Compliance Support

The LM module provides a series of reports designed to help businesses comply with the conditions set out in the legislation. **PCI DSS** and **SOX**.

Italy's **Privacy Authority** has published a provision which regulates the handling of information from systems in relation to the connections made by the system administrators. As well as the organization requirements, the Authority requires the adoption of tools to monitor the connections and disconnections of the system administrators. The LM module complies fully with the directive. In fact, the registrations (access log) are complete, unalterable and their integrity can be checked, which means they are adequate for the verification purposes for which they are required.

ISO 27001 PCI DSS COMPLIANT

"simplifying your IT"

MUCH MORE THAN A LOG REPOSITORY

The LM module of the SGBox platform natively supports the standard Syslog, but was designed to gather logs of any format from any data source without the need for installing any proprietary agent specially designed for any specific platform. It has all been made possible by a powerful recognition engine and normalization of the logs which, through a simple, intuitive interface, allows the user to add freely logs from any of the company's platforms. The data gathered will then be able to be analyzed and handled across the board in a dual system, or used in a real time analysis or an analysis on the log history. The data analyzed can also be displayed graphically through a series of very detailed reports.

Logs gathered from any platform and data source

Correlation of Events

Correlating events allows relationships between two or more logs to be detected based on a set of rules used to interpret the data contained within the events. The most common form of correlation is based on rules which enable more log entries (chains of events) from an individual source or from multiple sources to be linked on the basis of values in the logs such as the timestamp, the IP address, the type of event etc.

The correlation engine thus enables possible threats or cyber-attacks to be prevented or responded to automatically.

Anomaly Detection

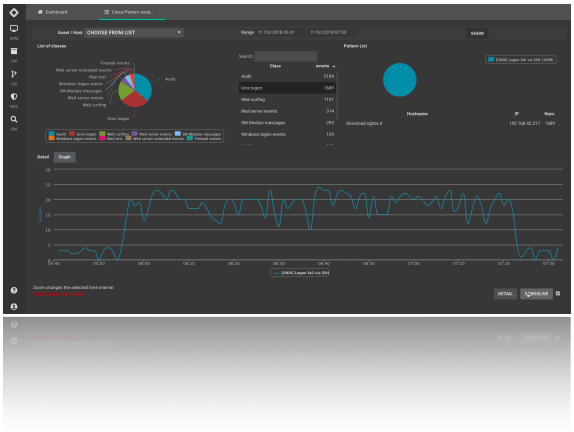
The function for detecting anomalies enables unusual situations concerning apparently consistent data traffic to be identified. Identification of anomalies is fundamental for the detection of frauds, network intrusions and other important events which would be impossible to identify.

Data Integration

Data from the infrastructure can be “enriched” with additional information such as geo-location, resolution of domain names and the creation of “aliases” to improve the navigation of the data itself.

Dynamic Searches

Events can be “drilled-down”, starting with an overview of historic data and then viewing the detail to analyze the individual event. Selecting a parameter in the event flow influences its display and enables a guided search.



Customised Dashboard

Using the flexibility of the user interface of the SGBox platform, it is possible to define a customised display of key information using a dashboard. Each user will be able to determine their own specific view of the most important elements of the information gathered, containing data of interest which relates to their own processes and operating area.

Optimised, quick access to data, whether in real time or historic.

Key Performance Indicator (KPI)

The tool is able to define complex KPIs because of an indicator which operates using variables which are the result of individual analysis of any event (network, application-oriented, database, security, etc.).

SGBox Log Management. Optimize your Log.

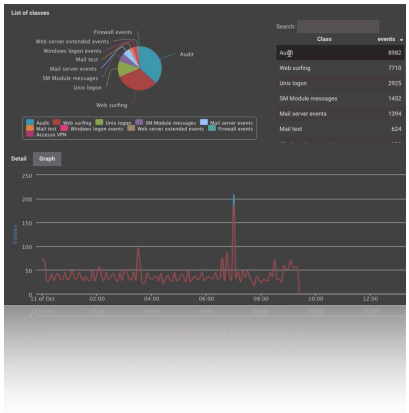
Windows Security

The Microsoft Windows Server monitoring pack function allows security events to be shown on each server and any activity carried out to be traced accurately. It is possible to identify events such as:

- the creation or cancellation of a user
- changing privileges
- changing a password
- programme implementation
- read access to a file/folder
- write access to a file

With this package, events generated by each individual host/user can be accurately traced to obtain complete control throughout.

SGBOX



“intelligent platform”