Ontinue

CUSTOMER STORY

Ontinue keeps the CWS IT infrastructure hygienically clean

Everyone knows the practical cloth towel dispensers that hang in almost every public washroom. And most people in Europe have probably heard of the brand behind them, CWS International GmbH. However, anyone who thinks that the company with the distinctive logo only provides hygiene products is very much mistaken. Founded in 1954 by Conrad Wolfgang Schnyder, CWS is now also one of the largest workwear rental companies in Europe and has now added the areas of fire protection, cleanroom cleaning and the cleaning of medical equipment to its service portfolio. In these business areas, the approximately 11,000 employees generate a total turnover of over 1 billion euros. The company has always been headquartered in Duisburg but is active in 15 European countries.

As an international company, the IT infrastructure is, as expected, diversified and extensive. This is partly due to the CWS having expanded through acquisitions over many years. Therefore, a very large number of legacy systems have accumulated. The IT team has been working on processing and dismantling these for some time and has been able to consolidate the large number of different data centers and active directories into a single one. A cloud strategy is also being implemented in practice,

CWS

Challenges

- Establishment of a Security Operations Center
- Round-the-clock monitoring of IT security tools
- Faster response to cyberattacks
- Improved visibility of the IT infrastructure
- More time to reduce the level of risk in business areas other than IT security

Solution

- Expansion of the company's internal security team into a complete Security Operations Center through MXDR service Ontinue ION and Microsoft Teams channel
- Partial externalization of the processing of security incidents
- Creation of a unified dashboard via Microsoft Sentinel and Microsoft Defender

Business Outcomes

- 24/7/365 monitoring of the IT infrastructure
- Faster response to critical security risks
- Greater visibility across the entire IT infrastructure
- Free up staff resources to improve process maturity and security levels in other business areas

About CWS International GmbH

CWS contributes to a healthier and safer future with innovative, sustainable and digital rental solutions. The range is divided into products and services from the areas of hygiene, mats, workwear, fire protection, cleanrooms as well as health and care. With its service model, the company pursues the basic idea of a circular economy in all areas: Materials are reduced, used multiple times and reprocessed in a resource-saving manner. CWS is a brand of CWS International GmbH and its subsidiaries.

although only around a third of the IT infrastructure is actually cloud-based, with the majority still running on-premises. However, CWS has been relying on software-as-a-service offerings for some time, particularly for everyday applications such as office software and other programs that are not an essential part of the core business. Microsoft in particular has proven to be a trustworthy partner in this respect, and the company has also switched its security infrastructure to the E5 suite with Microsoft Defender as an EDR (Endpoint Detection and Response) tool and Sentinel as a SIEM (Security Information and Event Management) platform.

"During our consolidation work, something happened that every IT department fears: Hackers managed to launch a successful cyberattack against us," reveals Benjamin Boecker, Information Security Manager at CWS. "We experienced first-hand what we already knew - namely that it is not enough to check the security tools every now and then to see if there is an attack in progress." What CWS urgently needed was round-the-clock monitoring of the security applications that would enable rapid intervention every day of the year. "However, it was not only clear to us that we needed a fully functional Security Operations Center, but also professional external support," says Boecker.

Time pressure and re-evaluation

As setting up a Security Operations Center (SOC) on their own was out of the question, but the cyberattack put Benjamin Boecker's team and the CWS IT department under time pressure, the decision was made to use an MDR provider that was available at short notice. However, after a year and the completion of the implementation of Microsoft Sentinel and Microsoft Defender, a reassessment of the security situation was required. The first step was to license Microsoft's E5 suite and put the platform approach into practice instead of a best-of-breed approach. The effort involved in getting the best security applications under one roof was disproportionate to the benefits of a security infrastructure from a single source. In this context, Microsoft itself recommended three MXDR (Managed Extended Detection and Response) providers, including Ontinue, the company that ultimately won over the CWS.

> " Ontinue manages to massively accelerate our response speed to threats. This allows us to focus on improving process maturity and risk levels in other areas of the business with a clear conscience."

Benjamin Boecker
Information Security Manager
CWS International GmbH

The biggest advantages of Ontinue were the speed at which all service and communication interfaces could be implemented, as well as the coherent overall package. From a human and business perspective, the collaboration was positive right from the start and just fit. "In contrast to other providers, we quickly realized that Ontinue is not a typical sales-driven MXDR provider. Their insistence on a holistic approach also convinced us in the end, even if we would have set other priorities ourselves," explains Boecker. "In the end, the implementation went so smoothly that we were able to start working together in record time."

Fixed processes and excellent results

Switching to the MXDR service Ontinue ION has hardly changed the security infrastructure at CWS. What has changed, however, is the management of the security software used: Ontinue's Cyber Defenders monitor the Microsoft tools around the clock and have thus established holistic visibility. Benjamin Boecker's team therefore knows what is going on in their IT infrastructure at all times, including which log-ins are taking place and which events are being executed by the domain controller. "We can now not only see when an infected file is opened, but also where it came from and in which emails it still appears. Our MXDR partner provides us with this information, including the relevant context, which helps us to make decisions. In this way, Ontinue is able to massively accelerate our response time to threats," says Boecker.

The fact that processes for escalation and alerting the company's internal IT department are clearly defined also creates a good feeling at CWS. Benjamin Boecker and his team are immediately notified in the shared Teams channel when a security incident occurs - outside of business hours, they are also notified by email and by phone if it is an urgent emergency. For smaller events, there are also action protocols, so-called playbooks, which define what type of incidents Ontinue is allowed to resolve itself and how. However, the Cyber Defenders always make a report to the CWS. If the IT department needs to be involved, Benjamin Boecker and his team take over. "Communication via teams in particular is worth its weight in gold," emphasizes Boecker. "This type of collaboration is much more intuitive and reliable than ticket systems or browser-based platforms. The MXDR service doesn't feel like an external entity; instead, we work together as a unified SOC."

The success also speaks for itself. The annual risk analysis carried out by an external service provider at CWS had shown the IT department its shortcomings and the need for improvement in terms of incident management year after year. Since the company has been working with Ontinue, this area is no longer a problem and receives the highest ratings. "In the future, we can focus on improving process maturity and risk levels in other areas of the business with a clear conscience. Ontinue gives us this freedom through the tireless work of the Cyber Defenders and Cyber Advisors," summarizes Boecker. "At the weekends, we can let our nerves rest and don't have to constantly check Twitter or the relevant news portals to see if there are any current threats - a good feeling."

Ontinue

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.