XM Cyber | Case Study

Manufacturing

XM Cyber and STIHL: Securing a Global Legacy Through Digital Sovereignty

The Challenge

Protecting a Century of Innovation through Continuous Security

STIHL is a third-generation, family-owned company with a long tradition of innovation. As its operations grew increasingly connected and digital, the company recognized early that proactive cybersecurity was essential to protecting its data, operations, and reputation. According to Chairman Dr. Nikolas Stihl, one of the company's key strengths has always been anticipating risks before they surface:

"Anyone who asks around and follows technological developments in the field of cybercrime knows that companies need to take targeted precautions. Because this has been our approach from the outset, we have so far escaped unscathed – despite numerous attempted attacks."

This philosophy guided STIHL's next step. The leadership team sought to secure their fast-growing global infrastructure while maintaining full control of data, systems, and processes. They required a solution that could deliver continuous visibility, provide clear priorities for remediation, and grant real-time protection—all while complying with stringent European data protection standards.

STIHL®

Industry:
Manufacturing

Chairman:
Dr. Nikolas Stihl

Location:
Waiblingen, Germany

Challenge:
Strengthening cybersecurity and digital sovereignty across a global enterprise

Solution:
XM Cyber exposure management platform on STACKIT infrastructure

Results:

XM Cyber exposure management platform on STACKIT infrastructure

The Solution

A Proactive, Sovereign Security Foundation

Before switching to XM Cyber, STIHL already had a well-functioning security system, but it operated based on the older method of trying to prevent every single attack. Dr. Stihl explained what convinced them to change:

"What convinced us about XM Cyber was the truly new and innovative approach: break-ins are inevitable. But the consequences of a break-in can be controlled and limited."

STIHL chose XM Cyber to enhance visibility and control across its global environment. Running on STACKIT's sovereign European cloud, the platform continuously maps exposures and attack paths, helping the company pinpoint and reduce risk before it can impact operations. As Dr. Stihl noted, the platform enables his company to focus its resources on the most critical risks:

"XM Cyber enables us not only to identify vulnerabilities, but also to prioritize them. This means we know the biggest risks to our business processes and can take targeted countermeasures."

XM Cyber helps STIHL map how small weaknesses can connect into attack paths that lead to critical assets. The platform's digital-twin functionality allows STIHL to validate what is truly exploitable in their environment without running risky payloads or disrupting systems. This eliminates blind spots across hybrid infrastructure and helps STIHL's security and operations teams align on the potential business impact of exposures and the best actions to take.

The XM Cyber implementation was quick and smooth. The platform rapidly provided STIHL with full visibility and clear guidance on where to act, helping the IT team cut risk and keep operations running without disruption. Dr. Stihl highlighted the collaborative approach:

"Right from the start, we have maintained close contact with the XM Cyber specialists in Israel, who support us in an advisory capacity."

Benefits and Outcomes

Visibility, Resilience, and Continuity

XM Cyber provides STIHL with a consolidated, real-time view of its digital environment and the ability to act before threats can escalate. Attack path analytics now highlight the few remediation steps that neutralize many risks at once, significantly improving operational efficiency across teams. With stronger resilience and greater confidence across all sites and systems, Dr. Stihl noted that his company's operations have remained remarkably stable:

"In times when there have been incidents at many well-known companies, we have not had to suffer any interruption to our business operations."

This continuous, attacker-aware visibility gives STIHL the foresight to detect weaknesses early and confirm that every fix strengthens the organization's overall security posture. Today, STIHL understands how attacks could unfold and uses that insight to protect its innovations, keep systems running, and maintain trust across its global network.

Recommendation and Outlook

Controlling Risk to Secure the Future

STIHL's partnership with XM Cyber reflects the company's strategic shift toward impact-focused security. The company recognizes that intrusions may occur, but the consequences can be managed and minimized through intelligent prevention, remediation, and rapid response. Dr. Stihl explained that the ultimate goal was not to eliminate all risk, but to contain its effects.

For STIHL, digital sovereignty means maintaining control of its data, systems, and technology. With XM Cyber, the company can continue developing its digital platforms on its own terms while protecting the secure foundation that drives innovation and global growth.

- **Continuous visibility across global systems**
- **Early detection and prioritization of risk via attack paths**
- **Compliance with European data protection standards**
- **Seamless deployment with no operational disruption**
- **Strengthened stability and decision-making confidence**