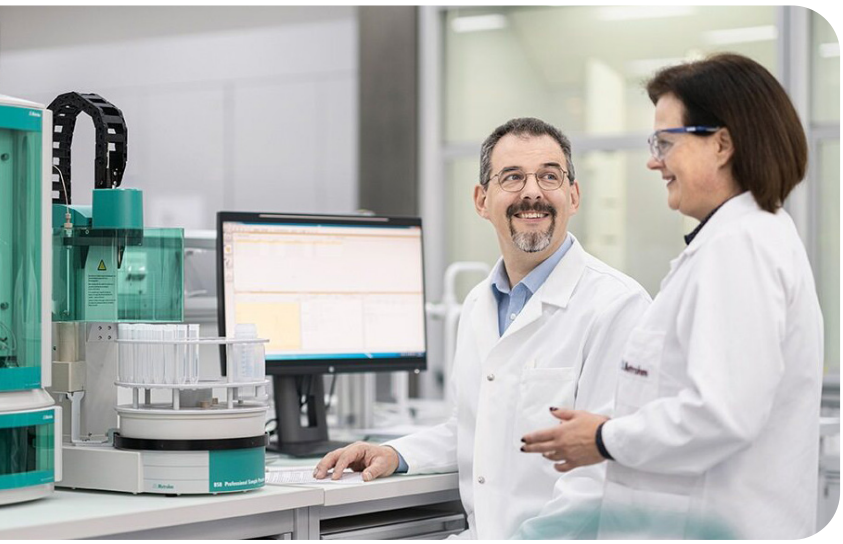
Ontinue

CUSTOMER STORY

Ontinue Strengthens Metrohm's Safety DNA



Switzerland's reputation for precision is embodied by Metrohm AG, a leading manufacturer of high-precision instruments for chemical analysis. With 80 years of experience, Metrohm AG has become a global leader. In addition to titrators, crucial for quantitative analysis, the company offers a wide range of laboratory instruments and technologies, such as ion chromatographs, Raman and near-infrared spectrometers. They also provide 'OMNIS' for process optimization, which enables laboratories to increase their productivity and efficiency. Founded in Herisau in 1943, the long-established company now operates in 45 countries with over 100 sites and around 3,300 employees, supported by an extensive partner network spanning over 80 countries.

The company's constant growth did not stop at the technological infrastructure: the number of workplace clients increased, and the internal network grew with each new development, production, and sales location. The more than 30 IT experts at Metrohm AG now manage around 3,300 workplace clients and three data centers. In addition, there are geo-redundant data centers from partners and the use of public multi-cloud services. The international threat situation due to hacker attacks and the tight staffing levels had already prompted the company to outsource the operation and protection of the SD-WAN some time ago.

Metrohm

Motivators

- Expansion of the security-first approach
- Taking more proactive and automated measures against cyber threats
- Strengthening the security DNA across the entire IT infrastructure
- 24/7 monitoring of all endpoints and assets
- Establishment of a security operations center for first response, threat intelligence and threat hunting
- Streamlined reporting to learn from security incidents and raise employee awareness of security issues.

Solution

- Partnering with Ontinue for traditional SOC activities, encompassing threat intelligence, threat hunting, data science, detection engineering, and automated threat detection.
- Deploying Microsoft Defender as the EDR solution for both clients and servers.
- Enabling Microsoft Sentinel as the primary SIEM platform.

Business Outcomes

- 24/7 monitoring of IT infrastructure
- Fully operational SOC
- Comprehensive visibility across all assets, spanning clients, data centers, and multi-cloud environments.
- Substantial support for the internal IT team
- Reduced occurrence of serious and critical security incidents
- Proactive defense measures against cyber threats
- Minimal alerts forwarded to Metrohm AG security team out of over 1,000,000 initial alerts.

About Metrohmv AG

Metrohm AG is one of the world's leading manufacturers of high-precision instruments for chemical analysis and was founded in 1943 by engineer Bertold Suhner in Herisau, Switzerland. Today, the company has over 100 of its own sites in 45 countries and is represented by subsidiaries and sales partners in 80 countries.

"Our belief is: Security First," explains Zeno Stämmer, Chief Information Officer at Metrohm AG. "The security DNA of Metrohm AG is based on the firm intention to consider and take appropriate measures everywhere and at every point in the IT infrastructure and services. This requires not only keeping an eye on the network, data centers and clients around the clock, but also having as comprehensive a picture as possible of the threat landscape. Our internal staff resources and expert know-how were not sufficient for this. What we effectively lacked was a Security Operations Center that would help us close our gaps in the area of detection and response and provide us with the visibility we urgently needed across all IT areas."

