LOGmanager

> Central Log Repository
> Affordable SIEM

HELP TO RESOLVE CRITICAL IT INCIDENT

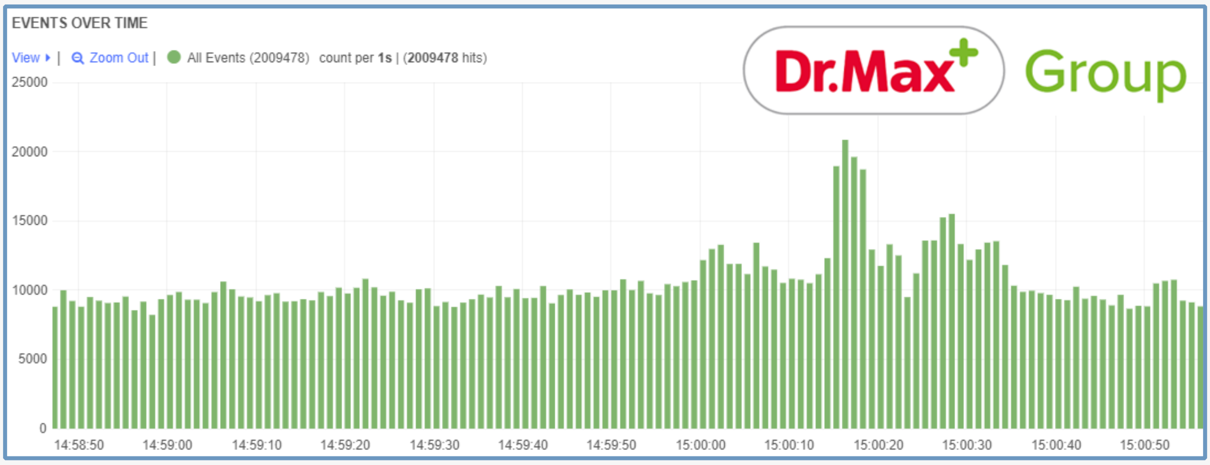
Case study - Dr.Max

About customer

The most accessible pharmacy chain in the Czech Republic is operated by Dr. Max. In the Czech Republic, the network comprises more than 400 pharmacies with more than 3,000 employees. Dr. Max Group is also present in 7 other European markets.

Customer's challenge

Dr. Max Group operates and administers a highly diverse IT environment that supports not only pharmacies but also warehousing operations as well as distribution, development and manufacture of medicines. It consists of multiple database systems and an extensive IT network. Each system generates a large amount of important machine data about its operation, status and administrator/user activities. Due to lack of centralized storage of logs, the customer found it extremely difficult to identify problems and also resolving them required a significant amount of time. This applied also to investigation of any suspected security breaches.
The customer wanted to unify the storage of logs using an external secured system in order to obtain a comprehensive overview of the security and operation of its IT systems. The customer wanted to implement a log repository supporting long-term storage of information that would be protected against tampering and would allow obtaining overview of the current status of the operated systems, accesses to individual applications, and to accurately track activities performed under privileged accounts. The repository had to be secured so that the collected data could not be deleted or otherwise modified. An additional requirement was that the chosen solution should not be bound by any license limitations such as a maximum number of events processed per time unit or maximum number of monitored devices and should allow processing really high number of events per second.



EVENTS OVER TIME

View ▸ | Zoom Out | ● All Events (2009478) count per 1s | (2009478 hits)

LOGmanager implementation steps

I. Phase

The objective of this phase was to verify the technical parameters of the solution and to adapt the data analysis environment accordingly. LOGmanager-M with a storage capacity of 12 TB was provided for testing purposes. During initial installation, Active Directory was set up for authentication of LOGmanager users. Devices for event collection were selected to verify the system performance, processing and analysis of stored data.

II. Phase

LOGmanager-XL with a 100 TB storage was supplied. This appliance was installed in the customer's data centre. The appliance was configured into a cluster with the equipment delivered in Phase I. After transferring the configuration and replicating all data, LOGmanager-M was deactivated and the equipment installed in the data centre was switched to production mode.

III. Phase

Selected applications and servers were configured to send logs to LOGmanager, which collects and stores them continuously. After the logs became available in LOGmanager, specific parsers were created. Due to extremely high number of events generated mainly by internal security elements, data processing had to be optimized. After optimization, LOGmanager receives and evaluates 10k events per second and is able to process up to 25k events per second at peak times, which often last for several hours. 250–350 GB of data are processed daily.

IV. Phase

Training was organized for administrators, IT support technicians, and the IT security staff focusing on how to use LOGmanager and how to create parsers. Several workshops were also held to address specific needs of each department.

CUSTOMER BENEFITS AND FEATURED VALUES

The system is primarily used by the IT security staff for supervision. The experience with the system's operation has shown that the solution can also become a very effective tool for IT support engineers and administrators responsible for individual applications or systems. The most frequently used functionalities include comprehensive retrieval and processing of user login events, the ability to quickly retrieve and filter necessary information from a huge number of logs, the ability to receive automatic notifications about any irregularities, and the ability to read logs from the operated network infrastructure including security devices.

Other benefits include also the possibility to further extend LOGmanager thanks to its open architecture, which enables easy creation of customized dashboards that capture necessary information, activities or situations. The customer also appreciates the ability to process logs from its proprietary applications by creating customized parsers.

Customer appreciate:

⇒ Rapid deployment including the initial verification of system functionality during pre-purchase tests and immediate use,
⇒ Correlation of logon/logoff events across the entire network infrastructure,
⇒ Analyzing user access to files and system resources,
⇒ Possibility to monitor configuration changes by administrators and system operators,
⇒ Quick diagnosis and resolution of security incidents,
⇒ Securing of evidence for forensic analysis and investigation of security incidents,
⇒ Accelerated troubleshooting,
⇒ Scalability from a centralized to a distributed solution on country level,
⇒ Open solution for easy integration of systems not directly supported by the vendor,
⇒ Unified and simple search across all types of data and devices,
⇒ Transparency and minimal operational requirements, high performance,
⇒ Fine settings of the access rights to stored data and useful approach to system authorizations.

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 160 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.