REFERENCE CASE - Willemen Groep

Van crisisrespons naar structurele, digitale weerbaarheid

Een meetbare transformatie voor Willemen Groep.

Over Willemen Groep

Willemen Groep is een van de grootste familiale bouwgroepen in België en actief binnen meerdere business lines: Bouw, Infra, Real Estate en Technieken. Vanuit een gecentraliseerde holdingstructuur worden transversale diensten zoals HR, Finance en IT georganiseerd voor de volledige groep.

Met 1.700 medewerkers – waarvan ongeveer 900 digitale gebruikers – en gemiddeld zo'n 100 gelijktijdig actieve werven, opereert de organisatie in een sterk verspreid en dynamisch IT-landschap.

Een complexe digitale bouwplaats

Daarbovenop komen tijdelijke samenwerkingen in maatschappen voor grootschalige bouw- en infrastructuurprojecten zoals de Oosterweelverbinding op Rechteroever en het nieuwe VRT-gebouw. Deze combinatie van schaal, geografische spreiding en tijdelijke digitale ecosystemen maakt centrale controle, monitoring en beveiliging structureel complex.

De uitdaging: van roadmap naar realiteit

Cybersecurity maakt al lang deel uit van de strategische IT-roadmap van Willemen Groep. In samenwerking met externe partners werd en wordt gewerkt aan een gefaseerde aanpak om de digitale maturiteit structureel te verhogen.

In september 2022 werd deze roadmap echter abrupt versneld door een ransomware-incident. De organisatie werd geconfronteerd met de operationele en strategische impact van een reële cyberdreiging. Wat tot dan toe een gepland toekomsttraject was, werd een onmiddellijke prioriteit.

"Onze kernactiviteit is de bouw, niet cybersecurity. Met een compact IT-team is het onmogelijk om zelf een 24/7 Security Operations Center (SOC) uit te bouwen dat de snelle evolutie van dreigingen bijhoudt."

Kenneth Claes, IT Infrastructure & Operations Manager

Het incident maakte duidelijk dat **klassieke perimeterbeveiliging en een reactieve aanpak niet langer volstonden** in een omgeving met zoveel digitale toegangspunten, externe partners en tijdelijke connecties.

De strategische keuze: focus op kernactiviteiten

De keuze om cybersecurity niet intern te organiseren, was een bewuste strategische beslissing. Niet alleen omwille van capaciteit, maar vooral omwille van focus, continuïteit en schaalbaarheid. Drie factoren waren daarbij doorslaggevend:

- **Core focus**: IT-security is geen kerncompetentie van een bouw- en infrastructuurgroep
- **24/7-vereiste**: continue monitoring vereist gespecialiseerde profielen en permanente bezetting
- **Dreigingsevolutie**: cyberdreigingen ontwikkelen sneller dan interne teams structureel kunnen bijbenen

Na een marktvergelijking in 2023 werd eind dat jaar gekozen voor ACEN als strategische partner. Doorslaggevend hierbij was de noodzaak aan een extern Security Operations Center (SOC). Door te kiezen voor een Managed SOC-dienst, beschikt Willemen Groep onmiddellijk over een team van security-experts dat de omgeving de klok rond bewaakt, zonder de overhead van een eigen interne afdeling.

De oplossing: intelligente detectie via SIEM & SOAR

De gekozen aanpak combineert centrale zichtbaarheid, intelligente detectie en geautomatiseerde respons binnen één geïntegreerd beveiligingsmodel. De oplossing steunt op drie pijlers:

- **SIEM (Security Information and Event Management)**: Dit fungeert als het 'digitale zenuwstelsel'. Alle beveiligingssignalen en logdata van werven en kantoorsystemen worden hier gecentraliseerd en gecorreleerd. Het SIEM herkent patronen die op een aanval kunnen wijzen, die anders onopgemerkt zouden blijven in de datastroom.
- **SOAR (Security Orchestration, Automation and Response)**: Waar het SIEM detecteert, onderneemt de SOAR actie. Bij een duidelijke dreiging (zoals een onmogelijke login) voert het platform geautomatiseerde workflows uit om accounts te blokkeren of systemen te isoleren. Dit gebeurt in fracties van seconden, zonder dat er menselijke interventie nodig is.
- **Managed SOC:** Een gespecialiseerd team van ACEN bewaakt deze systemen 24/7, voert proactieve analyses uit en grijpt in bij complexe incidenten die buiten de automatische scripts vallen.

