# Séminaire NIS 2

Eaux de Wallonie

12 décembre 2025

Alliance des opérateurs publics de l'eau

# La cybersécurité: un des enjeux majeurs de notre transformation digitale

Corinne Magis & William Poos

Coordinateurs de la plateforme sectorielle Digital

# La situation en Wallonie...

- Les résultats du baromètre de maturité numérique des entreprises wallonnes a été publié par l'AdN fin novembre
- En termes de cybersécurité, **46%** indiquent ne pas réaliser d'investissement dans la cybersécurité
- Le prochain défi des entreprises wallonnes consiste à passer d'une logique de soutien à une logique d'orchestration intelligente où la donnée, l'automatisation et l'IA permettant de repenser les modèles d'affaires

# Notre plan de transformation sectoriel

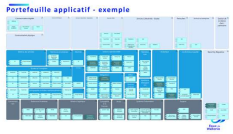
## Phase 1. AS-IS Business Architecture

- Les principales activités
  - Consolidation des objectifs stratégiques sectoriels (cee, spw, contrat de gestion, contrat de services)
  - Spécification de l'architecture fonctionnelle par métier (coordination, production/distribution, assainissement
  - Spécification du modèle d'information par métier (gestion, investissement, exploitation, ..)
- Les ateliers
  - W1.1 : modélisation de l'architecture business (organisation, fonction, information)
  - W1.2 : validation de l'architecture business (organisation, fonction, information)
- Les délivrables
  - DLV1 Architecture business existante- organisation, fonctionnelle, données (.ppt)

Eaux de Wallonie

**Phase 1 – Architecture métier**

## Phase 2. AS-IS Architecture Technique et initiatives

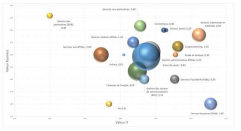


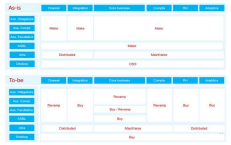

- Les principales activités
  - Consolidation des solutions existantes par fonction et par métier (appli/infra)
  - Consolidation des plateformes d'intégrations OAAs/SPGE, PRDs/SPGE (transaction, informations)
  - Identifier et décrire les cas d'usage AI existants ;
  - Identifier et décrire les projets existants ;
- Les ateliers
  - W2.1. Travail sur les solutions IT par fonction et par métier
  - W2.2. Validation de l'architecture existante par fonction et métiers
- Les livrables
  - DLV2. As-is Architecture IT (organisation, applications, interfaces, infrastructure, SLA)
  - DLV3. Inventaire des projets et initiatives

Eaux de Wallonie

**Phase 2 – Architecture technique**

## Phase 3. Synergies et priorisation





- Les principales activités
  - définir les critères de priorisation – faisabilité, valeur métier (alignement stratégique, ROI), compliance, soutenabilité écologique, ...
  - définir les critères d'évaluation – it, business, risques
  - consolider les composantes digitales des initiatives des plateformes sectorielles
  - évaluer les solutions existantes par fonction et par métier (business, it, cost)
  - consolider et prioriser le portefeuille de synergies digitales
- Les ateliers
  - W3.1. Travail sur l'inventaire des synergies digitales
  - W3.2. Validation du portefeuille de synergies digitales
- Les livrables
  - DLV4. Swot sectorielle v1
  - DLV5. Portefeuille de synergies priorisé v1

Eaux de Wallonie

**Phase 3 – Synergies et priorisation**

## Phase 4. Business Engagement

- Les principales activités
  - validation de l'architecture existante
  - validation de l'évaluation et de la priorisation
  - présentation de la SWOT v1 et du portefeuille de synergies priorisés
  - entretien avec les directeurs (7 OAAs, 2 PRDs, SPGE)
- Les ateliers
  - W4.1 9 Interviews
- Les livrables
  - DLV6. SWOT v2
  - DLV7. Portefeuille de synergies priorisé v2
  - DLV8. CR des Interviews

