channels: social networks, specialized sites, darknet and deep web.



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

User benefits

Threat coverage : Better knowledge of the threat landscape and increased threat coverage is provided by LastInfoSec feeds.

More reliable, faster, and better documented decision making on what to do about security events, what actions to take urgently, and how to adjust technical and human resources for cyber defense.

Expert efficiency : The analysis time of cyber defense experts, and the detection and reaction times, are reduced. This gain in efficiency enhances the coverage of events taken into account and analyzed. The satisfaction of cyber defense teams is improved.

Scalable capabilities : More than 5,000 new markers are disseminated per day. In the event of a large-scale attack, LastInfoSec's platform is not limited in its collection and processing capabilities and will not be saturated due to its deep technology integration.

Reduced noise and false positives : The data provided generates only meaningful alerts and provides all the information needed to understand them. Reduction of false positives from other Threat Intel sources or your solutions is facilitated by correlation with LastInfoSec data.

Time savings : By distributing markers 24 hours ahead of the market average, the LastInfoSec feed allows for earlier detection of incidents, faster analysis of events, and faster decision making by SOC teams.

Optimize the performance of existing solutions : LastInfoSec information can be connected to your existing security technologies. It increases the effectiveness of EDR, IPS, IDS, NGFW, NDR, BDS, Sandbox, SIEM and SOAR.

Instant improvement : LastInfoSec feeds can be integrated into your current setup with just a few clicks, providing an immediate improvement in your cyber defense posture.

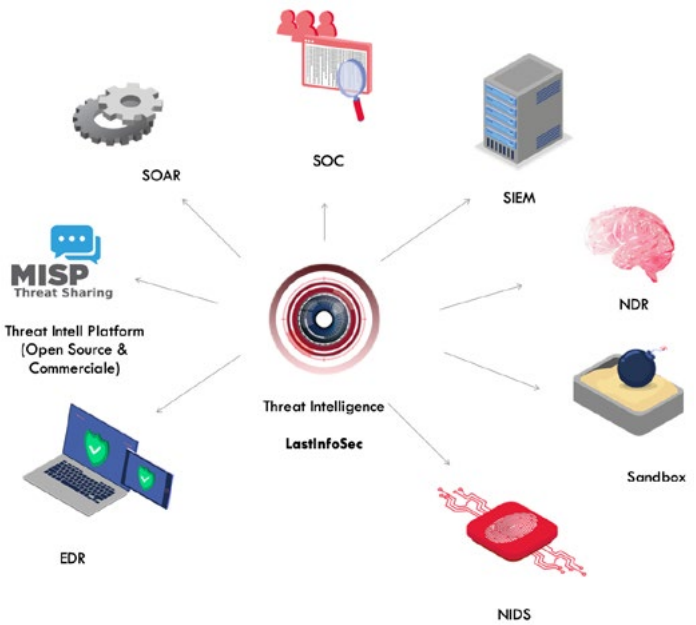
Use cases

Information provided by LastInfoSec can be used globally across an entire organization, or on a perimeter basis. Service offerings include deployments on a portion of detection technologies, such as IDS or EDR, tools within the SOC or CERT, or across the organization via Threat Intel platforms. LastInfoSec's workflow allows you to simply increase the effectiveness of your security solutions by improving threat landscape awareness and reducing noise. You can also automate your hunting to reduce incident detection time.

- Simple integration without changing your processes.
- Fully qualified and validated data flow to reduce false positives.
- Enrichment of your alerts for a better reactivity of your teams.
- Export format usable by cybersecurity solutions without human interaction.
- **Information** contextualization to ease the work of SOC teams.

Deployment

- Standard format and compatible with existing solutions.
- Deployment in a few clicks.
- Stream integration with Threat Intel's third-party platforms, existing network security solutions (IDS, IPS, NGFW, BDS, Sandbox, NDR), endpoint security solutions (EDR) and SOC analysis tools (SIEM, SOAR).



About us

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

Contact us

contact@gatewatcher.com
www.gatewatcher.com