



sirris





Cybersecurity Awareness

met focus op IloT

(Industrial Internet of Things)

Aanbod voor de metaal- en technologische industrie

Webinar 10/10/2024





Wat mag je verwachten van dit webinar?



Wat mag je verwachten van dit webinar?

- Belang van awareness cybersecurity



Wat mag je verwachten van dit webinar?

- Belang van awareness cybersecurity
- Wie willen wij bereiken?



Wat mag je verwachten van dit webinar?

- Belang van awareness cybersecurity
- Wie willen wij bereiken?
- Opleidingsaanbod in het domein cybersecurity



Wat mag je verwachten van dit webinar?

- Belang van awareness cybersecurity
- Wie willen wij bereiken?
- Opleidingsaanbod in het domein cybersecurity
- Cybersecurity toolkit



Wat mag je verwachten van dit webinar?

- Belang van awareness cybersecurity
- Wie willen wij bereiken?
- Opleidingsaanbod in het domein cybersecurity
- Cybersecurity toolkit
- (Financiële) ondersteuning
 - mtech+
 - Sirris
 - Agoria
 - Overheid (VLAIO)



Wie begeleidt je doorheen dit webinar?



Mario Naessens

Expert kenniscentrum - mtech+



Christophe Michiels

IoT Engineer - Sirris



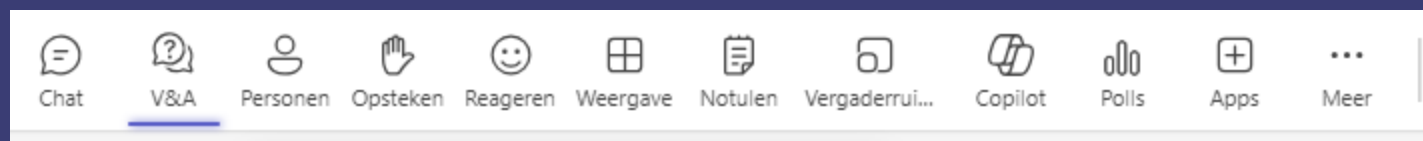
Bert Vanderhallen

Technical Coördinator/Trainer - Limtec+



Enkele praktische afspraken?

- Open de V&A in het webinar



- Polls

- Gesloten vraag: ja = 
- Open vraag: formuleer je antwoord in de discussie



Awareness - Poll

Heeft je bedrijf al een cybersecurity-incident meegemaakt?

Awareness



Awareness voorbeeld uit de industrie

- Tweede bekende ICS-aanval na Stuxnet
- Kwam het netwerk binnen via spear-phishingmail
 - Goed gemaakt dankzij social engineering
 - Bijlage bevatte malware
 - Toegang op afstand tot het controlecentrum van de hacker
 - **Aangepaste PLC-code**
 - Veroorzaakte een fout in de ovenbesturing
 - Resultaat -> ongecontroleerde oven
 - Veroorzaakte fysieke schade en stilstand van de staalfabriek