Eaux de Wallonie

**Phase 4 – Business Engagement**

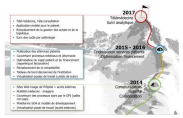
## Phase 5. Target IT Architecture

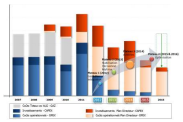

- Les principales activités
  - identifier les scénarii technologiques d'évolution
  - évaluation des scénarios d'évolution - risques techniques, fonctionnels, opérationnels et budgétaires
  - Spécification de l'architecture cible de la plateforme sectorielle
- Les ateliers
  - Atelier sur l'architecture cible et l'identification de scénarios évolutifs
  - Atelier de validation de l'architecture de la plateforme digitale
- Les livrables
  - DLV9 Evaluation des scénarii d'évolution
  - DLV10 Architecture (organisation, applications, interfaces, infrastructure, SLA)

Eaux de Wallonie

**Phase 5 – Architecture cible**

## Phase 6 Transformation plan





- Les activités principales
  - Élaboration du plan de transition et planification
  - Description des projets par chantier
  - Analyse d'impact sur le portefeuille de services, l'équipe informatique et la division projet
  - Définition de l'analyse de rentabilisation
- Les ateliers
  - Workshop sur le plan de transition
  - IT Roadmap présentations
- Les délivrables
  - DVV11 Plan de transition et business case

Eaux de Wallonie

**Phase 6 – Plan de transformation**

# Une démarche à entreprendre tous ensemble…

- La cybersécurité est un pilier fondamental de la transformation digitale globale
- Elle s'intègre dans une démarche collective où chaque acteur, au-delà des experts techniques, joue un rôle essentiel pour garantir la résilience et la performance du secteur
- Les technologies les plus avancées peuvent être déforcées par des actes de négligence ou par méconnaissance du personnel
- La formation est cruciale

# Contexte de ce séminaire et rôle des administrateurs

Fernand Vanseven
CISO - SPGE

# Cyber attaques sur les infrastructures industrielles : Opération Shady Rat

- En décembre 2012, Kyle Wilhoit souhaite déterminer à quelle fréquence les hackers malveillants ciblent les infrastructures industrielles;
- L'expérience consistait à créer une usine virtuelle de traitement de l'eau, un réseau de systèmes de contrôle industriels avancés, accompagné de documentation et d'un site web;
- À peine 18 heures après que le chercheur a connecté les systèmes de contrôle industriels à Internet, quelqu'un a commencé à attaquer l'un d'eux, et la situation s'est rapidement aggravée.

# Un phishing sophistiqué mène à une opération d'espionnage d'envergure internationale

- L'usine a attiré une avalanche d'attaques provenant de divers adversaires, notamment l'armée nord-coréenne, des gangs de ransomware russes et même des hackers des États-Unis et d'Europe;
- Cependant, une attaque s'est distinguée :
  une campagne de phishing qui a conduit Wilhoit au cœur de l'opération shady RAT

# Une cyber-espionnage mondial ayant pour objectif de ménager un accès durable

- Les emails contenaient des informations précises et pièces jointes légitimes pour tromper les victimes;
- Les pièces jointes exécutaient un code malveillant collectant des données sensibles de l'usine virtuelle;
- Les données volées étaient transmises à un serveur de contrôle en Chine, illustrant une opération mondiale;
- mais surtout: Les attaquants se déplacent latéralement dans les réseaux pour établir un accès durable, compromettant la sécurité des infrastructures critiques

# Les infrastructures critiques sont les cibles importantes pour des cyber attaques

- Ces attaques sur systèmes industriels ne sont plus isolées;
- Elles visent des infrastructures critiques, avec des acteurs étatiques et criminels;
- Cette réalité met en évidence la vulnérabilité des infrastructure essentielles de nos sociétés.

