Defensys

Managed security service provider

Each commercial SOC and MSSP organizes its own internal processes to provide premium service with the possibility of scaling and effective use of resources in mind. One of the key points is the choice of a platform which can eliminate manual processes and speed up incident monitoring and response.

› 1 800 employees

› 1 000 implemented projects annually

Challenge

The Computer Security Incident Response Team of MSSP, was facing a typical for a MSSP challenge of choosing the right SOAR platform for automation of their internal incident management processes.

Key requirements

While choosing the product the company looked at several criteria with the following key requirements:

- ✓ MSSP-ready product with all necessary functions in place for delivering high-speed incident response service
- ✓ High quality and reliability
- ✓ Minimum resources required for product maintenance and support
- ✓ A mature development team and responsive first line technical support helping to adapt the product to their needs

The managed security service provider team selected 6 SOAR products for initial comparison 4 of which were tested during the pilot projects.

After comparative analysis and testing, the team selected Defensys SOAR platform.

The specifics of the MSSP

The MSSP has 3 Tiers for incident monitoring working 24/7 with separate response and maintenance groups, forensic, threat hunting and other experts. The whole team follows one single integrated workflow that regulates the incident management process and specifies tasks for each team member at certain stage. This automated workflow includes

140 playbooks covering more than 100 scenarios of threat detection.

The provider offers both on-site and on-premise service models to customers. Cloud access to security tools and SIEM is provided by subscription. The on-premise model comprises incident monitoring and response using the SIEM and security systems deployed within the customer's infrastructure. Defensys SOAR is integrated with all types of SIEMs that customers of the MSSP may have and enables incident processing for both service models.

First, MSSP team re-designed their internal processes, specified the procedure of incident management and playbooks according to the adopted internal regulations. At the same time, they started testing and customizing the SOAR system, validating the newly established processes.

The whole project took about 9 months, including three months for deployment of Defensys SOAR. During this time certain MSSP-specific features were added to the product, integrations with other solutions were set up and the necessary reports and metrics were adjusted. As a result, the MSSP completely automated its' incident monitoring and response workflow with Defensys SOAR platform and maximized its efficiency.

Results

The Defensys SOAR platform allowed to increase the speed of incident processing up to 3 times.

The efficiency of the Tier 1 analysts increased 4 times thanks to the automated collection and enrichment of data, triage and routing of incidents. Defensys SOAR controls SLA on-the-fly, helping MSSP to observe strict service level to customers: 25 minutes to response to highly critical incidents, another 45 minutes for basic analysis and customer notification, and additional 60 minutes for technical response. The product provides integrated statistics and reporting, which is used for internal needs of the MSSP team and delivered to customers.

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