Defensys

The Bank

Banking organization with a wide variety of branches approximately 11,000

› 15 000 employees

› 2,5 million customers

Challenge

Initially, the incident response process was conducted by the SIEM system. The customer had about 7 instructions for different types of incidents with a brief description of what needs to be done in such situations. Also, colleagues did not have a response process. Security specialists used to look at the screen, and if they saw the incident in the SIEM they started working with it according to the instructions. If the incident was something not common, then it was processed randomly.

Results

- ✓ The Bank didn't have the response processes, so our main task was to create and develop them. We identified a rubricator for incidents, expanded it from 7 incidents to 30, and worked out a response process for each type of incident, and then this process was automated in the Defensys SOAR solution.
- ✓ Defensys SOAR created a unified notification system. Earlier in the Bank, if it was necessary to request information, a common email box was used. Employees had to keep track of the answers. Now all this is done through the SOAR system. A request or notification is sent via SOAR and all responses are stored there. Also, the information goes to the general box additionally. Thus, our solution helped to reduce the response time and simplified the process for cyber security analysts.
- ✓ In addition, the problem of obtaining information about hosts was perfectly solved. Now users can see all the needed details regarding equipment from multiple sources just ready to be read in the incident card after the new incident is registered
- ✓ Integration with a tutor system: if a regular user is not the first time detected when violating cybersecurity

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

requirements, then he is forced to go through a training course. For example, there might be a quite «popular» incident like connecting a third-party device to the workstation. A person connects a device to a workstation that is not in the Defensys SOAR whitelist that is tailored for these needs, then an incident is automatically registered by the SIEM in the SOAR and the repeat violation check box is automatically ticked after auto checks for the fact of the repeated violation. Based on this check box all the other procedures will be automatically chosen by the SOAR and only this part of the whole playbook will be executed. The result of this playbook is an automatically created course for this employee in the Bank's tutor system and a notification to his supervisor.

- ✓ Filling in the fields: the process provided that the first line receives the incident, analyzes the fields, and if it sees that some fields are not filled, they must fix it. Then, at the post analysis, you need to figure out why these fields are not filled. It so happened that at first many incidents came with empty fields, employees got tired of describing it in the conclusion, and during the post-analysis no one returned to this. It turned out that the first line wasted time. The customer suggested to automate this process. What was done: an incident card arrives, Defensys SOAR gets all the fields of this card with an API request, processes them with a script, and display the result in evidence. The evidence displayed a snapshot of all fields at the time of the creation of the incident, which were empty and which were filled. That is, now on the post-analysis, it will always be possible to see how the card was filled in at the beginning.