# L’Europe renforce la cyber résilience avec la directive NIS2

- La directive NIS2 impose un renforcement de la cybersécurité en Europe.
- Les entreprises doivent se conformer à des obligations strictes notamment en matière de gouvernance et de gestion des risques;
- La loi impose que les organes de décisions soient formés afin de pouvoir prendre des décisions éclairées en matière de risques cyber.

# Quel est votre rôle ?

- La cybersécurité est avant tout une question humaine et requiert une culture portée par la direction;
- Les risques cyber doivent être abordés avec la même rigueur que les autres risques stratégiques, financiers ou opérationnels;
- Les administrateurs n'ont pas besoin d'être des experts techniques, mais ils doivent disposer des connaissances essentielles pour comprendre les enjeux, poser les bonnes questions et prendre des décisions éclairées.

# Séminaire NIS2: Introduction

Axel Legay
Expert en cybersécurité

# Qu’est ce que la cybersécurité ?

- La cybersécurité consiste à protéger les systèmes, les réseaux et les données contre les cybermenaces.
- Cela implique des technologies, des processus et des contrôles pour se protéger contre les accès non autorisés, le vol ou les dommages.
- La cybersécurité est essentielle dans un monde de plus en plus connecté.

# Quand la première cyberattaque a-t-elle eu lieu ?

Séminaire NIS 2

# Perception erronée :
# la cybersécurité est récente

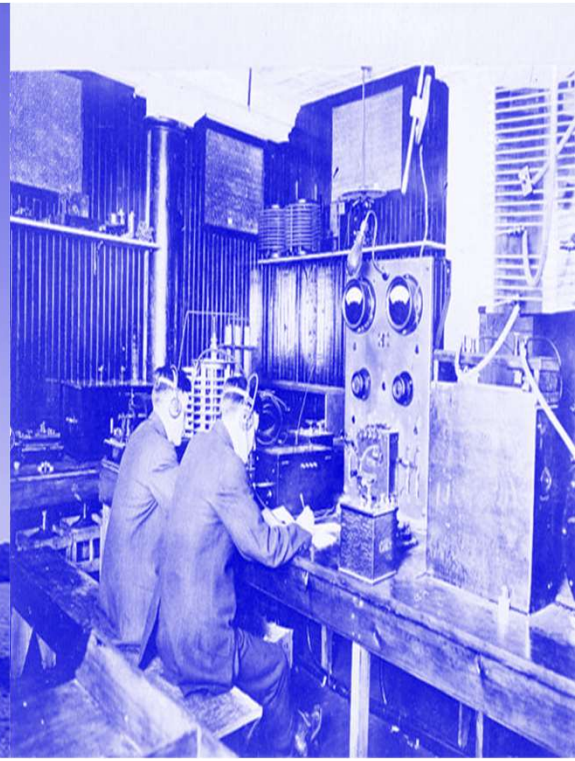



# La cybersécurité est un vieux sujet (1)

- Télégraphe bien avant (1843) :
  - Le cours de la bourse de Paris arrive à Bordeaux dans 3 jours
  - Le télégraphe de Chappe (visuel) dans quelques heures
- **Comment pourrions-nous exploiter cela pour faire un cyber-exploit ?**

# La cybersécurité est un vieux sujet (2)

- **Télégraphe bien avant (1843) :**
  - Le cours de la bourse de Paris arrive à Bordeaux dans 3 jours
  - Le télégraphe de Chappe (visuel) dans quelques heures
  - Piratage de messages télégraphiques pour ajouter des informations boursières
  - Au départ de Tours
  - Pas de condamnation parce qu'il n'y a pas de règles
- **Détournement d'un moyen de communication**



