AIONBYTES ®

SANDBOXING DETECTION
Dedicated, controlled and protected environment

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]

AIONBYTES®: Analyze any malware in a dedicated and monitored environment. (strategy, targets, behavior and actions)

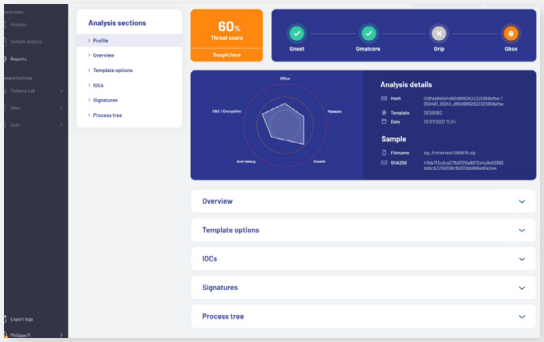
In a digital world where suspicious files and software are exploding, AIONBYTES is a sandbox solution that creates a secure and isolated environment from critical infrastructures, for the search of exploitable vulnerabilities.

Analyzing suspicious files and URLs to detect types of malware is an effective way to understand potential future behavior and make the necessary protection decisions to avoid possible compromises. This is made possible by the AIONBYTES and the protected environment it provides, which executes the malware and provides information about the changes made on the system.

In a few minutes, SOCs, CERTS and Security Analysts get a first estimation of the capabilities of a malware or shellcode, their communication with the outside world and the possible files created.

AIONBYTES allows to complete the detection system in place to :

- ☑ Observe malware execution in mutex, registry, API calls, file system access, network behavior and artifacts.
- ☑ Understand the actions of the malware in its complete life cycle cycle: By observing its operating mode, its access to the Internet, by Internet, by simulating an interaction with the malware execution by recording the network behavior.
- ☑ Identify evasive behaviors such as deferred execution, environment diagnostics, and human interaction verification.
- ☑ Share malware forensics data with other security components for immediate prevention and protection against future attacks.



How does AIONBYTES work ? 5 analysis engines, easy on-premise or Saas deployment

AIONBYTES provides deep file analysis and randomly generated domain detection without the need for an external service to reduce the risk of compromise.

AIONBYTES displays the result of the analysis:

- The file is safe. No threats are detected.
  The file can be used, stored, and distributed.
- The file is infected. A threat is detected.
  It is recommended not to use, store and distribute this file.
- The file is suspicious. A program that in some cases could be dangerous has been detected. It is therefore dangerous to use, store, and distribute this file.

OPERATING PRINCIPLE

AIONBYTES is easily deployed and does not require additional skills to the security teams (SOC, CERT, Analysts..). The solution is scalable to adapt to the volume and number of target users. It is easily deployed on premise or in SAAS mode.

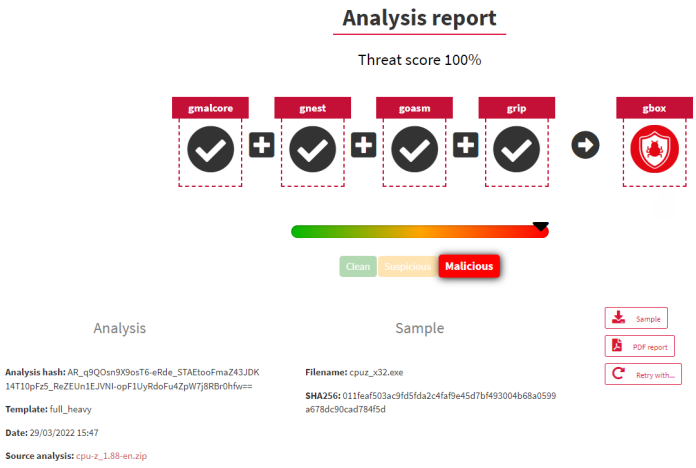
Three modes of updates are possible:

- in connected mode: AIONBYTES connects to the Gatewatcher datacenter
- in offline mode by manually loading the update packages.
- by connecting to a "repository server" that connects to the Gatewatcher datacenter.

5 analysis engines to assess threats

AIONBYTES delivers detailed results from each engine with global statistics for better decision making in the face of threat elimination challenges

- Static analyzer for fast analysis of file metadata.
- Dynamic analyzer to assess the behavior of the execution of a file in a virtual machine. Possibility to extract data generated during the analysis (memory dump, pcap, ...).
- Heuristic analyzer, based on 16 antimalware engines running in parallel. Selected by the Gatewatcher Lab Center for their complementarity, relevance, detection technology, and geopolitical origin of the security information used.
- Shellcode analyzer, for identifying certain encodings and detailing the system calls made.
- DGA (Domain Generation Algorithm) detector



Benefits: a quick and complete analysis to anticipate threats

- No risk to your host devices or operating systems not exposed to potential threats.
- Simplified assessment of potential malware threats.
- Testing of software changes to assess potential vulnerabilities prior to production release.
- Quarantine zero-day threats.

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