



Cybersecurity Verbetertrajecten

Zet vandaag de eerste stap naar betere
cyberveiligheid en profiteer tot
50% VLAIO-steun

Inhoud

Hoe ziet een traject eruit?

2

Een gestructureerde aanpak, afgestemd op jouw noden.

De cybersecurity menukaart

3

Kies de optie bij jouw organisatie past.

START-pakket

3

Laagdrempelige instapformule die snel inzicht geeft in jouw cyberweerbaarheid.

MEDIUM- en PLUS-pakket

5

Een uitgebreid pakket, aangepast aan jouw bedrijfscontext en -grootte.

Extra opties

13

Ga voor extra zekerheid dankzij de uitbreidingen.

Over Cingulum

15

Leer ons wat beter kennen.

Hoe ziet een traject eruit?



Cyberaanvallen stoppen niet bij grote ondernemingen. Ook kmo's worden steeds vaker het doelwit, en vaak met grotere gevolgen. Toch ontbreekt het veel organisaties aan tijd, kennis of middelen om echt werk te maken van structurele cyberbeveiliging.

Daarom ontwikkelde Cingulum, in samenwerking met VLAIO, **drie modulaire pakketten op maat van de kmo**. Elk pakket bevat een helder afgelijnd traject, waarbij we samen een aanpak op maat uitstippelen: inzicht in je risico's, duidelijke prioriteiten, en concrete stappen om beveiliging structureel te versterken.

Een gestructureerde aanpak, afgestemd op jouw noden.

Onze START-, MEDIUM- en PLUS-pakketten zijn opgebouwd rond de principes van informatiebeveiliging: Identify, Protect, Detect, Respond en Recover.

Het START-pakket is een vast traject van 10 dagen, met focus op analyse, risico-inschatting en een actieplan. MEDIUM en PLUS bouwen hierop verder. Deze omvatten de volledige START-analyse, aangevuld met respectievelijk 14 of 24 dagen extra ondersteuning die je zelf kan samenstellen op maat van jouw organisatie.

Bovenop een MEDIUM- of PLUS-pakket kunt u bijkomende uitbreidingspakketten van 6 of 10 dagen afnemen.

In deze brochure ontdekt u de duidelijke "menukaart" met bouwstenen per domein en inschatting van de benodigde tijd.

Zo krijg je een concreet en doordacht traject, afgestemd op de maturiteit en prioriteiten van jouw organisatie.

Onze cybersecurity menukaart

Kies de optie die bij jouw organisatie past.

START-pakket

10 dagen

Eerste analyse van je huidige situatie, kwetsbaarheden en basismaatregelen, met een helder actieplan en opvolgingsdashboard.

Originele totaalprijs:

€10.300 excl. btw

tot -50% subsidie

€5.150

MEDIUM-pakket

24 dagen

Kies zelf de bouwstenen die voor jouw organisatie het meest nodig zijn. Na analyse begeleiden we de eerste verbeteracties mee in de praktijk.

Originele totaalprijs:

€24.720 excl. btw

tot -50% subsidie

€12.360

PLUS-pakket

34 dagen

Volledige begeleiding bij de analyse, uitwerking én implementatie van beleid, processen en technische verbeteringen in jouw organisatie.

Originele totaalprijs:

€35.020 excl. btw

tot -50% subsidie

€17.510

Uitbreiding

Kom je niet toe met de bouwstenen uit het MEDIUM of PLUS pakket? Dan kan je opteren voor een bijkomend uitbreidingspakket van 6 of 10 mandagen. Het maximaal af te nemen totaalbedrag bedraagt € 60.000 excl. btw.

*Aanbod onder voorwaarden van VLAIO.

START pakket

Een laagdrempelige instapformule die snel inzicht geeft in je cyberweerbaarheid, met een kwetsbaarheidsscan, top-risico's en gerichte aanbevelingen om de cybersecurity van jouw organisatie te verbeteren.

Cingulum Aanbod	CyFun* Thema	Inschatting dagen KMO <50 FTE	Inschatting dagen KMO 50-250 FTE	Inschatting dagen KMO >250 FTE
Interne kwetsbaarheidsscan	Analyse & Roadmap	2	2	2
Externe kwetsbaarheidsscan	Analyse & Roadmap	1	1	1
Basisanalyse van de huidige veiligheidsmaatregelen	Analyse & Roadmap	4	4	4
Risico-inschatting & roadmap	Analyse & Roadmap	2	2	2
Opmaak basis dashboard	Analyse & Roadmap	1	1	1



Het START-pakket biedt een breed en gebalanceerd beeld van waar jouw organisatie vandaag staat, inclusief concrete tools om de eerste stappen richting betere cyberveiligheid te zetten.

