



# SandaS

Global Security Knowledge  
for your Business

DATA LEAK

RANSOMWARE

MALWARE

## Find out what's going on with your company's IT security in an agile and immediate way

Nowadays organizations are facing a context of increasingly complex IT threats, such as persistent advanced attacks or industrial espionage, and at the same time the need to meet the legislation and regulations in security matters.

SandaS offers a new approach to your company's externalized security management. Its technology will help you globally manage your company's information from a tactical and operational point of view.



### Innovation

Advanced detection of security incidents thanks to the combination of external and internal information.



### Intelligence

Its advanced intelligence algorithms detect security incidents that go unnoticed for SIEMs.



### Collaborative Detection

It adds multiple external and internal data sources, acquiring information from the Internet and the physical world.



### Integral Solution

Analysis, categorization, notification and immediate response to information security incidents.



### Real Time

Real time visualization of information regarding incidents and alerts detected.

## Benefits

- Improved resolution time for incidents and mitigation of their impact thanks to the automatic response.
- Advanced detection in comparison with other market solutions thanks to the combination of multiple sources of both internal and external information.
- Greater efficiency on management thanks to real-time information, adapting relevant notifications to the indicated persons for each incident.
- Real-time visualization of information thanks to its immediacy: incidents and alerts, indicators and service levels and configurable dashboards.

## Target Group

- Companies with an IT architecture that need to manage their security infrastructure.
- Organizations that need real-time management on a preventive level through the correlation of events from the different environments and devices.
- Private and public companies that need to ensure their security and duly manage risks, meet obligations and internal policies imposed by legislators, regulators and clients.
- Organizations that need to shield and protect information in order to maintain the confidentiality, availability and integrity of it.

## Technical Features

- Integration with HP Arcsight, Alienvault and Intel Security SIEMs for collecting alerts and events expanding their advanced correlation capacity.
- Powerful rules engine that allows SOC (Security Operations Center) personnel to configure the categorization, notification and response to detected alerts.
- Web portal with real-time alerts and operational and configurable dashboards for the management of security incidents.
- API that allows integration with ticketing tools belonging both to the SOC and your own organization.