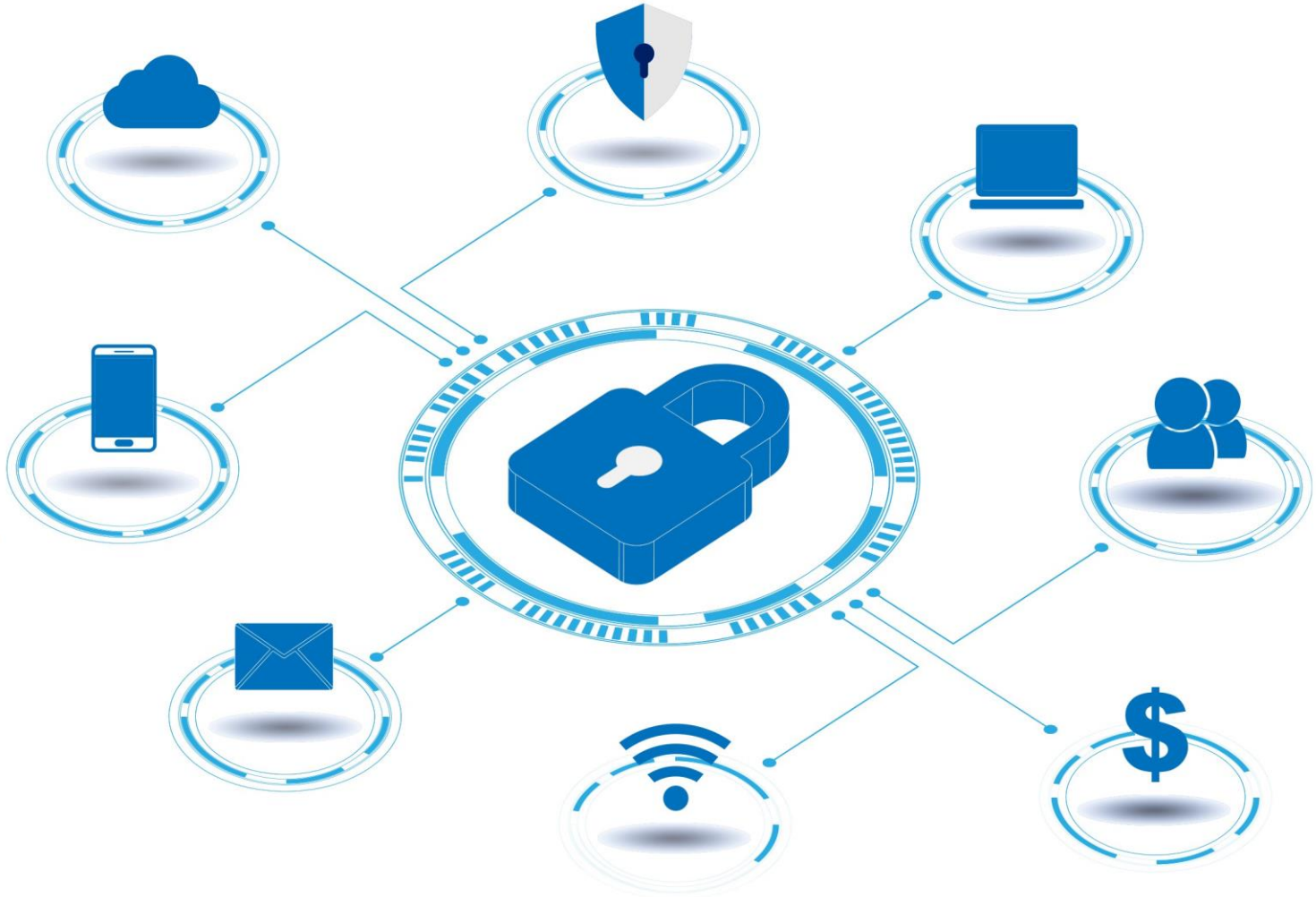
Objectif Cyber-sérénité

RELEVEZ LES DÉFIS DE LA CYBERSÉCURITÉ DANS UN SECTEUR MANUFACTURIER EN PLEINE DIGITALISATION

THIERRY COUTELIER - SIRRIS

CYBER RESILIENCE

CyberActive



sirris innovation forward

VUB VRIJE UNIVERSITEIT BRUSSEL

UCLouvain

howest hogeschool

Funded by

economie

Funded by the European Union

NextGenerationEU

Agenda

- Mise en contexte – quelques chiffres
- Convergence IT-OT
- Connaître son ennemi et vecteurs d'attaque
- La gestion de votre parc IT-OT (prestataires et/ou ressources internes)
- Ransomware
- Contrôles d'accès et mots de passe
- Machines et atelier connectés
- Accès à distance sécurisée
- Phishing
- NIS2
- Conclusion

Introduction

50 % des entreprises craignent d'être victimes d'une cyberattaque au cours de l'année à venir
58 % des grandes entreprises industrielles ont connu une faille de sécurité sur leur système OT en 2021
61 % déclarent que les systèmes OT obsolètes constituent un défi pour la réduction des cyber-risques
38% manquent d'expertise interne pour détecter une attaque
93 % des entreprises admettent que leur stratégie de cybersécurité est inadéquate
25 % des entreprises belges disposent d'un plan d'urgence qui couvre à la fois l'IT et l'OT

www.agoria.be/fr/etude-Cyber-securite-dans-industrie-manufacturiere
www.agoria.be/nl/studie-Cybersecurity-in-de-maakindustrie

- La plupart des PME **manquent de sensibilisation et de connaissances sur les risques de cybersécurité** dans le domaine des technologies de l'information.
- Leur environnement OT est **extrêmement vulnérable** sur le plan technologique et elles ne sont pas en mesure de réagir de manière adéquate et de se remettre rapidement d'un incident de cybersécurité OT.
- Les responsables de l'OT manquent souvent d'informations de base essentielles pour mettre en œuvre une politique de sécurité efficace. Une politique de sécurité OT appropriée est souvent inexistante et **rarement intégrée à la politique de sécurité IT**.