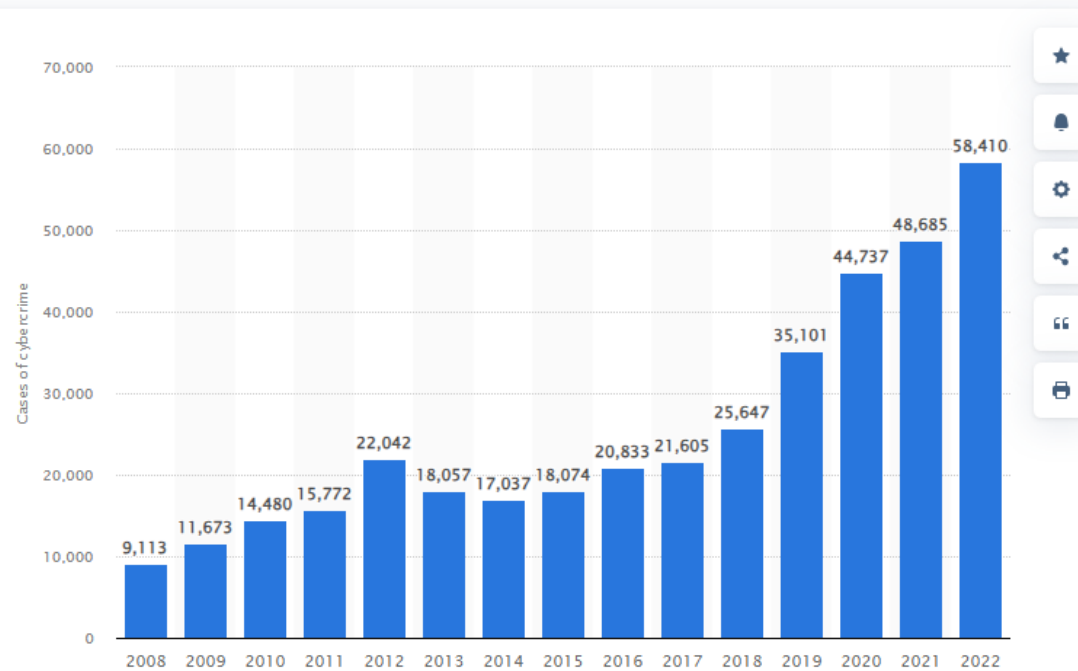
Awareness

€€€€€

Awareness

One in three companies faced at least one cybersecurity incident in 2022

Registered cases of cybercrime in Belgium from 2008 to 2022



[Additional Information](#)

© Statista 2024

[Show source](#)



Awareness

Awareness - Poll

Wie ondernam er reeds acties op de werkvloer (productieomgeving) om zich te wapenen tegen cyberincidenten?



Awareness

Awareness - Poll

Wie ondernam er reeds acties op de werkvloer (productieomgeving) om zich te wapenen tegen cyberincidenten?

Welke actie werd ondernomen?



Awareness



Specifieke acties in te zetten naar de IIoT omgeving



Specifieke acties in te zetten naar de IIoT omgeving

- Opleiding





Specifieke acties in te zetten naar de IIoT omgeving

- Opleiding
- Toolkit





Specifieke acties in te zetten naar de IIoT omgeving

- Opleiding
- Toolkit



Opleidingsaanbod



Opleiding

Opleidingsaanbod

- mtech+
- Sirris
- Agoria



Opleiding

Opleidingsaanbod

- mtech+
 - Cybersecurity – preventie, detectie & reactie
19/11/2024 - Roeselare
 - IIoT cyberveiligheid – een praktische aanpak
Start 04/11/2024 - Gent
Start 03/02/2025 - Diepenbeek
 - Internet of Things – datacaptatie & visualisatie
Start 27/11/2024 - Roeselare
 - IO-Link technologie – intelligente industriële systemen
Start 25/11/2024 - Roeselare



Opleiding

Opleiding

Cybersecurity – preventie, detectie & reactie

- Doelgroep

Information Technology Managers, Information Security Officers, Risk Managers, Quality Managers en Business Executives met het doel om meer te leren over de Informatiebeveiliging Managementsysteem eisen zoals gespecificeerd in de ISO 27001 norm.

- Programma

1. Wat is ISO 27001 (informatieveiligheidsmanagement)?
2. Waarom is een ISO27001 certificering belangrijk?
3. Wat zijn de voordelen om ISO 27001 gecertificeerd te zijn?

- Aanpak

Klassikale opleiding

- Link

<https://mtechplus.be/opleidingen/cybersecurity-preventie-detectie-reactie/>



Opleiding

Opleiding

IIoT - cyberveiligheid in de praktijk

- Doelgroep
 - Onderhoudstechnici, procesingenieurs, technische aankopers, technisch verantwoordelijken of profielen met een technische background die hun bedrijf/afdeling cybersecure willen organiseren en vrijwaren.
- Programma
 - General cybersecurity awareness + cybersecurity toolbox
 - How to manage devices security
 - Aligning IT-OT on cybersecurity
 - Incident response
 - Supply Chain Security
 - Byers Guide to shopfloor assets
- Aanpak
 - Klassikaal, interactief, praktisch & per onderwerp een relevante demo
 - In de opleiding zit een train the trainer vervat voor het overbrengen van de thema's naar de werkvloer
 - Iedere deelnemer ontvangt de toolkit
- Link

<https://mtechplus.be/opleidingen/iiot-cyberveiligheid-een-praktische-aanpak/>

ma. 04 nov.	13:00 - 17:00
wo. 13 nov.	13:00 - 17:00
ma. 18 nov.	13:00 - 17:00
ma. 25 nov.	13:00 - 17:00



