SGBOX

SGBOX BUNDLE

Next Generation SIEM & SOAR

SGBox is an all-in-one platform for ICT security management. Its modular architecture enables it to adapt to different business security needs.

www.sgbox.eu

SECUREGATE

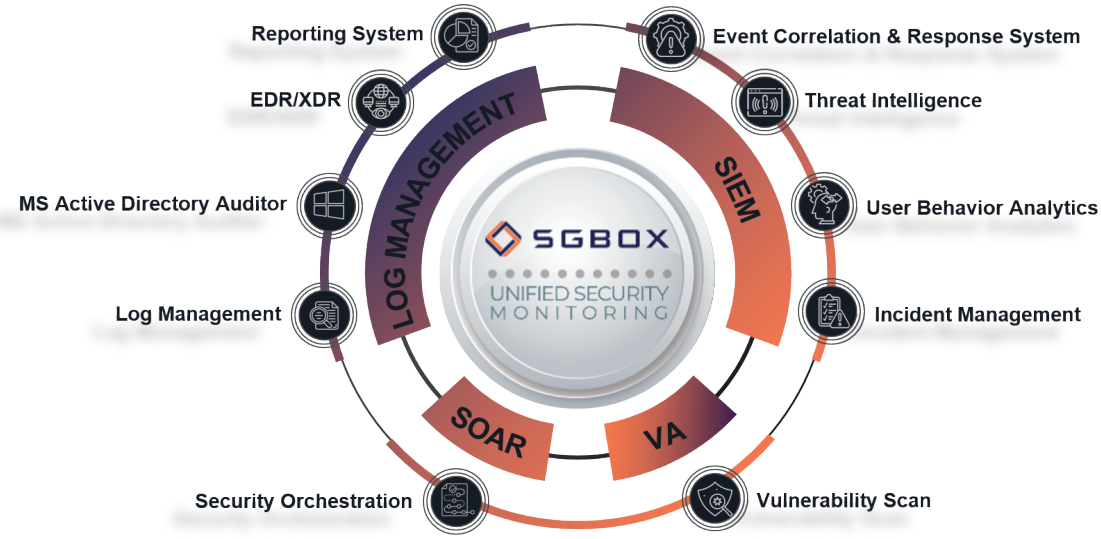
SGBOX OVERVIEW

What is SGBox

SGBox is a **Next Generation Modular SIEM & SOAR platform** developed for **ICT security management** and compliance with current regulations, such as Privacy Guarantor, GDPR, nLPD, ISO 27001.

Available in **Cloud, On Premise or Saas mode**. Each module has its own specific functionality and can be added to collaborate with other modules and share the information collected, facilitating and ensuring compliance with the requirements imposed.

The Platform



LICENSES

PROGRESSIVE LICENSES PLAN

Licenses are based on the number of modules chosen and the number of data sources that send logs, allowing a linear and predictable cost.

Access

The Access plan allows the collection and management of logs, ensuring full compliance with the directive of the Data Protection Authority, with the possibility of extending its functions (even retrospectively) through a simple license upgrade.

Basic

The Basic plan allows the collection and management of all logs, ensuring full compliance with the relevant national directives, with the possibility of extending its functions (even after the event) through a simple license upgrade.

Advanced

The Advanced plan includes almost all the functions of the platform, and in addition to gathering, analyzing and monitoring security information, it includes modules for the correlation and proactive detection of the most complex threats.

Premium

The Premium plan alows you to take advatage of all the features, from the collection and analysis of logs, the correlation of information to the orchestration and automation of countermeasures to be taken, for a complete management of ICT security activities.

Advantages

- Modular solution: you can choose between different bundles and upgrade at any time.
- The SGBox license is based on the total number of devices that send logs and not the number of events per second (EPS).
- The archiving process allows for secure data storage through protection, encryption, digital signature application and time stamping.

30 %

Annual growth

150 +

Partners worldwide

INTUITIVE DASHBOARD
REAL TIME VIEWS OF SECURITY STATUS

Compliance with regulations

The collection of information takes place in compliance with privacy regulations.

Scalability

Choose the features you need in a progressive and scalable way.

Predictable price

The price is commensurate with the actual use of the platform.

