Machine factory

The factory produces unique goods and was struggling with APT attacks before the TOP management decided to build a comprehensive and effective cybersecurity system.

> 4 000 employees

> 10 employees use the Defensys ecosystem

Challenge

The Factory has purchased step by step all Defensys products: SOAR, Security GRC, Threat Intelligence, SENSE and Threat Deception platforms. As a part of large project on software installation and customization, our target was to build an ecosystem based on Defensys software which will cover all cybersecurity needs of the factory.

Implementation

Since each company has its own internal procedures, Defensys takes into account all customer requests and adapts software to specific requirements. The factory has 5 types of incidents to be detected, so there were tailored 5 SOAR playbooks that utilize different connectors during the response and investigation processes.

The company stored most of the assets data in a SIEM system and all incidents for further processing are being taken from the SIEM too. Besides, it's connected with AD and antivirus solution.

At the moment, by using Defensys software, the company can do the following:

- Control brute force attacks and withstand malware campaigns (SOAR)
- Conduct assets inventory without agents (SOAR)
- Identify unnatural infrastructure behavior (SENSE)
- Identify indicators of compromise inside the corporate network and respond rapidly before the cyber incident occurs (SIEM-sensor feature of the Defensys TIP)

The factory has highly appreciated TDP as an up-to-date platform to enhance the state of cybersecurity and actively generates traps and lures in its subnets.

The SGRC is used at the factory for conducting regular audits according to the legislation. The most of the time saved after the SGRC implementation is related to the feature of automatic reports creation after all the requirements are assessed by involved colleagues.

Results

The factory is still in process of implementing SIEM and not all sources are integrated with SIEM yet. Not all the security tools are implemented as well.

But using the Defensys ecosystem of cybersecurity technologies the Factory's cybersecurity team unified the approach in dealing with different CS routine. Everybody works from a single console, and the CISO manages the whole process much more effectively than it was done before.

Automatically drawn by the System performance metrics help to speak the same language with stakeholders when, for example, it comes to extending security budget as a result of some new business initiative.

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