atarlabs

CASE STUDY

Social Security Institution Started using **ATAR**® in the Security Operation Center

SGK SOSYAL GÜVENLİK KURUMU | ATAR SSI SOC SOLUTIONS

Overview

SSI SOC Requirements

To strengthen the cyber security infrastructure in the Social Security Institution and bridge the employment gap in SOC, a SOAR software is required.

ATAR Solutions

With ATAR, the existing security tools were integrated to communicate with each other. The interconnection of existing technologies helped the institution decrease investigation and response time. Repetitive tasks and time-consuming mechanical work were offloaded to ATAR automation and the SOC staff spent their time on complex correlations.

The Achievements of SSI with ATAR

Investigation and response to an incident has been reduced from a few hours to a few seconds. The task performed by 9.5 men/day by the SOC staff was transferred to ATAR with orchestration, automation and response. The rate of return of ATAR SSI SOC investment has been calculated on less than one year.

Social Security Institution (SSI) is a public institution that implements social security systems for the citizens of the Republic of Turkey. SSI is responsible for the development and implementation of all social security policies in Turkey and provides services to both natural and legal persons by means of compulsory insurance.

SSI exchanges data with various institutions to perform operations for millions of employers, thousands of pharmacies and hospitals as well as 80 million citizens. It receives data from 43 institutions while it provides data to 112 institutions. SSI has 28K local clients abroad with remote access to over 500 web services. More than 50 million transactions are carried out daily in the headquarters.

SSI established the Security Operation Center (SOC) in 2016 to protect the institution's critical data, information and infrastructure from potential cyber threats and attacks.

In SSI's SOC, the intensity of the alerts is usually high on days and at hours when the number of staff is relatively low. The average number of alerts/correlations that SSI faces on a monthly basis is around 16,000. In order to not miss any incident, SOC operates with over 100 devices from 20 different vendors. The number of analysts required for incident management is more than the resources allocated by SSI. In order to overcome the challenges in SSI SOC and increase efficiency, SSI began using ATAR in January 2018.

atarlabs

CASE STUDY

ATAR Solutions for SSI Security Operation Center

ATAR increased the analyst efficiency with orchestration in SSI SOC. Instead of switching screens and logging in/out of these tools, ATAR provided SOC staff a unified investigations interface to command and control from a single pane of glass. ATAR incident management desk's one-click evidence collection and actions decreased individual investigations from several hours to a few minutes.

ATAR is fed by three alert sources in SSI SOC. The alerts from these sources are examined by ATAR incident management desk and repetitive activities were offloaded to ATAR automation with pre-defined playbooks, resulting in increased efficiency of the SOC staff. ATAR service desk allows collaboration and teamwork, enhancing the overall performance of the SOC team. All tasks performed in the SOC are recorded by ATAR, with executive summaries and reports being created on a daily basis.

SSI Chief Information Security Officer, Dr. Yenal Arslan, placed emphasis on the contribution of ATAR to SSI SOC as follows: ***"There are many features that bring ATAR to the foreground among other SOARs, but as a CISO, the most important feature for me is that when we receive an incident at 3:00 a.m., ATAR takes the action to the incident no more than 3:01 a.m. This is priceless."***

Improvement of SSI Security Operation Processes by ATAR

SSI Chief Information Security Officer, Dr. Yenal Arslan, placed emphasis on the contribution of ATAR to SSI SOC as follows: "There are many features that bring ATAR to the foreground among other SOARs, but as a CISO, the most important feature for me is that when we receive an incident at 3:00 a.m., ATAR takes the action to the incident no more than 3:01 a.m. This is priceless."

ATAR has shortened the response time to incidents; more than 300K automatic actions were taken by ATAR with the integration of more than 20 different security devices by orchestrating and transferring the repetitive ones to automation, resulting in enhanced SSI SOC team performance and reduced response time. This corresponds to the work performed by 9.5 men in one year. Therefore, the cyber security employment gap, one of the institution's most significant problems, has been reduced and the efficiency of the SOC has been increased.

ATAR compensated the investment cost of the one performed in January 2018 in a couple of months and provided SSI data security and better SOC process management.