GRUPO
Anticipating a
cyber secure world

CASE STUDY

Mobility Sector

01

Introduction

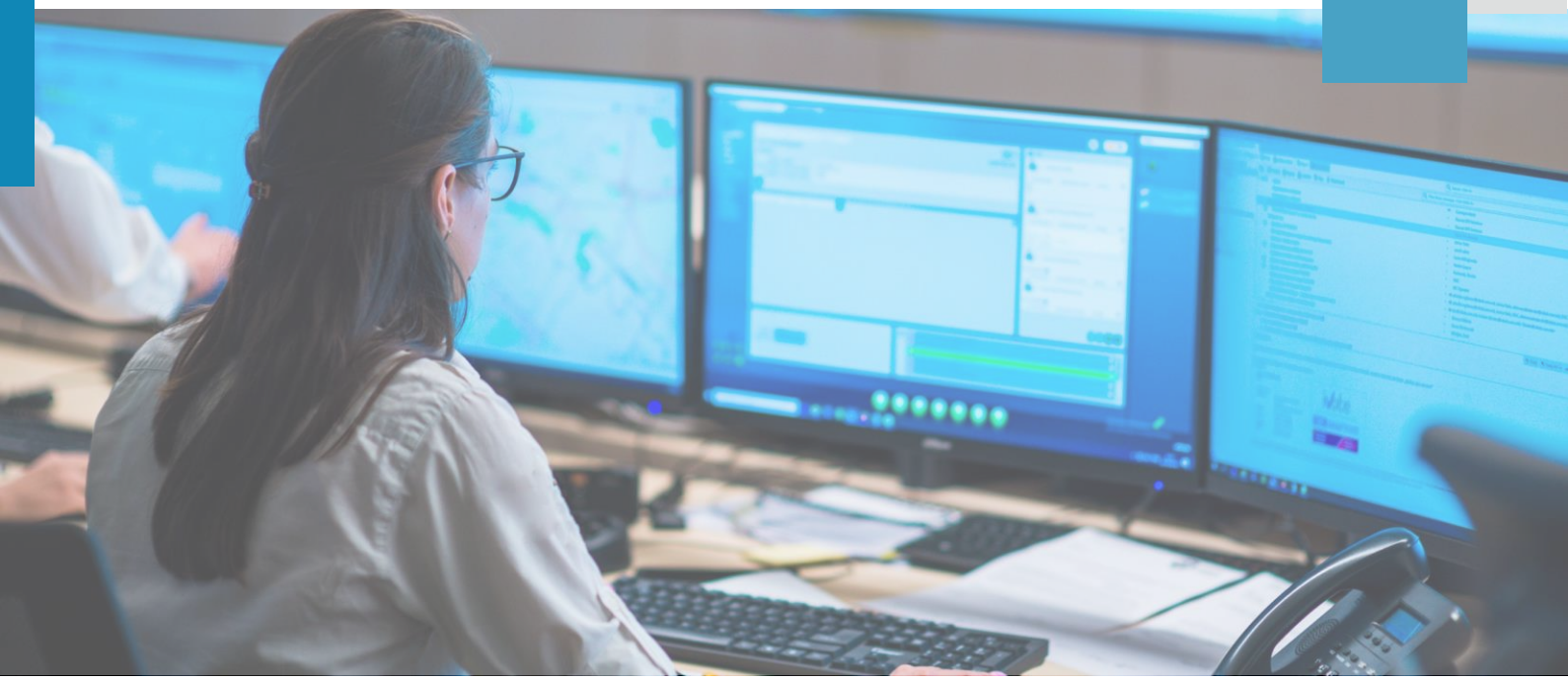
Our client is a public passenger and freight rail transport company with more than 5,000 trains running every day throughout the country, more than 500 million passengers per year and nearly 15,000 employees.

The organization is constituted as the head of a group of 5 public limited companies and is expected to close 2023 with revenues of more than 1,332 million euros.

They have a cybersecurity and privacy management department, with an investment of over €245 million in digitization and cybersecurity between 2018 and 2023.

02

Problem/challenge



The company **has specialized personnel** for the operation of the cybersecurity operations center for all of the organization's assets, as well as for its clients' information, and **currently has a SIEM** (Security Information and Event Management solution) for this purpose.

The SIEM deployed in the company provides due traceability of cybersecurity actions, so that in case of internal needs or external requirements, such as those derived from judicial or police actions, the requested information can be provided.

However, **the current SIEM is insufficient to the needs of the organization and is totally obsolete.**

For this reason, they need to deploy a new, more powerful and updated tool **for the continuous and real-time comprehensive operation and management of their cybersecurity service center, which allows them** to identify trends in alerts, enabling them to draw conclusions about the organization's security posture and status, identifying significant variations in the number of alerts that may be due to changes in the security policy of an element, configuration changes or a bad authentication policy.

