Case Study: Luxmed

With over 20 years of history, Luxmed is an absolute leader in the health sector in Poland, owning the largest network of private medical clinics in the country, while being part of a large international organization.

On a daily base, they process over 1 terabyte of data from their IT environment, collecting information from their servers, applications, networks, and medical devices.

In the past, their security department was using Splunk for ongoing security analysis and threat search, but due to the high license costs of the solution, they were able to cover only few percents of their actual needs.

Luxmed’s goal was to implement a central system for collecting logs from network devices, security systems and server infrastructure, which would serve as a source for other domain-specific security and infrastructure monitoring systems. After careful market analyses, their cyber security team selected the proposal of Energy Logserver, which covered most of the Customer's expectations:

- Flexible solution architecture
- Licensing not based on the amount of data entering the system
- The ability to integrate with the Splunk system through a dedicated application
- Ability to accept any data from the IT environment
- Extensive possibilities of visualization and analysis of large ranges of data

Due to the very high flexibility of adapting of Energy Logserver, the implemented solution not only covered Luxmed’s core needs, but managed to provide them with the same functionalities and correlation rules that were previously used in Splunk. The success of the implementation drew the attention of the department responsible for developing the application to the internal needs of the client. It was decided to migrate the open-source Elasticsearch environment to the Energy Logserver system and collect and analyses the performance data of the customer's applications within a single environment.

Because of the huge collection of critical data of the organization in one environment, we implemented data replication between the two data centers. Moreover, the data access was restricted according to a strictly defined policy.