Establishing an in-house Security Operations Center (SOC) was impractical. It would have strained our already limited employee resources, leading to significant constraints on IT operations and ongoing projects. Moreover, our team lacked the requisite experience in the diverse tasks handled by security advisors and threat hunters. Therefore, Metrohm AG opted to collaborate with a trusted partner, mirroring the successful approach taken during the setup, operation, and protection of the SD-WAN. Zeno Stämmer summarizes this decision as follows: "In addition to a dedicated security team, systems for detecting cyberthreats and automating defensive measures are the absolute advantage of SOCs. Companies also need appropriate software that they have to operate - unfortunately, we at Metrohm are not equipped to do this."

> " **We rigorously evaluated multiple providers, assessing how their offerings aligned with our requirements. Ontinue proved to be a strong contender, matching up well against the competition"**
>
> Zeno Stämmer
> **Chief Information Officer**
> Metrohm AG

A Simple Decision

The requirements for an ideal MXDR service provider were promptly identified. It was advantageous for the provider to specialize in Microsoft technologies, aligning with Metrohm AG's heavy reliance on Microsoft technology. Utilizing Microsoft Defender for Endpoint Detection and Response (EDR) was a natural choice, given its existing use on endpoints, with plans to transition to servers. Additionally, Metrohm AG's CISO, Zeno Stämmer, and the company's IT architects were resolute in integrating Microsoft Sentinel as a SIEM solution into the tool stack, ensuring a comprehensive security infrastructure from a unified source.

The potential MXDR provider also needed to have sufficient capacity to monitor Metrohm AG's large IT infrastructure around the clock, as well as provide threat intelligence and automation mechanisms as part of the service package. As you would expect from a company that puts precision first, there was a clearly defined roadmap for evaluating a suitable SOC provider. " We rigorously evaluated multiple providers, assessing how their offerings aligned with our requirements. Ontinue proved to be a strong contender, matching up well against the competition," emphasizes Zeno Stämmer. "After our positive experience with Open Systems, the company from which Ontinue emerged, we were not surprised in this regard."

Once the decision had been made in favor of Ontinue's MXDR service ION, Metrohm AG laid the necessary software foundation by purchasing Microsoft E5 security licenses and thus Microsoft Defender for all the company's endpoints and servers. Zeno Stämmer and his team also put Microsoft Sentinel into operation. A Microsoft Teams Channel was established as the designated communication platform for agreements between Ontinue's SOC and Metrohm AG's IT team.
The MXDR Cyber Advisors oversee strategic alignment of the security infrastructure and offer guidance, while the Cyber Defenders handle operational security checks. They serve as direct points of contact, available around the clock for immediate assistance in critical risk situations.

Security First in Action

Within just seven days of collaboration initiation, the security posture saw a significant enhancement. Initial analyses conducted by Ontinue's SOC provided a clearer insight into the threat landscape, facilitating proactive countermeasures. Concurrently, the MXDR professionals successfully resolved a considerable portion of non-critical security incidents, freeing up resources for Metrohm AG's IT team to address more serious issues independently. In quantifiable terms, Ontinue only forwards four events out of over one million to Zeno Stämmer's security team. Leveraging Microsoft's EDR and SIEM solution, Ontinue ensures 24/7 monitoring of the IT infrastructure, crucial given cyber threats' disregard for business hours. Notably, over a quarter of attacks on Metrohm AG occurred during weekends in the last six months. Moreover, Ontinue benefits from a streamlined process, as less than a third of incoming incidents necessitate ticket creation.

"Before our collaboration with Ontinue, we were one thing above all: reactive. We had neither the means nor the resources to know all types of attacks and counteract them preventively. That has now changed completely," says Zeno Stämmer, summarizing the positive development. Ontinue not only aids Metrohm AG in initial response and incident triage but also extends support to threat hunting and intelligence. Collaborating closely with Zeno Stämmer's team, Ontinue's experts proactively identify vulnerabilities and assist in their mitigation. Additionally, the SOC shares insights gathered from threat intelligence endeavors, fortifying Metrohm's security infrastructure against present and emerging threats."

"I'm not sure what could have happened to us without Managed SOC. During the first three months, we had several dozen high-severity security incidents that we were able to fend off - even one of these incidents could have cost several hundred thousand francs if successful," reports Zeno Stämmer.

> **" Since partnering with Ontinue, we've successfully identified several dozen high-severity incidents promptly. The prevention of even one of these incidents, each potentially costing hundreds of thousands of francs, underscores the value of our collaboration with Ontinue as our SOC and MXDR provider. Moreover, the absence of critical incidents for several months solidifies our confidence in this decision."**
>
> Zeno Stämmer
> **Chief Information Officer**
> Metrohm AG

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.

©2024 Ontinue All Rights Reserved. Approved for public use.