Defensys

The Bank

The financial organization with wide range of subsidiaries around the world.

› 19 000 employees

› 5 million customers

Challenge

The bank has implemented the Service Desk solution. However, there was insufficient interaction with other systems, in particular, there was no interaction with TI tools and repositories.

The Bank wanted a comprehensive system overhaul and one of the key decisions in the global cybersecurity overhaul was the Defensys SOAR solution.

Results

Thanks to Defensys's technologies, a number of key issues were resolved:

- ✓ Daily delivery of IoCs is now a process. The integration of Defensys SOAR with already existed TI system was set up, which generates files with new indicators every day. Special playbooks in the SOAR work frequently and pour these IoCs into information security tools. For example, Proxy and IDS systems update their block lists automatically due to this kind of automation.

- ✓ The implementation of the SOAR allows now the IoC – TI system data transfer while incidents investigation. A Bank's TI system forms a daily file after some time, which is picked up by the Defensys SOAR and delivered to security tools. If it is necessary to urgently block the indicator of compromise, Defensys SOAR delivers it directly, bypassing TI system.

- ✓ Integration with antivirus solution was configured just to orchestrate this procedure when for example some number of scans is required as the last stage of some response playbook.

- ✓ Setting up integration with the SMS gateway. If there are incidents and they are critical (depending on the

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

🌐 defensys.com

criticality of hosts that are imported from the Service Desk), then the connector to the SMS gateway sends a pool of phone numbers and sends SMS messages with notifications.

- ✓ The case with the granting of rights was solved. The Bank has the first line of SOC , its second line, branches, respectively, it was necessary to make sure that certain people or branches could not edit any fields in cards of incidents and assets.
- ✓ SLA metrics. There are counters that control the delay at one stage or another, and then this data is displayed on a chart sorted by people, line, status.
- ✓ Dashboards are displayed on big screens in the SOC room. Some number of them are distributed in the CISO's account of Defensys SOAR