Case study / Telecommunication Operator

Defensys

# Telecommunication Operator

Well-known Telecommunication Operator in the county. Provides mobile communication and Internet services.

- 25 years of business
- 50 million customers
- 10 tenants
- 5 companies in the holding

## Challenge

The Telecommunication Operator, a company with multiple subsidiaries across the country, needed a solution for automation of cyber security processes in the SOCs.
The Company demanded a lot of integrations with internal systems, easy access to information regarding all branches and multiple tools for information handling from software vendors.

The Operator chose Defensys products after a PoC project during which Defensys demonstrated the required functionality of software and additional managing options.

Among all Defensys products, the Company has purchased the SOAR, SGRC and TI platforms.

## Implementation

Defensys has a great experience in working with companies, that provide different mobile services. That's why we managed to avoid typical pitfalls and could concentrate on important tasks.

As mentioned above, Defensys software had to be integrated with several systems for data collection and transfer between tenants and the HQ according to certain attributes. Generally, the software was integrated with more than 40 systems with various functionalities.

Along with standard integrations (AD, antivirus, scanners), the Defensys SOAR was connected to the Company's internal system, that collects data regarding all user accounts and their unique numbers. Each account is stored as a customized asset and has a status. Depending on it, a certain scenario had to be started, for example, user account must be blocked for a short period of time. IT department receives a daily report with the list of failed scenarios, which is created based on accounts' statuses. Thanks to this, responsible departments can quickly monitor all accounts and start incident handling.

All incidents are distributed among SOCs' employees based on the duty schedule and the number of tasks of each SOC

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.

specialist at the moment. The schedule is generated in the Defensys SOAR with consideration of time zones, employees' vacations etc.

Besides, the Defensys SOAR can enrich information regarding internal breakers. Every time an employee is confirmed as an incident participant this information is stored in asset card and the incident is linked to the card too. Afterwards, during investigations employees involved in several incidents can be penalized.

As a further step, Defensys's engineers have developed a mechanism to monitor the coverage area of DLP systems, check compliance with the Company's policies and manage agents' efficiency. Defensys has set up a customized dashboard, that clearly presents the state of DLP systems, highlights issues with agents on hosts and aims at a fast problem solving.

2 systems are used as incident sources: SIEM system and a platform, that collects all customers' incidents. The Defensys SOAR receives all correlated events, saves data in necessary fields, and then incidents are prioritized according to the criticality level. Two factors play an important role for categorization: expert review from the MITRE ATT&CK® database and reference/absence of reference of the incident to a special privileged group. Considering all the information above the incident is assigned a score (rating). Depending on the rating incident card changes and provides customized fields with additional data.

During investigation a host can be isolated to prevent further spread. It can be unlocked in the infrastructure after the incident closure.

Software users are able to follow all update processes step by step. Incident card contains information regarding sequence of updates on certain hosts. In case of bad results, responsible employees can quickly check, which processes have failed, and solve the problem.

The Telecommunication Operator has a large infrastructure and a huge number of employees and users, that's why a lot of informational systems have to be constantly monitored. The SOAR platform can track statuses of different users accounts in several systems and notify users of expired passwords, locked accounts etc. For each case a service incident is created with a full description. That leads to a better control over the entire system's security.

Defensys

✉ sales@defensys.com

defensys.com

Moreover, the process of vulnerabilities management was successfully built due to the integration with implemented scanners.

A customized graph shows the number of incidents coming from a SIEM system, so users can notice a rush increase or absence of incidents in a few moments. The analytics is an important part for avoiding anomalies and program failures.

Consequently, updated reports together with advanced analytics now help Defesys's users to manage controls and monitor results in the most effective way.

As for the SGRC, the Company has a separate department responsible for audits conducting. Along with standard SGRC functions, Defensys's engineers created customized audits related to security profiles, installed check-lists for audits according to internal Operator's policies. Defensys's provided out-of-the-box methods of risk assessment, that fully complied with the Customer's requirements and the Company actively uses them along with advanced analytics for processes automation.

Before the Operator purchased the Defensys TIP, the Company's employees entered the all data into a separate document, the process was very time-consuming, especially during analysis. Now the TIP collects IoCs from multiple security feeds and consolidates them in one database. The software searches for IoCs through integration with several SIEM system nodes and performs retrospective analysis. All data is collected automatically in a convenient format and the Telecommunication Operator saves valuable time of SOCs' engineers.

## Results

Before the purchase of Defensys software the Operator had to fulfill a lot of tasks manually, that caused a lot of work and led to mistakes. After the Defensys implementation information from the entire Company's infrastructure could be consolidated and enriched automatically, response time was shortened and the state of defense systems could be checked much faster.