Defensys

One of the largest industrial manufacturing and producing companies

› **50 000** employees

› **80** branches across the globe

› **500** clients across the world

Challenge

Each of the company's subsidiaries and branches has its own IT and OT networks.

The OT Cyber security department's main desire was to aggregate data on OT assets in one place because standing on this up-to-date data they could proceed with different compliance procedures: national and internal.

Inventory data was stored in absolutely different places:

- Industrial IDS and AV system databases
- Custom databases
- Electronic documents
- Paper documents
- Etc

There was also one more complicated thing in this distributed chain of tenants – a lot of them were built based on one standard project, that's why there were a lot of different subnets with the same addresses.

Colleagues felt the need for automation because it wasn't at all efficient to try to gather all the information by email.

Results

After the PoC process, the Defensys SGRC solution was selected to close all the objectives.

The system works in multitenancy mode. With this functionality, all assets can be stored in the same location for future use in other cybersecurity processes, regardless of whether they have the same addresses.

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

All the inventory data from the sources described above is merged into specially designed asset cards forming the unified resource-service model of the OT part of the company.

Based on this data and automatic assignment policies for tags and properties of the SGRC every asset is labeled with cyber security standards and checklists applicable for them that saves a huge amount of time for routine work of a lot of qualified specialists. For example, an annual compliance campaign is set up automatically with all the required deadlines, notifications for users, admins, owners, etc.

Everything is uploaded timely on the central server of the Defensys SGRC so to monitor the entire state of cybersecurity for the company.

Of course, there may be very remote areas where cybersecurity colleagues have to go to do various audits with a certain frequency. And this company is not an exception to this rule.

For these purposes, there are 2 crucial options in the SGRC:

- A "light" version of the system for laptops with the similar interface to conveniently fill all the required data which is then uploaded to the central server.
- The ability to combine the results of different audits in some kind of digest to process the results more effectively.

Besides similar requirements of different standards and checklists were combined by Defensys's experts and colleagues from the partner company to assess all the needed requirements once in a time without wasting expensive time of cybersecurity professionals for assessing the same things multiple times for different standards.

Now the core processes are automated as fully as possible for OT equipment and the customer is preparing to choose a system for their SOC needs.