Opleiding

Opleidingsaanbod

- **Sirris** - masterclasses
 - **NIS2 voor de maakindustrie**
 - 7/11/2024 HoM - Kortrijk
 - <https://www.sirris.be/nl/agenda/cybersecurity-de-maakindustrie-nis2-van-kracht-wat-nu>
 - **Cybersecurity en software ontwikkeling**
 - 28/11/2024 Technologie park - Gent
 - <https://www.sirris.be/nl/agenda/cybersecurity-voor-ontwikkelaars-van-digitale-diensten-betrouwbare-toepassingen-ontwikkelen>
 - <https://www.sirris.be/nl/agenda>



Opleiding

Opleidingsaanbod

- Agoria



Opleiding

Opleidingsaanbod

- Agoria

.A



Het is 2 voor 12!
Cybersecurity is niet langer een optie, maar een absolute noodzaak.

Vergroot je kennis. Schrijf je nu in voor de **gratis e-tutorial**.

Cyberstart

- Ontvang **1x per week** een **e-mail** met heldere, concrete tips & tricks die makkelijk toepasbaar zijn
- Maak je bedrijf weerbaarder op vlak van cyberveiligheid
- Zet haalbare stappen naar meer gemoedrust
- Vergroot je kennis dankzij balans tussen theorie en praktijk

Tijdens dit traject van 30 weken bouw je stap per stap kennis en een concreet implementatieplan uit om binnen je bedrijf aan de slag te gaan met cyberveiligheid.



www.cyberstart.be

AGENTSCHAP INNOVEREN & ONDERNEMEN **AGORIA** samen voor
sirris **#sterkondernemen**

Opleiding



Opleidingsaanbod

- Agoria

.A

Masterclass: Cybersecurity in 30 steps

- Are you looking to elevate your knowledge and understanding of cybersecurity? Look no further than our comprehensive basic training course 'Cybersecurity in 30 Steps'.
- Whether you are a beginner venturing into this field or someone seeking to refresh your existing knowledge, this course offers an excellent foundation for creating a robust cybersecurity policy in your office environment.
- Upon completion, you will be:
 - ✓ Well informed on essential aspects of cybersecurity.
 - ✓ Able to implement effective security measures.
 - ✓ Ready to minimise the risks of digital threats.
- Dates
 - [22/10/2024: Gent \(NL\)](#)
 - [12/11: Hasselt \(NL\)](#)
 - [12/12/2024: Kortrijk \(NL\)](#)



Opleiding





Specifieke acties in te zetten naar de IIoT omgeving

- Opleiding
- **Toolkit**



Cybersecurity toolkit



Toolkit



Cybersecurity toolkit

- Doel
 - Op *regelmatige basis* de cybersecurity awareness van de shopfloor- medewerkers verhogen (operatoren, proces- & onderhoudsengineers, ...)
- Wanneer
 - Dagstart, team of shift transfer meetings
- Hoe
 - Kaart deck



vraag

Wat is een **jump host** en waarom wordt deze gebruikt?

mtech+ + sirris



antwoord

Een jump host is een sterk beveiligde server die wordt beheerd door IT. Het is de toegangspoort tot andere delen van het netwerk.

mtech+ + sirris

Toolkit

Cybersecurity toolkit

▪ Leer mode

- Een persoon neemt een kaart -> leest vraag & antwoord luid voor
 - Bespreek in groep of deze kaart toepasbaar is en hoe te implementeren
 - Bewaar in de toepasbare of niet toepasbare hoop
 - Indien nodig een proces- of onderhoudsengineer kan extra uitleg geven
- Herhaal
 - Meerdere kaarten per sessie, elke dag, elke week, ...

▪ Quiz mode

- Een persoon neemt een kaart -> leest de vraag luid voor
 - Probeert een goed antwoord te formuleren
 - Beslis/bespreek in groep of het antwoord voldoende was
 - Controleer het juiste antwoord
 - Indien nodig een process of onderhouds engineer kan extra uitleg geven
- Herhaal
 - Meerdere kaarten per sessie, elke dag, elke week, ...



