



SECURERESULT Vertrouwelijk

# ASSESSMENT INFORMATIEBEVEILIGING HUMANKind



YOUR INFORMATION SECURITY & PRIVACY PARTNER

Wie we zijn

Wat we doen

Voor wie we werken

Ons voorstel

## Kenmerken

- Sinds 2016
- 25 medewerkers
- Utrecht
- Onafhankelijk



## Missie

- Wij maken de digitale wereld veiliger!

## Kernwaarden

- Vertrouwen
- Authenticiteit
- Samenwerken
- Expertise

## Visie

- Onze digitale wereld is snel en complex en vraagt om steeds verder gaande bescherming van data, intellectueel eigendom en netwerken. Met de expertise van Securesult streven we ernaar om voor de klant een wendbare, innovatieve en leidende rol te spelen als meest betrouwbare partner in informatiebeveiliging en cybersecurity.

Daarmee dragen we bij aan het beveiligen van de digitale toekomst van Nederland.

# Wet- en regelgeving schept kaders en eisen

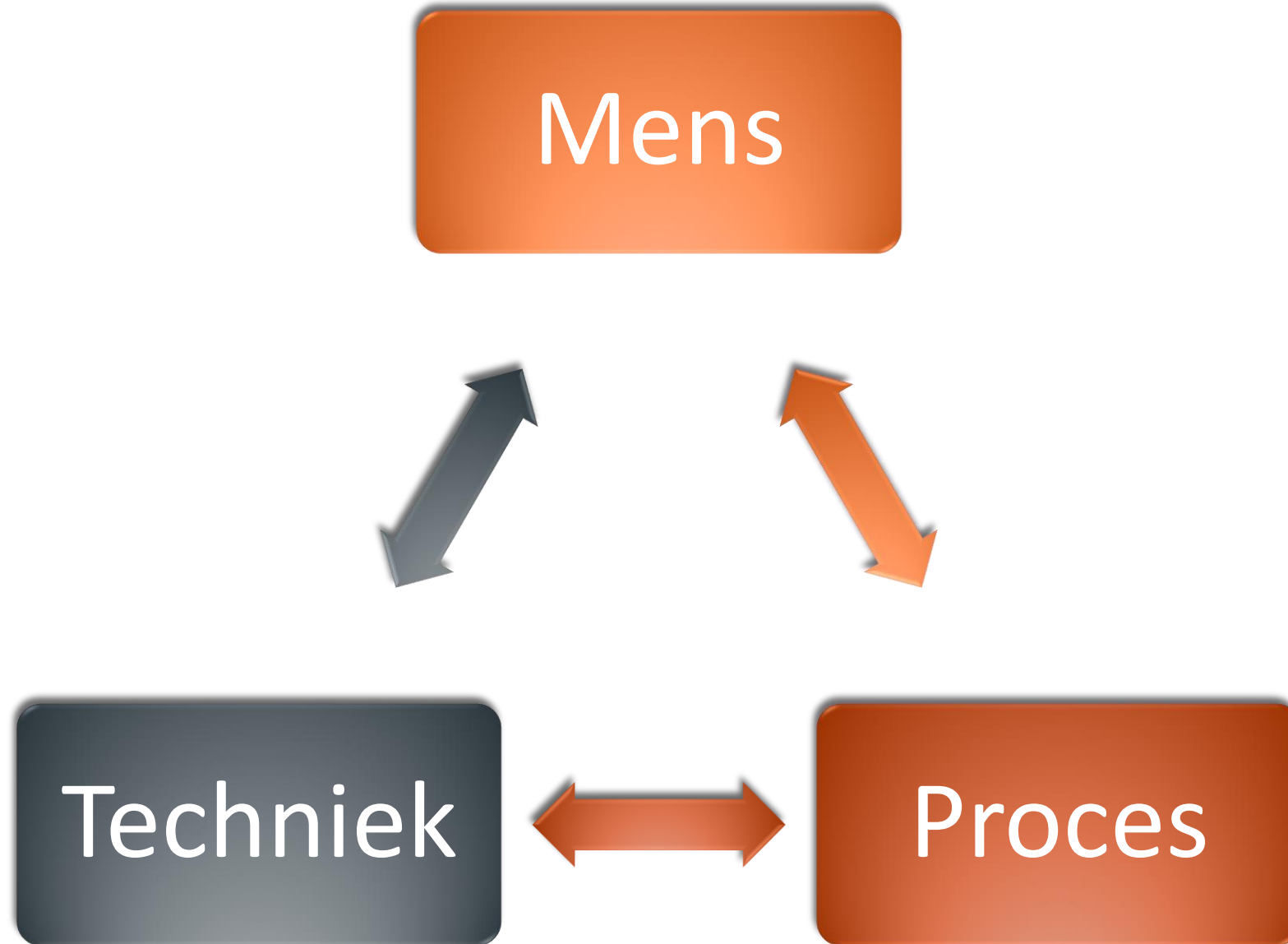


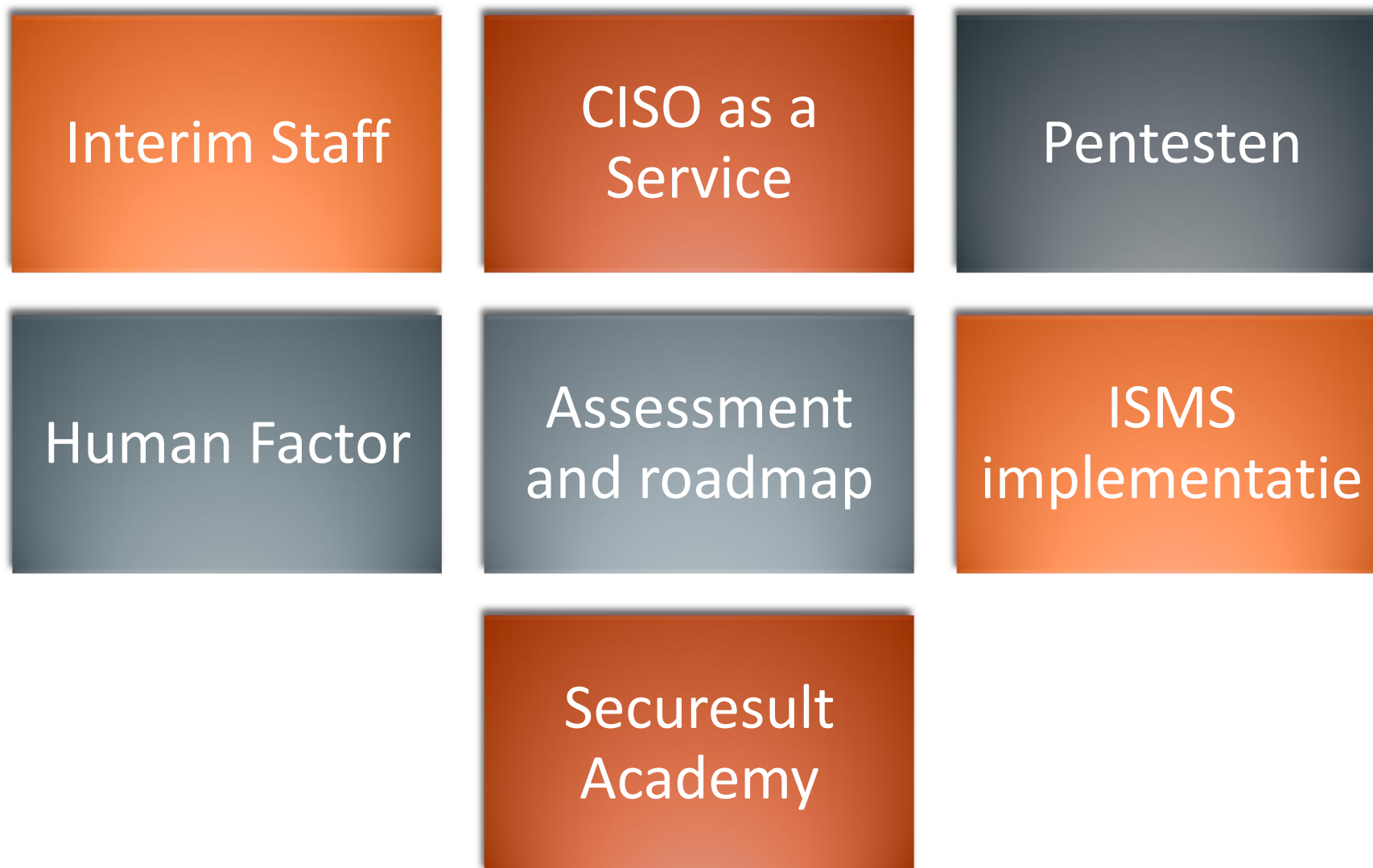
**BIO**

Baseline  
Informatiebeveiliging  
Overheid



YOUR INFORMATION SECURITY & PRIVACY PARTNER









**YOUR INFORMATION SECURITY & PRIVACY PARTNER**

- Overheid
- Onderwijs
- Zorg
- Financiële dienstverleners
- Commercieel







# ONTWIKKELINGEN

YOUR INFORMATION SECURITY & PRIVACY PARTNER

# EU's Digital Decade Strategy



# Observaties waar het vaak beter kan

Bedrijfscontinuïteit

Risicomanagement

Assetmanagement

Eigenaarschap

Leveranciersmanagement

Bewustwording en gedrag

Monitoring en respons

IB organisatie niet aanwezig



- ISO 27001 / NEN 7510 / BIO 2.0
- NIS-2
- DORA
- NIST CSF
- CIS controls
- ...

