DETECTIFY CASE STUDY: BÜHLER GROUP

How Bühler Group leverages Detectify external attack surface monitoring to discover, assess and remediate vulnerabilities

detectify

AN INTERVIEW WITH:

Patrick Zimmermann
INFORMATION SECURITY MANAGER

BÜHLER

About Bühler Group

Industry:	Mechanical and industrial engineering
Company size:	> 12 500 employees
Location:	Headquarters in Uzwil, Switzerland with employees located in 140 countries

Bühler Group is a multinational plant equipment manufacturer with over 160 years of history in producing machinery equipment and solutions in various industries, including the food & feed industry and the automotive material industry.

Headquartered in Uzwil, Switzerland, Bühler Group has a strong presence in over 140 countries, with 30 manufacturing sites.

About Patrick Zimmerman

Patrick has worked in Information Security since 2012. Alongside colleagues in Uzwil and Bangalore, he is responsible for securing both company and customer data. Product security is also another area of involvement due to Bühler Group's use of software solutions and digital services.

Patrick Zimmerman
INFORMATION SECURITY MANAGER

Adjusting security to Bühler Group's increasing digital ecosystem

A rise in Bühler's publicly accessible web assets and domains resulted in a bigger attack surface which their security team found challenging.

Unlike a few years ago, they are now responsible for hundreds of subdomains and new projects for digital services - mostly involving web applications. In the past, Bühler Group had a traditional gate-based security process where new assets or applications had to get a security sign-off before going live, including an internal or external security review.
However, they learned that this approach is not scalable.

Keeping track of all public accessible domains and their potential vulnerabilities can be an arduous task without the right set of tooling.

The machinery and infrastructure industry is known for dragging its feet in strengthening both its digital infrastructure and cybersecurity procedures.

Machinery equipment and its control software are usually static and often have a lifespan of more than 20 years. As expectations continue to change with digital services such as Bühler Group's plant automation solutions, their customers demand regular releases with new features, just like any other software.

How Bühler Group leverages of Detectify

When Bühler Group became ISO 27001 certified in 2019, a large part of the certification introduced a new secure development process, including specific toolings such as static code analysis and software composition analysis.

Bühler Group could easily give their developers access to the tool, allowing them to check for new vulnerabilities regularly. Their primary goal was to decrease the time between detection and remediation and provide a frictionless process for them.

Detectify enabled Bühler Group to bring the information to their standard tools for potential vulnerabilities and work items. When Detectify finds a new issue, it gets exported via the API and added to the related team's backlog based on the affected asset.

> "Detectify has produced high-quality results with zero false positives, which is a significant advantage for Bühler Group."

Bühler Group now covers their entire external-facing attack surface with Surface Monitoring and targets business-critical applications with individual Application Scanning profiles for stateful testing.

“We picked Detectify because it continuously monitors our entire external attack surface, discovers new subdomains, and automates scans and security tests sourced by the 400 ethical hackers of Crowdsource”, says Patrick.

In that way, Bühler Group leverages a scalable security solution, both product capabilities and the security knowledge available to employees via the platform. A successful cybersecurity program requires everyone involved to stay up-to-date with new vulnerabilities that might appear daily, and Detectify enables Bühler Group to do that.

The tool gets frequent updates for new vulnerabilities that automatically become part of scanning routines. Detectify has produced high-quality results with zero false positives, which is a significant advantage for Bühler Group.

“We picked Detectify because it continuously monitors our entire external attack surface, discovers new subdomains, and automates scans and security tests sourced by the 400 ethical hackers of Crowdsource”.

Time and cost-saving

In the past, a security review based on different tools took Bühler Group 2-5 days depending on the complexity of the web application and resulted in various false positives. They would have to send reports to relevant people, manually keeping track of remediation statuses. It was a laborious process that required a lot of manual effort.

Remediation time is as critical as detection. It only takes a minute for Bühler Group to add a root asset. Detectify discovers subdomains, starts scanning, and sends findings with actionable information about the issues and the remediation tips directly to the developers.

Bühler Group can cut time and costs as they don't need to manually extend the findings or search for reference content.

> "It takes a minute for us to add a root asset and Detectify will discover subdomains and start scanning."

Detectify's Crowdsource community enables constant updates of the scanning engines with new vulnerabilities, allowing Bühler Group to discover and scan faster and learn about new vulnerabilities while having the remediation knowledge sources next to the potential threat.

The reduced time required to determine security issues' validity allows the teams to be more creative and develop new tools and products.

"It takes a minute for us to add a root asset, and Detectify will discover subdomains and start scanning," says Patrick.

Patrick’s security tips

Patrick’s advice to companies in the sector is to consume a lot of news, stay up to date, and react to changes. ”Try to be as agile as possible, e.g., by making processes lean and using the right tools to help you achieve that,” he says.

”Security should follow your business - if your software is developed in an agile way, you will sooner or later face challenges if security testing is becoming a source of noise instead of an enabler,” continues Patrick.

Patrick believes that giving software developers the know-how and toolset to perform their automatic security assessment ensures that potential security issues can be identified by security teams early, not once a vulnerability evolves into an actual security incident.

Using Detectify, Bühler Group’s security team can guide other teams and look from the sideline, and only need to jump in during cases of very critical findings or zero-day releases.

go hack
yourself.