Dit pakket is bewust compact gehouden, met 10 mandagen, inzetbaar voor elk type kmo. Voor organisaties die verder willen bouwen op deze basis zijn er het MEDIUM- en PLUS-pakket, waarin we dieper ingaan op implementatie, continuïteit en langetermijnbegeleiding.

*CyFun (CyberFundamentals) is een Belgisch cybersecuritykader van het Centrum voor Cybersecurity België (CCB) dat organisaties helpt hun digitale basisbeveiliging op orde te brengen. Het geeft concrete maatregelen en niveaus om cyberrisico's te verminderen en weerbaarder te worden tegen aanvallen.

In detail

Interne kwetsbaarheidsscan

Analyse & Roadmap

Een **geautomatiseerde controle van de zwakke plekken in je interne netwerk, foutieve configuraties en ongeautoriseerde apparaten**. Inclusief simulatie van interne aanvallen om de effectiviteit van de beveiliging te testen.

Externe kwetsbaarheidsscan

Analyse & Roadmap

Een **niet-invasieve analyse van de openbare gegevens en publieke IT-omgeving** die toont welke systemen zichtbaar zijn op het internet en welke kwetsbaarheden daaruit voortvloeien.

Basisanalyse van huidige veiligheidsmaatregelen

Analyse & Roadmap

Op basis van interviews en technische scans **beoordelen we de maturiteit van de cybersecurity**. Afgetoetst aan het "IMPORTANT" niveau van het CyFun framework en bedoeld als voorbereiding op een gerichte risicoanalyse en roadmap.

Risico-inschatting & roadmap

Analyse & Roadmap

We identificeren wat écht waardevol is, waar de grootste dreigingen zitten en welke maatregelen prioriteit krijgen.

Het resultaat is een **heldere, haalbare roadmap met acties, timing en verantwoordelijkheden**, bruikbaar als leidraad voor management en IT-partners.

Opmaak basis dashboard

Analyse & Roadmap

Een eenvoudig en overzichtelijk dashboard, dat in een oogopslag toont hoe het gesteld is met de cybersecurity van jouw organisatie.

Het dashboard **volgt de acties uit de roadmap op, koppelt ze aan risico's en toont ook de status van leveranciers en maturiteitsindicatoren**. Zo blijft het management betrokken en behoudt men grip op vooruitgang en prioriteiten.

MEDIUM & PLUS-pakket

Met het MEDIUM- of PLUS-pakket breid je het traject respectievelijk met 14 of 24 dagen uit. Hierbij focussen we op het structureel verankeren van cybersecurity in jouw organisatie.

Kies zelf welke bouwstenen uit ons aanbod relevant zijn voor jou. We begeleiden je graag bij die keuze zodat dit pakket realistisch, haalbaar en afgestemd is op jouw context. Hieronder vind je een overzicht van alle onderdelen.

Cingulum Aanbod	CyFun Thema	Inschatting dagen KMO <50 FTE	Inschatting dagen KMO 50-250 FTE	Inschatting dagen KMO >250 FTE
Uitgebreide Gap-analyse op basis van CyFun of ISO27001	Identify	2	2	2
Model inventaris van Activa (Assets)	Identify	1	1	1
Ondersteuning bij inventarisatie van Activa (Assets)	Identify	3	4	6
Opstellen rollen en verantwoordelijkheden	Identify	0.5	0.5	1
Change Management	Identify	1	2	2
Monitoring en metingen	Identify	1	2	2
Risicoregister	Identify	1	2	4
Opstellen Risk Assessment proces	Identify	1	1	2
Basis Ketenbeheer (TPRM Basic)	Identify	0.5	2.5	4

Cingulum Aanbod	CyFun Thema	Inschatting dagen KMO <50 FTE	Inschatting dagen KMO 50-250 FTE	Inschatting dagen KMO >250 FTE
Uitgebreid Ketenbeheer (TPRM full)	Identify	3	4	5
Identiteits- en Toegangsbeheer	Protect	2	2.5	3.5
Information Security Training for Management (uitgebreid)	Protect	1	1	1
Phishingtest	Protect	1.5	1.5	1.5
Classification & Labeling	Protect	1	2	3
Cloud, Network & Applicatiebeleid	Protect	1	2	3
Toegangsbeheer (Identity & Access Management)	Protect	1	1.5	2
Veilige instellingen en configuraties (Secure Configuration)	Protect	1	1.5	2
Bescherming van netwerken (Network Security)	Protect	1	2	3
Beheer van bedreigingen en kwetsbaarheden	Protect	1	2	3
Beveiliging van toepassingen (Application Security)	Protect	1	2	3.5