Toolkit

Aansluitend opleidingsaanbod Limtec+



Opleiding



Aansluitend opleidingsaanbod Limtec

- Praktische demo's binnen cybersecurity



Opleiding

Aansluitend opleidingsaanbod Limtec

- Praktische demo's binnen cybersecurity
- Opleiding IO-Link



Opleiding

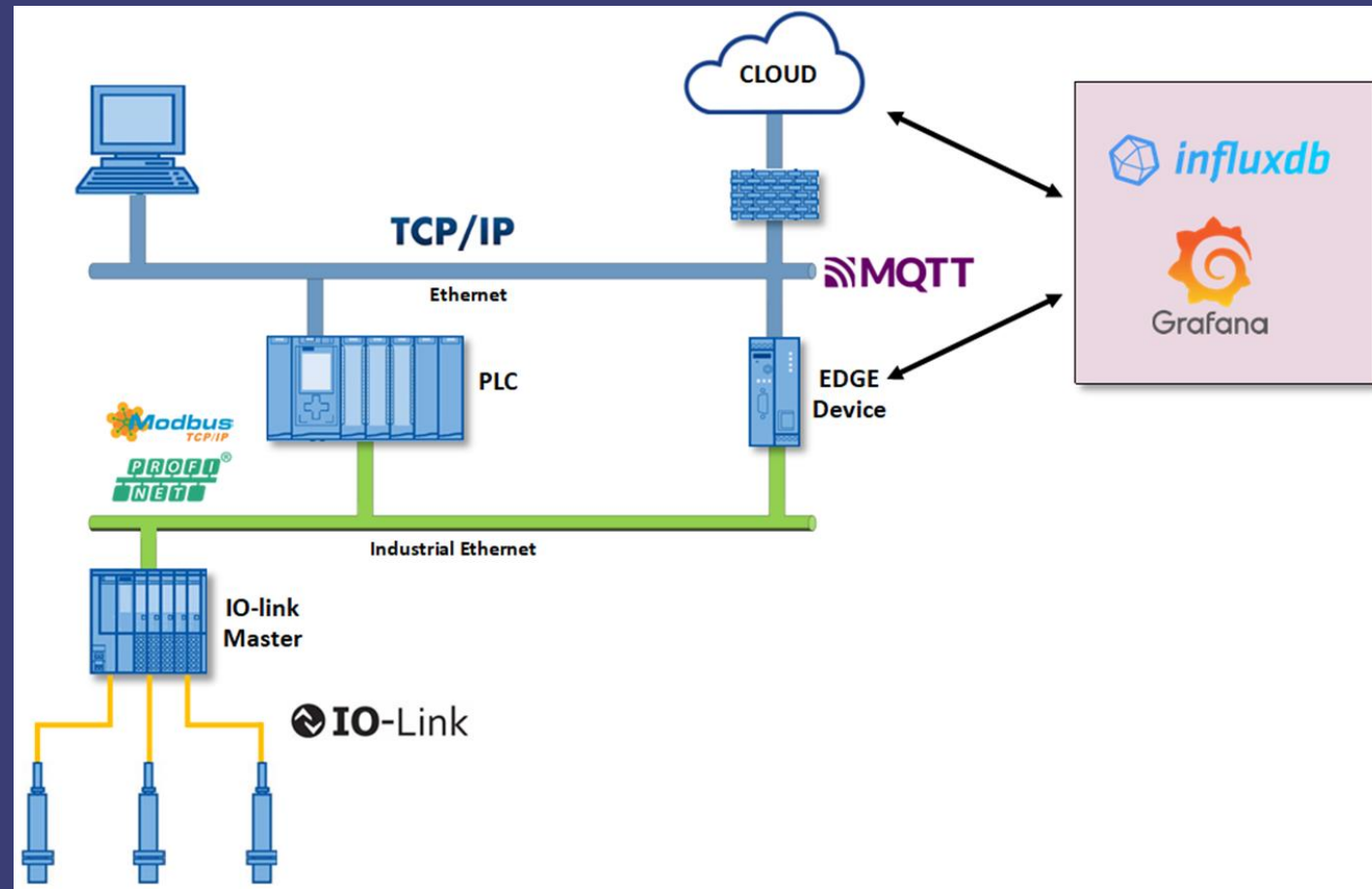
Aansluitend opleidingsaanbod Limtec

- Praktische demo's binnen cybersecurity
- Opleiding IO-Link
- Opleiding IIoT data captatie en visualisatie



Opleiding

Opleidingen IIoT?



