Engelbert-Strauss

How LogPoint helps Engelbert Strauss stay ahead on the Cybersecurity curve and keep an eye out for anomalies in the IT infrastructure

LogPoint

- Cuts response time to cyberthreats by 50-60%
- Ingests logs from a wide variety of sources
- Increases visibility in the IT infrastructure by 70-80%

Manufacturing

German workwear company Engelbert Strauss is using LogPoint to collect and analyze logs from a diverse IT infrastructure. The LogPoint SIEM solution provides the IT department with a centralized overview, helps them stay in control and respond in real-time to potential cyberthreats

Background

Strauss was founded in 1946 by Engelbert Strauss with a commitment to creating the world's finest work safety clothing. Today, Europes leading workwearbrand is still a family-owned company, managed jointly by Engelbert's son Norbert Strauss and his own sons Steffen and Henning. As a very forward-looking, cutting-edge company, Strauss thinks and acts with a cross-generational view, offering a large portfolio of over 30,000 individual product lines for the whole family. The company logo, the red ostrich, is a reference to the family name Strauss, which means Ostrich in German.

Today the company is Europe's leading manufacturer of workwear and work-equipment with a talented staff of more than 1.300 people. Engelbert Strauss is headquartered in Biebergemünd / Frankfurt am Main in a campus soon to include a brand-new manufacturing facility with a capacity of up to 400,000 shoes per year, a textile advertising agency and high-tech logistics. Products are sold through a number of company-owned flagship stores, a global network of retailers, and online.

The Engelbert Strauss IT infrastructure includes more than 300 servers, including WMware virtualized servers running Windows and Linux, as well as a plentitude of other devices such as firewalls, routers, and even a telefax-system, that remains the preferred way for submission of purchase orders for some retailers. The company manufacturing line is not yet connected to the IT infrastructure, but as the new production facility goes online that may change.

The Challenge

"There were multiple drivers in our decision to go look for a SIEM solution. But the overarching motive was to do better: provide better services, increase the security level, and use resources more efficiently. We needed the ability to analyze logs from different sources such as Active Directory, Firewalls and servers, and the ability to securely store logs for forensics," says Markus Buss, Infrastructure Systems Administrator at Engelbert Strauss.

Facts	
Customer	Engelbert Strauss
Industry	Manufacturing - Workwear
Location	Biebergemünd, Germany
Objectives	Achieve GDPR compliance, strengthen security and eliminate false positives

Most enterprises today know that that implementing perimeter, endpoint, and access control security measures are excellent first steps to reducing the risk of damage and disruption due to breaches in the IT infrastructure. But effective cybersecurity strategies also have to take into account the very real possibility that systems can be compromised, regardless of security implementation, necessitating a solid holistic view the entire infrastructure.

Markus Buss
Infrastructure Systems Administrator
Engelbert Strauss

"Using LogPoint fundamentally changes the way you work with log data in your infrastructure. With LogPoint log data becomes a useful tool. It allows us to take control and get a meaningful, constant output that enables us to spot potential problems and react promptly. Before things turn into a real threat."

"We experienced a lot of unsuccessful- and automated login attempts in Active Directory and in the infrastructure in general. It's not like we had any major incidents, as we had the means to block these attempts, but it was clear to us that pressure was mounting and we needed a solution give us a full overview, help us keep a close eye on things, and alert us in case of potential breaches," says Markus Buss.

The Solution

"Our interest in LogPoint was based on a recommendation from our IT service partner Telonic. We did an in-house Proof-of-Concept, where we tested the LogPoint solution extensively. LogPoint came as an out-of-the-box solution that we installed in our VM Ware environment. And it really was up and running in half a day. Setting up the Use Cases to support our specific needs was the part that took time, and I guess it's a job you never really finish as your systems evolve," says Buss.

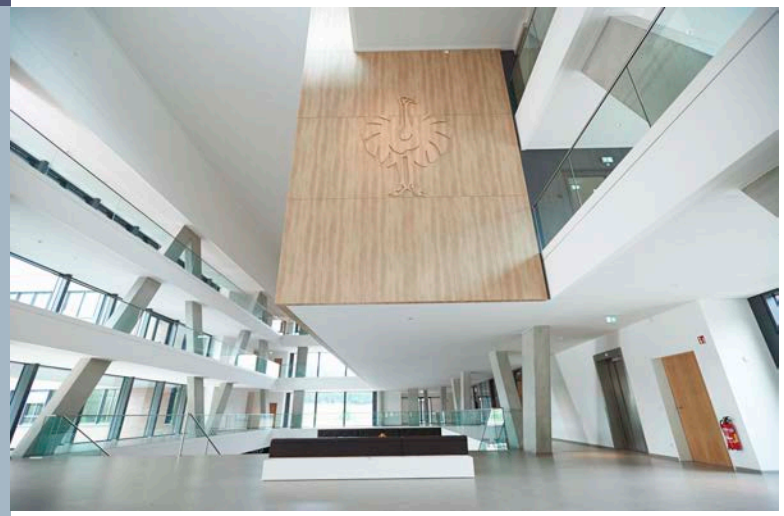
Engelbert Strauss settled on LogPoint's solution for ingesting log data from its numerous IT systems and then correlating it to find indicators of compromise/attack or patterns of threatening behavior. LogPoint's system is designed to be simple, flexible, and scalable, providing modular design, streamlined deployment, and integration tools that make it easy to implement.

"For us, a key feature in LogPoint is the ability to ingest and store logs from a wide variety of sources, whether it be Windows or Linux servers, Windows Backup, Active Directory, Firewalls, or even logs from the Telefax-system. LogPoint supports all environments and log sources and provides easy access to logs for all users that might need it across the IT department," says Markus Buss.

Contact LogPoint

If you have any questions or want to learn more about LogPoint and our modern SIEM solution visit **www.logpoint.com**

LOGPOINT



Engelbert-Strauss campus

The Results

"Using LogPoint fundamentally changes the way you work with log data in your infrastructure. Previously logs would only be checked in case of problems, and they would be difficult and time-consuming to access and analyze. With LogPoint log data becomes a useful tool. It allows us to take control and get a meaningful, constant output that enables us to spot potential problems and react promptly. Before things turn into a real threat," says Buss.

Further ahead with LogPoint is an expansion of the number of data sources ingested in the SIEM solution, possibly integration of SCADA systems in the new state-of-the-art manufacturing facility at the Engelbert Strauss campus in Biebergemünd. Buss and his team also want to take advantage of the automated reporting features included in LogPoint, supporting compliance with a wide range of industry standards, certifications, and regulations. And the cost of expanding the use of the LogPoint solution does not keep Buss awake at night.

"A particular advantage of the LogPoint solution is the licensing model. Based on the number of nodes rather than data volume, it's a good model for us as IT administrators. It's very easy to calculate the price you are going to pay, as you always know the number of nodes. In that way you can start out small and expand the coverage as you go along, and you can keep the finance department happy," he says.

Engelbert-Strauss produces high-tech workwear, safety footwear and personal protective equipment designed in Germany