Defensys

Managed security service provider

> 10 customers of the MSSP are under the cybersecurity monitoring service

Challenge

One branch of the global presence telecom company used a primitive IRP system with a very limited functionality. Since the company is a managed security service provider, arose the need of a new, more flexible platform with a significantly greater range of functions. After a series of negotiations and the PoC project, the Defensys SOAR was chosen as a core solution.

The Provider offers its SIEM and TI systems to each customer and, depending on the customer infrastructure, one company can have several platforms. For that reason, Defensys software had to be integrated with all installed systems.

Implementation

The Provider's client database was connected with the Defensys SOAR and stored information is being synchronized with custom assets. Due to this, when an incident occurs, the Provider has very exact information, which SIEM system it comes from, which company is involved, and all the data is already stored and up-to-date in the client's card for further processing.

It made possible a customized incident notification via, for example, ITSM systems or messengers. As a result, it became a very effective tool with the workflow for a particular incident type created exactly for the Provider's needs.

Moreover, the Provider uses well-liked mailing for subsequent reporting involving several mail-boxes. The Provider's TI platform sent out filled-in bulletins to these boxes. After implementation of the SOAR, received TI bulletins information was saved in the relevant incident card on the additionally created tab. Instead of a time-consuming bulletin and its status searching, the user now can easily manage the workflow, designate responsible employees for

resolving vulnerabilities and monitor tickets status.

Besides, to keep every process under control, all responsible employees and managers receive current notifications via a messenger.

As each incident card contains the history of the whole incident processing steps, all responsible SOC users of different response lines can access information anytime and, when needed, react rapidly.

After creating of additional API connectors for retrieving data from the SOAR according to a particular request and transmitting it to the Provider's customer portal and visualization platform, the data is shown on dashboards and the user could keep an eye on the incident statistics.

Considering the peculiarities of the service user companies, into 5 SOAR playbooks were integrated more than 100 scenarios accommodating all details of workflow steps.

Results

This project turned out to be a 100-Day challenge for Defensys, during which engineers fulfilled all customer's requirements and provided the multifunctional SOAR Platform for covering all processes.

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