CYWARE™ | Case Study

CERT-WM rapidly adopts Cyware, for operationalized threat intelligence and collective defense

CERT Water Management (CERT-WM) is a collaborative initiative between 21 water authorities in the Netherlands and Rijkswaterstaat, the Dutch Ministry of Infrastructure and Water Management. Founded in 2016, the group — powered by a small team that supports the 12,000 people employed by water boards across The Netherlands — is a computer emergency response team that seeks to optimize operational information security across the Dutch water management sector.

CERT-WM

Needing to fortify cyber defenses and keep critical systems safe

As an organization dedicated to protecting critical infrastructure, CERT-WM needs to sharpen its cybersecurity defenses as much as possible. That way, the organization is able to help protect Dutch water supplies against significant risks by managing and cleaning waste water, preventing disruptions in distribution, and ensuring optimal drainage to mitigate flooding.

To keep water systems safe, CERT-WM had been using a robust cybersecurity solution that helped mitigate cyber threats. Unfortunately, the organization eventually learned that the tool was nearing its end of life.

To maintain a strong cybersecurity posture, the team began looking for a new operationalized threat intelligence and collective defense solution at the beginning of 2024.

> **"They (Z-Cert a close partner) shared a demo of Cyware with us, and we were quite enthusiastic about what we saw."**
>
> **Jarno Baselier**
> Operational Coordinator, Cert-WM

Choosing Cyware for speed of integration after a word-of-mouth recommendation

As the CERT-WM team began its search for new cybersecurity tooling, they reached out to colleagues at other Dutch-based CERTs, including Z-CERT, which helps healthcare institutions protect their digital systems.

"We have a close relationship with them," explains Jarno Baselier, an operational coordinator who's been working with CERT-WM for seven years. "They shared a demo of Cyware with us, and we were quite enthusiastic about what we saw."

After a positive first impression of Cyware, the CERT-WM team researched the platform on a deeper level. At the same time, they also explored other options, including open source tools.

"Cyware kind of had a monopoly in a way because the functionality we were searching for is not as broadly available in other products," Baselier continues. "It is very specialized. So we narrowed it down to a few options; we had open source options, too, but that meant we'd have to develop a lot of things around our internal processes."

Ultimately, the team decided that Cyware's automated threat intelligence and collaborative defense capabilities — as used by over 90% of global ISACs — were the perfect fit for their requirements, unrivaled by other solutions on the market.

CYWARE™

Getting up & running quickly thanks to top-shelf support

After deciding to move to Cyware, the CERT-WM team needed to deploy the platform as quickly as possible to keep its mission-critical systems safe.

"That was the requirement for us because we had to be operational as quickly as possible since we didn't have access to the old toolkit anymore," Baselier explains. Thanks to Cyware's support team, implementation was a breeze. "The support from the team has just been great. It's an amazing tool to work with, it does what it needs to do, and it comes with a team that really wants to evolve and improve. Those are all really positive points."

As is the case with any piece of technology, the CERT-WM team ran into a couple of issues when they rolled out Cyware initially. Working with Cyware's support team, CERT-WM was able to figure out how to use the platform productively in short order.

"We met with the product team a couple of times over the first couple of weeks, and they helped us learn more about the platform every time," says Jeremy Daal, an analyst at CERT-WM who's been with the organization for a year and a half. "I think it worked out very well."

Feature-rich tooling & ease of integration

Since rolling out Cyware, Baselier has been particularly impressed by the platform's polished front end and feature-rich nature. He's happy that the platform has an internal messaging tool, and he also likes the fact t hat he has more options when it comes to integrating data into the system.

"We can use multiple feeds and API connections to get data in," Baselier continues. "We couldn't use API connections in the old application so that's a plus as well."

> **"Cyware gives us peace of mind."**
>
> **Jarno Baselier**
> Operational Coordinator, Cert-WM

Improved internal and external collaborative defense

In the past, when the CERT needed to push out information to its community, they had no other options but email. Now, the team is able to send messages directly within Cyware; constituents log in through a portal online or via mobile app to access them, making life easier for everyone.

"It all works out well," Daal says. "I think it's very helpful in terms of keeping our constituents up to date through a single pane of glass. We're more in touch with our community because of Cyware, everyone can see what we're doing, and this helps us fulfill our mission of keeping our water safe throughout our country."

Similarly, Cyware makes it easier for CERT-WM colleagues to collaborate.

"We're a small team, so usually one of us has the shift for a day, and just one of us is working in Cyware," Daal explains. "I can put up a draft and whoever comes in after me can immediately see what I've done and maybe rearrange or adjust some things. It works really well."

Any last words for other cybersecurity teams considering a solution like Cyware?

"Cyware gives us peace of mind," Baselier concludes.

About Cyware

Cyware enables security teams to operationalize threat intelligence data and take real-time action by integrating intelligence management, automating workflows, and facilitating secure collaboration for stronger, more unified defense.