Track record – Cyber-attaques

January
- Lush
- Foxsemicon
- Schneider Electric
- Benetton
- Veolia
- Hewlett Packard
- Southern Water
- Muscatine Power and Water

February
- Etesia
- Kind
- Varta
- Aztech Global
- ThyssenKrupp
- AB Texel
- GCA
- HAL Allergy
- Continental Aerospace
- International Paper
- Kampf
- EAS

March
- Koffie Beyers
- Stadtwerke Bruck
- Sprimoglass
- Duvel Moortgat
- MEPSO
- Radiant Logistics
- BerlinerLuft
- Polycab
- Nampak

April
- LivaNova
- Nexperia
- HOYA
- Swisspro
- Targus
- Taiwan United Renewable Energy
- Le Slip Français
- Octapharma Plasma
- Schuette
- Skanlog
- Tipton Municipal Utilities
- BECOM
- Max Wild
- Dell
- Barnett's Couriers

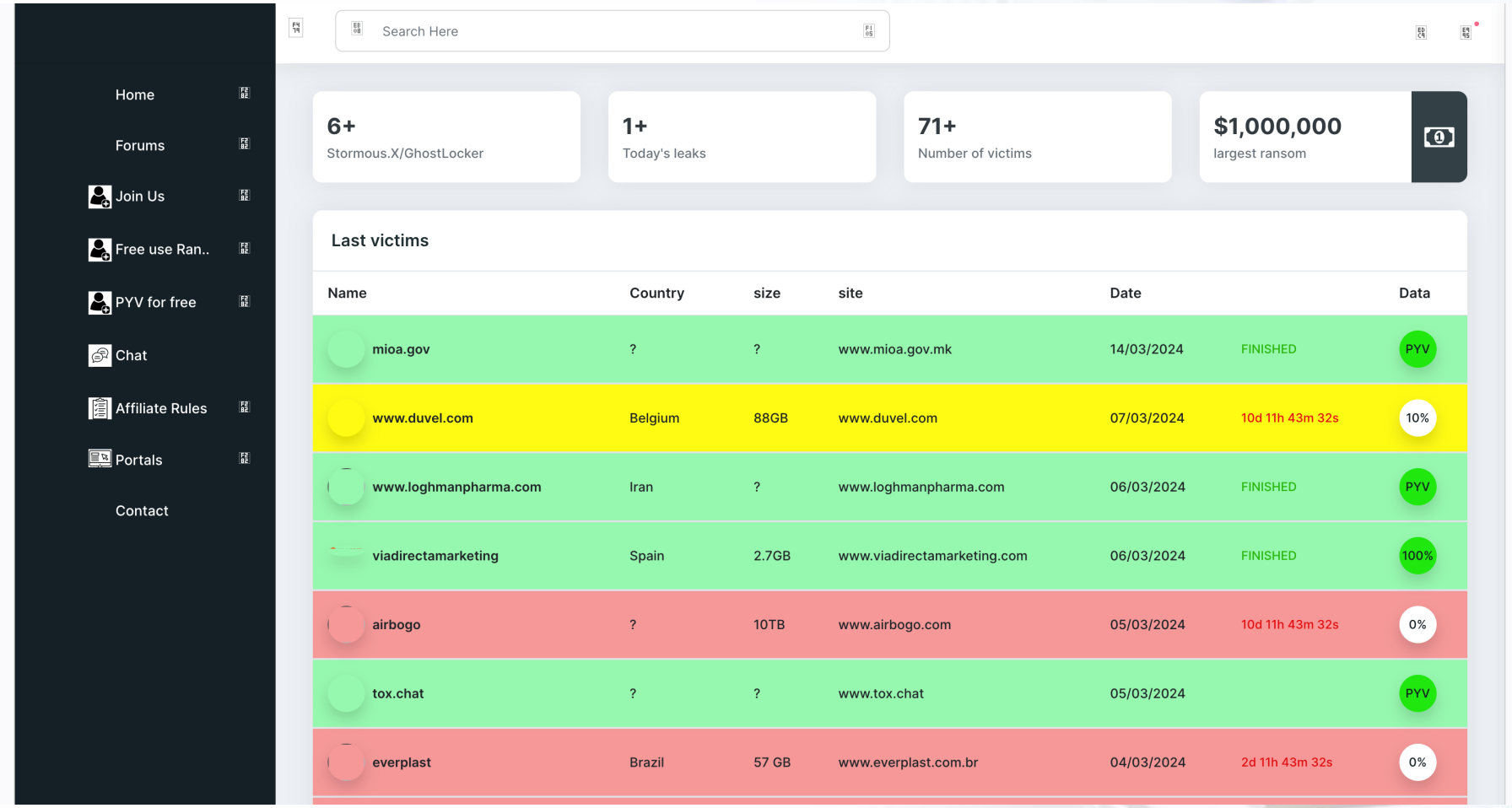
May
- Eucatex
- Key Tronic Corporation
- Porto de São Francisco do Sul
- Sawnee EMC
- Lewis Brothers Bakeries
- Lemken
- Wehrle-Werk

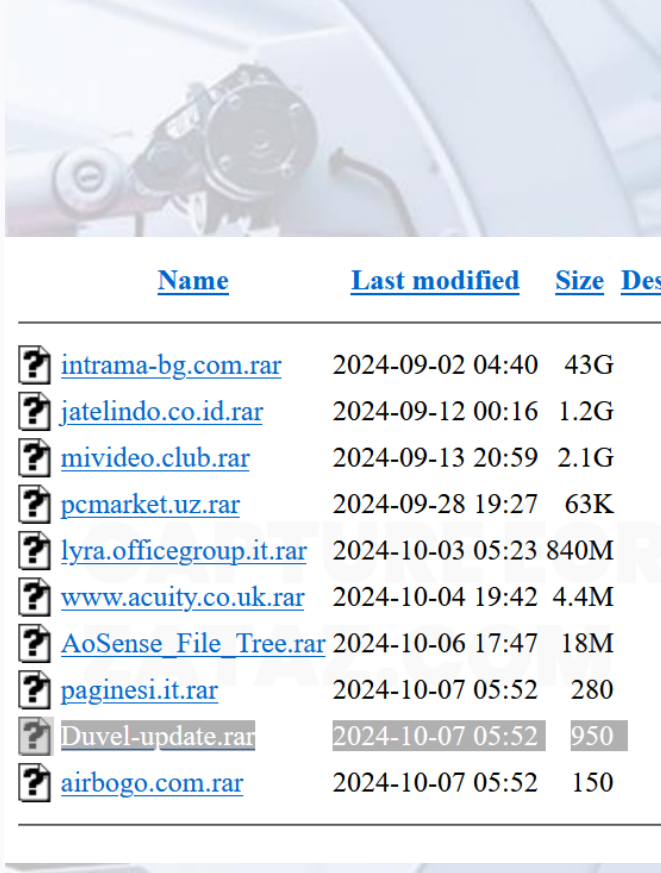
June
- Agropur
- Northern Minerals
- Pharmascience
- Iluka Resources
- Westfälische Stahlgesellschaf
- Emcali
- Crown Equipment
- GlobalWafers
- Rekah
- CDK Global
- Sandhar Technologies
- Ocasa
- Meiller Kipper

Source : Kaspersky

https://ics-cert.kaspersky.com/publications/reports/2024/06/03/q1-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/
https://ics-cert.kaspersky.com/publications/reports/2024/11/08/q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/