95 %

Renewals

1500

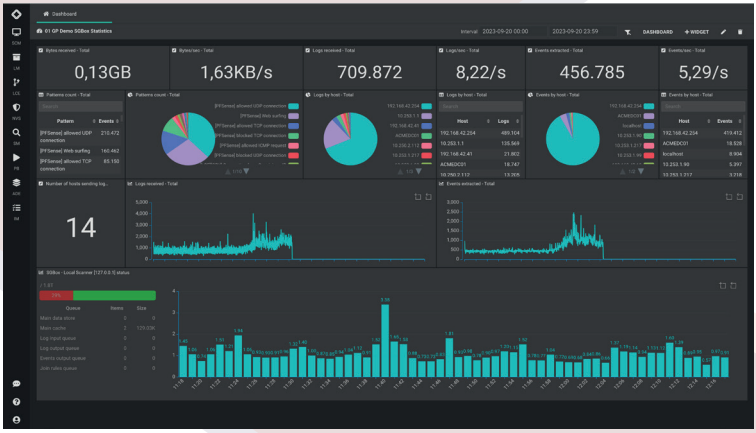
Customers worldwide

FEATURES

ADVANCED LOG MANAGEMENT

The Log Management module is able to manage the event logs related to the security of any type of data source.

- √ Easy and intuitive dashboards with multiple widgets. Multiple ready-to-use, pre-defined dashboards. Possibility to create new ones easily.
- √ Clear and simple analysis panels that allow investigations at various levels.
- √ Ability to generate and query data for deeper searches.



EDR/XDR

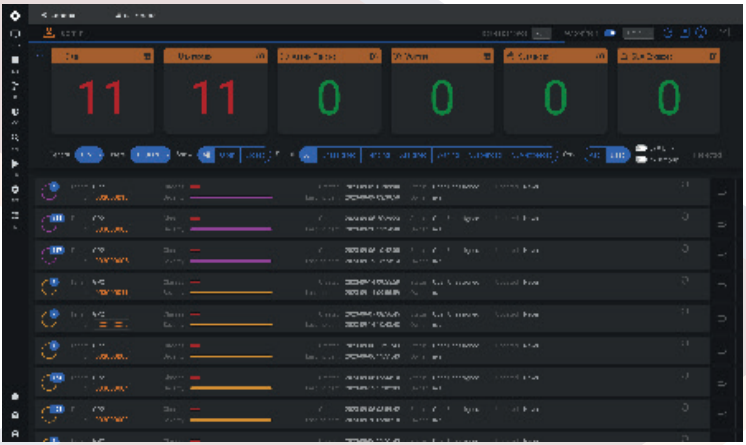
The integration of EDR (Endpoint Detection and Response) and XDR (Extended Detection and Response) products with SIEM allows for the unification of granular data with broader network logs, creating a centralized ‘single pane of glass’ to improve threat detection and accelerate incident response.

FEATURES

INCIDENT MANAGEMENT

The Incident Management module provides a unified platform for the management of incidents or anomalies encountered by other SGBox modules.

This module also allows to correlate more similar incidents, thus reducing the number and false positives, allowing a more filtered and more correct analysis.
Report System functionality allows the generation and consultation of reports in a completely new, safe and interactive format.



THREAT INTELLIGENCE FEED MANAGEMENT

The Threat Intelligence feature allows the identification of anomalous activities by collecting information from multiple open source or commercial intelligence feeds.

SGBox collects the safety information in Indicators of Compromise (IoC) and is able to correlate the data to produce reports and alarms.

FEATURES

ADVANCED EVENT SEARCH

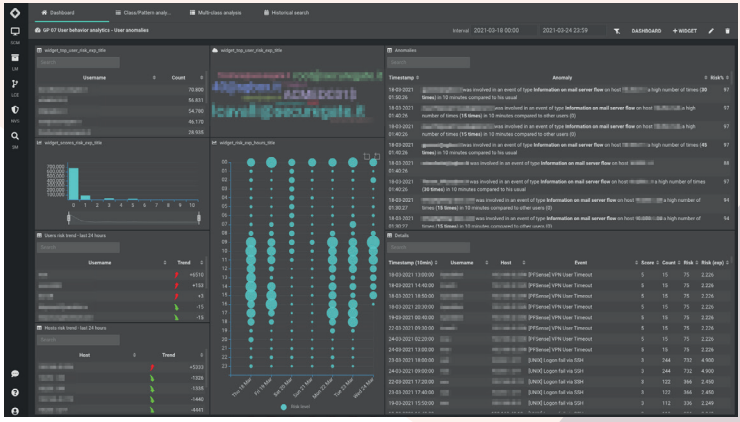
The Advanced Event Search module exploits the information collected by the other modules of the platform and allows you to create specially structured rules in order to detect the presence of anomalies attributable to risk scenarios.

- √ Intuitive Drag & Drop interface
- √ Correlation rules applicable to real-time and historical data.
- √ The correlation engine aggregates data from different sources and gives the ability to create custom rules to activate automatic countermeasures.

USER BEHAVIOR ANALYTICS

The module of User Behavior Analytics (UBA), allows to analyze data related to user activities identifying potentially abnormal behaviors.

By automatically creating a user-specific behavioral baseline, the solution allows you to identify any abnormalities or deviations from normal behavior.

