Defensys

# Timber company

Leading sawn timber, paper, and packaging producer.

Owns several production sites across the country.

› **8** years of business

› **20 000** employees

## Challenge

The Timber company with several sites uses an outsourced SOC, which, however, is not sufficient and isn't able to meet all company's demands. So appeared the need for a cybersecurity software to respond on incidents within the company and control its assets. One of the key requirements for cybersecurity vendors was an experienced team of professional engineers, who could develop and implement an absolutely new business processes.

After a range of meetings and a PoC project, the Timber company has chosen the Defensys SOAR for automation and orchestration.

## Implementation

As the first step, Defensys needed to set up the incident handling process considering incident types. Using provided information regarding all existing types, the Defensys' engineers have designed an incident handling scheme and successfully implemented it.

Incident response now can be conducted in 2 modes: automatically and manually. New incidents coming from firewalls and a SIEM system to the SOAR are classified according to the developed rules.

As the Company has a distributed infrastructure, there're responsible employees in each site and the System has to choose the right person for each incident. According to the related incident the SOAR automatically chooses the parameter, that leads to a particular Company's site. Therefore, a responsible person is chosen from a customized list and assigned to the incident. If the process requires an action confirmation, a relevant request will be automatically send to the site's responsible employee.

As the second way of incidents processing, the Defensys' engineers have set up a manual process. A customized list is used as the directory with contacts of IT and CS departments, that helps System's users to quickly find

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

defensys.com

contact information and get in touch with responsible employees as soon as possible.

If an incident is connected with a user profile, additional information on this profile incl. access levels, last sessions is provided via AD integration to the incident card. Profile's type (administrator, user etc.) is automatically determined and depending on the result different response playbooks can be started both automatically and manually.

An important role for incident handling plays the factor, if IP address is external or internal. This data is displayed in incident cards and has an impact on the following response scenario.

In order to enrich information in the SOAR, a special integration with an external platform was implemented. The platform transfers data regarding malicious IP addresses (pulses). When the number of pulses connected to a particular address reaches a certain quantity, this IP address is processed as a malicious one. It will be blocked through a separate connector to firewalls by adding the address to the list of malicious entities to prevent the spread of cyber threats till the SOAR user decides which measures should be taken.

In addition to standard e-mail notifications, Defensys team has also set up notifications through messengers. This helps System's users to be aware of a current situation any time and to rapidly take actions, when needed.

## Results

The Defensys SOAR's implementation has significantly simplified the interaction between the outsourced SOC and responsible departments within the Timber company thanks to a well-established information exchange process. Users can easily find necessary information in one System, create reports in a visible form and quickly send them to the SOC.