LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Case Study - Telco Pro Services a.s., member of CEZ group

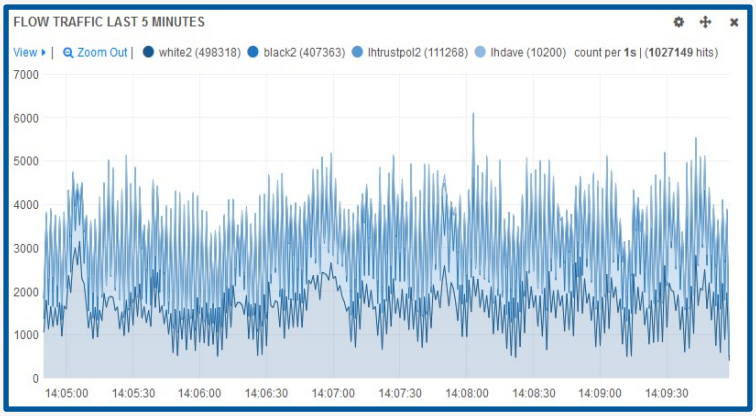
About customer

Telco Pro Services, a. s. is a telecommunication operator whose business activities focus on providing telecommunication services to customers in the Czech market, mostly CEZ Group companies. Its product portfolio includes both public e-communication services and customer-oriented services tailored to customers' individual requirements. Range of operations render company with significant market power on the telecommunication market. The company owns and operates extensive telecommunications systems forming a technical base for a wide range of voice and data services. A major part of them consists of telecommunications tailored for customers from the energy sector and used, among other things, for industrial systems providing support for dispatch control of electricity generation and distribution.

What customer solve?

Telco Pro Services, a. s. is a telecommunication operator having at its disposal extensive infrastructure based on both classic TDM data and voice service systems (PDH/SDH, a network of digital PBXs including transit exchanges) and advanced data networks built on a universal multi-service architecture platform (MPLS). It mainly provides the following services :

- Publicly accessible electronic communications services
- Data and voice services in corporate networks
- Data communications for control system operation
- Leased data circuits, services for operators and ISPs
- Control systems for the energy sector
- Administration of customer operated/owned technologies



LOGmanager was selected primarily to ensure compliance with Act No. 181/2014 Coll. and it serves as an asset supporting Critical IT Infrastructure (CII) assets operated by the company. Operational events data, which are sent to LOGmanager by the CII systems, are stored as operation logs, and the system further conveys the obtained data to a corporate SIEM solution. This ensures availability of operation logs required for analysis of cybersecurity events and incidents.

LOGmanager implementation in Telco Pro Services a.s.

The speed of deployment and the versatility of LOGmanager, a solution independent of infrastructure assets from which the data are obtained, allowed rapid deployment and extended coverage of the entire heterogeneous infrastructure. The customer had been testing this solution on a long-term basis and, as result of their positive experience with system operation and ease of use facilitated by an intuitive graphical interface, they decided to deploy the solution across their entire infrastructure. LOGmanager now fully covers the customer's needs to collect operational events data from telecommunications, security and ancillary systems. With a simple rule-based logic, the customer has been able to independently define event structures and rules for monitoring individual technologies, which enable notification about selected events requiring operator's attention.

Currently, the system is routinely used by the operational staff and by administrators of individual technologies, for which the rules for flagging selected events as well as customized dashboards and notification service have been developed based on their requirements. With LOGmanager's high performance, it is easy to find historical records about first occurrences of an event, retrieve related information from other infrastructural assets or search for additional context. Individual teams are able to use their own environments, such as systems for firewall management, monitoring of configuration changes to telecommunication assets, monitoring and status reporting of HW server platforms, AAA infrastructure management, and more.

CUSTOMER BENEFITS AND FEATURED VALUES

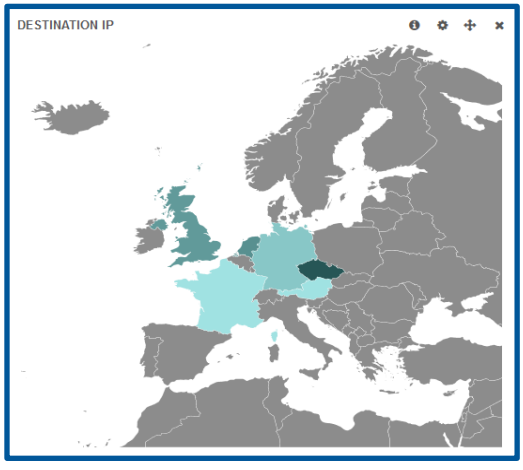
The system meets the specifications required to serve as a forensic data warehouse where data with more than one-year retention period are stored to support investigation of past events, or to serve as evidence during investigation of cybersecurity breaches and incidents. Due to its ability to guarantee data integrity and confidentiality, LOGmanager is used as a trusted source of information for securing evidence.

LOGmanager is operated as a supporting system shared by the individual CII assets and other operating environments. To enable operational deployment and to ensure compliance with Act No. 181/2014 Coll., the system has been developed to provide full-fledged operation log collection functionality without any license restrictions and it has been designed with performance, ease of use, and speed of deployment in mind. It provides a reliable environment for collecting operation logs from individual CII technologies and other operating communications systems of the company and it serves as a single point of collection and provision of information about operational events with sufficient capacity, performance and reliability.

LOGmanager has proven successful at Telco Pro Services a.s. to such an extent, that the company currently implements projects for development and extension of LOGmanager infrastructure to cover also back-up systems and other smaller dedicated installations in isolated parts of their communication infrastructure.

The following features are most appreciated:

- ⇒ Ease of use
- ⇒ Diagnostics of crashes or operational issues up to application level
- ⇒ Prediction and prevention of accidents, data security breaches, overview of unusual and suspicious transactions, accesses etc.
- ⇒ Possibility to monitor configuration changes by system operators
- ⇒ Diagnosis and resolution of security incidents
- ⇒ Tracking of access, user activities, fulfilment of SLAs, audit requirements, etc.
- ⇒ Securing of evidence for forensic analysis and investigation of incidents
- ⇒ Compliance monitoring and audit.



ABOUT THE MANUFACTURER AND CUSTOMER REFERENCES

LOGmanager has been developed since 2014 as a flagship product of Sirwisa a.s., a company based in Prague. By the release date of this case study, LOGmanager has had more than 130 satisfied customers and you can find selected customer references at www.logmanager.com. Our customers include not only government authorities but also businesses of all sizes from all sectors, business corporations, banking organizations and more. Do not hesitate to contact us for more detailed customer references directly from your area of business.