REFERENCE CASE - Willemen Groep

From crisis response to structural, digital resilience

A measurable transformation for Willemen Groep.

About Willemen Groep

Willemen Groep is one of the largest family-owned construction groups in Belgium and is active in several business fields such as: construction, infrastructure, real estate and engineering. Transversal services such as HR, finance and IT are organized for the entire group from a centralized holding structure.

With 1700 employees, of which around 900 are digital users, and an average of 100 active construction sites, the organization operates within a highly diverse and dynamic IT landscape.

A complex, digital construction site

In addition, there are temporary partnerships in joint ventures for large-scale construction and infrastructure projects such as the 'Oosterweelverbinding' on Rechteroever and the new VRT-building.

This combination of scale, geographical distribution and temporary digital ecosystems makes central control, monitoring and security structurally complex.

The challenge: from roadmap to reality

Cybersecurity has been part of Willemen Groep's strategic IT roadmap for a long time. In collaboration with external partners, a phased approach was and is being developed to structurally increase the digital maturity.

However, in September 2022, this roadmap had to abruptly be speeded up by a ransomware incident. The organization was confronted with the operational and strategic impact of a real cyber incident. What had been planned for future trajectory, became an immediate priority.

"Our core business lies in construction, not cybersecurity. With a compact IT team, it is impossible to build a 24/7 Security Operations Center (SOC) that can keep up with the fast evolution of threats."

Kenneth Claes, IT Infrastructure & Operations Manager

The cyber incident made it clear **that traditional perimeter security and a reactive approach were no longer sufficient** in an environment with so many digital access points, external partners and temporary connections.

The strategic choice: focus on core activities

The decision to not organize cybersecurity internally was a conscious, strategic decision. Not only for reasons of capacity, but above all for reasons of **focus**, **continuity** and **scalability**. Three factors were key in this decision:

- **Core focus**: IT security is not a core competence of a construction and infrastructure group.
- **24/7-requirement**: Continuous monitoring requires specialized profiles and permanent staffing.
- **Threat evolution**: Cyber threats develop faster than internal teams can keep up with, structurally.

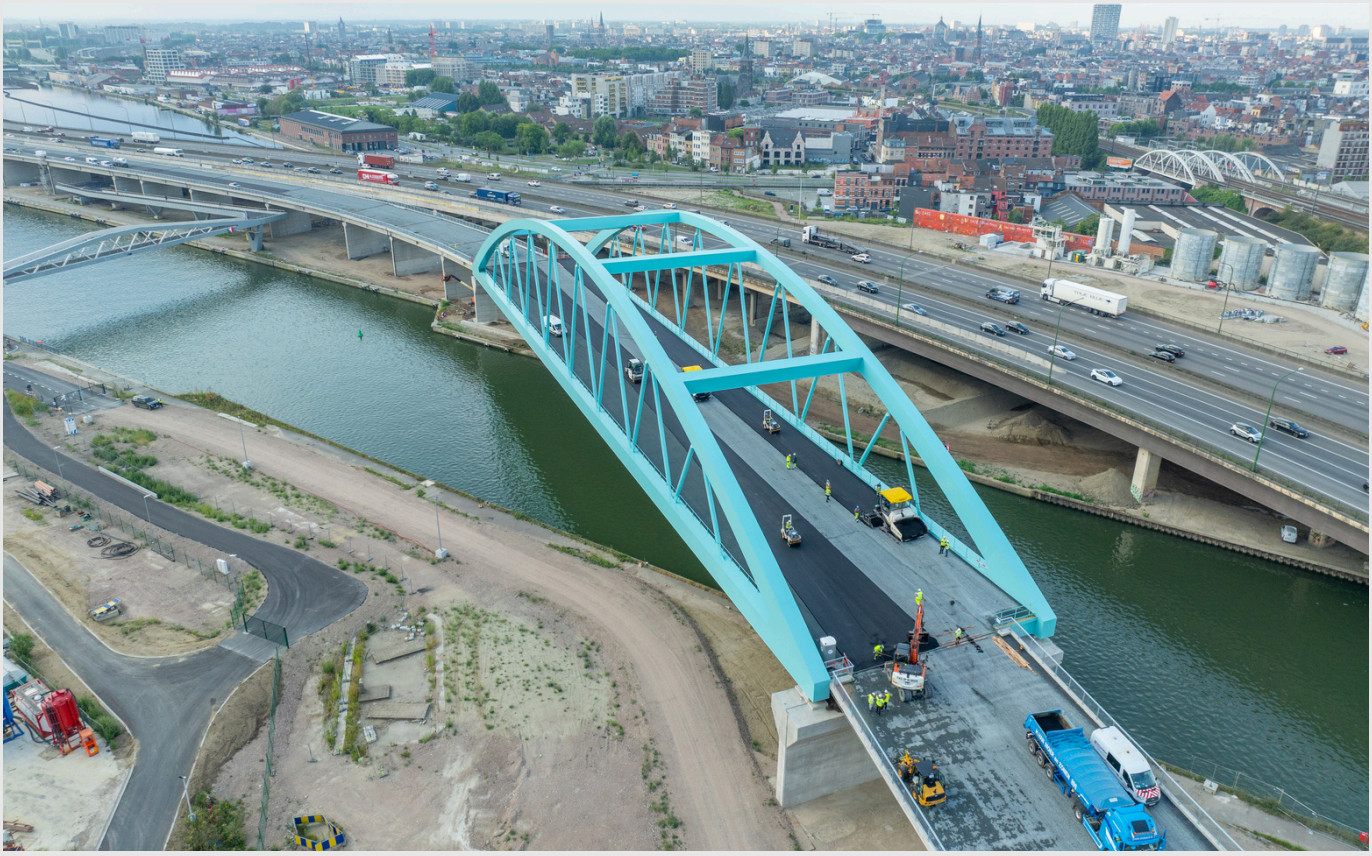
After a market research in 2023, ACEN was chosen as a strategic partner at the end of that year. The decisive factor was the need for an **external Security Operations Center (SOC)**. By choosing a **Managed SOC-service**, Willemen Groep immediately had access to a **team of security experts** who monitor the environment around the clock, without the overhead of its own internal department.