Daarnaast wordt actief gemonitord op externe dreigingen, zoals gelekte toegangsgegevens en sectorgerichte aanvalspatronen.

De implementatie: snelle integratie, minimale storing

De implementatie zelf was al na enkele weken volledig afgerond. In de daaropvolgende twee maanden hebben we de alerts verder geoptimaliseerd tot alles perfect op punt stond.. Dankzij eerdere investeringen in een gestandaardiseerde en volwassen IT-architectuur konden kritieke systemen snel gekoppeld worden.

De implementatie focuste in eerste instantie op:

- Kritische toegangen
- Identiteiten
- Kernsystemen
- Externe connecties

Daarna volgde verdere optimalisatie en finetuning op basis van normaal gebruikersgedrag en operationele processen.

De resultaten

Een meetbare transformatie in weerbaarheid De transitie naar een managed security-model heeft geleid tot een significante verschuiving op vier cruciale niveaus:

1) Operationele slagkracht en efficiëntie

Door de inzet van SOAR-automatisering worden routine-incidenten meteen geïsoleerd en afgehandeld. Dit zorgt voor een drastische daling in 'false positives', waardoor het team de handen vrij heeft voor incidenten die écht menselijke expertise vereisen. Een echte win-win!

2) Strategische continuïteit en maturiteit

Dankzij de centrale SIEM-monitoring heeft het management nu een transparant overzicht van het risicoprofiel, waarbij de beveiliging organisch meeschaalt met de groei van de groep.

3) Gemoedsrust en focus

De "altijd aan"-cultuur wordt nu gedragen door het 24/7 Managed SOC van ACEN. Dit ontlast het interne IT-team van de druk om buiten kantooruren stand-by te staan, waardoor de focus volledig kan verschuiven naar digitale innovatie binnen de bouwprojecten.

4) Commercieel voordeel en risicobeheer

Last but not least... Een robuust security-beleid is essentieel bij grote bouw- en infrastructuurprojecten. Willemen Groep kan nu zwart-op-wit aantonen dat hun ketenbeveiliging op topniveau staat. Dit is een troef bij aanbestedingen en zorgt voor een gunstiger risicoprofiel richting cyberverzekeraars.

WILLEMEN GROEP

De samenwerking

De samenwerking wordt gekenmerkt door structurele afstemming, transparantie en gezamenlijke evolutie. Via vaste overlegmomenten, dashboards en duidelijke afspraken over verantwoordelijkheden is cybersecurity geïntegreerd in de dagelijkse werking. De relatie overstijgt operationele dienstverlening en evolueert richting een strategisch partnership.

De volgende stappen binnen de roadmap richten zich op verdere automatisering, uitbreiding van monitoring en versterking van identiteitsbeveiliging. De focus ligt niet op losse oplossingen, maar op het structureel verhogen van de digitale maturiteit. Cybersecurity wordt daarbij niet gezien als een project, maar als een permanent organisatievermogen.

De conclusie

Wat begon als crisisinterventie, groeide uit tot een structurele transformatie. Willemen Groep maakte de evolutie van reactieve incident respons naar proactieve digitale weerbaarheid, met continue monitoring, automatische bescherming en strategische controle als fundament.

Een model waarin cybersecurity geen aparte discipline meer is, maar een geïntegreerd onderdeel van professioneel ondernemerschap in een digitale bouwsector. Samen bouwen we aan de toekomst.

Ready to map Your Security Future?

Ken Van Hasselt
Account Manager
ken.vanhasselt@is4u.be
+32 497 11 55 90

ACEN