Breitenfeld

Breitenfeld Edelstahl AG is an Austrian producer of stainless steel. The company was founded in 1942 and has over 320 employees serving customers in the renewable energy production, oil and gas, tool making, machine building, transportation/racing, aerospace, shipbuilding, and high-pressure industries.

Breitenfeld Edelstahl

At a Glance

- Recognized that increased digitalization of infrastructure brings new cyber security risks
- Implemented Darktrace across the entire digital infrastructure
- Developed trust in AI detections and decision-making; now upgrading to Autonomous Response

"Before Darktrace, network traffic and associated visibility was a 'black hole.' Now our network traffic is totally transparent and also secured by an additional pair of eyes from the SOC."

Simon Pucher, Head of IT, Breitenfeld

New Challenges in the Manufacturing Sector

In recent years, Breitenfeld has realized the value of significant digitalization, but also recognizes the increased cyber security risks that this transformation inevitably carries. "Today, the need for digitalization on the store floor is increasing, so the risk of production downtime due to ransomware or other attacks is also increasing," said Simon Pucher, Head of IT at Breitenfeld.

To protect the integrity and availability of its systems, ensure quality, and maintain productivity, the organization needed to safeguard its production systems from cyber disruption. Darktrace's Self-Learning AI supports the company's interests in visibility and detection of the most advanced threats. Like the human immune system, Darktrace continuously learns the 'patterns of life' for the entire ecosystem and identifies subtle deviations indicative of a threat.

Self-Learning AI Defense

An early adopter of AI cyber security, Breitenfeld trialed Darktrace's Industrial Immune System in 2017, and went directly from the Proof of Value (POV) period to contract. "The POV setup was extremely fast and smooth. It was only a few hours before we were seeing results," noted Pucher.

Breitenfeld recognizes that machine-speed attacks need to be met with machine-speed defense. "AI fights against AI" said Pucher, "You can already see today that the majority of attacks are already fully automated, so the defense must also be fully automated."

When the time came to renew the contract 2020, Breitenfeld did a wider evaluation of their security products, considering other systems such as QRadar, Zeek, Corelight, Empow, Vector, Stealthwatch and

ExtraHop. Pucher explained that ultimately it was their “high satisfaction with Darktrace, the excellent customer support, as well as the ease of use” that naturally persuaded them to renew the contract.

Powered by Self-Learning AI, Darktrace’s ability to learn ‘on the job’ has helped the company identify threats in their earliest stages, without the use of rules, signatures, or prior assumptions. With Darktrace’s alerts, Breitenfeld has been able to detect anomalous activity before it has the opportunity to escalate into a crisis.

> “You can already see today that the majority of attacks are already fully automated, so the defense must also be fully automated.”
>
> **Simon Pucher, Head of IT, Breitenfeld**

Transparency Across the Entire Ecosystem

Darktrace proved critical in providing greater visibility for Breitenfeld early on. After deployment, when Breitenfeld was experiencing problems after an antivirus update, Darktrace’s Threat Visualizer allowed Breitenfeld to surface insights across their entire digital infrastructure and see the issue in detail.

“We activated an antivirus update on all clients, which also had the impact of partially disabling TLS protocols. We immediately detected an increase in TLS connection problems in the Advanced Search and were able to solve the problem within minutes, before the update was rolled out to all clients. This also prevented the network from being blocked and our internal customers from getting a bad experience” explained Pucher.

Breitenfeld no longer lacks visibility across their organization! Darktrace illuminated the company’s entire digital ecosystem, analyzing data from every user, device, and the complex relationships between them.

“Before Darktrace, network traffic and associated visibility was a ‘black hole.’ Basically, no one knew who was accessing where, or when. Now our network traffic is totally transparent and also secured by an additional pair of eyes from the SOC,” commented Pucher. “Security can only be optimized if you have transparency. Without transparency on packet-level, this will not be possible. Through Darktrace’s AI, we are able to have transparency with minimal alerts.”

Seeing the effectiveness and accuracy of Self-Learning AI, Breitenfeld has decided to upgrade to Antigena, Darktrace’s Autonomous Response technology that neutralizes fast-moving and unpredictable attacks in seconds, without interrupting normal operations. Pucher explained: “We have been working with the system in order to now have the knowledge that everything fits and have taken the logical step for the activation of Antigena.”

> “The POV setup was extremely fast and smooth. It was only a few hours before we were seeing results.”
>
> **Simon Pucher, Head of IT, Breitenfeld**