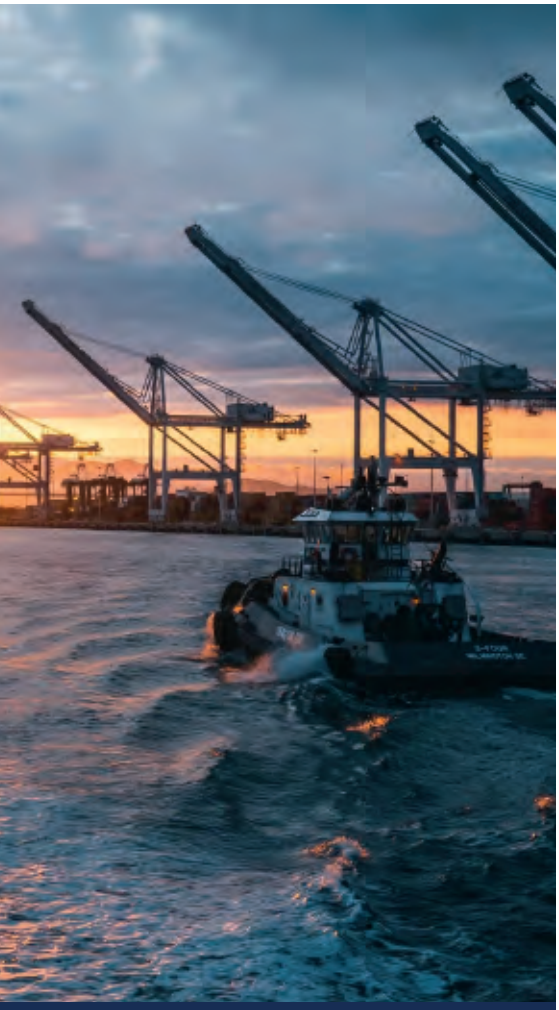
Defensys

Oil company



One of the top oil mining companies across the globe.

The company is distributed by more than 100 branches and owns several oil deposits.

› **20 000** employees

› **15** software users

Challenge

The Oil company has a colossal infrastructure and its SOC contains 3 response lines. Undoubtedly, a new system should have been customized and adapted to all internal processes. After the PoC project, for incident orchestration the Company has chosen the Defensys SOAR.

Implementation

The Company already had a plenty of installed systems, such as SIEM, CMDB and others. Of course, the SOAR had to be integrated with all of them. Therefore, Defensys successfully set up several connectors for incidents receipt and their enrichment. Much information is taken into SOAR from antivirus and AD.

5 standard response playbooks were offered to the Company. To meet shifts in demand, some playbooks were upgraded and completely automatized. After incident detection, several responsible departments now immediately receive tasks via integrated Service Desk system. Each task contains necessary fields in question-and-answer form. The user chooses "fulfilled" or "not fulfilled" in the answer field depending on the process steps. When SOAR receives requested information back, the scenario changes according to the results without any human intervention. For instance, after the answers review, a particular switch port can be automatically turned off in the company's large infrastructure. To put the idea into practice, Defensys engineers prepared a customized entity to keep the track of all network segments and implemented this up-to-date list in the response procedure to find the exact port and disable or enable it when needed. Meanwhile, the computer that is switched off the segment, it's still functioning.

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

Results

Thanks to the flexibility of the SOAR, the Company has been able to reach targets and automate incident handling processes as much as possible. By leveraging modified algorithms, the Platform can make decisions independently and significantly reduce the company's risks and save a very valuable time. After the latest tests and full launch of the system, Defensys has received a lot of positive feedback from satisfied users, who no longer need to manually search for detailed incident information, the host where it's registered and start processing in a very short time.