Focus sur le cas Duvel



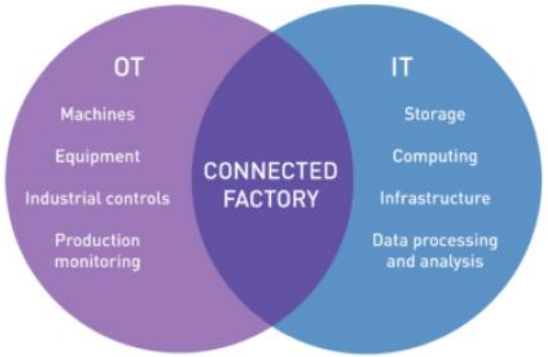


Focus sur le cas Duvel

Références/sources :

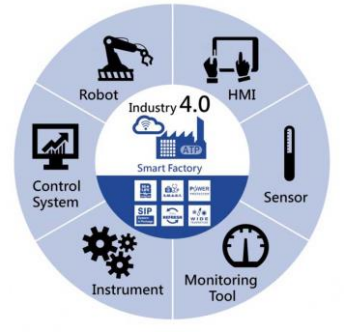
- https://datanews.levif.be/actualite/securite/lattaque-contre-duvel-moortgat-revendiquee-par-deux-bandes-differentes/
- https://therecord.media/stormous-claims-duvel-beer-attack
- https://www.zataz.com/duvel-menacee-de-represailles-par-les-pirates-de-stormous-huit-mois-apres-sa-cyberattaque/

Convergence IT-OT



- Convergence due à
  - Evolution d' Internet, réseaux sans fil, technologies Cloud, big data, IIoT, …

  - Fusion de :
    - Systèmes d'information avec équipements de productions
  - Avec le potentiel de :
    - Réduire les coûts opérationnels
    - Utiliser plus efficacement l'énergie et les ressources
      - moins de temps d'arrêt non planifié, maintenance prédictive, inspection qualité …
    - Time-to-market plus rapide
    - …



Cela augmente

- Le volume à traiter
- La complexité
- La connectivité
- …

⇩

Augmentation de la surface d'attaque

Connaître votre ennemi et vecteurs d'attaque

Equipes de mercenaires

CONTI

Hacktivistes

Cyber-terroristes

Insiders (employés, sous-traitants,...)

Organisations structurées et hiérachisées

Hackeurs amateurs

Ex-employés

Équipes cybernétiques nationales et parrainées par l'État

Hackeurs non éthiques

Connaître votre ennemi et vecteurs d'attaque

Vecteurs d'attaque :

- Ransomware (augmentation de plus de 50% par an)
- Phishing et dérivés
- Périphériques IoT (vulnérabilités, mauvais configuration,…)
- Accès légitime de menaces internes (employé, sous-traitants,…)
- Accès distants / « Internet-facing devices » & apps
- Attaques par déni de service distribué (+/- 10 par mois en Belgique)
- Malwares / virus
- Autres systèmes et logiciels vulnérables

Gestion du parc IT-OT

- Assurez-vous d'avoir des partenaires IT ou des ressources internes sur lesquelles vous pouvez compter en cas d'incident…
  - Quelle est la capacité de réaction de mon prestataire en cas de cyber-incident ?
  - Ne faudrait-il pas tester notre capacité à traiter l'incident et notre capacité de récupération ?
  - Ai-je bien délégué la responsabilité de la cybersécurité à quelqu'un ?
- Vous ne pouvez pas défendre ce que vous ne connaissez pas… (inventaire des actifs)
- Sauvegardes selon la stratégie
  3-2-1-1-0

Gestion du parc IT-OT

- Inventaire et hygiène cyber
- CVE (Common Vulnerabilities and Exposures)

CVE List ▾ CNAs ▾ WGs ▾ Board ▾ About ▾

Search CVE List | Downloads | Data Feeds | Update a CVE Record

TOTAL CVE Records: 205154

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format J

NOTICE: Changes are coming to CVE List Content Downloads in 2023.

HOME > CVE > SEARCH RESULTS

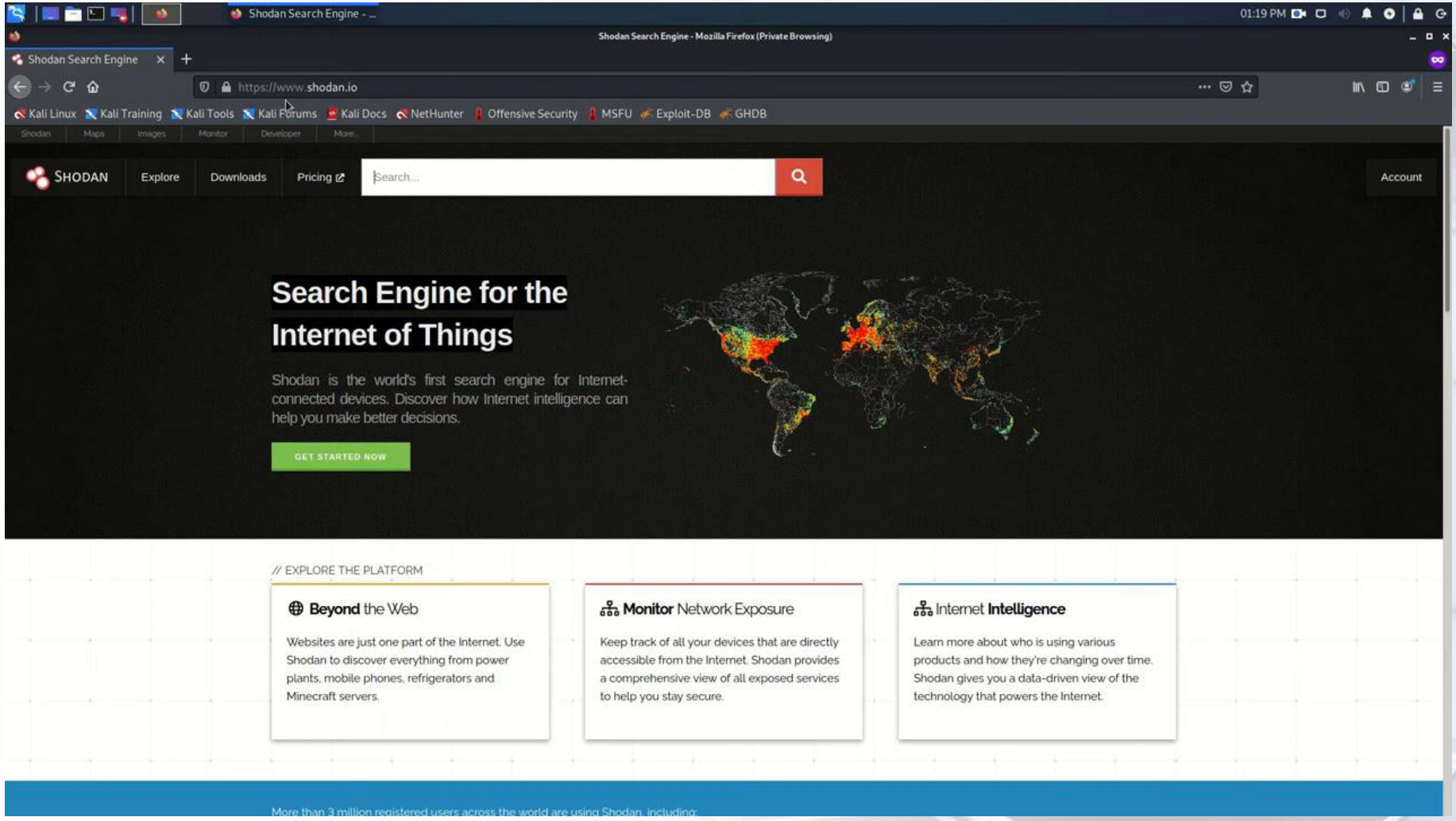
Search Results

There are **41** CVE Records that match your search.