- Interne beheersing
- Verantwoording + eigenaarschap
- CISO + IB(&P) team
- ISMS
- Risicomanagement + risicoregister
- BCM
- Incidentbeheer + melden
- (Keten)Leveranciersmanagement
- Bewust zijn
- ...

## Wachten of op anticiperen?





# VOORSTEL HUMANKIND

YOUR INFORMATION SECURITY & PRIVACY PARTNER



HumanKind (3.800 medewerkers, 500 locaties) hoeft niet te voldoen aan een norm zoals ISO of NEN, echter er is wel eens wens om grip te krijgen op de informatiebeveiliging.

De huidige ICT leverancier heeft een aantal maatregelen genomen, echter of deze passend en effectief zijn is niet bekend.

Er is behoefte aan een assessment van de status van de informatiebeveiliging, organisatiebreed, alsmede een advies op welke vlakken zaken verbeterd kunnen worden.

- Waar liggen de risico's?
- Hoe ziet de informatiebeveiligingsorganisatie eruit?
- Welke belangrijke leveranciers zijn er, welke eisen hebben jullie gesteld en hoe hebben zij hun informatiebeveiliging ingericht?
- Hoe ziet de ICT omgeving eruit?
- Worden medewerkers bewust gemaakt van risico's?

## 1. Intake en Planning

- Een initiële intake op locatie om uw specifieke behoeften en uitdagingen te begrijpen. We stemmen de planning af en bepalen de taakverdeling.

## 2. Business Impact Analyse (BIA)

- Identificeren van kritieke processen en systemen, en het bepalen van de impact van potentiële onderbrekingen.

## 3. Assessment (Nulmeting)

- Uitvoeren van een uitgebreide nulmeting om te bepalen in hoeverre uw organisatie voldoet aan de relevante normen (zoals ISO 27001, NEN 7510, BIO en NIS-2). Dit omvat interviews, documentstudie en technische analyses.

## 4. Human Factor

- Interviews en een vragenlijstonderzoek geven inzicht in het huidige bewustzijn, kennis en gedrag van medewerkers.

## 5. Technische Analyse (Pentest Light)

- Scannen van uw infrastructuur op aanwezige kwetsbaarheden en het opnemen van deze kwetsbaarheden in een risicoregister.

## 6. Risicoanalyse

- Op basis van de resultaten van de BIA, Human Factor Assessment en Technische Analyse, voeren we een risicoanalyse uit om prioriteiten vast te stellen.

## 7. Roadmap

- Ontwikkelen van een gedetailleerde roadmap met stappen om van de huidige situatie (ist) naar de gewenste situatie (soll) te komen, inclusief planning en kostenraming.

## 8. Rapportage en presentatie

- U ontvangt een uitgebreide rapportage met onze bevindingen, aanbevelingen en een op maat gemaakte roadmap. Deze resultaten presenteren we aan uw team.

- Uitvoering information security assessment
  - Mens
  - Proces
  - Techniek
  - 8 stappen plan
- Na uitvoering assessment en roadmap vaak lange termijn ondersteuning in regievoering over informatiebeveiliging middels CISO as a Service contract
- Prijs € 7.000 - € 15.000 afhankelijk van scope

- In eerste instantie een brede vraag over status van beveiliging.
- Later aangescherpt op IT dienstverlening
  - Networks-as-a-Service
  - Firewalls-as-a-Service
  - WiFi-as-a-Service
  - Werkplek-as-a-Service
  - SOC (?!)
- Meer een second opinion vraag over de mate van beveiliging van de geleverde diensten.



Binnen de scope van deze scan vallen:

- Testen van de beveiliging van de door Ilionx geleverde Microsoft business platforms/services tegen externe dreigingen: hoe makkelijk/moeilijk is het om bij informatie/resources van Humankind te komen, zijn er zwakke plekken?
- De beveiliging van de infrastructuur op één kinderopvang-locatie (Ilionx levert deze ‘as a service’ eenvormig voor alle locaties: internetverbinding, modem, wifi-router, accesspoints): hoe makkelijk/moeilijk is het om toegang te krijgen tot informatie/resources van Humankind?
- Een beoordeling van de veiligheid van de architectuur zoals Ilionx die heeft ingericht om de dienstverlening aan Humankind in te vullen.
- Toelichting bij dit laatste punt: hoewel Ilionx zich wil beperken in het vrijgeven van teveel details over de ‘interne’ beveiliging, staan ze open voor een dialoog op consulting basis over hoe een en ander is ingericht.
- Dit zal dan de vorm hebben van één of enkele gesprekken tussen een specialist van jullie en een specialist van Ilionx.

