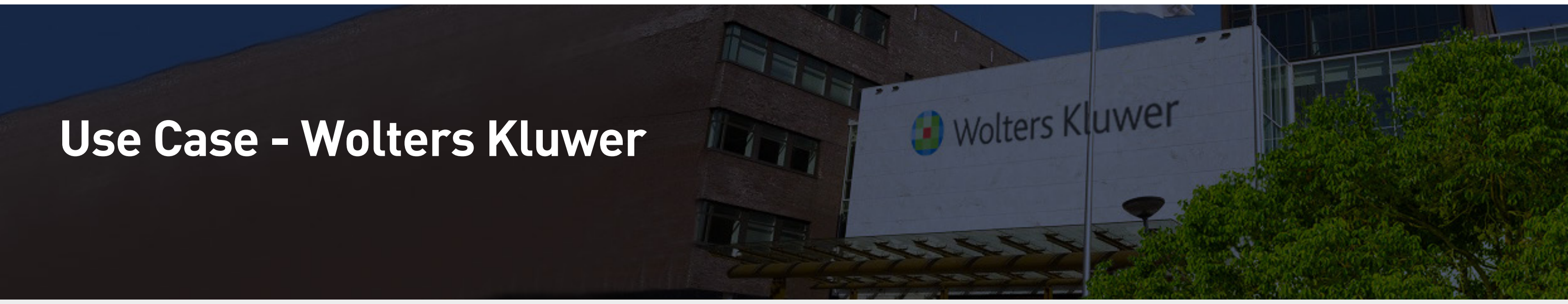
Wolters Kluwer

Cymulate



Use Case - Wolters Kluwer

Gaining operational efficiencies and staying ahead of threat evolutions with Cymulate Continuous Security Validation

Organization

Wolters Kluwer is a global provider of professional information, software solutions, and services for clinicians, accountants, lawyers, and tax, finance, audit, risk, compliance, and regulatory sectors. Wolters Kluwer reported 2019 annual revenues of €4.6 billion. The group serves customers in over 180 countries, maintains operations in over 40 countries, and employs approximately 19,000 people worldwide.

Daniel Puente, the CISO of Wolters Kluwer Tax and Accounting Spain is an accomplished security professional, holding CISM, CRISC, CDPSE, CISSP, CHFI, CEH, LA27001 & LA22301 certifications. In addition to leading the central information security team and operations, he also has a distributed team of security champions that are embedded in application development, responsible for protecting the Software Development Life Cycle (SDLC).

Business Challenge

Wolters Kluwer core business is based on HR and HCM applications, that handle extremely sensitive, personal information, for example payroll information.

Protecting personal data is crucial to them, and they must comply with PII regulations globally, including GDPR.

Additionally, as a service provider they have to ensure that their network, systems and applications are secure.

A breach that provides a threat actor access to their customer networks in the form of a supply chain attack, would be devastating to their business.

Daniel summarizes; "Our main challenges are two.

First one, is to know what level of security we have in our environment and in our applications. The second one is to be updated, as soon as possible about the new threats that could affect our ecosystem."

Challenge

Wolters Kluwer provides services and applications that handle sensitive PII data for their customers. This demands a high level of vigilance from their security team.

Solution

With Cymulate, Wolter Kluwer were able to rapidly and accurately assess their security posture by challenging their security stack to a broad spectrum of attacks that are updated daily with new threats.

Benefits

Risk based prioritization enabled the team to be more efficient, and together with the understanding how the attacks work allowed them to resolve them fast and effectively.

Solution

Wolters deploy and use various tools to integrate security and compliance within their SDLC, to continuously perform application security testing and vulnerability discovery and management. Deploying Cymulate enabled them to operationalize the MITRE ATT&CK® Framework and extend this methodology to continuously challenge and validate their IT cyber security architecture.

Impressed by its ease of use, they immediately gained benefits from improvements in their testing programs. Cymulate provided visibility into the performance of their security stack, and threat intelligence led assessments showed the potential impact of threat evolutions on their security posture. "We noticed a lot of attacks and vulnerabilities that we weren't aware of before and knowing how these attacks work is very powerful " It also decreased the time it took to detect security gaps and vulnerabilities and it enabled the security team to focus their efforts on the most important ones.

"Sometimes we found ourselves wasting time on harmless vulnerabilities or taking the wrong approach to solve an issue. Cymulate helps us to optimize our efforts and time. And knowing the way the attacks perform their activity is the best way to stop them, so Cymulate makes a crucial contribution to learn about these procedures," summarizes Daniel.

Cymulate visualization of attack paths provide Wolters Kluwer the information on where and which systems are vulnerable to attacks. This provides a true measurement of risk. For example, when sensitive data could be potentially compromised, they treat it like an actual incident, and focus efforts to fix the issue immediately.

Wolters were also impressed with the level of Cymulate customer support. Past experience, onboarding other solutions, was typically accompanied with a lot of frustration. "With Cymulate the onboarding process was an easy one, we were always assisted by great professionals that allowed us to make the most of it, always going beyond giving a correct answer, they collaborate with you in order to improve your actions and obtain better results," notes Daniel. In summary, if asked by a colleague Daniel would say **"Try it! Don't hesitate. After the PoC I'm sure you won't be able to tell me that Cymulate won't save efforts, optimize costs and give you a clear picture of the status of security in your organization. It's a must-have element of every modern security architecture."**

Benefits

Security stack visibility – Wolters Kluwer became aware of security gaps and vulnerabilities that were invisible prior to deploying Cymulate.

Faster resolution – Decrease the time to detect vulnerabilities and resolve them faster by understanding how the attacks work.

Threat intelligence validation – Know how new threats could impact the environment and how to remediate the vulnerabilities they created.

C-level engagement – Executive reports provides visibility to C-level executives about Wolters Kluwer security status in a simple manner.

Operational efficiency – Risk based prioritization to allocate resources effectively and improve productivity by leveraging automation.

Team enhancement – Improve team skills by helping them think like the adversary and become better defenders.

> "In Security it's almost impossible to estimate a Return of Investment or even a cost saving number, but it's crystal clear that we have optimized our resources by using Cymulate, allowing us to start new projects and other ones that we have had in a drawer for months or years."
>
> Daniel Puente, CISO, Wolters Kluwer,
> Tax and Accounting, Spain

Ready to Cymulate? Get started with a free trial