Name	Description
CVE-2022-43768	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLU versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543SP-1 (All versions), SIMATIC CP 443-1 (All versions < V3.3), SIMATIC CP 443-1 (All versions < V3.3), SIMATIC CP 443-1 Advanced (All versior 200SP CP 1543SP-1 ISEC (All versions), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions), SIPLUS NET CP 1242-7 V2 (All versions), SIPL < V3.3), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions), SIPLUS TIM 1531 IRC (All versions < V2.3.6), T a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation of the webserver of the affected pr
CVE-2022-43767	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLU versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543SP-1 (All versions), SIMATIC CP 443-1 (All versions < V3.3), SIMATIC CP 443-1 (All versions < V3.3), SIMATIC CP 443-1 Advanced (All versior 200SP CP 1543SP-1 ISEC (All versions), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions), SIPLUS NET CP 1242-7 V2 (All versions), SIPL < V3.3), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions), SIPLUS TIM 1531 IRC (All versions < V2.3.6), T a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation of the webserver of the affected pr
CVE-2022-43716	A vulnerability has been identified in SIMATIC CP 1242-7 V2 (All versions), SIMATIC CP 1243-1 (All versions), SIMATIC CP 1243-1 DNP3 (incl. SIPLU versions), SIMATIC CP 1243-7 LTE EU (All versions), SIMATIC CP 1243-7 LTE US (All versions), SIMATIC CP 1243-8 IRC (All versions), SIMATIC CP 1543SP-1 (All versions), SIMATIC CP 443-1 (All versions < V3.3), SIMATIC CP 443-1 (All versions < V3.3), SIMATIC CP 443-1 Advanced (All versior 200SP CP 1543SP-1 ISEC (All versions), SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (All versions), SIPLUS NET CP 1242-7 V2 (All versions), SIPL < V3.3), SIPLUS S7-1200 CP 1243-1 (All versions), SIPLUS S7-1200 CP 1243-1 RAIL (All versions), SIPLUS TIM 1531 IRC (All versions < V2.3.6), T a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation which leads to a restart of the web

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Gestion du parc IT-OT – Démo faille CISCO RV320



Gestion du parc IT-OT

Quelques exemples de vulnérabilités :

- NAS : https://www.bleepingcomputer.com/news/security/d-link-wont-fix-critical-flaw-affecting-60-000-older-nas-devices
- NextGen firewalls : https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-potential-pan-os-rce-vulnerability
- CVE Microsoft – 5 zero-days : https://www.darkreading.com/vulnerabilities-threats/5-cves-microsofts-october-2024-update-patch-now

Ransomware

MICHEL LAUWERS

23 octobre 2024 06:00

Près de la moitié des entreprises belges ont été touchées par de la cybercriminalité en 2023, selon BDO. Les PME sont plus souvent rançonnées que les grandes entreprises.

Près d'une entreprise belge sur deux (48%) a été **touchée par des actes de cybercriminalité l'an dernier** et **une sur vingt (4,9%) a versé une rançon** à des cybercriminels. Ces chiffres pour le moins inquiétants proviennent du dernier **Baromètre des entreprises** rédigé par le cabinet de consultance **BDO** au départ d'un **panel de 521 managers**.

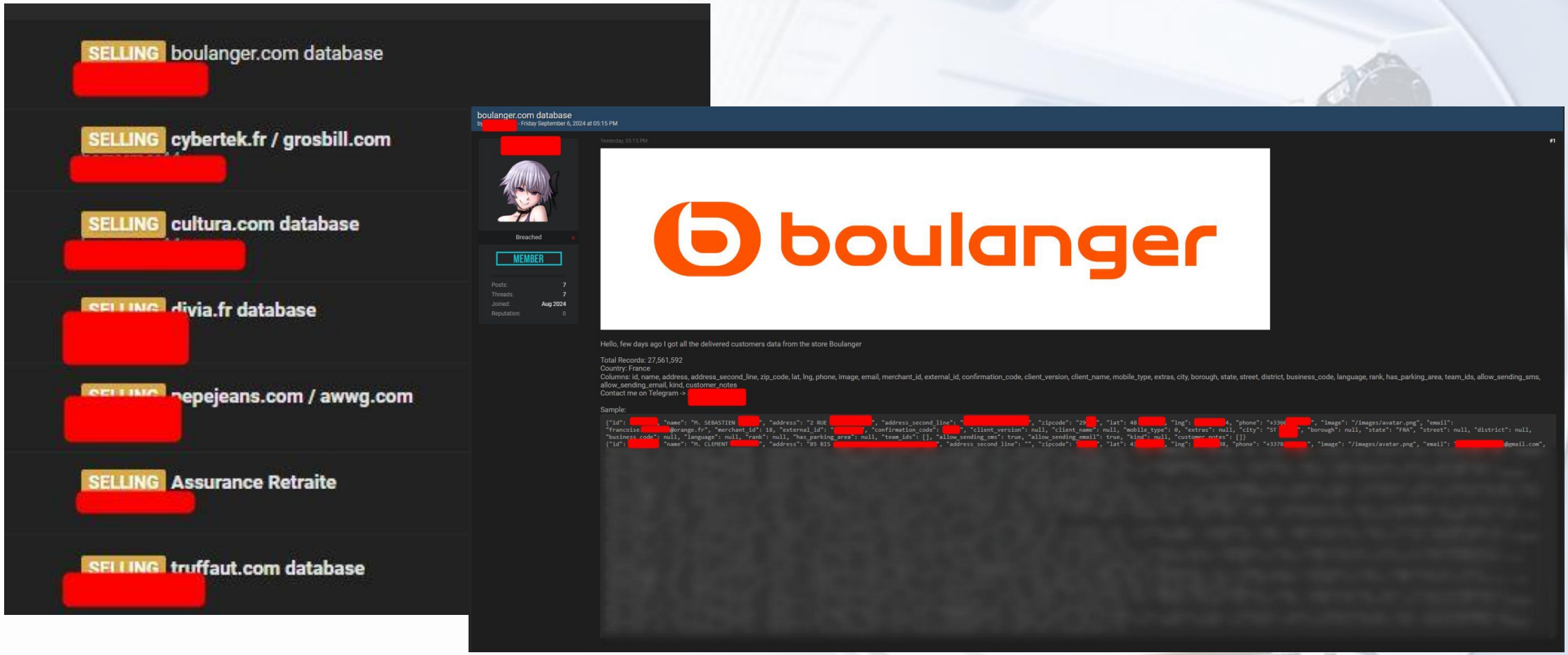
L'enquête concerne des sociétés de toutes tailles et de tous les secteurs à travers les trois Régions du pays, "avec une marge d'erreur assez faible", selon les auteurs de l'étude. Elle montre aussi que **30% des entreprises interrogées ont subi des tentatives d'hameçonnage**, que 9% d'entre elles ont vu leurs systèmes affectés par un virus, ou encore que **7% ont été victimes d'une fuite de données** en interne (et 6% en externe, via un fournisseur par exemple).