Cingulum Aanbod	CyFun Thema	Inschatting dagen KMO <50 FTE	Inschatting dagen KMO 50-250 FTE	Inschatting dagen KMO >250 FTE
Beschikken over tijdige en werkende back-ups	Protect	1	1.5	2
Procedures voor continue monitoring	Detect	1	1	2
Opstellen detectieprocessen	Detect	2.5	3	4
Incidenten- register (opgemaakt, niet ingevuld)	Respond	0.5	1	1
Incidenten- register (opgemaakt en ingevuld)	Respond	3	3	4
Opstellen Incident Management Procedures	Respond	1	1	2
Business Continuity & Disaster Recovery Procedures (basis)	Recover	0.5	1.5	1.5
Business Continuity & Disaster Recovery Procedures (uitgebreid)	Recover	2	2	2.5

In detail

Uitgebreide Gap-analyse op basis van CyFun of ISO 27001

Identify

Een diepgaandere **evaluatie van het cybersecuritybeleid en -praktijk aan de hand van het CyFun-framework (Important/Essential) of ISO 27001**. We spreken meerdere stakeholders, bekijken zowel technische als organisatorische domeinen, en brengen de volledige werking in kaart, van gebouwtoegang tot softwarebeheer. Je ontvangt een helder rapport per domein, afgestemd op het gekozen kader.

Model Inventaris van Activa (Assets)

Identify

Een **praktisch overzicht van wat beschermd moet worden: hardware, software en de gegevens die daarop verwerkt worden**.

Voor kmo's zonder geavanceerde tools bieden we een eenvoudig maar doeltreffend model dat direct inzetbaar is als basis voor risicobeheer en verdere beveiligingsmaatregelen.

Ondersteuning bij inventarisatie van Activa (Assets)

Identify

We helpen je actief bij het opstellen van een **volledig en correct overzicht van de bedrijfsmiddelen**.

Dit kan via ons standaardmodel of met eigen tools van de organisatie. Zo ontstaat er een gedragen en actueel overzicht, essentieel voor elke vorm van risicobeheer.

Opstellen rollen en verantwoordelijkheden

Identify

We ondersteunen bij het vastleggen **wie waarvoor verantwoordelijk is binnen informatieveiligheid**. Dit gebeurt via een helder en pragmatisch beleid, eventueel aangevuld met een RACI-matrix om taken en betrokkenheid duidelijk af te bakenen.

Change Management

Identify

We helpen bij het **invoeren van een werkbaar wijzigingsproces, zodat elke wijziging aan systemen of processen vooraf wordt geëvalueerd op risico en impact**.

Dit verhoogt niet alleen de cyberweerbaarheid, maar ondersteunt ook bredere controle over groei en verandering binnen de organisatie.

Monitoring en metingen

Identify

We zetten samen een **eenvoudig maar effectief kader op om veiligheidsmaatregelen te monitoren en te meten**. Zo krijg je zicht op de doeltreffendheid van de aanpak, kan je risico's tijdig bijsturen en ondersteun je structurele verbetering met meetbare resultaten.

Risicoregister

Identify

Een centraal document waarin alle relevante informatieveiligheidsrisico's gestructureerd worden vastgelegd. Het register **helpt je risico's te prioriteren, verantwoordelijken aan te duiden en investeringen beter te onderbouwen**. Zo worden risico's niet langer ad hoc aangepakt, maar systematisch opgevolgd en beheerd.

Opstellen Risk Assessment proces

Identify

We stellen een gestructureerd proces op dat toelaat om **risico's te identificeren, analyseren, beoordelen en beheersen** op een herhaalbare manier. Potentiële problemen worden sneller gedetecteerd en aangepakt, nog voor ze schade kunnen aanrichten.

Basis Ketenbeheer (TPRM Basic)

Identify

We brengen de **belangrijkste leveranciers en klanten in kaart die toegang hebben tot gevoelige gegevens of systemen**. Per partij schatten we het beveiligingsniveau in, zodat je zicht krijgt op risico's in de keten. Dit is de basisversie van Third Party Risk Management zoals voorgesteld in CyFun; eenvoudig, maar effectief.

