LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

Case Study - Hospital Jihlava

About the Customer

Jihlava Hospital is a budgetary organization established by the Vysočina Region. As the largest hospital in the region, it employs more than 1,500 people. It is a catchment area hospital serving the population of approx. 200,000 and up to 500,000 in selected specializations. It offers 621 acute care beds, 75 aftercare beds and 10 beds for palliative care. The hospital is primarily responsible for provision of health care including outpatient and inpatient diagnostics, treatment, preventive care and pharmacy activities. In addition, it also carries out scientific research, educational and information activities, and other health care related activities.

Challenges Faced by the Customer

The ICT Department at Jihlava Hospital currently manages dozens of IT systems including thousands of diverse HW and SW components. In its procurement specifications, the customer requested ability to collect status information from the managed devices, in particular from security and networking elements, including retention of historical records. The key criterion was the performance of the solution and the offered data storage capacity. The customer preferred a domestic product with support in Czech. A great advantage of LOGmanager, reported already in the studies, was its favorable price. A large SIEM system is usually not suitable and affordable for an organization of this type. LOGmanager, on the other hand, provides an accessible solution and can be successfully “tendered” under a public procurement procedure.

Project scope and description

The customer placed biggest emphasis on improving the security of their IT network including all of its sub-systems. This was taken into account also during the implementation process. The installation of hardware took approximately 4–5 hours, after which the settings were defined according to the customer's requirements addressing first the firewalls and the network elements. After LOGmanager had been in operation for a month, the customer and the contractor collaborated on fine-tuning of the system. During implementation, the hospital became familiar with standardization of logs and alerts as these were gradually integrated into the solution. A number of unknown and hardly identifiable logs were discovered during implementation for which it was necessary to define appropriate rules to allow effective use of the information they contained. Deploying LOGmanager is an ongoing process constantly adapting to growing data traffic requirements (the volume of the customer's data grows by tens of GBs per day) and to the developments and changes of the IT environment. In Jihlava Hospital, LOGmanager proved to be an affordable and high-quality SW log management and SIEM solution.

Customer benefits and appreciated features

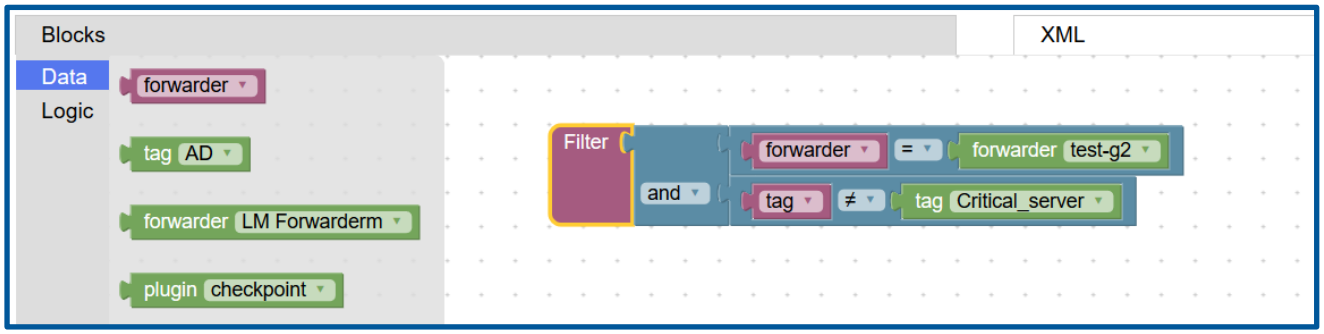
LOGmanager can be easily integrated into the existing operating environments to support collection of machine data from any source system in an organization. A very easy integration is one of the strengths of this product. Integration with various platforms provides an option to log (record) and present in an easy-to-follow graphical or text form events and logs from any network or active element, from security devices, operating systems or application software. The simplicity and ease of use of the solution allow to provide information and send alerts according to ICT administrators' requirements.

With its speed of log search and analysis, LOGmanager has perfectly met the client's expectations. The customer also appreciates the simplicity of system upgrades and access to Webinars providing information about changes and news and other technical information from LOGmanager creators.

Another benefit for the customer is full availability of logs from firewalls and network elements with long-term retention. By deploying LOGmanager, cases of compromised security were detected including DHCP server spoofing, cryptocurrency mining on networked devices, and so on.

What features are appreciated the most by Hospital Jihlava

- ⇒ Fast deployment
- ⇒ High performance, long retention of on-line data, simple back-up
- ⇒ Easy identification of root causes of system malfunctions based on machine data passed by the systems to LOGmanager
- ⇒ Near real-time identification of operational failures and issuing of automatic alerts
- ⇒ Customized queries, charts, reports, and dashboard views
- ⇒ Quick identification of events describing the cause of a particular issue, data loss, or communication failure
- ⇒ Source documentation for security audits
- ⇒ Option to limit access rights and filter data shown to non-privileged users (*see sample db rights policy in the screenshot below*)



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 140 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. This case study & LOGmanager certified partner is AUTOCONT a.s.