LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

# Case study - G.EN. GAZ Energia

## About customer

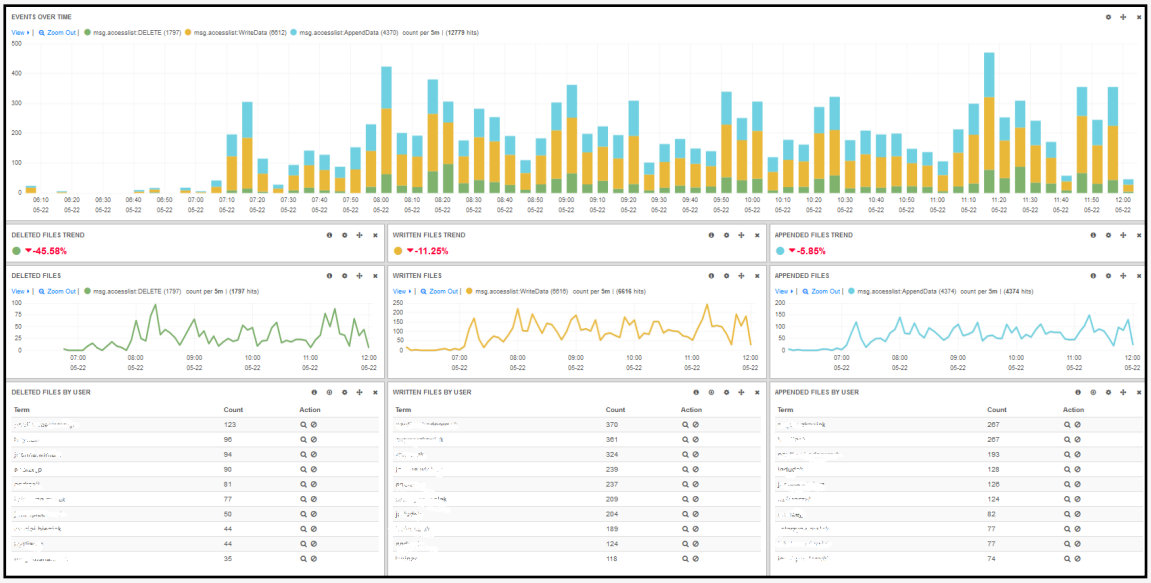
G.EN. GAZ ENERGIA Sp. z o.o. is the biggest private distributor of natural gas in Poland, covering an area of 87 Municipalities in 5 districts, with a base of around 40,000 clients and 1M MWh gas sold in 2019.

## Customer's challenge

Clients IT department was looking for a solution that would aggregate data from large distributed environment comprised of hundred of systems and would help with the analysis of security events coming from internal file systems. Client also wanted collected data to be stored without any possibility of modification. High efficiency, quick implementation process and no license restrictions were other assets considered by the client.

During 4 week PoC client positively assessed LOGmanager capabilities, ease of use, no license restriction and flexibility, allowing them to collect data from wide breadth of systems, which ultimately led to the purchase decision.

As an alternative, client considered purchasing the full SIEM solution, but after a detailed investigation, this kind of solutions proved to be inadequate, due to the complexity of usage and maintenance, as well as high license costs.



## LOGmanager implementation steps

**I. Phase**

During the Proof of Concept project phase, LOGmanager was implemented to a demo box delivered to the client. The Goal of the PoC was to verify LOGmanager capabilities in the context of client needs and do the proper sizing of the solution.

**II. Phase**

During the second phase, LOGmanager platform was configured to present clients data in custom made dashboards tailored to their needs. Alerts had been created for high severity security events, such as high volume of file deletions in short time-frame. Additionally, client asked for configuration of scheduled reports informing about user access to sensitive files.

**III. Phase**

PoC outcome was positive and client decided to purchase LOGmanager-M platform. Apart from capabilities tested during PoC, implementation service also included configuration of Windows and VMware sources. Creation of additional security alerts revolving around user accounts, such as changing account configurations or multiple failed logins.

# CLIENT BENEFITS

LOGmanager completely fulfilled client requirements. Thanks to professional approach and ongoing support delivered by Advatech (LOGmanager certified partner), platform was implemented fast and seamlessly, without any interference to production environment.

Currently, client is using LOGmanager to monitor their infrastructure (VMware/Windows/Network) and to solve day to day operational and security issues. Most used capabilities include collecting, analyzing and reporting user activities on important files, quick search and filtering operational data (such as system state) required for various issue solving and automatic alerting on detection of defined conditions inside logs (such as multiple failed login attempts).

## Client appreciates:

⇒ Easy PoC, fast implementation process and immediate readiness to process logs.
⇒ Easy access to file system events (who and when deleted/edited/copied data).
⇒ Support in systems diagnostics and resolving security incidents.
⇒ Security of stored data.
⇒ Support in solving day-to-day operational issues.
⇒ No license restrictions.
⇒ Transparency, high efficiency and radical simplicity.

## Client opinion:

*"Because to the constant lack of time due to the high workload, we were looking for the solution which would make our jobs easier, instead of complicating it. Competitive solutions, even though effective, didn't really follow this convention. LOGmanager perfectly addressed our needs – it's simple to use and maintain and at the same time has all the crucial functionalities."*

- Artur Lech, IT manager

# ABOUT THE MANUFACTURER

LOGmanager has been developed since 2014 as a flagship product of Sirwisa a.s., a company based in Prague. 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. We will be happy to provide contacts to existing customers, who have agreed to be included on our list of references.