CASE STUDY AIL AZIENDE INDUSTRIALI LUGANO

SGBOX PLATFORM
NEXT GENERATION SIEM & SOAR

COMPANY PROFILE

Aziende Industriali Lugano (AIL) is the most important retail and wholesale distributor of water, natural gas, and electricity in the Canton of Ticino.

Their products and services are purchased daily by over 110,000 private and business customers, distributed across approximately 54 Municipalities. AIL builds and manages the networks necessary for transporting products from the point of production or purchase to the customer.

THE NEED

AIL's security infrastructure is composed of multiple devices that generate a large number of logs, which are important pieces of information that need to be centrally stored and managed. AIL was looking for an in-house solution to collect and analyze all the logs generated by network devices, web applications, data sources, and OT (Operational Technology) devices.

In the past, the client had run tests with SGBox's competitors, but had not found the most suitable solution due to the difficulty in adapting to the existing IT and OT infrastructure.

The choice fell on SGBox because of the platform's flexibility and its ability to provide a centralized and immediate view of the company's security status.

> **After careful analysis, we chose SGBox as the ideal partner that could easily integrate with our systems. It proved to be an open log platform capable of collecting information from any type of system. It is easy to use and quick to implement, and is compatible with all IT security infrastructures.**
>
> **Michele Rusconi - Head of the IT/OT Services and Cybersecurity Unit**

info@sgbox.eu
www.sgbox.eu
Via Melchiorre Gioia 168, Milano

> **The SGBox team carried out a thorough assessment and supported us throughout the start-up and implementation phase of the solution, taking our specific needs into account**
>
> **Michele Rusconi - Head of the IT/OT Services and Cybersecurity Unit**

APPROACH

After performing several preliminary analyses for the configuration of approximately 250 data sources, the SGBox team started the development phase of an ad-hoc system, working alongside AIL's IT department.

The starting point was the creation of correlation rules, which allowed the client to identify various suspicious/malicious behaviors using MITRE ATT&CK techniques.

Once the on-boarding phase was complete, AIL was able to continue the implementation independently thanks to the ease of configuration and SGBox's flexibility in recognizing sources.

IMPLEMENTED FEATURES

- **Advanced Log Management:** collection, normalization, and advanced management of all logs coming from the data sources.
- **SGBox SOAR Playbook:** upon detecting a malicious IP, it is possible to block it on the firewall using SGBox's SOAR functionalities, adapted to specific needs, such as notification through the Swiss messaging app "Threema".
- **Template Function:** a useful function for extracting information following a potential threat, which allows for the production of easy-to-interpret security reports and audits.

ADVANTAGES

The solution implemented by SGBox has allowed AIL to utilize a ready-to-use solution for managing security information from a large number of devices.

This has made it possible to gain a real-time view of the company's security status and to proactively identify threats before they occur, which is a decisive factor for maintaining operational continuity.

FUTURE SCENARIOS

The client is continuing to use the SGBox solution and has expressed the desire to also implement the Incident Management function. This will transform alerts generated by the correlation rules not only into e-mail notices, but into actual alarms to be managed through IM (Incident Management).

The SGBox team made themselves available to conduct a specific training course, through which AIL was able to acquire the fundamental technical skills to autonomously leverage the platform's potential.

info@sgbox.eu
www.sgbox.eu
Via Melchiorre Gioia 168, Milano