Breaking down silos to enable log data collection on a central platform

Log management with archiving, analyzes and alerts as the basis for a SIEM

An IT infrastructure for 16 schools, 2 hospitals, 26 municipalities, 2 cities and an entire canton: KSD is the IT enterprise of the canton and city of Schaffhausen. The different client profiles entail varying requirements. terreActive implemented a solution that everyone could use.

Challenge: Breaking down silos

terreActive was familiar with the situation in public administration through experience: Their IT organizations are typically set up in silos (e.g. one team for basic services, one for network, etc.). The teams often use different tools for monitoring. While every silo has a good setup, they do not have any insight into the tools of the other departments. As soon as the systems are networked, dependencies are created that cannot be monitored.

KSD was fully aware of this. "We needed a central overview of all relevant systems in order to be able to react quickly in our heterogeneous environment," says Roger Speckert, Executive Board Member and Head of Infrastructure, Client Engineering & Security at KSD.

Goal: Central log management as the basis for monitoring to ensure secure operations

In future, central data collection and analyzes were to ensure long-term security as well as provide quick answers to problems – for example, if a server does not work or a subsystem suddenly slows down. To this end, silos had to be broken down and logs recorded centrally. This would allow data to be accessed by all of the teams based on access permissions. The overall picture could thus be monitored and targeted analyzes could be used to find problems.

Hybrid solution with tacLOM and Splunk

tacLOM, terreActive's monitoring software, was deployed. This tool offers a central platform for archiving, analyzes and alerts for log data. And tacLOM makes use of synergies from system monitoring, log management and log analyzes. Thus it makes a combination of passive and active monitoring possible.

tacLOM's license model is geared towards high volumes of data: Licenses are bought per system.

Splunk was also integrated and is used for automatic data compression. Through the hybrid solution with the targeted usage of tacLOM *and* Splunk, various tasks are carried out cost effectively while saving resources.

KSD

The canton and city of Schaffhausen's IT enterprise supports the canton, 2 cities, 26 municipalities, 2 hospitals and 16 schools with around 50 employees. This includes 2,200 IT workstations.

KSD provides the IT base and application infrastructure and ensures daily, safe operation using proven ICT technology.

www.ksd.ch

What the central platform offers

- A central solution supports analysis of errors across multiple teams.
- The inclusion of all KSD systems ensures a quick and proficient reaction.
- The heavy strain on administrators is reduced.
- Previously hidden correlations are made visible. Synergies can finally be used.
- System failures can be understood in detail so as to gain insights into how they can be avoided in future.

Providing more security:

- tacLOM monitoring software
- Splunk data analyzes
- Threat intelligence service
- Operational support 24/7 by terreActive in standby duty

The solution in detail

High storage capacity – real-time logging – available during system failures

The new centrally collected operational logs of the different components are recorded in real-time and saved for one year. This is unusually long for logs. They are usually erased quickly to save storage space.

The advantage: Saving logs over longer periods allows irregularities as well as system failures to be understood in detail. tacLOM saves the data as a copy so that all data of a system failure is available. This can be used to understand why failures take place and prevent them in future.

Understanding raw data and simplifying troubleshooting

tacLOM works with events and eventpacks when analyzing log data. An event is generated by the system based on specific log events.

The corresponding line in the log is saved for each event. In this way the raw data can be accessed quickly during the subsequent analysis.

The automatic compression of eventpacks makes troubleshooting much more simple as correlations become understandable for people outside the team.

Less maintenance work

A central event console and a standard alarm system facilitate active monitoring of log data and events.

The central data collection and monitoring also reduce maintenance work and operational costs.

Customized for the user

What used to be the realm of the administrator is now open for collaboration between the teams. Every user can customize the analyzes in line with their requirements. They can configure their personal view including the reports and dashboards.

Visualizations help the users in their day-to-day work. Access authorization can be adjusted to meet in-house standards. This was particularly important because KSD has to maintain high data privacy standards for their clients (for example, to protect the data of a municipality's citizens).

Outlook: Ready for the future

With the introduction of central log management, KSD is in a good position for the future because the new platform offers an ideal starting point for further security measures:

- Step-by-step setup and expansion of a security information and event monitoring solution (SIEM)
- Fulfilling compliance requirements
- Protection against cyber attacks