Defensys

Bank

About company

A big Financial Organization for legal entities and individuals.

The network of bank offices covers 49 cities.

- > 3000 employees
- > 3 million customers

Challenge

The Bank combines a variety of solutions and services for collection and analysis of cybersecurity alerts. To make the incident response process more efficient the bank needed an advanced tool which would allow to relate incident alerts to assets and users, automatically assign tasks to members of the cybersecurity department team, automatically collect context and additional data from multiple sources and automate security operations. The implemented automation had to accelerate incident response and help to minimize the potential damage to the bank.

Key Requirements

- Incident response automation
- Automated collection of additional information
- Automated task assignment and management for the employees
- Automated vulnerability management process

Defensys products

PoC for Defensys SOAR lasted for a quite long time comparing to the average period of testing Defensys products and proved all the features of the cybersecurity management platform which combines Defensys SOAR and Defensys SGRC products to cope with the tasks.

All critical assets were discovered and structured in the Defensys platform during the testing period. Tight integration with security tools in use and external monitoring services was configured.

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

Implementation

By the time of the formal implementation the Bank had a ready-to-use information security management center based on Defensys platform. Each incoming security alert was recorded in one single, centralized database with automatic indication of its criticality and related assets and users. Preconfigured playbooks automatically ran, specifying algorithms and the required operations for the cybersecurity team. A big variety of technical scripts were executed helping to get aggregated incident analytics.

Now the Defensys platform stores information about all completed actions during the incident response process, enables information sharing with trusted parties and automatically generates reports.

There is a set of control checks for all assets for compliance control with key cybersecurity standards as well. Based on the data about these control checks the Defensys SGRC generates cybersecurity related Key Risk Indicators (KRI) metrics for management.

Vulnerabilities imported from the scanner are automatically prioritized and then the Defensys platform generates tickets in the ServiceDesk system for IT personnel and draws the needed metrics.

Results

The Bank strengthened the security of information assets and accelerated incident response through the use of Defensys products. It helped to save time of the cybersecurity team for performing another crucial tasks.