Defensys

Digital Service provider

The customer is the largest national state telecommunications provider of digital services to a wide range of consumers, households, private companies, governments, municipalities and other telecommunications service providers.

> **50 000** employees

> **10** million clients

> **200** subsidiaries

Challenge

The customer had a need to take in order internal IT & cyber security processes. So a large research across the market was made.

After the careful search Defensys ACP was preferred.

The customer has a huge infrastructure with a large number of servers, active network equipment and of course workstations.

During the project implementation several customer's departments were involved. At the beginning, the work was established with IT department, further the cyber security department joined with their own requirements.

The main objective just from the beginning of the project was to make a single repository of assets and to put them in order there. Defensys ACP was tuned to receive data from different network segments. By working together with two Cyber security and IT departments, a lot of different types of systems were successfully integrated with the ACP system but of course there were some specific requirements during this process. For example the customer's network has different segments that are not interconnected on a physical level. That's why some part of data was uploaded to the system with the files integration capabilities, from custom databases and via specified questionnaires that were sent using built-in task manager of the ACP.

The PoC project was dedicated to the automation of Vulnerability management process but then during the implementation the following processes we also automated:

- Technical asset inventory with the ACP capabilities without agents

- Critical infrastructure assets management

- Integration with the customer's SOC. This is the case when different departments ask for the account in the system to enrich their processes with the up-to-date assets' data.

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

Results

Integrations:

- ✔ Devices monitoring solution
- ✔ Antivirus solution management server
- ✔ SIEM
- ✔ Vulnerability scanner
- ✔ Custom databases
- ✔ Network equipment management system
- ✔ Registers from electronic documents

Finally, the ACP counts 30 000 different technical assets from multiple sources above that are merged in a single database with the Defensys's unique technology.

Also a lot of technical information is collected by ACP's collectors that are placed in different network segments – this is one more source of the inventory data used by the ACP.

As a result, the Defensys ACP is now:

- ✔ A central point of all the assets in the company and their interconnections: both technical and business. For each type of the asset a custom status model was designed.

- ✔ An enrichment point of assets available via the documented API for a lot of implemented systems;

- ✔ A central point for launching specific technical scripts and store its results in custom dedicated fields in assets' cards. Than using the dashboard builder the ACP automatically generates and sends reports to all the interested colleagues.

The customer, especially noted the speed and quality of the project implementation, as well as the fact that all wishes were taken into account.

Additionally, the customer plans to expand the total amount of managed assets from 30,000 to 100,000 units in the future.