CASE STUDY

Environment Sector

Cybersecurity of the
circular economy

Introduction

There is no future for our society without a sustainable economy, with the responsible use of the planet's resources. The EU is a model for the world with the European Green Deal and as a model of a modern, efficient, and competitive economy that makes the circular economy one of its fundamental principles.

Our client is a **multinational group in the Environment sector**. Specialized in recycling and waste management. It has almost a hundred treatment plants in different countries around the world. In some cases, it is the owner of the facilities and in others it is the holder of a concession or service contract.

Having such an **extensive network of interconnected infrastructures in different countries** with different cultures makes your surface area of exposure to any threat a considerable risk.

It is an "important" entity in the classification established by the NIS 2 Directive. Its activity is subject to international cybersecurity regulations as it involves critical services essential to society and cybersecurity is part of its strategic lines.

02

Problem/challenge
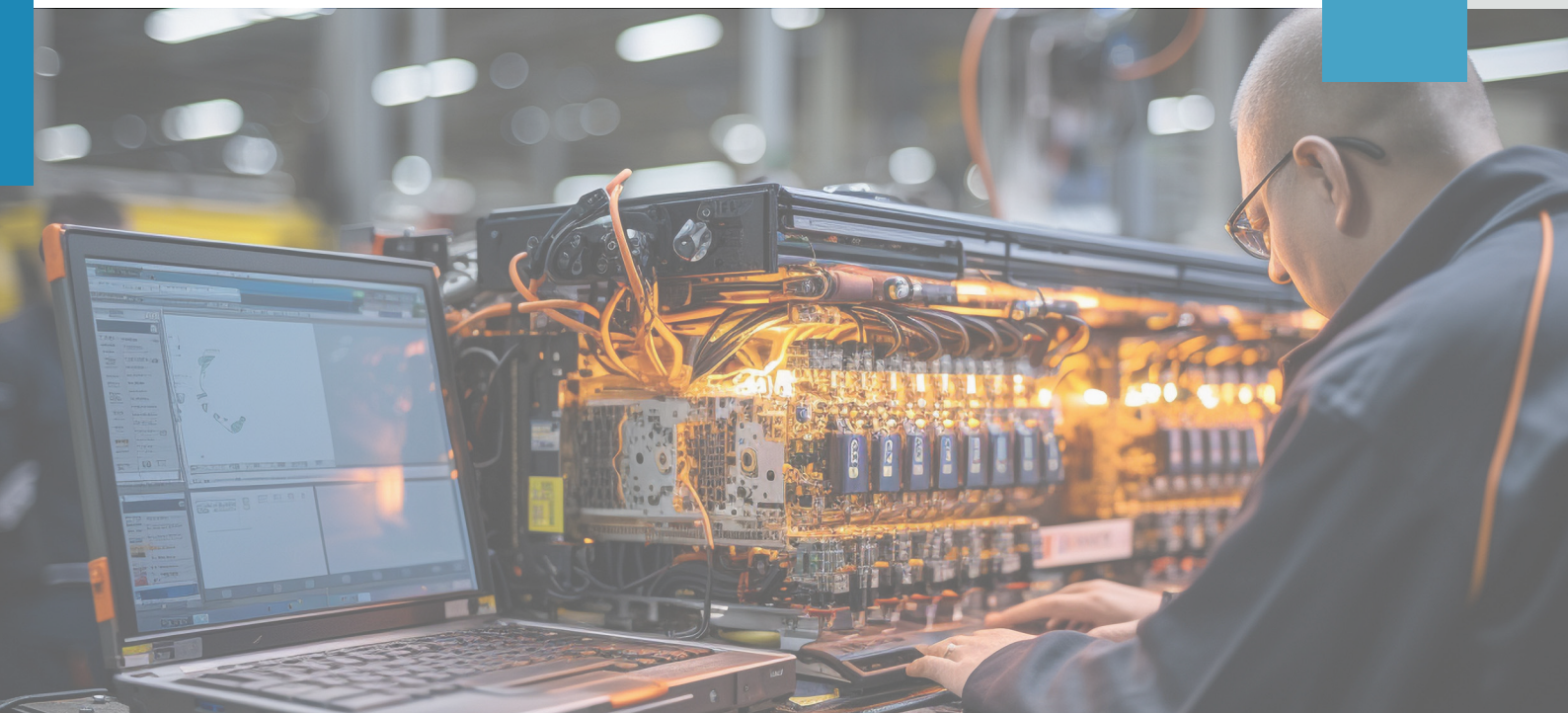
The organization already has a cybersecurity department. Until now it has been developing **the cybersecurity strategy of its corporate IT** part where it has a high degree of maturity.

For some time now, it has been making a great effort in the development of **cybersecurity for the operational part of OT**. It already has a Work Plan for the development of this part of its corporate policy. However, **the special characteristics of this sector require expert knowledge**. Furthermore, some of the measures to be adopted are urgent. And the availability and limitation of their resources have made them decide to look for a specialized provider to accompany them.

03

Action carried out

To support the medium-term development of a General Plan, it has contracted the services of an *Industrial Cybersecurity Office*. S2 Grupo provides expert advice with different specialists in different disciplines of industrial safety that allow you to have the necessary knowledge throughout the process.

Various resources are permanently assigned as a workforce and knowledge available to the client, who will coordinate the different lines of work and the objectives to be achieved.

Our experts provide their experience to:

- **The analysis of the organization's initial state**, which has a wide variety of plants with different security maturity degrees. To understand its threat environment and determine the set of vulnerabilities that could compromise it.

- **The establishment of clear objectives** as a result of the proposed project. Acceptable risk level.

- The preparation of a **Risk Analysis** and a series of specific OT cybersecurity procedures that can be applied to the company's different plants.

- Taking advantage of the process of the work that the company has already been carrying out until now, with the preparation of a security dashboard for the entire organization.

- Suggesting **alternative improvements** to the initial plans that contribute to the development of a structured, solid, and consistent industrial cybersecurity documentary framework.

04

Benefits obtained

Having the support of a company specialized in industrial cybersecurity like S2 Grupo has allowed our client to:

✓ Have the **support of a series of experts in different disciplines** who offer it an objective overview of its initial state and the possible initiatives to be proposed.

✓ Develop in record time a **general industrial cybersecurity strategy**, which is impossible to carry out without help by their own means,. Applicable to the entire organization. With the variety of facilities it has and the different cultural nuances in different countries around the world.

✓ Provide continuity to its **General Cybersecurity Plan** with the convergence of the IT part and the OT part and its integration into the company's Management System as a continuous improvement process.

S2 GRUPO

Follow us: **X** **f** **in** **◎** • @s2grupo • s2grupo.es