LOGmanager

> Central Log Repository
> Affordable SIEM

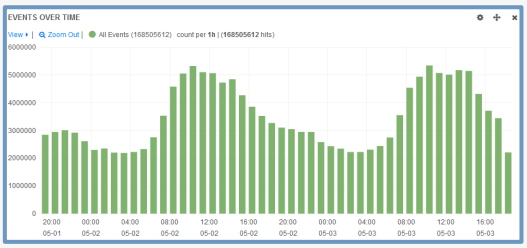
HELP TO RESOLVE CRITICAL IT INCIDENT

Case Study ČD Cargo a.s.

About the Customer

ČD Cargo a.s. ("ČDC") is the largest Czech rail freight carrier. ČDC is a subsidiary of the national carrier České dráhy, a.s. Both companies, together with other subsidiaries, belong to the ČD Group. ČD Cargo a.s. was established on 1 December, 2007 and employs 7,000 employees. It operates 859 locomotives and more than 24,000 freight wagons. In terms of volume of transported goods, it ranks among the five largest rail freight carriers in the European Union.

Challenges Faced by the Customer



The ICT environment in ČDC consists of many sub-systems including finance and accounting, operations, and technology sub-systems plus a number of applications with varying degrees of interdependence. Overall, it includes dozens of physical and virtual servers operated on platforms from leading manufacturers such as Microsoft, Oracle, SAP as well as open-source solutions. The majority of key applications are operated by ČDC's sister company. Some of the sub-systems are operated directly by ČDC using its own resources and assets while others are outsourced from external suppliers. ČDC does not own a large majority of the ICT infrastructure it uses. Mostly, it uses it as a service provided by its affiliate, ČD Telematika, a.s. Due to the complexity of the ICT infrastructure and the contractual relations between ČDC and its service providers, ČDC often lacked sufficient overview over the management and operations of the outsourced systems.

The customer requested to have the ability to use the stored logs for obtaining a comprehensive overview of the security and operational status of its ICT environment in order to be able to respond to emerging events and incidents and to have the ability to trace back information about activities and transactions affecting the data, user accounts and user privileges. The customer wanted to have a log repository supporting long-term storage of readily accessible 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 their parts, and to accurately surveil activities performed under privileged accounts. An additional requirement was that the chosen solution should not be bound any license limitations such as the maximum number of events processed per time unit or the maximum number of monitored devices. LOGmanager was selected as the winning solution.

In addition to centralization and long-term storage of logs from selected technologies and systems, ČDC also identified user accounts in individual identity repositories as the priority key area to be monitored and analyzed by LOGmanager in the initial stage of the project. Specifically, the customer's requirements were as follows:

Tracking and evaluation of SAP logs

- ⇒ Successful and unsuccessful user logon attempts
- ⇒ Key transactions
- ⇒ For accounts set up for ČDC employees and for external staff with access to a part of the ČDC system: account creation, account cancellation, role assignment, role removal

Tracking and evaluation of LDAP server logs

- ⇒ Successful and unsuccessful user logon attempts
- ⇒ Successful and unsuccessful sign in under privileged accounts (including supplier accounts)
- ⇒ For accounts set up: account creation, account cancellation, account activation, account deactivation, role assignment, role removal

HR and payroll applications

- ⇒ Successful and unsuccessful user logon attempts
- ⇒ Successful and unsuccessful sign in under privileged accounts (including supplier accounts)
- ⇒ Key personal data operations

Active Directory

- ⇒ Successful and unsuccessful user logon attempts
- ⇒ Successful and unsuccessful sign in under privileged accounts (including supplier accounts)
- ⇒ Key operations

PROJECT SCOPE AND DESCRIPTION

Phase I

LOGmanager appliances with a capacity of dozens of TBs for storing logs were delivered. These appliances were installed in the ČDC environment according to the provided address plan. In order to ensure high availability of a cluster consisting of two LOGmanager installations, the appliances were installed in two physically separate locations. Immediately after installation in the respective data centers, LOGmanager installations were configured into a cluster. Both appliances in the cluster are controlled via a single web interface. During the initial installation, the authentication of LOGmanager users was mapped to Active Directory.

Phase II

Selected applications and servers were configured to send logs to LOGmanager, which continuously collects and stores them. After the logs became available in LOGmanager, specific parsers were created. The parser acts as a "Translator", which means that it converts RAW data in native formats into a standardized format that can be readily searched and enables use of additional advanced features such as alerting, system behavior prediction, correlation, and reporting.

Phase III

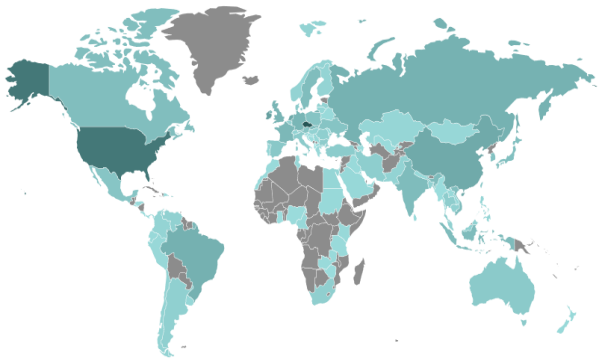
Training was organized for administrators, IT support team, and the IT security staff focusing on how to use system and create new parsers, alerts.

CUSTOMER BENEFITS AND APPRECIATED FEATURES

The system has met all customer's requirements. It serves primarily as a support tool for IT support technicians, administrators, and security management. However, its deployment does not end with the initial implementation. In the next steps, other applications and systems will be added that were not part of the initial project. This continuous expansion is possible thanks to the open design of LOGmanager, which makes it easy to create summary overviews for each system, activity or situation in the form of customized dashboards, or to further process logs from other applications using customized parsers. The LOGmanager system has been easily integrated into the existing complex and non-homogeneous ICT environment in ČDC. The customer highly appreciates comprehensive retrieval and processing of extended logs from Microsoft systems, 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 understand logs from the operated network infrastructure including security devices.

What features are appreciated the most by ČDC

- ⇒ Diagnostics of crashes or operational problems of individual applications in the ČDC ICT environment
- ⇒ Prediction and prevention of accidents, data security breaches, overview of unusual and suspicious transactions, accesses etc.
- ⇒ Possibility to monitor configuration changes by external and internal administrators and system operators
- ⇒ In terms of security and cyber security law, it ensures availability of auditable, tamper-proof logs generated by ČDC information system in a separate, independent repository. The logs can be used to monitor and evaluate operations performed by system users (both authorized and unauthorized)
- ⇒ Diagnosis and resolution of security incidents
- ⇒ Tracking of access, user activities, fulfilment of SLAs, audit requirements, etc.
- ⇒ There is evidence available for forensic analysis when investigating security 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. We will be happy to provide contacts to existing customers who have agreed to be included on our list of references.