Opleiding



Opleiding

IO-Link technologie – intelligente industriële systemen

- Doelgroep

- Onderhoudstechniekers en engineers die aan de slag willen gaan met IO-Link of er al mee gestart zijn maar nog niet over voldoende kennis beschikken.

- Programma

- Inleiding tot IO-Link technologie
 - Wat is IO-Link?
 - Basisprincipes van point-to-point communicatie
 - IO-Link systeem architectuur
- IO-Link protocol stack
 - Fysieke laag : bekabeling, connectoren en elektrische specificaties
 - Data Link laag : communicatie protocollen
- IO-Link masters
 - Siemens ET200SP – CM 4xIOlink
 - MURR Impact67
 - Sick SIG350
 - Commissioning van IO-Link masters
 - Siemens PCT-Tool
- IO-Link slaves
 - Siemens PCT-Tool
 - MURR IO-Link Device tool
 - Web-based commissioning (SICK SIG350)
- IO-Link communicatie
 - Cyclische en acyclische communicatie
 - Diagnose mogelijkheden en foutopsporing
 - Procesalarmen
- IO-Link devices
 - SICK WL4SC, IFM PQ3809 en TURCK H1 141
 - IO-DD – IO Device Description
 - Commissioning van IO-Link devices
 - ONLINE : Port and Device Configuration Tools
 - OFFLINE : IO-Link USB-masters
 - IO-Link backup en restore



Opleiding

Opleiding

Internet Of Things – datacaptatie en visualisatie

- Doelgroep

- Onderhoudstechniekers en engineers die aan de slag willen gaan met dataverwerking of er al mee gestart zijn maar nog niet over voldoende kennis beschikken.

- Programma

- Node-RED

- Kennismaking met Node-RED
 - Werking en debugging van flowgebaseerde programmering
 - Datacaptatie via industriële protocollen: S7-comm, TwinCAT ADS,...
 - Datacaptatie via industriële protocollen: Modbus-TCP, OPC UA,...
 - Datacaptatie via IT protocollen: MQTT, REST API,...
 - Visualisatie via Dashboards

- Siemens IoT2050

- Kennismaking met linux gebaseerde edge device
 - Putty gebruiken als interface naar de edge device
 - Configuratie en beheer via WinSCP, BalenaEtcher,...
 - Basis Linux instructies voor instellingen van: boot, netwerk,...
 - Installeren en updaten van applicaties

- IoT stacks

- Overzicht van de verschillende IoT stacks: MING, TICK, MING,...
 - Praktisch aan de slag met de MING Stack
 - Werking en gebruik Mosquitto als MQTT broker
 - Historisch opslaan van data m.b.v. influxDB
 - Visualisatie van data m.b.v. Grafana

- Cloud communicatie

- Verzamelde data via MQTT naar de cloud sturen



Opleiding



Ondersteuning

- mtech+
- Sirris
- Agoria
- Overheden (VLAIO)

Ondersteuning



Ondersteuning mtech+

- **Gratis opleiding**

Ondersteuning



Ondersteuning mtech+

- **Gratis opleiding**
- **Financiële ondersteuning interne opleidingen**

Ondersteuning



Ondersteuning mtech+

- **Gratis opleiding**
- **Financiële ondersteuning interne opleidingen**
- **Subsidiedossier**

Ondersteuning



Ondersteuning mtech+

- **Gratis opleiding**
- **Financiële ondersteuning interne opleidingen**
- **Subsidiedossier**
 - **Werkbaar werk**
 - **Duurzame inzetbaarheid**
(bijv. traject om digitale vaardigheden en kennis te verhogen)
 - **Geëngageerd leiderschap**

Ondersteuning

Meer info: contacteer uw regionale account



Ondersteuning Sirris

- **Advies in veilige Industrie 4.0 architectuur**
 - <https://www.sirris.be/nl/expert/christophe-michiels>
- **NIS2 voor de maakindustrie**
 - 7/11/2024 HoM - Kortrijk
 - <https://www.sirris.be/nl/agenda/cybersecurity-de-maakindustrie-nis2-van-kracht-wat-nu>
- **Cybersecurity en software ontwikkeling**
 - 28/11/2024 Technologie park - Gent
 - <https://www.sirris.be/nl/agenda/cybersecurity-voor-ontwikkelaars-van-digitale-diensten-betrouwbare-toepassingen-ontwikkelen>