Source : https://www.lecho.be/entreprises/tech-science/cybercriminalite-une-entreprise-sur-20-a-paye-une-rancon-en-belgique-en-2023/10570011.html

- Souvent la dernière étape d'un hacker quand tout le reste a été exploré
- Double extorsion :
  - Données exfiltrées et revendues sur le dark web si une rançon n'est pas payée

    ➔ Potentiel non-respect des clauses de confidentialité de vos contrats partenaires

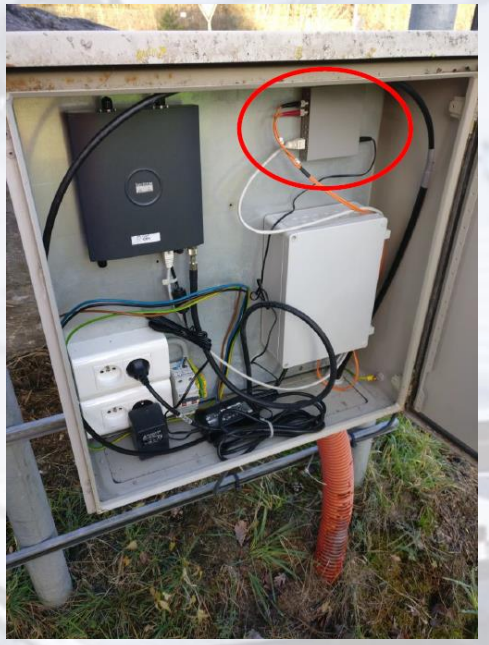
Ransomware



https://www.linkedin.com/posts/clementdomingo_boulanger-activity-7238085044349669376-s8qX

Contrôle d'accès et mots de passe

- Vérifications physiques, logiques et facteur humain
- Physique :
  - Vérifier et optimiser tous les accès physiques permettant d'accéder à la couche logique



Source : Secudea

Contrôle d'accès et mots de passe

- Logique :
  - Enumérer et gérer les accès IT<>OT
  - Identifier toutes les solutions VPN, DSL et autres (Teamviewer,…)
  - Trouver les connexions cellulaires indésirables
  - Scruter les points d'accès Wifi non souhaités
  - Sécuriser chaque segment réseau (VLAN) et chaque interface (réseau ou autre)
  - Définissez les règles de sécurité (ne rien laisser par défaut)

Contrôle d'accès et mots de passe

- Facteur humain :
  - Crédulité/stress (phishing), amabilité, volonté de contournement,…

Démo

BAD USB

Contrôle d'accès et mots de passe

- Les mots de passe : un sujet à part entière…
  - Ne prenez pas cela à la légère (pas de partage, post-it,…)
  - Une bonne stratégie de gestion est importante
    - Gestionnaires de mots de passe
  - Activer le 2FA partout où c'est possible
  - Suivez proactivement les « leaks » et changer les mots de passe au plus vite: https://haveibeenpwned.com/
  - En cas de doute, modifier également votre mot de passe directement

En savoir plus ? Rejoignez un webinaire CyberActive

- Gestion des mots de passe et contrôle d'accès :
  26 novembre 10-12h

- Ransomware et gestion des mots de passe :
  11 décembre 10-12h

Machines et atelier connectés

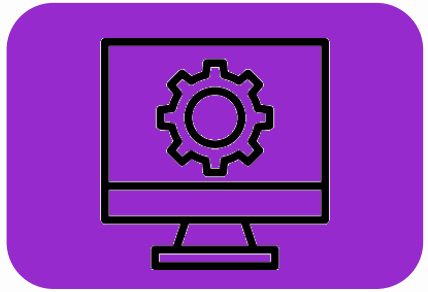
- Traditionnellement, les systèmes OT n'ont pas été conçus en tenant compte de la connectivité à l'internet.
  - Pas de « secure by design »
- Les anciens systèmes OT sont modernisés avec des dispositifs IoT
- Toute machine devient plus intelligente et connectée
- Le "trou d'air" originel entre l'OT et l'IT n'existe plus (Purdue Model).
  - Pas connecté du tout
  - Pas connecté au réseau IT
  - Pas connecté à Internet

Peu importe → Toujours vulnérable

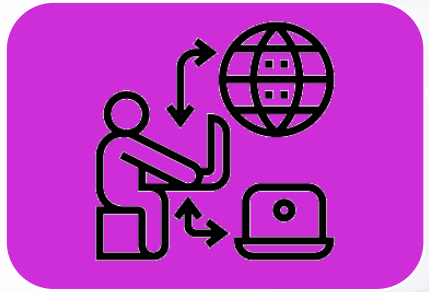
- Des données sont échangées
  - Fichiers (clés USB, carte SD)
- Les réseaux ne sont souvent pas dignes de confiance

Le CRA (Cyber Resilience Act) arrive…
-> Sécurisation « by design » de tout produit contenant un élément digital et connecté à un autre système

Guide d'achat des machines (Sirris)



Logiciel – 2 questions



Accès distant – 8 questions

Gestion des sessions – 2 questions

Gestion des credentials et authentification – 2 questions

Stockage des données et communication - 6 questions

Mise à jour et gestion des "patches"– 2 questions

Garantie/assurance – 3 questions

Spécifications PLC et protocoles – 2 questions

Accès à distance sécurisé

- Besoin de sécuriser, monitorer, uniformiser les différents points d'entrée
  - Pour vos besoins en interne (télétravail, monitoring distant,…)
  - Pour des sociétés tierces devant réaliser le commissionnement, la maintenance ou le support d'équipements ou logiciels
- Des stratégies doivent être mises en place
  - Segmentation / micro-segmentation / zero-trust architecture / suivi des sessions
    - Isoler
    - Restreindre au minimum (« least privilege principle »)
    - Eviter le déplacement du hacker sur votre réseau
    - Le blocage de la communication devient le comportement « par défaut »

- https://www.computerweekly.com/news/366578657/RDP-abused-in-over-90-of-cyber-attacks-Sophos-finds