Uitgebreid Ketenbeheer (TPRM full)

Identify

We bouwen een **volledig proces voor leveranciers- en klantenbeheer uit, als vast onderdeel van het securitybeleid**. Inclusief opvolging, geautomatiseerde bevestigingen en externe monitoring. Ideaal voor organisaties met veel partners of in gereguleerde sectoren, waar structurele controle vereist is.

Identiteits- en Toegangsbeheer

Protect

We zetten een **doordacht toegangsbeleid** op waarbij **alleen bevoegde personen toegang krijgen tot de juiste informatie**. Zo beperken we het risico op fouten, misbruik of datalekken. Ook zaken als het gebruik van gedeelde accounts, het ontbreken van MFA en vergeten toegangen van ex-medewerkers pakken we structureel aan.

Information Security Training for Management (uitgebreid)

Protect

Een **toegankelijke opleiding voor directie en management** die uitlegt wat cybersecurity inhoudt, waarom het essentieel is en welke rol het management speelt. Dit verhoogt de betrokkenheid en voldoet tegelijk aan de NIS2-verplichting rond jaarlijkse awareness.

Phishingtest

Protect

Een **gecontroleerde test waarbij medewerkers een nepmail ontvangen om hun waakzaamheid te meten**. We analyseren wie klikt of gegevens invult, en koppelen dit aan een rapport en optionele korte opleiding. Ideaal om bewustwording te vergroten en gerichte training te voorzien.

Classification & Labeling

Protect

We helpen je jouw informatie **correct te labelen volgens gevoeligheid** (bijv. 'vertrouwelijk' of 'intern'), zodat medewerkers weten hoe ermee om te gaan. Dit voorkomt fouten, zoals onbedoeld delen van gevoelige data, en zorgt voor consistent gedrag binnen de organisatie.

Cloud, Netwerk & Applicatiebeleid

Protect

We vertalen de inzichten uit analyses en risicobeoordelingen naar **concrete beleidsafspraken over cloudgebruik, netwerkstructuur en applicatiebeheer**. Deze structurele maatregelen leggen de basis voor veilige technologische keuzes en passen binnen de 'Protect'-functie van CyFun.

Toegangsbeheer (Identity & Access Management)

Protect

We zorgen ervoor dat informatie afgeschermd wordt van ongeautoriseerde personen door enkel toegang te geven tot bepaalde delen van de informatie en pas nadat iemands identiteit vastgesteld werd.

Veilige instellingen en configuraties (Secure Configuration)

Protect

Standaardinstellingen van systemen en clouddiensten zijn vaak onvoldoende veilig. We versterken deze **instellingen volgens best practices en jouw specifieke context**.

Bescherming van netwerken (Network Security)

Protect

Een veilige IT-omgeving begint bij een goed gestructureerd netwerk. We **evalueren en versterken de netwerkinrichting, segmentatie en beveiligingsmaatregelen zoals web filtering en firewallbeheer**.

Beheer van bedreigingen en kwetsbaarheden

Protect

Kwetsbaarheden in software blijven een belangrijke ingang voor cyberincidenten. We helpen met een **werkbaar proces op te zetten waarmee kwetsbaarheden tijdig opgespoord, beoordeeld en opgelost worden**.

Beveiliging van toepassingen (Application Security)

Protect

Toepassingen die zelf ontwikkeld worden of op maat worden aangepast, brengen vaak specifieke risico's met zich mee. Wij zorgen ervoor dat **veiligheidsafspraken worden ingebouwd in het ontwikkelproces en dat fouten vroegtijdig opgespoord worden**.

Beschikken over tijdige en werkende back-ups

Protect

We zorgen dat **bedrijfskritieke systemen en data voldoende worden beschermd via betrouwbare back-ups**. Samen met jou, en indien van toepassing je IT-leverancier, controleren we of de bestaande back-ups voldoen.



Procedures voor continue monitoring

Detect

Het is niet langer voldoende om slechts periodiek te monitoren. Cybercriminaliteit slaapt nooit, dus moet onze **cyberveiligheid ook voortdurend operationeel zijn en monitoring is daar een essentieel onderdeel van**. Wij zetten deze procedures voor u op.

Opstellen detectieprocessen

Detect

We stellen een **detectieproces op voor dreiging van buitenaf**. Detectieprocessen zijn de basis van alles wat met dreigingsdetectie te maken heeft binnen informatieveiligheid.