Ondersteuning

Ondersteuning Agoria

A



Buyers guide: Software supply chain risk management



Deze gids helpt u met:



- U krijgt aan de hand van reële voorbeelden inzicht in de bekendste supply chain risico's.
- U komt meer te weten over een aantal **nieuwe (Europese en Amerikaanse) wetten en regels** die deze risico's moeten helpen indammen.
- U leert, aan de hand van een stappenplan en een handig overzicht van vragen om zeker aan uw softwareleveranciers te stellen, **hoe uw onderneming aan risicobeheersing kan doen** voor software die ze van derden betreft.
- Ten slotte bevat deze buyer's guide ook heel wat **verwijzingen naar meer informatie, hulp en steun**, bijvoorbeeld van de Vlaamse overheid.

Ce guide peut vous y aider :



- Des exemples concrets vous permettront de mieux comprendre les **risques les plus connus liés à la chaîne d'approvisionnement**.
- Vous en apprendrez davantage sur un certain nombre de **nouvelles lois et règles (européennes et américaines)** visant à endiguer ces risques.
- À l'aide d'une feuille de route et d'une liste pratique de questions à poser à vos fournisseurs de logiciels, vous apprendrez **comment votre entreprise peut gérer les risques liés aux logiciels qu'elle acquiert auprès de tiers**.
- Enfin, ce guide d'achat contient en outre de nombreuses **références permettant d'accéder à des informations, une aide et un soutien complémentaires**, comme ceux proposés par les autorités flamandes.

Ondersteuning



VLAIO – Subsidiering en financiering Cybersecurity verbetertrajecten

Ondersteuning



VLAIO – Subsidiering en financiering Cybersecurity verbetertrajecten

- Voor wie?
 - Vlaamse kmo's / niet kmo's die onder de NIS2-richtlijn vallen
 - Kmo-definitie
 - NIS2-richtlijn: maakindustrie valt hier onder

Ondersteuning



VLAIO – Subsidiering en financiering Cybersecurity verbetertrajecten

- Voor wie?
 - Vlaamse kmo's / niet kmo's die onder de NIS2-richtlijn vallen
 - Kmo-definitie
 - NIS2-richtlijn: maakindustrie valt hier onder
- Voor wat?
 - Inkopen van extern advies en begeleiding inzake cyberveiligheid

Ondersteuning



VLAIO – Subsidiering en financiering Cybersecurity verbetertrajecten

- Voor wie?
 - Vlaamse kmo's / niet-kmo's die onder de NIS2-richtlijn vallen
 - Kmo-definitie
 - NIS2-richtlijn: maakindustrie valt hier onder
- Voor wat?
 - Inkopen van extern advies en begeleiding inzake cyberveiligheid
- Voor welk bedrag:
 - 50% steun voor kmo's voor trajecten tussen de € 8.500 en € 35.000
 - Verlaagd steunpercentage van 35% voor niet-kmo's die onder de NIS2-richtlijn vallen

Ondersteuning



VLAIO – Subsidiering en financiering Cybersecurity verbetertrajecten

- Voor wie?
 - Vlaamse kmo's / niet kmo's die onder de NIS2-richtlijn vallen
 - Kmo-definitie
 - NIS2-richtlijn: maakindustrie valt hier onder
- Voor wat?
 - Inkopen van extern advies en begeleiding inzake cyberveiligheid
- Voor welk bedrag:
 - 50% steun voor kmo's voor trajecten tussen de € 8.500 en € 35.000
 - Verlaagd steunpercentage van 35% voor niet kmo's die onder de NIS2-richtlijn vallen
- Aangeduide dienstverleners bij wie je terecht kan
- Link VLAIO: <https://www.vlaio.be/nl/subsidies-financiering/cybersecurity-verbetertrajecten>

Ondersteuning



Nog vragen naar aanleiding van dit webinar?

Neem gerust contact op

Christophe Michiels – Sirris
christophe.michiels@sirris.be

+32 478 43 99 64

Bert Vanderhallen – Limtec
+32 89 20 32
bert.vanderhallen@limtec.be

Mario Naessens – mtech+
mario.naessens@mtechplus.be
+32 497 52 97 78

In samenwerking met



mtech+

sirris innovation
forward

.AGORIA





sirris