En savoir plus ? Rejoignez un webinaire CyberActive

- Atelier connecté et maintenance à distance sécurisée :

  9 décembre 10-12h (FR)

  19 novembre 10-12h (EN)

Phishing (et apparentés)

- Vise à vous tromper et vous faire réaliser une action
- Toujours plus crédible et plus performant
  - Automatisé, personnalisé et sans erreurs d'orthographe ou de grammaire (IA générative)
  - Les vols de bases de données facilitent la tâche des hackers
- Personne n'est à l'abri, les stratégies évoluent sans cesse
  - Nécessité de former votre personnel dans le temps
- Mais aussi smishing, quishing, vishing,… besoin de vigilance accrue peu importe le canal de communication

Démo

VOL D'INFORMATIONS D'IDENTIFICATION

NIS2

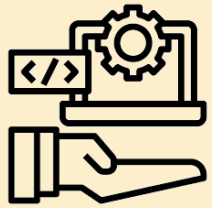
- En Belgique, la directive NIS2 et sa transposition en droit Belge impose de nouvelles exigences à de nombreuses entreprises.

- NIS2 vise à renforcer la résilience des entités qualifiées d' **importantes** ou **essentielles**, ce qui inclut l'industries manufacturière, et touche indirectement les acteurs critiques de la chaîne de valeur qui ne seraient pas soumis de facto à NIS2.

Network & Information Security 2 (NIS 2)

- Les nouveautés par rapport à NIS1

Rapports d'incidents : dispositions précises, y compris le contenu des rapports et les échéanciers.



Autres secteurs industriels soumis à l'application : services numériques, fournisseurs de données, TIC…

Exigences de sécurité : renforcement

Amendes : augmentation

Formation à la cybersécurité : obligatoire pour les dirigeants et les employés

Sous-traitants/prestataires : la sécurité sur une base contractuelle

NIS2

NIS 2 : approche « tous risques (*all hazards*) » qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents. La loi impose de prendre des mesures appropriées et proportionnelles en fonction de l'analyse de risques de l'entité. Ces mesures portent au moins sur :

- Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information
- La gestion des incidents
- La continuité des activités et la gestion des crises
- La sécurité de la chaîne d'approvisionnement
- La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités.
- Une politique de divulgation coordonnée des vulnérabilités
- Des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité
- Cyberhygiène et la formation à la cybersécurité
- Des politiques et des procédures sur la cryptographie et, le cas échéant, du chiffrement
- La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
- Des solutions d'authentification à plusieurs facteurs, de communications sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins

Ces mesures de sécurité peuvent être implémentées avec les référentiels CyberFundamentals (CyFun®) ou ISO 27001.

ISO 27001

NIS2 : Guide de démarrage rapide du CCB

https://atwork.safeonweb.be/fr/tools-resources/guide-de-demarrage-rapide-avec-nis2

1. Suis-je concerné par NIS2 ?

A. Dans le champ d'application : Entités NIS2

Utilisez notre outil de test du champ d'application pour déterminer si votre organisation entre ou non dans le champ d'application de la loi NIS2 belge.

Télécharger le Scope tool

Source : CCB

CENTRE FOR CYBERSECURITY BELGIUM

Scope Assessment

The following questions aim to determine if your organisation may potentially be in scope of the Belgian NIS2 legislation. Depending on its size and the service provided, your organisation may be considered as an essential or important entity.

More information about the NIS2 law can be found here

A. Organisation size ("size-cap") (i) Further information

Please select the size of your organisation before continuing.

These thresholds are calculated on the basis of the figures for the entire legal entity (including all its activities, even outside of the EU), proportionately consolidated with the figures from its partner or linked enterprises.
For more details on the method for calculating these thresholds, see the annex I of Commission Recommendation 2003/361/CE of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, the guide released by the European Commission, or its online tool (linked below).

Link to Commission Recommandation 2003/361/EC
Link to the "User guide on the SME definition" from the European Commission
Link to the SME self-assessment tool from the European Commission

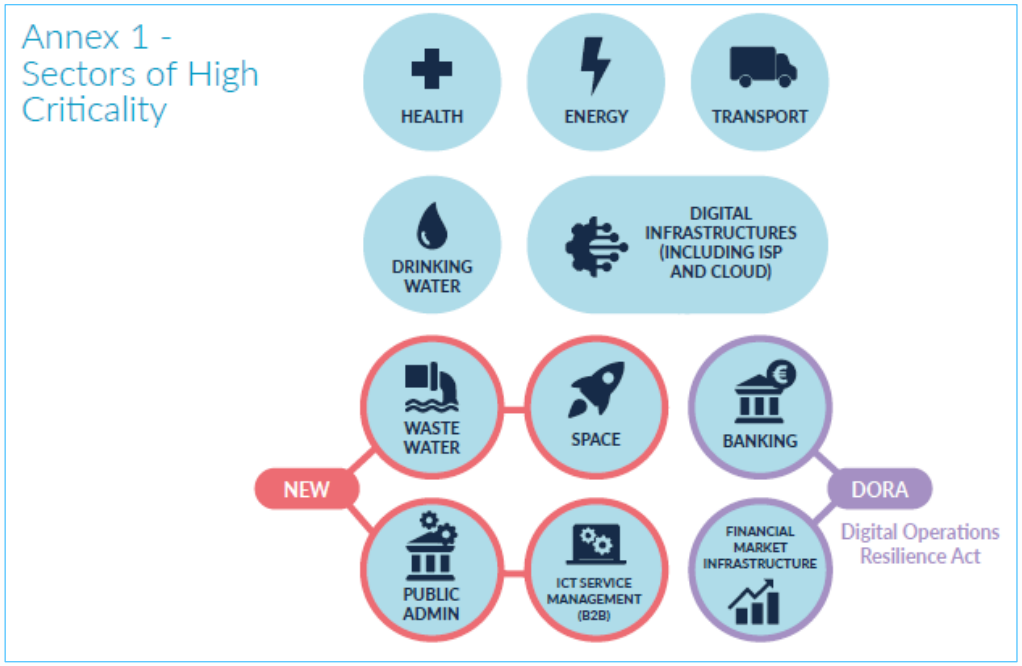
Select your staff headcount range (in full-time equivalents - FTE):	50 - 249 FTE
Select your turnover range:	< 10 million € annual turnover
Select your balance sheet total:	< 10 million € annual balance sheet total
Your organisation's size :	Medium-sized Enterprise

B. Sectors and service provided

Please select at least one sector, or the field 'None of the above' if your organisation does not correspond to any of the sectors, before you can continue.

NIS2 : Secteurs concernés

Entités ESSENTIAL ou IMPORTANT



Entités IMPORTANT

Source : CCB

NIS2 : "Essential", "Important" ou "out of Scope" ?