Incidentenregister

Respond

Een incidentenregister **houdt gestructureerd bij welke beveiligingsincidenten zich voordoen, hoe die werden aangepakt en wat eruit werd geleerd**. Dit register is essentieel binnen het “Respond”-domein van het CyberFundamentals Framework en verhoogt de paraatheid bij toekomstige incidenten.

Opstellen Incident Management Procedures

Respond

Een goede incidentprocedure **beschrijft wie wat doet bij een beveiligingsprobleem**. We helpen om dit proces helder en toepasbaar te maken: van eerste signalering tot communicatie en opvolging. Zo voorkom je onduidelijkheid en verhoog je de slagkracht bij incidenten.

Business Continuity & Disaster Recovery Procedures (basis)

Recover

Bij deze basisaanpak wordt gekeken naar **hoe de organisatie zich voorbereidt op onverwachte uitval: stroomonderbreking, IT-storing of cyberaanval**.

We brengen bestaande back-ups en herstelopties in kaart en geven advies om de continuïteit van de werking beter te beschermen.

Business Continuity & Disaster Recovery Procedures (uitgebreid)

Recover

Dit is een uitgebreid traject waarin we samen met de organisatie analyseren welke processen kritiek zijn, hoeveel uitval ze aankunnen (RTO/RPO) en wat er moet gebeuren bij een crisis. We bouwen een **volledig plan voor bedrijfscontinuïteit en herstel op, inclusief communicatiestrategie**. Crisismanagement is een belangrijke vereiste binnen de NIS2-regelgeving.

Extra opties

Ga je graag voor de volledig implementatie?
Dan kan je uitbreiden tot max. 50 dagen. Deze opties
kan je ook kiezen binnen het MEDIUM of PLUS Pakket.

Cingulum Aanbod	CyFun Thema	Inschatting dagen KMO <50 FTE	Inschatting dagen KMO 50-250 FTE	Inschatting dagen KMO >250 FTE
ISMS/GRC setup en tooling	Protect	2	4	6
Microsoft security baseline reconfiguration	Protect	4	6	8
Interne audit	Identify	2	3	5
Pentest (greybox)	Identify	6	7	8
M365 secure configuration analysis	Identify	2	3	4
Business Environment: Opstellen Scope & Context van de organisatie	Identify	0.5	1	1
Governance: Controle wettelijke vereisten	Identify	0.5	1	1

ISMS/GRC setup en tooling

Protect

We richten samen met jou een tool in voor het **beheren van alle processen rond beveiliging: risico's, incidenten, leveranciers, beleid, opvolging...** Zo wordt het securitymanagement gestructureerd en overzichtelijk.

Microsoft security baseline reconfiguration

Protect

We analyseren **hoe de Microsoft 365-omgeving is ingesteld en vergelijken dit met aanbevolen beveiligingsinstellingen van Microsoft** en onze eigen best practices. Denk aan toegangsbeheer, logging, dataclassificatie en detectie van incidenten.

Interne Audit

Identify

Voor organisaties die werken met het CyberFundamentals framework of streven naar ISO 27001-certificatie biedt Cingulum een **interne audit aan, uitgevoerd door erkende auditoren**. Deze audit kan ook gelden als verplichte interne controle voor ISO-trajecten.

Pentest (greybox)

Identify

Via een **gecontroleerde simulatie testen we of je systemen kwetsbaar zijn voor echte aanvallen**. Met beperkte voorkennis voeren we doelgerichte interne en externe aanvallen uit volgens erkende standaarden (OWASP/OSSTMM).

M365 secure configuration analysis

Identify

We analyseren **hoe je Microsoft 365-omgeving is ingesteld en vergelijken dit met aanbevolen beveiligingsinstellingen van Microsoft en onze eigen best practices**. Denk aan toegangsbeheer, logging, dataclassificatie en detectie van incidenten. Zo brengen we stille risico's aan het licht die ontstaan doordat standaardinstellingen niet aangepast zijn aan je organisatie. De analyse biedt gerichte aanbevelingen om de M365-omgeving beter te beschermen tegen misbruik.

Business Environment: Opstellen Scope & Context van de organisatie

Identify

We brengen in kaart welke activiteiten de organisatie uitvoert, welke data je verwerkt en wie daarbij betrokken is. Dit vormt de basis voor een doordacht informatieveiligheidsbeleid en maakt duidelijk wat precies beschermd moet worden.

Een helder afgebakende scope en context zorgen ervoor dat maatregelen gericht kunnen worden ingezet, en zijn bovendien verplicht binnen ISO 27001 en het CyFun-framework.

