Telecommunication Operator

About company

Large Telecommunication Operator with regional hubs (including cybersecurity hubs) in different time zones

› 30 000 employees

› 70 million customers

Challenge

With 5 independent regional SOCs connected to the main SOC in HQ the Company's cybersecurity staff had to register incidents in service desk, that wasn't connected to an IT SD but all the other data needed for the investigation was manually collected from multiple sources: security tools, data lakes, billing systems.

Also, it was quite difficult to quickly find properties of the technical equipment involved in the cyber incident.

Threat Intelligence data was processed semi-automatically without any connections to other systems.

Defensys products

After a comprehensive procedure of comparing different technologies for building the next version of SOC the Company have chosen Defensys as a leader in automating cybersecurity processes. The decision was to use SOAR and TIP to enhance capabilities of an existing SOC with a lot of systems not connected with each other.

Results

All the incidents from different security tools along with customers' enquiries are processed in one system that helps to use the same investigation frameworks for different teams that is important when it comes to collect performance metrics.

These incidents are automatically registered based on the MITRE ATT&CK framework so the whole team operates with the same terms when working during the response process.

Every system needed to properly respond to the incident is integrated with the SOAR:

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

- Mail servers
- SIEM systems
- CMDB systems – with the ability to merge data with the information collected from AV tools, VM scanners and Defensys's inventory engine
- Data lake
- Active Directory with the ability to tune users' rights in the domain directly from the SOAR
- Antivirus Tool
- Billing System
- Customers' enquiries database
- And many others (almost 50 connectors were used during the implementation process)

Now a team of 50 security analysts operates with automatically generated response playbooks that use the Defensys TIP to enrich incidents cards with the most useful context.

Threat Intelligence Data is aggregated from multiple sources without any duplicate information. Then it's enriched automatically from external services and available for using by SOAR playbooks. Also SOC team uses SIEM sensors developed on the side of Defensys TIP to search for IoCs in raw logs collected by the SIEM. This is a perfect way not to load SIEM with this extra task. When an IoC is found, a new incident is automatically created in SOAR with the specified playbook launched to rapidly respond on this case.

SOAR helps to monitor the performance of SOC and draw metrics for top management as well as using dashboards and report builders.

These two products covered above helped to drastically reduce the time spent for the investigation process, especially for the technical routine part.

Further plans of the company include the implementation of other products of the Defensys's ecosystem: SGRC, SENSE and TDP.