CERT

Challenge

This is CERT, which main task is to collect information about incidents from its subordinates , as well as inform them about the main threats, attacks, vulnerabilities etc.

Before taking a look at the SOAR class systems almost all the procedures of interacting with different representatives of the regulated companies were manual. CERT communicated with everyone via mailbox. For manual enrichment of IoCs delivered from subordinates, CERT analysts used various services, for example, WHOIS.

Also there was a demand from the regulated companies to have an electronic service to operate with this CERT with the possibility to automatically register incidents and IoCs.

Defensys products

The customer wanted to estimate comprehensively different types of building automation for their needs covered above:

- matured software from some vendor with features specially tailored for such needs
- ServiceDesk-like systems with some added programming and customization
- fully custom programmed software based just on the needs of this CERT

As a result a part of Defensys's ecosystem: SOAR + TIP was chosen among other respectful vendors for building this self-service cybersecurity portal.

Results

The following number of important issues was resolved after the implementation of Defensys SOAR+TIP:

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

- Build a personal account based self-service portal which allows subjects to access their accounts via API or UI, to send incidents to the regulator, creating incident cards of a particular category (the card depends on which fields you fill in and on the role of a user), register incidents via API for other vendors. In addition to the fact that subjects can transmit messages to the regulator, the regulator can also transmit messages to the subject through the personal account. Subjects can see messages and correspond live in the chat giving additional information and what's more important requesting the help from skilled CERT analysts.
- All the threads between involved parties are logged in a convenient way for post analysis and statistics
- Cyber security Bulletins that are originally created by analysts in Defensys TIP are automatically transferred into the portal based on the Defensys SOAR. After the investigation process of some specific incident, a CERT analyst decides whether appeared IoCs are needed to be delivered to the TI system. If necessary, when incidents are closed, they are transmitted to the TI system automatically so this way bilateral integration SOAR-TIP works for the full enrichment of the TI data.