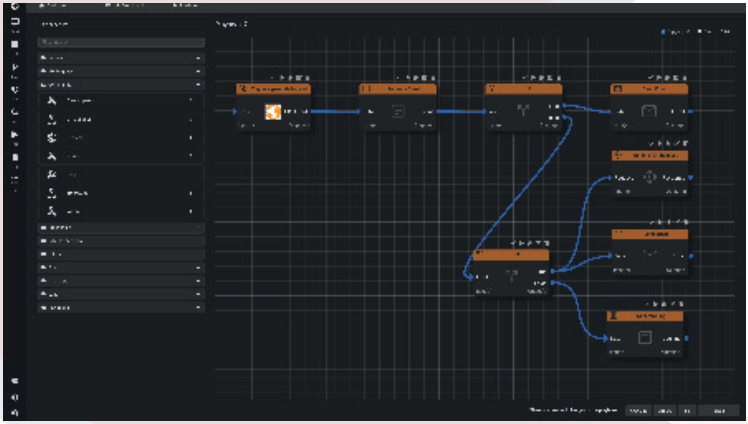


FEATURES

SOAR (Security Orchestration, Automation & Response)

The Security Orchestration, Automation, and Response (SOAR) system focuses primarily on threat management, security operations automation, and security incident responses.

The SOAR module can immediately evaluate, detect, intervene or perform investigation of accidents and processes without the need for human interaction.



FIM (File Integrity Monitor)

The solution allows the collection of multiple information from Windows systems, both client and server.

Through the proprietary agent of SGBox for Windows, it is possible to collect logs and information generated by Windows devices, from login and logout activities, up to the operations that took place within the file servers.

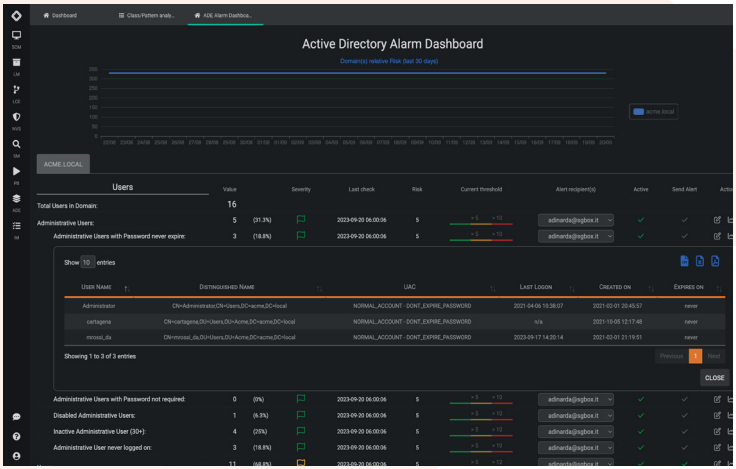
This functionality also permeates the monitoring of the integrity of files, to detect in real time any alterations and unwanted accesses of the corporate users and send timely alerts.

FEATURES

ACTIVE DIRECTORY AUDITOR

ADA is a tool designed to constantly monitor the status of Active Directories, determine the risk and warn when the set KPI thresholds are exceeded.

This module is perfectly integrated with all other SGBox features, in fact it is able to generate lists that can be used by other modules to perform specific tasks such as event correlation, filtered reports, etc.



FEATURES

NETWORK VULNERABILITY SCANNER

The SGBox Network Vulnerability Scanner (NVS) module allows you to detect vulnerabilities on your network.

The module is seamlessly integrated with all other SGBox features and is capable of generating lists that can be used by other modules to perform specific tasks such as event correlation, filtered reports, etc.

The NVS module integrates the Qualys-based scanning engine to perform state-of-the-art and in-depth scans of all vulnerabilities.

SGBOX PRODUCT MATRIX

SGBox Product Matrix

Features	ACCESS	BASIC	ADVANCED	PREMIUM
Access Log	✓	✓	✓	✓
System Monitor	✗	✓	✓	✓
Advanced Log Management	✗	✓	✓	✓
Advanced Event Correlation	✗	✗	✓	✓
Windows Auditor	✗	✓	✓	✓
Threat Intelligence Feed	✗	✗	✓	✓
User Behavior Analytics	✗	✗	✓	✓
Vulnerability Scanner*	O	O	O	O
SOAR	✗	✗	✗	✓
Incident Management	✗	✗	✓	✓

*Optional feature

- The Access and Basic plans comply with the regulations of the Data Protection Authority, while the Basic and Advanced
- The vulnerability scan function is independent of the number of Data sources.
- Licenses are available both in “Subscription” mode (1-3 years) and in “Perpetual” mode.

CONTACT US !

We are ready to support you in finding the security solution that best suits your needs! Request a free demo to learn more about the features of SGBox.

Address
Via Melchiorre Gioia 168- 20125 Milano, Italy

Telephone
+39 02 60830172

Website
www.sgbox.eu

Email
info@sgbox.it