Defensys

Government entity

The government entity that operates with a lot of city services.

There are 2 SOCs that operate with incidents in the infrastructure and with information systems incidents (application and user levels).

Systems of this government organization have millions of users.

Also, this organization acts like an MSSP for other government entities that want some cybersecurity services to be outsourced to them.

› 2 000 employees

› 35 million customers people visits customer's resources monthly

Challenge

Most of the SOC analysts' time was spent daily for manual prioritizing security alerts from the SIEM and then for manually generating IT tickets in SD. Between these two big processes were chaotic enquiries for colleagues to find out what equipment was involved in incidents and numerous attempts to reactively respond to these incidents.

There literally was no time for something else in terms of cybersecurity needs of the Organization.

When a new organization wanted to use SOC services, all the generated data during this process was stored in different shared folders and electronic documents. It was a great challenge to combine the whole picture of how the interaction with this specific organization was handled. Plus, there was a demand to keep the control not only of IT assets, but also cameras, physical control points, USB tokens and fetch them with the IT asset model.

Results

There is a structure of playbooks designed for every type of registered incidents and implemented in SOAR. All the correlation rules of the SIEM alert to the SOAR, where everything is instantly mapped and labeled with MITRE ATT&ACK tactics and technics.

There is a main playbook that contains subplaybooks that are launched depending on the conditions that are gathered during the playbook execution.

One of the must have enhancements compared to the previous incident handling process was the ability to alert about incidents in messenger + the ability to control the response playbook via chat bot in the messenger. And it was automated using one of the Defensys SOAR connectors.

Of course, there appeared the automation of the ticket generation in the IT Service desk.

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

There are 20 SOC users working in Defensys SOAR daily.

Besides all the needed data is aggregated from SIEM system and AV solution. Additional connectors can be launched if there is a demand for some enrichment from external systems. These procedures are also prepared to be used in the playbook. For instance users occasionally manage the AV solution scan queue via Defensys SOAR.

Corporate users can be blocked/unblocked via connector to the PAM and IDM systems.

Connector to the Application Firewall helps the customer with instant fetching consumer's request about the portal with internal servers supporting some specific service and vice versa.

All the controlled entities are kept in the SOAR in Multitenancy mode so the customer can be sure that nothing from one specific organization can be mixed with other non-related data.

Another important case of using the SOAR is the automation of Vulnerability Management process. When the system is integrated with VM scanner, with a system that shows the reachability of some of the vulnerabilities and with list of assets (services) with their criticality, all this data is used by Defensys SOAR to automatically calculate the final score of every found vulnerability and then this information is distributed to IT department via automatically generated SD tickets.

So this is how the process that usually took a lot of time for SOC specialists is now conveniently represented on the side of Defensys SOAR. Users just control the needed metrics and read reports that SOAR delivers based on the customized schedule.

In the process of adding new organizations to the SOC Defensys SGRC solution was implemented for keeping all the third party audits in one place linking them with the organization's assets collecting during the response procedures. With multitenancy mode switched on the customer can control internal compliance campaigns along with third party audits in one system. User Access is granted by the system based on the built-in role model.

Defensys platform is used for asset management challenges as well. During the implementation was designed the lifecycle of assets with status model and all the needed workflows.