The solution: intelligent detection through SIEM & SOAR

The chosen approach combines central visibility, intelligent detection and automated response within a single integrated security model. The solution is based on three principles:

- **SIEM (Security Information and Event Management)**: This serves as the 'digital nervous system'. All security signals and log data from sites and office systems are **centralized** and **correlated** here. The SIEM recognizes patterns that could indicate an attack, which would otherwise go unnoticed in the data stream.
- **SOAR (Security Orchestration, Automation and Response):** Where SIEM detects, **SOAR takes action**. In the event of a clear threat (such as an impossible login), the platform executes **automated workflows** to block accounts or to isolate systems. This happens in a fraction of a second without the need for human intervention.
- **Managed SOC**: A specialized team at ACEN monitors these systems 24/7, performs proactive analyses, and intervenes in complex incidents that fall outside the scope of the automated scripts.

In addition, external threats such as leaked access data and sector-specific attack patterns are actively monitored.



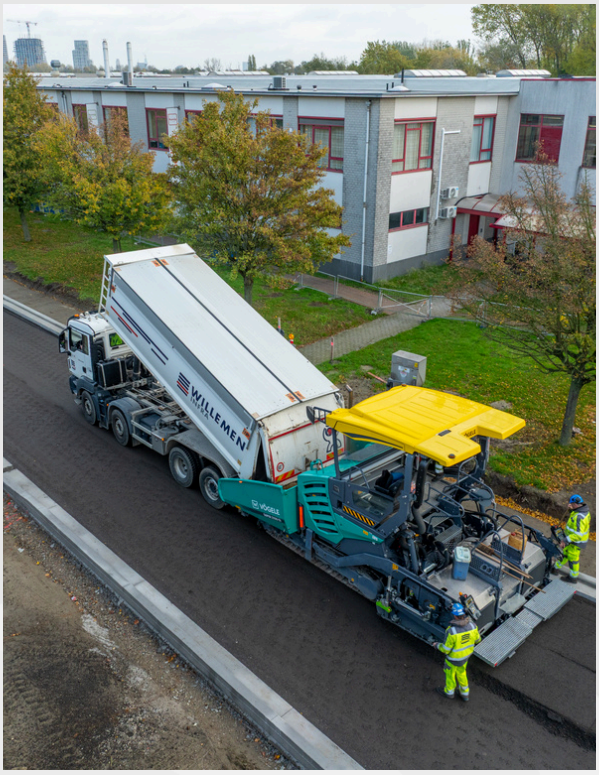
The implementation: fast integration, minimal disruption

The implementation itself was fully completed after just a few weeks. Over the following two months, we further optimized the alerts until everything was perfectly tuned. Thanks to previous investments in a standardized and mature IT architecture, critical systems could be linked quickly. The implementation initially focused on:

- Critical access points
- Identities
- Core systems
- External connections

This was followed by further optimization and fine-tuning based on normal user behavior and operational processes.

The results



A measurable transformation in resilience
The transition to a managed security model has led to a significant shift on four crucial levels:

1) Operational effectiveness and efficiency:

Through the use of SOAR automation, routine incidents are immediately isolated and dealt with. This results in a drastic reduction in false-positives, giving the team more time to focus on incidents that truly require human expertise. Talking about a win-win!

2) Strategic continuity and maturity

Thanks to central SIEM monitoring, management now has a transparent overview of the risk profile, with security scaling organically with the growth of the group.

3) Peace of mind and focus

The ‘always on’ culture is now supported by ACEN’s 24/7 Managed SOC. This relieves the internal IT team of the pressure to be on standby outside office hours, allowing them to shift their focus entirely to digital innovation within construction projects.

4) Commercial advantage and risk management

Last but not least... A robust security policy is essential for large construction and infrastructure projects. Willemen Groep can now demonstrate in black and white that their security chain is at the highest level. This is an asset in public tenders and ensures a more favorable risk profile for cyber insurers.

WILLEMEN GROEP

The collaboration

The collaboration is characterized by structural coordination, transparency and joint evolution.

Through regular meetings, dashboards and clear agreements on responsibilities, cybersecurity has been integrated into their daily operations. The relationship exceeds operational services and is evolving into a strategic partnership.

The next steps in the roadmap focuses on further automation, expansion of monitoring and strengthening identity security.

The focus is not on individual solutions, but on structurally increasing digital maturity. Cybersecurity is not seen as a project, but as a permanent organizational capability.

The conclusion

What began as a crisis intervention grew into a structural transformation. Willemen Groep has evolved from reactive incident response to proactive digital resilience, with continuous monitoring, automated protection and strategic control at its foundation.

A model in which cybersecurity is no longer a separate discipline, but an integrated part of professional entrepreneurship in a digital construction sector.

Together, we are (literally) building the future.