Retail company

One of the leading retailers in the country selling food products under several brands.

The Company's shares are traded on several stock exchanges.

› 25 years on the market

› 15 000 shops across the country

› 200 000 employees

Challenge

The Company's cyber security specialists have been actively using Threat Intelligence tools in their daily routine for a long time. Nevertheless, the necessity to change the existing solution to another one arose due to new internal policies. Since the specialists had a lot of experience with TI, there were high demands for a new on-premises system.

It was especially important for the client to choose an alternative analogue with functionality and performance that would not be inferior to capabilities of the used platform. The second criterion was the ability to connect previously used feeds and integrate the software into existing systems.

At the same time, the transition had to be implemented without disrupting of the running processes for collecting forensic information, which is then used in incident response and retrospective data analysis.

After a range of demonstrations and a PoC project the Retailer has concluded, that the Defensys TIP platform meets all the requirements.

Implementation

Defensys's engineers have connected more than 15 commercial and open-source data sources (feeds) that provide IoCs and additional TI context. One more data source was the vendor's own Threat Feed, which automatically extracts IoCs and related context from TI reports. An important feature is the ability to parse data from open-source feeds without using regular expressions, which makes the process very convenient.

For more complete information regarding threats, the Defensys has set up support for IoCs enrichment services, which allow the platform to receive additional context not only about IoCs, but also about their relationships, vulnerabilities and related malware.

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

www.defensys.com

One of the key requirements was data reception about hackers' techniques and tactics from the knowledge base MITRE. Since the Defensys TIP had already been integrated with the MITRE ATT&CK®, the issue was quickly resolved.

One more advantage of the Defensys TIP is the data model, where work is being done at all levels of the Pyramid of Pain by David J. Bianco: from IoCs related to IP addresses, hashes, domains to techniques and tactics that use these groupings.

In turn, the integration of the Defensys TIP with the Company's SIEM system allowed analysts to automatically search for the IoCs in security events.

Moreover, the Retailer highly appreciated the TIP's new functionality: users can create security bulletins summarizing current cyber threats, use effectiveness analytics of feed source and indicator model ratings - indicator danger score, that TI analysts use to define the most dangerous and relevant IoCs.

Results

Thanks to the Defensys TIP's flexibility, the product implementation was realized in record time of just 1.5 months, and the process of adapting was as seamless as possible for users.

The new platform enabled the Company to manage its TI processes more efficiently through enhanced functionality.

As a result, the Company has a platform that allows it to gather all the necessary context about potential threats in one place and provides extensive opportunities to automate actions with the available data.