

Energetic System operator



Challenge

The customer had some number of implemented systems not integrated between each other among them that logically caused frequent problems.

Moreover, there were 3 main types of information that were processed in the company:

- ✓ Data on critical information infrastructure (CII) objects. During the work on the project, Defensys's engineers along with colleagues from the partner's side imported all CII objects into the Defensys SGRC and updated them
- ✓ Trade secret type
- ✓ "For internal use" type of Information

All cyber security audits were carried out in 3 areas:

1. CII
2. Trade secret
3. Compliance with internal checklists

The hard challenge to find the right solution which could be flexible in settings and integrations and solve collected problems was set by the customer. After a careful search, the company has chosen Defensys SGRC solution.

Results

First of all, regulatory and physical security requirements were fetched between each other via control checks framework built in Defensys SGRC. This way the user receives only one list with all the requirements needed to be assessed depending on the type of an asset and his role in the process (not all the requirements).

Also 6 additional types of custom assets were designed and implemented along with those types that exist in the SGRC out-of-the-box just by using built-in settings capabilities without any coding. For instance, these new entities were added to

- > **8 000** employees
- 7** Joint Dispatch Offices
- > **50** Regional Dispatch Offices
- > **10** representations

Defensys

Defensys is an award-bearing and nationally acknowledged vendor of cybersecurity solutions.

Since 2011, we have been fostering government agencies and private-sector companies to confidently withstand modern cyber threats and ensure reliable security management worldwide.

Defensys technologies are embedded in financial, public, oil and gas, energy, metal industry, and other sectors.

✉ sales@defensys.com

📞 +65 3159 47 50

🌐 www.defensys.com

manage cryptographic security tools, electronic signatures, equipment used by supply chain company's representatives.

Using report builder feature of the SGRC equipment and facility passports are now simply generated when it's needed with accordance with all the requirements for the documentation in the Company. There is a process built for these purposes, when all the involved colleagues are notified by the SGRC that they need to update the information that they are currently in charge for.

There were several integrations done during the implementation process of the SGRC: email system, AD, ITSM in terms of asset management, vulnerability scanner, AV solution, CMDB system. This helped the customer to see the whole picture regarding different types of assets in the company.

One of the most important results was the ability to automatically set the needed properties for assets.

According to internal customer's requirements in the SGRC was customized automatic procedure of information systems classification based on the chosen preconfigured parameters. The logic was as follows: integrity, accessibility, confidentiality levels of the IS were selected by the user or as a result of some import from external system and the final level of IS class was set automatically based on the procedure implemented in the organization. For instance, if the integrity level is average, accessibility and confidentiality levels are low then overall level of the IS class is average. Based on the automatically obtained level, cyber security requirements (set of the requirements for industrial systems also included) were set automatically by the Defensys SGRC for all the ISs in the register based on their classes set during the previous process. For example, the need for fault tolerance for a low level required regular backup of the system, for a medium level a cold cluster was required, for a high level a hot or warm cluster was needed to be implemented.

Of course, the audits themselves are also planned, controlled and processed in the Defensys SGRC.

So the SGRC fetches all the needed properties, requirements and tags just after some new entity is imported in its database. Everything is stored and kept up-to-date in one place by the system. This is also applicable for automatic assignment of assets' locations.

Now the Defensys SGRC gathers 30 different cyber security related specialists in one place perfectly designed for their needs.

All the required results and statistics are distributed on dashboards and geographical map.