Ontinue

CUSTOMER STORY

Decorative and Safe – Thanks to Seamless Monitoring

Schwan Cosmetics adds color to the everyday lives of people around the world, producing decorative pen cosmetics for both small and large brands. As part of the STABILO Group, widely recognized for its writing instruments, Schwan Cosmetics operates alongside other well-known brands in the group's outdoor division, such as Deuter, Ortovox, Maier Sports, and Gonso.

While the IT departments across STABILO subsidiaries collaborate through an IT Council, each company independently manages its hardware and software due to differing production processes that require unique ERP (Enterprise Resource Planning) systems and various application interfaces. To ensure reliable computing power, Schwan Cosmetics maintains its own data centers.

schwan cosmetics

Challenges

- Establish a professional Security Operations Center (SOC) with 24/7 monitoring.
- Introduce advanced security systems to enhance protection.

Solution

- Enhance and expand Microsoft's existing security portfolio.
- Implement Microsoft Identity Protection for robust identity management.
- Leverage Ontinue's SOC for comprehensive alert management.

Business Outcomes

- Real-time 24/7 alert monitoring for continuous protection.
- Streamlined incident communication via a dedicated Teams channel.
- Coordinated escalation processes with a structured escalation matrix.
- Faster response times and heightened security levels, reducing the workload on IT teams.

About Schwan Cosmetics

Schwan Cosmetics is a global leader in private-label decorative cosmetics manufacturing. Headquartered in Heroldsberg, Germany, the company employs over 3,000 people across seven countries and operates state-of-the-art production facilities worldwide.

To enhance security incident management, Schwan Cosmetics partnered with MXDR (Managed Extended Detection and Response) provider Ontinue in October 2023. The initiative to outsource the Security Operations Center (SOC) was proposed by Robert Hans, Director of Security at Schwan Cosmetics, following insights gained at a security congress. During the internal evaluation, it became evident that an MXDR provider would significantly improve efficiency and optimize resource utilization in cybersecurity.

Prior to implementing Ontinue's services, the team encountered approximately one critical incident per month. However, the high volume of false positives consumed considerable time and detracted from their ability to focus on value-adding and innovative projects. "We could just about manage the time needed for incident investigations, but it left us with little capacity for other priorities," explains Alexander Wurm, Network and Security Administrator at Schwan Cosmetics Germany. "Fortunately, no attack had severe consequences, but the workload severely limited our progress on other tasks."

With Ontinue's support, Schwan Cosmetics has streamlined its incident response processes, enabling the team to focus on strategic initiatives and ensuring both security and efficiency remain at the forefront.

Seamless Monitoring Thanks to 24/7 Operation

Following an internal risk assessment that revealed the significant potential damage of a successful cyberattack, Schwan Cosmetics chose to invest in a Security Operations Center (SOC). Given resource constraints, the company opted for a 24/7 managed SOC provided by an external MXDR partner - Ontinue. For an international organization with nearly 1,500 users, the continuous monitoring offered through Ontinue ION quickly proved essential.

One of the key advantages of partnering with Ontinue is the enhanced transparency regarding potential cyberattacks. "There was always some concern about whether we could detect everything quickly enough," admits Robert Hans, Director of Security at Schwan Cosmetics. "With critical incidents, there must be no gaps or delays. Even though our traditional measures felt robust, we still faced blind spots."

Leveraging Microsoft Defender, which was already partially implemented, accelerated the onboarding process. The existing Microsoft security technologies formed a strong foundation for integrating Ontinue ION, with the necessary infrastructure set up within weeks. "What impressed us was Ontinue's focus on MXDR as their core business," says Hans. "Their Cyber Defenders and Cyber Advisors collaborate with us as equals, fostering a trusting and efficient working relationship."

> "Through our collaboration with Ontinue, the security level has improved significantly. Furthermore, internal capacity has been freed up, which we can use for strategic security projects."
>
> **Robert Hans**
> Director Security
> Schwan Cosmetics

The partnership's effectiveness is further enhanced by seamless communication via a shared Microsoft Teams channel, allowing real-time collaboration between Ontinue and Schwan Cosmetics. This setup is a significant improvement over traditional email-based incident management.

Faster Incident Response and Proactive Security

Within the first year of collaboration, Schwan Cosmetics has seen a marked improvement in incident response times. Ontinue's pre-screening process ensures that only relevant cases reach the internal IT team, reducing their workload significantly. Additionally, Ontinue's proactive security advice helps identify vulnerabilities and misconfigurations early, enabling Schwan Cosmetics to implement countermeasures before attackers can exploit any gaps. The time saved through Ontinue's services has allowed the company to focus on strategic security initiatives, strengthening their overall cybersecurity posture.

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.

CONTACT US