Defensys

Mining company

Challenge

Before the project launch, the Company already had its SIEM system and the implemented Defensys SOAR. During this project, our target was to update the system for cybersecurity compliance with the national state standards.

Implementation

The SOAR is used for handling both IT and OT incidents and is integrated with the company's CMDB.

Following purchasing of the new license, a part of the existing processes had to be reconsidered. According to the new role model, all company's network segments were divided into critical and non-critical. Depending on the segment status, the responsible department receives an incident notification and gets involved in its processing.

After discussing of the new incident handling policy, Defensys modified asset cards to meet company's demands and created 60 response instructions. They're being automatically pulled into the incident card according to the certain incident parameters. Besides, these cards contain necessary fields for the cybersecurity authority notification and allow data mapping, when an incident occurs on the critical network segment.

The rich customization features of the Defensys SOAR made possible the notification of the cybersecurity authority in a report form by pushing a button.

All incidents in the company are categorized based on the state-approved hierarchy. Thanks to this, users can create reports and statistics regarding critical network segments available in the company.

The company is distributed by 6 branches across the country.

One of the top 50 mining companies worldwide.

› **20 000** employees

› **15** software users

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

🌐 www.defensys.com

Results

Due to the upgraded Defensys SOAR and performed customization works, the Mining company got a useful platform for incidents managing of critical and non-critical network segments together with a user-friendly notification tool. Now responsible employees can easily and quickly sum up information, prepare reports and send them to the governmental authority.