SUCCESS STORY

MIMACOM
Digital. Innovation. Engineers.

360° view for the Bühler Group: Log management and monitoring for visibility, security and stability in the global corporate network

Source: Bühler Group

PROJECT DETAILS

Industry: mechanical engineering

Users: Security Team, Global Service Desk, Automation Team, Network Team, Infrastructure and Server Team, Consumer Services Team

Team: 1 Software Engineer, 1 Scrum Master

Development timeframe:
March to September 2020

TECHNOLOGIES USED

- Elastic Stack (Elastic Search, Elastic Beats, Logstash)
- Kibana
- Apache Kafka®
- rsyslog
- Java
- Spring Boot
- Jira, Confluence (Wiki)

mimacom's log service solution has created a backbone for IT security and availability of the IT infrastructure across the entire company of the internationally active Bühler Group.

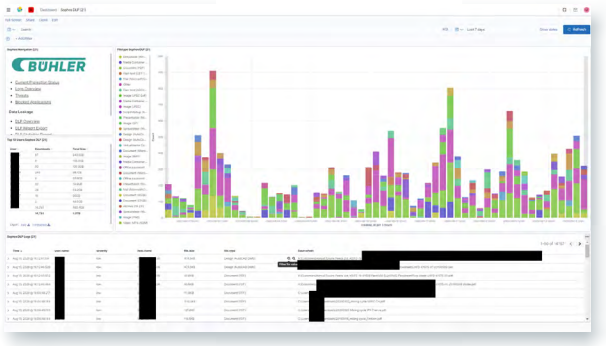
BÜHLER

For Bühler, IT security is a central factor in ensuring the success of the company. The Security Event Management and Incident (SIEM) solution provides group-wide transparency, helps to identify weak points and increases efficiency in the company.

> *mimacom already convinced us during the evaluation phase with the highest level of competence in the areas of Apache Kafka® and elastic. Our choice proved itself in the project. The cooperation has been cooperative and efficient – despite the difficult conditions caused by the pandemic. The log service designed and developed by mimacom was convincing in every respect.*
>
> **Thomas Wick,** Security Engineer, Bühler Group

Bühler Log-Service: Overview of the last 30 days

Background → The Buhler Group employs over 12,500 people and runs subsidiaries and production sites worldwide. The availability of resources around the clock is central to ensuring productivity. IT security on a global scale is a monumental task: hacker attacks, data misuse, or theft are omnipresent dangers for any industrial company. Bühler's design plans and innovation inventions are valuable and must therefore be protected against industrial espionage. This makes IT security and the associated goals of availability, confidentiality, and integrity a key factor for Bühler in ensuring the company's success.



Dashboard Bühler Log Service: Overview of the different file types with advanced filter options

SIEM & Data Lake: Control over BigData

The Bühler Group log service includes a Security Incident and Event Management (SIEM) and also serves as a data lake. It thus enables 360° transparency of logs and events across the Group. The log service collects information from a wide variety of sources in the heterogeneous IT environment of Bühler Group, processes it, and makes it available to the various user groups in near real-time on a dashboard (Kibana).

Many stakeholders, one solution: Multi-layered demands combined

For complex problems, the helpdesk can create a ticket for the 2nd level support directly from the system.

The **IT security team** can identify potential security issues in a timely manner and respond adequately before any damage occurs.

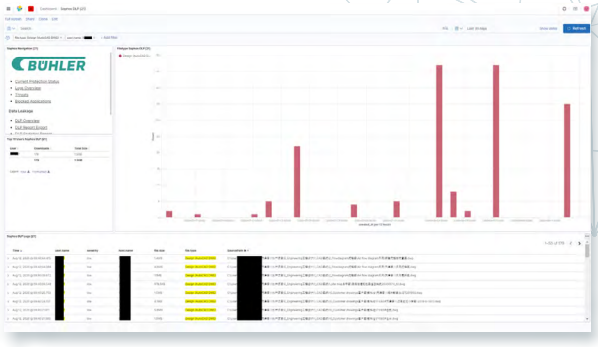
The **compliance and governance team** can more easily meet its objectives and successfully manage audits and certifications thanks to the central availability of all data.

The **network team** can analyze the behavior of over 500 network devices and has a troubleshooting tool.

The **automation team** can control and manage the access of the sensors of systems or virtual technologies that need access to certain network segments.

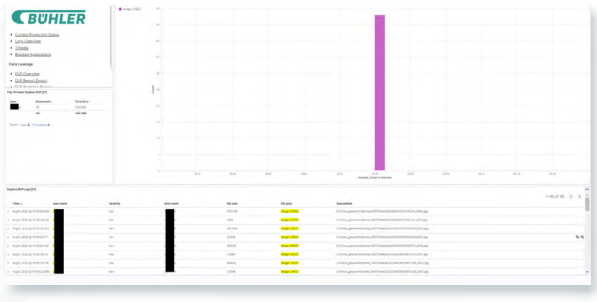
The **infrastructure team** can analyze logs when incidents arise and quickly resolve problems with Active Directory login.

The log service is used by the **customer care team** of the B2B portal **myBühler** to improve the customer experience.



Downloads of a specific user structured or filtered according to file types

Solution → With its agile project approach and extensive technological experience, mimacom created a high-performance log service with a clear dashboard for the Bühler Group in a very short time:



The Bühler Log Service is a highly available and scalable solution which, in addition to SIEM monitoring and alerting, covers a wide range of other requirements and increases productivity. Apache Kafka® serves as the data collector and Elasticsearch for processing the data. The solution is characterized by its easy extensibility and does not cause any additional operational overhead. The data collected by the log service is made available to employees according to the need-to-know principle and automatically destroyed – of course always in compliance with the GDPR guidelines and Bühler's internal security requirements.

Facts & Figures about the solution

Elastic stack in combination with Apache Kafka®

Evaluation → The technologies available for selection were Elastic's ELK stack in combination with Apache Kafka® or Splunk as an alternative. Based on a convincing presentation, optimal support during the selection process, and comprehensive know-how in the areas of Elastic and Apache Kafka®, Bühler decided to implement the log service dashboard with mimacom.

Conclusion & Outlook → mimacom's log service is an important component of Buhler's IT security. Not only does it contribute centrally to IT security at Bühler, but it also helps to increase efficiency on many levels within the company. In order to enable Buhler to implement simple adjustments without the help of mimacom, great importance was attached to the training of the personnel involved in the development of the project scope. Because the solution designed by mimacom is largely based on the standard Elastic stack, it can be easily extended by Bühler at any time or in collaboration with mimacom as a partner. erweiterbar.

> *The log service is a milestone in the Bühler Group's IT security. Numerous factors contributed to the success of the project: The technical know-how, the transparent communication, the Scrum approach, as well as the strong customer friendliness and motivation of the mimacom team. I can therefore warmly recommend mimacom as a partner for software projects.*
>
> **Thomas Wick,** Security Engineer, Bühler Group