Governance: Controle wettelijke vereisten

Identify

We brengen in kaart welke wetten en regels van toepassing zijn op jouw organisatie, van GDPR en NIS2 tot specifieke regelgeving zoals de camerawetgeving of cao nr. 81. Je krijgt een duidelijk overzicht van wat wettelijk vereist is en hoe dat zich vertaalt naar concrete maatregelen, aangevuld met advies om eventuele lacunes weg te werken.

CUSTOMER CASE

XPO Group zet in op cyberveiligheid

Weten waar je staat

Xpo Group organiseert beurzen en exposities, op locatie in Kortrijk en internationaal. Tijdens evenementen moeten alle systemen perfect werken. De afhankelijkheid van externe partijen en cloud groeit, en Xpo Group wou daar bewust grip op krijgen. Daarom liet de organisatie haar securitybeleid en processen grondig doorlichten.

Cybersecurity structureel aanpakken

Cingulum voerde een Security Maturity Assessment uit op basis van ISO 27001, aangevuld met een gap-analyse. In gesprekken met de CEO, de IT-partner en andere sleutelfiguren ontstond een volledig beeld. Xpo Group deed dit via het VLAIO Cybersecurity Verbetertraject, met tot 50% subsidie.

"We hechten belang aan security. Dankzij Cingulum wisten we waar we stonden, en kregen we een duidelijk plan waarmee we de juiste stappen gezet hebben."

Vincent Windels,
IT & Digital & Innovation Manager, XPO Group

Mens, proces en technologie

De technische beveiliging bleek al goed op punt. De groeipunten lagen vooral bij de interne structuur, de samenwerking met leveranciers en het bewustzijn bij medewerkers. Ook de cloudmigratie kreeg extra aandacht, met het oog op een duidelijke opvolging in de toekomst.

Een concreet actieplan

Xpo Group ontving een score per onderdeel van ISO 27001 en een actieplan met stappen in volgorde van prioriteit: een securitybeleid, een applicatie-inventaris en een raamwerk voor leveranciersrisico's. Zo weet de organisatie vandaag precies waar ze staat en wat de volgende stappen zijn.



Zelf ook inzetten op cyberveiligheid?

Boek een vrijblijvende kennismaking met Lisa vandaag.



Over Cingulum

Cingulum is een Belgisch cybersecuritybedrijf dat kmo's, overheden en kritieke sectoren ondersteunt bij het opbouwen van een weerbare digitale organisatie.

We combineren technische diepgang met beleidsmatige helderheid, zodat je niet alleen ontdekt wat nodig is, maar ook hoe je het concreet kan waarmaken.

Waarom kiest u voor Cingulum?



Erkend door VLAIO

Als erkende leverancier van cybersecurity verbetertrajecten onder VLAIO, geniet je van tal van voordelen.



Pakketten op maat

Onze pakketten zijn flexibel en volledig af te stemmen op jouw noden en bedrijfscontext. Stel eenvoudig zelf je ideale pakket samen uit ons aanbod.



Pragmatische partner

Cingulum behoort tot de CRANIUM Group. Op die manier kunnen we op pragmatische manier werken als one-stop-shop voor digital compliance & governance.



Focus op cybersecurity governance

Cingulum is gespecialiseerd in cybersecurity governance en het opzetten van een ISMS. Deze expertise en ervaring nemen we rechtstreeks mee in je organisatie.

Onze missie

Pioneering a cyber-resilient society.

Wij willen elke organisatie, klein of groot, helpen om beter bestand te zijn tegen digitale dreigingen. Niet door angst aan te wakkeren, maar door helderheid, structuur en vertrouwen te bieden. Zo maken we cybersecurity werkbaar én doeltreffend.



Vragen of opmerkingen over jouw gepersonaliseerd traject?
Contacteer ons!



willem.magerman@cingulum.eu

lisa.botteldoorn@cingulum.eu
+32 (0)4 72 84 29 34

**Geïnspireerd? Vragen over onze
VLAIO offering? Contacteer
Willem, of Lisa en ontdek wat we
voor jou kunnen betekenen.**

**lisa.botteldoorn@cingulum.eu
+32 (0)4 72 84 29 34
willem.magerman@cingulum.eu**

**Algemeen telefoonnummer:
02 310 39 63**

© Cingulum, 2026

Alle rechten voorbehouden.
Niets uit deze uitgave mag
worden verveelvoudigd en/of
openbaar gemaakt worden door
middel van druk, fotokopie,
microfilm of op welke andere
wijze ook, zonder voorafgaande
toestemming van Cingulum.