CUSTOMER STORY

With Ontinue, Vossloh AG is setting its course towards security

The train is coming. In most cases where this former Deutsche Bahn slogan becomes reality worldwide, Vossloh AG has something to do with it. The listed rail technology group from Germany specializes in the development, production and maintenance of rail fastening systems, concrete sleepers, switch systems and innovative services relating to the life cycle of the rail track. Founded in 1888 in Werdohl, Sauerland, the company now employs more than 4,000 people in around 30 countries and recently generated a turnover of 1.2 billion euros. The rail technology group's products ensure safe and reliable rail transportation in more than 100 countries.

Over the years, three overarching divisions have emerged: "Core Components", where everything revolves around rail fastening systems of all kinds, "Customized Modules", where Vossloh AG develops and produces products that can be individually adapted to customer requirements. Such products are switch systems, as well as "Lifecycle Solutions", with which the company offers services relating to the maintenance of rails and switches, welding services and rail and switch logistics. Until around six years ago, all of these divisions were still very autonomous and the IT infrastructure was organized in a decentralized manner.

vossloh
enabling green mobility

Challenges

- Establishment of a fully functional Security Operations Center
- Consolidation of the IT security infrastructure
- 365/24/7 monitoring according to the follow-the-sun principle
- Creation of a holistic overview of the entire IT landscape
- Leveraging synergies from security tools provided by a single vendor

Solution

- Complete migration of IT to the Microsoft tech stack (ongoing)
- Implementation of Microsoft Defender as an EDR solution for clients and servers with the help of Ontinue
- Operationalization of Microsoft Sentinel as SIEM platform with the help of Ontinue

Business Outcomes

- Centralized IT security infrastructure
- Round-the-clock monitoring of the entire IT
- Holistic SOC consisting of internal and external security experts
- Visibility across the entire IT landscape
- Significant relief for the company's internal IT team
- Only a few out of over 10,000,000 alerts reach the Vossloh AG security team

About Vossloh AG

Vossloh is a globally active, listed railway technology group and a leading provider of the construction and value preservation of railway infrastructure. The company offers an integrated offering for rail transport under one roof. This includes unique, high-performance key products and complex systems, including rail fastening systems, concrete sleepers, switch systems and crossings, as well as innovative services covering the life cycle of the rail route.

As a result of the "One Vossloh" initiative, which made it necessary to centralize the company, the "One IT" project and thus the consolidation of the IT infrastructure was also tackled. Frank Bäcker, Head of Shared Services and Platforms at Vossloh AG, and the cybersecurity department played a key role in this development and developed a security concept against the backdrop of an increasing threat situation.

"On the way to centralizing IT, we are clearly focusing on cloud services and Microsoft technologies such as Office 365 and Sharepoint for collaboration, and hosting is also increasingly taking place via Azure," explains Bäcker. "When it comes to cybersecurity, we naturally recognized that as a global company we need a Security Operations Center that is organized according to the follow-the-sun principle and is on duty around the clock." However, setting up our own SOC was out of the question, as the resources of the employees could not provide such holistic coverage of all associated tasks. In addition, the omnipresent shortage of skilled workers put a damper on all such ambitions.

"Home-field advantage" for Ontinue

The evaluation process began with the consideration of what the future IT security infrastructure would have to look like in order to achieve the maximum synergy effect. Vossloh AG therefore quickly decided to rely on Microsoft technologies for cyber security as well. "Having everything from a single source ensures less friction," says Frank Bäcker. The company selected Microsoft Defender for endpoint detection and response (EDR) and Microsoft Sentinel was at the top of the list of desired security tools for the SIEM (Security Information and Event Management) platform. The next step was to find the right MXDR (Managed Extended Detection and Response) service provider who was familiar with these technologies and could work with Vossloh AG to implement them.

> " "With Ontinue ION, we have successfully implemented a unified and centralized security strategy. Together with our partner, we have laid the foundation for further measures in the fight against cyberattacks."

Frank Bäcker
Head of Shared Services and Platforms
Vossloh Ag

In addition to demonstrating proficiency with Microsoft's tool stack, the MXDR provider undertook the necessary steps to transform Vossloh AG's internal IT department into a fully operational Security Operations Center (SOC). This also included the option of being able to monitor the IT infrastructure around the clock, 365 days a year. "We relatively quickly and easily decided on Ontinue as our choice. Of course, we looked at many service providers and compared them with each other, but Ontinue's service portfolio convinced us. At the end of the day, they also had a slight home advantage, as we were already working very successfully with Open Systems in the area of network security, the company from which Ontinue emerged," says the Head of Shared Services and Platforms. Once the decision had been made, Defender and Sentinel were implemented together so that the data from Network Detection and Response (NDR) and Endpoint Detection and Response (EDR) now converge in the SIEM platform. This gives Ontinue's Cyber Defender and Cyber Advisor as well as Frank Bäcker and his team a holistic picture of the company's security situation at all times.

The Head of Shared Services and Platforms is very satisfied with the current development: "With Ontinue ION, we have successfully implemented a unified and centralized security strategy. Together with our partner, we have laid the foundation for further measures in the fight against cyberattacks."

About Ontinue

Ontinue offers nonstop SecOps through an AI-powered managed extended detection and response (MXDR) service. Ontinue ION MXDR combines powerful proprietary AI with the industry's first collaboration with Microsoft Teams to continuously build a deep understanding of our customers' environments, informing how we prevent, detect, and respond to threats.
Continuous protection. AI-powered Nonstop SecOps. That's Ontinue.