ENERGY LOGSERVER

SUCCESS STORY

Customer: Poczta Polska S.A.

Poczta Polska

In 2020, Polish Post faced the challenge of finding a new SIEM supplier, responsible for the central collection, monitoring and analysis of the security incidents in the capital group.

The internal changes of the organization's structure demanded urgent investment in new IT solutions, and with the growing technology, there was a significant increase in the data that the systems produced. Therefore, an implementation of a new SIEM technology as well was a natural response to the growing needs.

The project team performed detailed study of the SIEM solutions available on the market, which followed with a series of meetings with representatives of the selected SIEM providers. Based on their experience with the existing solution they used in the past, the numerous interviews with the vendors, and the design assumptions, they summarised with a detailed description of the RFP.

Below are some of their key requirements:

- The system had to run in a distributed architecture with several log gathering points
- Central management of the entire cluster from the GUI
- System capacity ready to process an average of 60.000 EPS, while at the same time being prepared to carry a maximum load of 90,000 EPS
- Possibility of storing the online data for few months and archiving the offline data for few years with a built-in restoration mechanism.
- Ability to work for at least 30 simultaneous users.
- Flexibility in parsing various types of messages and the ability to easily parse new data.
- Possibility to configure the system with the Polish Post's own resources, without the participation of an integrator.
- No limits for connecting further data sources.
- The security of using the SIEM system is ensured by a precise system of access authorizations and by ensuring encryption of communication between the operator and the system and between system components.

The purchasing procedure resulted with selecting the Energy Logserver's SIEM solution offer. The presented proposal turned out to be more advantageous than the other offers provided by RSA, McAfee, Splunk and IBM Qradar.

At the implementation stage, it was confirmed that the Energy Logserver system fits excellent with the defined design requirements. The proposed architecture leaded to excellent performance of the system even in the case of creating very demanding queries or increasing the amount of indexed data. Energy Logserver's modern components and innovative features are providing an efficient working environment for the security department. Flexibility of the system provides relevant set of tools to constant development by adding and identifying new data sources while building precise correlation rules.

At the same time, it is worth emphasizing that the vendor is open to the ideas for the system development that we proposed.

In the last two years, we managed to ensure ourselves in the high quality of Energy Logserver's solution, which proved to be the right choice for us. The system works excellent as a central point of collecting security information for our security department, and at the same time, it gives us the comfort of developing conscious and elastic IT security strategies inside our organization.