Deutscher Alpenverein

Secure Member Administration: DAV ensures GDPR compliance using the LogPoint SIEM solution

LogPoint

- Ensures GDPR compliance across one million members
- Provides a complete, failure-resistant, tamper-proof and audit-ready storage of all log data.
- Reduce the number of false positives remarkably

Membership

Association

DAV has implemented LogPoint to protect the personal data of more than one million members and comply with GDPR. The SIEM solution supports the IT department with comprehensive analytics and user-friendly dashboards, visualizing log data and threat information collected throughout entire IT infrastructure

Background

More than one million alpinists and mountain fans are organised in 356 regional associations, under the Deutscher Alpenverein (German Alpine Club) established in 1869. It a remarkable club and the enthusiasm for it's guiding principles remain unwavering also after 150 years of existence. Today more and more young people, boys and girls alike, joins the club.

In particular the DAV indoors climbing halls across Germany attracts new generations to the regional associations, that offer a wide variety of activities, content, special offers, insurances and more to support the passion for alpine sports. A cornerstone in the membership administration is the DAV ID, which each member receives upon registration. It allows for participation in membership activities and enables members to receive special offers and discounts.

The personal member data are also used for administrative purposes, including the collection of membership fees, as well as communication via e-mail or other channels. Data are either fed directly in through Citrix connected IT systems or stored on local servers However, the DAV digitalization strategy aims for further.

centralization of services at headquarters in Munich and potentially also cloud based solutions.

The Challenge

Protecting personal data against unauthorised access and ensuring GDPR compliance was a key requirement for DAV in the process of upgrading IT security. The process was supported by the Munich-based IT systems house microCat, a certified LogPoint partner and a long-term service provider toDAV with extensive knowledge of the IT security infrastructure in the organization.

"DAV handles more than one million membership data sets and has to manage numerous IT systems, which are accessed by more than 150 full-time employees and numerous voluntary staff every single day. Following a comprehensive security analysis, we concluded that the only way to deliver on DAV requirements was a SIEM solution", says Markus Stinner, the CEO of microCat. Preparations for upgrade in IT security were launched years before the GDPR regulations formally came into effect in 2018. "We realized, that we needed a solution that would both meet our high security standards as well

as the GDPR requirements. That is why we reached out to the team at microCat at a very early stage. When they introduced us to LogPoint during the Proof-of-Concept, we were particularly surprised by the flexibility of the solution and the wide range of possibilities in the LogPoint dashboard", says IT manager Klaus Vogler at DAV headquarters in Munich. Shortly after the Proof-of-Concept, the LogPoint SIEM was operating, collecting and analysing data from 25 different log sources.
.

DAV
Deutscher Alpenverein

LOGPOINT

The Solution

With the LogPoint SIEM solution, all log data is collected in a central repository and translated into a uniform log format, time stamped and stored. Already at this point, LogPoint provides a complete, failure-resistant, tamper-proof and audit-ready storage of all log data. In real-time data is analysed based on a

"We realized, that we needed a solution that would both meet our high security standards as well as the GDPR requirements. That is why we reached out to the team at microCat at a very early stage. When they introduced us to LogPoint during the Proof-of-Concept, we were particularly surprised by the flexibility of the solution and the wide range of possibilities in the LogPoint dashboard"

Klaus Vogler, IT Manager
Deutscher Alpenverein

number predefined rules. Some "out-of-the-box", others defined in collaboration between the DAV IT department and the LogPoint support team.

If the threshold of a rule is passed, the DAV IT team will receive a notification, including detailed information pinpointing where the in the IT infrastructure the deviation has been detected. All unusual events are visualised through different charts in a single dashboard providing a real-time visualization of the of the entire IT infrastructure.

Using LogPoint, Vogler and his team were able to detect a number of incidents in which search engines were occupying unnecessary resources on DAV servers. With LogPoint solution, the IT team was quickly alerted, able to identify the cause, and ultimately remedy the

LOGPOINT

situation. Other incidents proved to be harmless, but very quickly identified as such, which provided Vogler even more reassurance about the LogPoint solution "We were able to reduce the number of false positives remarkably, and a glance of a dashboard we now know what is happening in our entire IT infrastructure. This ultimately provides us with reassurance, that we are able to better assess the security situation at any given point in time", says Klaus Vogler. Security checks are now much faster and more targeted. Furthermore, unnecessary communication from security systems were identified and turned off, providing a much more efficient operation.

The Results
The LogPoint solution has enabled the DAV to increase performance of existing IT systems and provided the ability to detect unusual events in the network. Providing support for full GDPR compliance, Vogler and his department fulfils an important requirement. Required by law and demanded by DAV

members. The security of personal data is now safeguarded by a centralised security system, which analyses and makes relevant information available.

"LogPoint has developed a professional solution in this area, and together with microCat, we have achieved what we set out to do. We now have a much better overview of our own security", Voegler says. Similar to an alpinist standing at the top of the mountain, Vogler and his team now have the best possible view standing on top of the data mountain, knowing where their members may be at risk. By now, all external and almost all internal systems are monitored by the LogPoint solution. Going forward Vogler wants to integrate the few virtual machines not connected yet, by expanding the LogPoint licence. As DAV develops new tools and services to support the full-time staff and volunteers in the regional associations, the LogPoint installation will likely also grow. Among future options considered is to incorporate a Security Operations Center delivered as a service, depending on the future cloud strategy.

Indoor climbing halls with DAV regional associations across Germany, is a very popular activity among the younger members of the club

LOGPOINT