03

Upgrade performed

S2 Group has carried out the supply, deployment, installation, commissioning, training and maintenance of the hardware and software necessary for the implementation of the **SIEM GLORIA solution**, sized for 70,000 EPS and with a retention of 30 days of online logs and 365 days of offline logs.

A study was carried out for the sizing of the hardware required for the implementation of Gloria, based on the volume of EPS that the solution will have to support, the average size of the logs and their retention period.

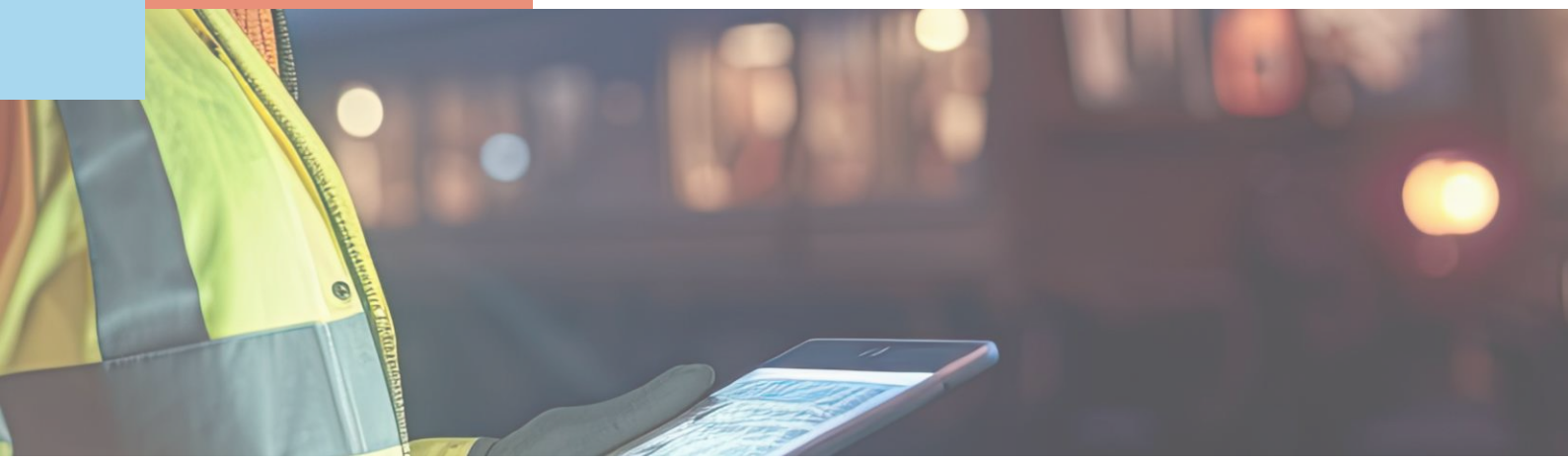
The most appropriate deployment model for the proposed solution was designed, establishing a model through Kubernetes that allows for greater stability and scalability if necessary. Subsequently, the necessary hardware for Gloria's implementation was provided and installed at the client's facilities, and the new SIEM was deployed under the previously defined model.

The platform was installed and configured and functional tests were carried out **to ensure its correct deployment**. These tests verified the installation and base configuration of the platform, checking the availability of all platform components through the solution's self-diagnosis utility, the correct reception of events, the correlation and generation of alerts in the management console and, finally, the availability of the dashboards.

Subsequently, the sources required by the client were integrated and calibrated, amounting to a total of 350.

Lastly, once the service was implemented, **four platform training courses were held** for the users of the organization's operations center. This training was given twice in order to ensure the attendance of all the necessary people in the organization.

.



04

Benefits obtained

With the completion of this project the client has:

The GLORIA solution for the **continuous and real-time operation and management of its cybersecurity service center**.

A solution developed jointly by S2 Grupo and the CCN, which is included in the catalog of products and services for information and communication technology security in the **CCN-STIC 105 guide** as a **HIGH category** solution according to the National Security Scheme.

A platform with **security monitoring and collection capabilities**, with a flexible orientation towards surveillance of the IP world, including **IoT and the OT world in general, advanced intelligence** through complex event correlation techniques or **pattern analysis for the identification of anomalies and management of the processes** linked to the service, with a unique alert and incident management console, which brings efficiency and effectiveness to its operation.

A solution that will gradually integrate the sources most needed by the organization, thus being able to prioritize or not those sources most needed according to the needs of the moment.

S2 GRUPO

MADRID
BARCELONA
VALENCIA CERT
VALENCIA HQ
SEVILLE
SAN SEBASTIAN

SANTIAGO DE CHILE
C.D. MEXICO
BOGOTA
LISBON
ROTERDAM

Follow us: @s2grupo s2grupo.es