Main selection mechanism via size-cap						
	Entities of Annex I					
(Staff) FTE	<10 M€	10 – 50 M€ (43 M€)	> 50 M€ (43 M€)	Pub Admin (Federal) + DNS, TLD	Pub Admin (Federated after identification)	Electronic comm netw. provider
0-49	Out of Scope	Important	Essential	Essential	Imp/Ess	Important
50-250	Important	Important	Essential	Essential	Imp/Ess	Important
>250	Essential	Essential	Essential	Essential	Imp/Ess	Essential

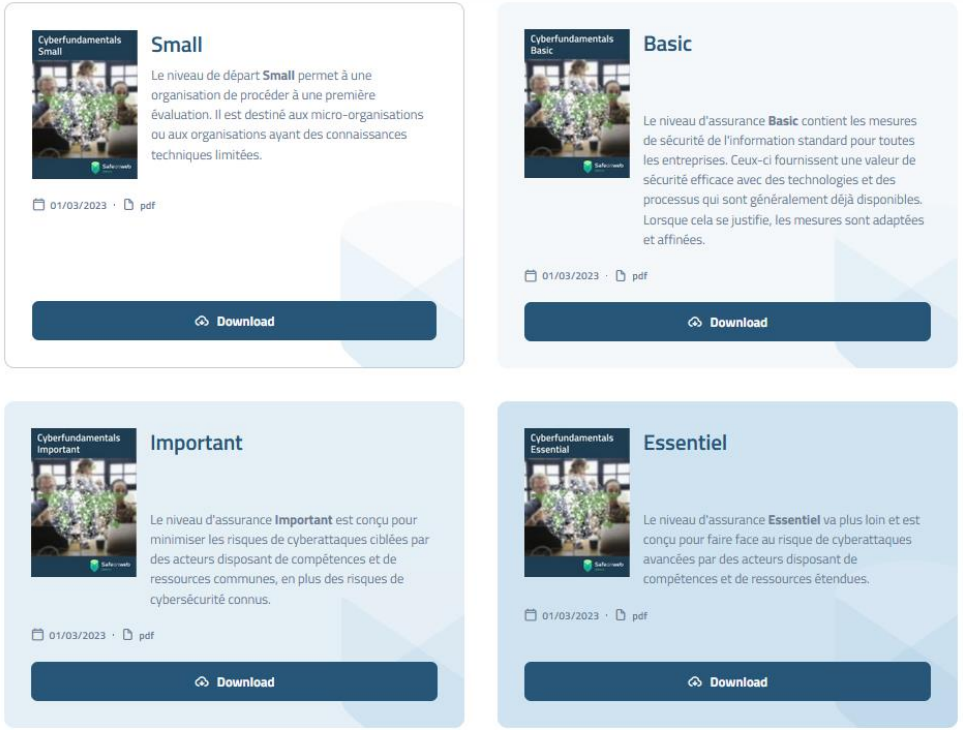
	Entities of Annex II		
(Staff) FTE	<10 M€	10 – 50 M€ (43 M€)	> 50 M€ (43 M€)
0-49	Out of Scope	Important	Important
50-250	Important	Important	Important
>250	Important	Important	Important

Source : CCB

NIS2 : Règles applicables

	NIS2 entity	Other entity
Scope & Registration	✓	Voluntary registration on atwork.safeonweb.be
Security Measures	✓	✓
Training	✓	✓
Incident Notification	✓	Voluntary notification

En Belgique – CyberFundamentals (ou CyFun)

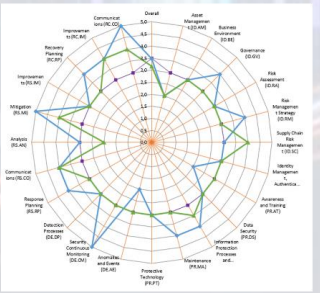


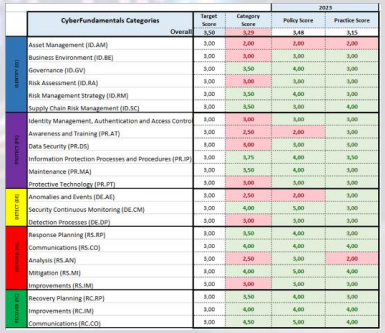
Source : CCB

Outil de selection CyFun (Risk Assessment)

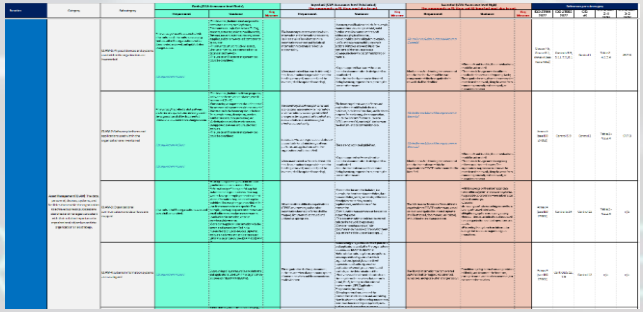
Energy			Common skills		Common skills		Common skills		Extended Skills		Extended Skills			
Organization Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideologues Hactivists		Terrorist		Cyber Criminals		Nation State actor			
Cyber Attack Category	Global or Targetted	Impact	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score		
Sabotage/ Disruption (DDOS,...)	2	High	Low	0	Low	0	Med	30	Med	30	High	60		
Information Theft (espionage, ...)	2	High	Low	0	Low	0	Low	0	High	60	High	60		
Crime (Ransom attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0		
Hactivism (Subversion, defacement...)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Med	7,5		
Disinformation (political influencing)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0	Score	CyFun Level
	Total	Total		0		7,5		30		120		127,5	285	ESSENTIAL