Buiten de scope van deze scan vallen:

- De beveiliging van devices/endpoints.
- SaaS oplossingen MerCash en KidsVision, deze zijn in een eerdere scan al beschouwd.



## Scoping + Offerte

- Exacte scope afstemmen
- Offerte opstellen
- Akkoord?

## Kick-off

- Voorbereidingen en afspraken
- Vrijwaring (incl Ilionx) en credentials
- Op te leveren documentatie
- Contactgegevens

## Cyber Security assessment op hoofdkantoor.

- Netwerk en netwerkcomponenten

## Servers (Azure en evt. on premise)

- Aanleveren van IP-adressen (wat wel of juist niet)
- Microsoft omgeving (Exchange Online, Sharepoint Online, Microsoft 365, Teams, Azure platform, Azure Active Directory)
- Scans van buitenaf (zonder credentials) en van binnenuit (met credentials) om risico's goed inzichtelijk te krijgen.

## Pentest infra van KDV locatie

- Netwerk
- WiFi

## Review Architectuur

- Documentstudie
- Interview met architect van Ilionx

## Red Teaming

- Testen van SOC alarmeringsniveau
- Testen van SOC escalatielijnen

## Rapportage en presentatie

- Analyseren van resultaten
- Opstellen van rapportage
- Presenteren van Bevindingen, conclusies en aanbevelingen

## Optioneel: hertest

- Hertesten van opgeloste bevindingen

- Gebruik van standaard Microsoft security tooling
  - Zelf of managed?
- Bevindingen gebruiken om betere (beveiligings)eisen te stellen aan Ilionx.
- Scan uitbreiden met Mens en Proces
- Scan gebruiken om risico's Co-Pilot for M365 te inventariseren (classificeren + labelen van informatie)
- CISO-as-a-Service / Security Office-as-a-Service

# Security Office as a Service abonnementen

<b>Bronze</b> max 50 fte € 1.500/mnd	<b>Silver</b> 50-100 fte € 3.250/mnd	<b>Gold</b> 100-250 fte € 4.500/mnd	<b>Platinum</b> 250-5.000 fte Vanaf € 5.000/mnd
<ul style="list-style-type: none"> <li>• 4 uur CISO per maand</li> <li>• ISMS / IRM360 <ul style="list-style-type: none"> <li>• Risico analyse</li> <li>• Incidentenregister</li> <li>• Roadmap en actieplan</li> </ul> </li> <li>• Jaarlijkse Awareness workshop (digitaal)</li> <li>• Management meeting (mnd/kwartaal)</li> </ul>	<ul style="list-style-type: none"> <li>• 8 uur CISO per maand</li> <li>• ISMS / IRM360 <ul style="list-style-type: none"> <li>• Risico analyse</li> <li>• Incidentenregister</li> <li>• Roadmap en actieplan</li> <li>• Normbegeleiding (ISO/NEN/NIS-2/DORA)</li> </ul> </li> <li>• Jaarlijkse Awareness workshop</li> <li>• Eens per kwartaal Awareness training voor nieuwe medewerkers</li> <li>• 1x per jaar basis pentest</li> <li>• Management meeting (kwartaal)</li> </ul>	<ul style="list-style-type: none"> <li>• 16 uur CISO per maand</li> <li>• ISMS / IRM360 <ul style="list-style-type: none"> <li>• Risico analyse</li> <li>• Incidentenregister</li> <li>• Normbegeleiding (ISO/NEN/NIS-2/DORA)</li> <li>• Leveranciersmanagement</li> </ul> </li> <li>• Security Awareness Programma <ul style="list-style-type: none"> <li>• Dashboard</li> <li>• E-learning nw medewerkers</li> <li>• Jaarlijkse E-learning</li> <li>• 2x per jaar Phishing campagne</li> </ul> </li> <li>• 1x per jaar pentest + hertest</li> </ul>	<ul style="list-style-type: none"> <li>• Maatwerk op basis van analyse</li> <li>• X uur / mnd CISO</li> <li>• Normering / Standaarden (ISO, NEN, NIS-2, DORA)</li> <li>• ISMS / IRM360</li> <li>• Security Awareness Programma <ul style="list-style-type: none"> <li>• Phishing</li> <li>• Training</li> <li>• Vishing</li> </ul> </li> <li>• Pentesten</li> <li>• Vulnerability scanning</li> <li>• SOC</li> <li>• Incident response</li> </ul>



DANK

YOUR INFORMATION SECURITY & PRIVACY PARTNER