Outil d'auto-évaluation CyFun

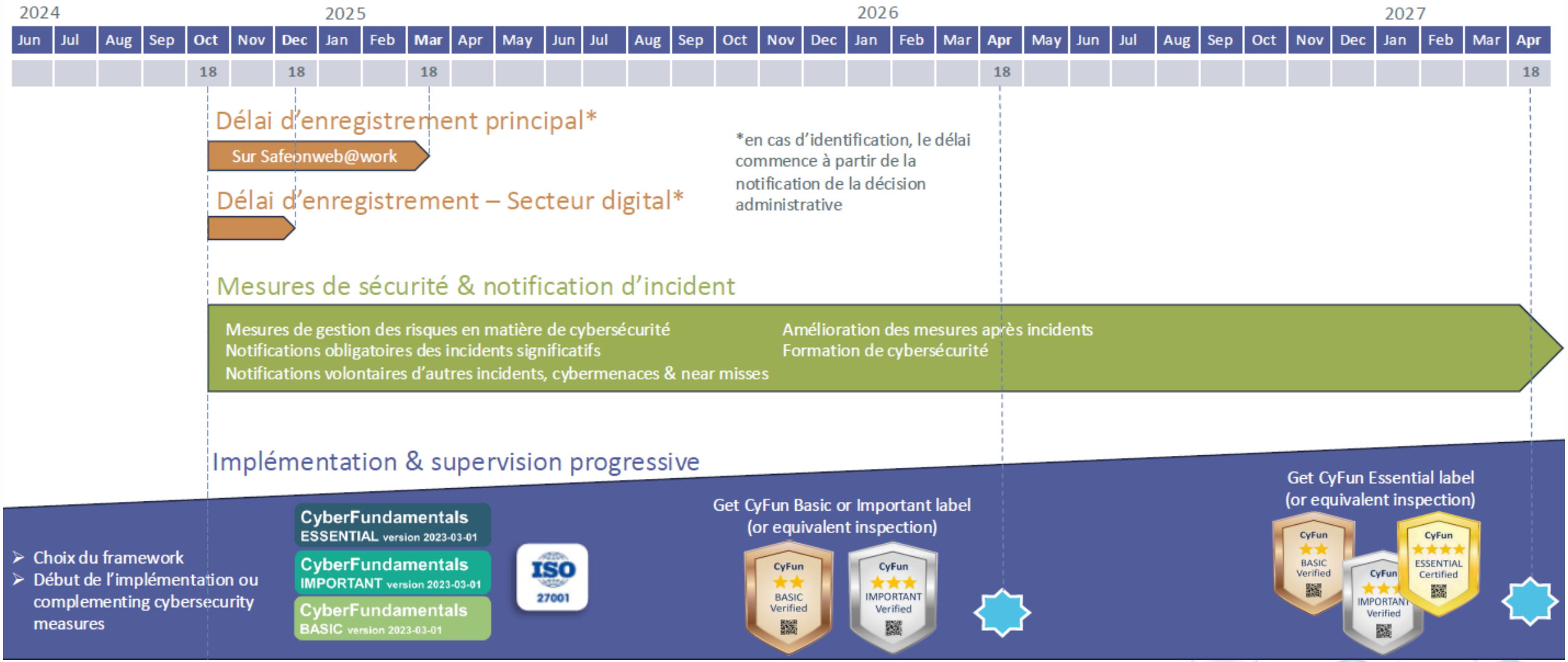




CyberFundamentals Framework mapping (CyFun vs norms)



NIS2 : Calendrier



En savoir plus ? Rejoignez un webinaire CyberActive

- NIS2 : quel impact et quelles actions pour les PME manufacturières ?
  13 décembre 10-12h (FR)

Conclusion

- Afin de vous rendre plus cyber-resilient :
  - Découvrez les formations gratuites CyberActive pour approfondir chacun des sujets évoqués
    - Plusieurs personnes d'une même entreprise peuvent participer gratuitement
  - Ne tardez plus à prendre connaissance de vos obligations suite à l'entrée en vigueur de la loi NIS2 (session le 13 décembre 10h00)
    - Obligation d'enregistrement
    - Déclaration d'incident (notifications et délais à respecter)
    - Mise en route vers la conformité à travers le cadre CyberFundamentals
  - Faites le point avec votre prestataire IT et/ou ressource(s) interne(s) pour évaluer votre situation et définir un plan d'action
  - Formez régulièrement votre personnel contre les menaces (phishing, …) : Agoria Cyberboost, CyberCoach Emergency,…

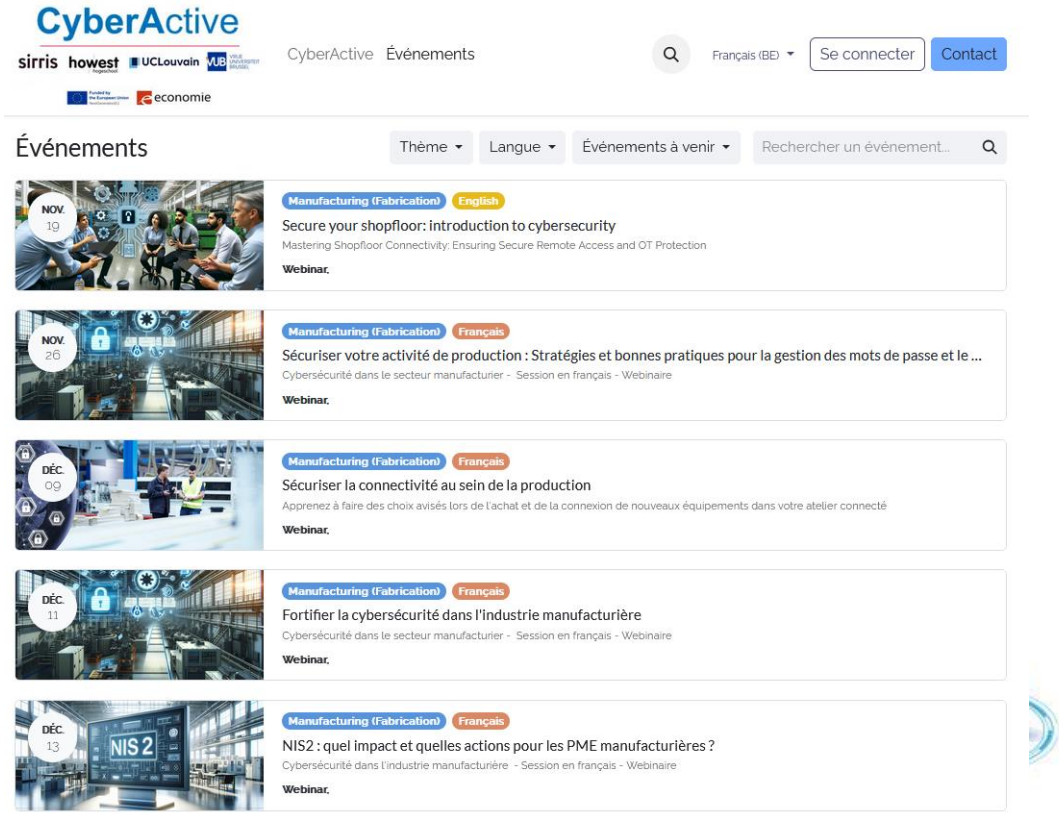
CyberActive

Strengthening Cybersecurity Skills

Vous êtes une PME ou un indépendant actif dans l'industrie manufacturière ?
Bénéficiez gratuitement de contenus d'experts adaptés à vos besoins et aux challenges relatifs à la cybersécurité :

- **Sessions de formation courtes - max 2h (Web/Live)**
- **Vidéos instructives**
- **Ressources didactiques (« cheat sheets »,…)**

Site web : https://www.cyberactive.be
Sessions de formations : https://event.cyberactive.be



Funded by economie
Funded by the European Union NextGenerationEU

Questions - réponses

MERCI POUR VOTRE ATTENTION

Thierry Coutelier

SENIOR EXPERT

+32 496 61 01 41

Thierry.Coutelier@sirris.be

innovation forward