# Quand le premier ransomware a-t-il eu lieu ?



BBC

Home News Sport Business Innovation Culture Arts Travel Earth Video Live

## ministry website

24 April 2018

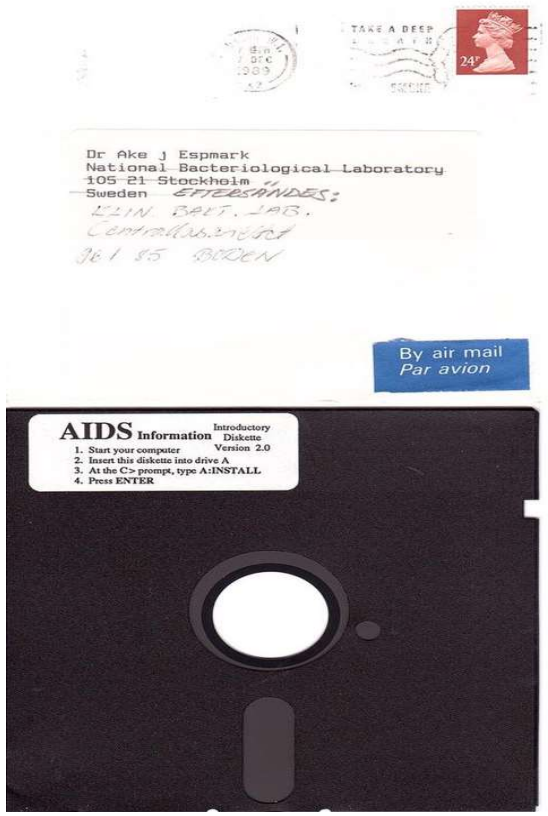
Share Save

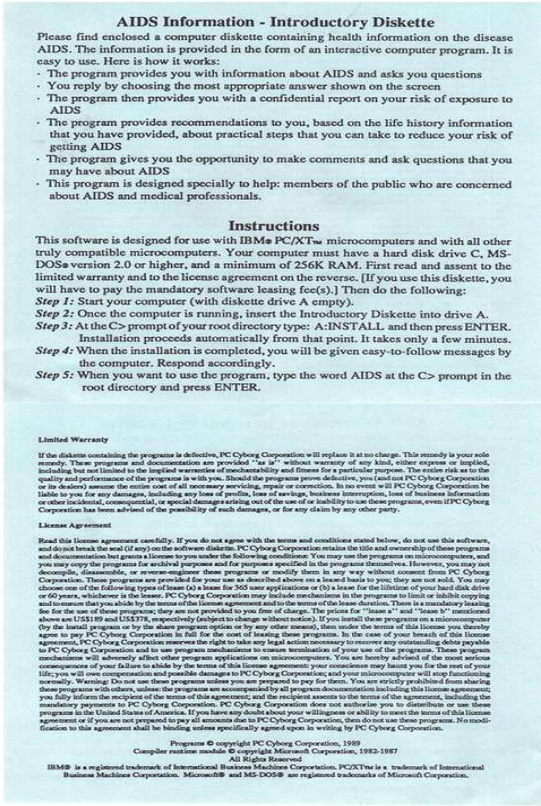

Hackers have used a ransomware cyber-attack to compromise a Ukranian government website

**Hackers have used ransomware to take the website of Ukraine's energy ministry offline and encrypt its files.**

# Ransomware dans les années 80

- Premier ransomware par le biologiste Joseph Popp
- Envoi d'une disquette dans le monde entier
- Cryptographie symétrique
- Envoyez 189 USD à Cyborg Corporation au Panama



**AIDS Information - Introductory Diskette**

Please find enclosed a computer diskette containing health information on the disease AIDS. The information is provided in the form of an interactive computer program. It is easy to use. Here is how it works:

- The program provides you with information about AIDS and asks you questions
- You reply by choosing the most appropriate answer shown on the screen
- The program then provides you with a confidential report on your risk of exposure to AIDS
- The program provides recommendations to you, based on the life history information that you have provided, about practical steps that you can take to reduce your risk of getting AIDS
- The program gives you the opportunity to make comments and ask questions that you may have about AIDS
- This program is designed specially to help: members of the public who are concerned about AIDS and medical professionals.

**Instructions**

This software is designed for use with IBM® PC/XT™ microcomputers and with all other truly compatible microcomputers. Your computer must have a hard disk drive C, MS-DOS® version 2.0 or higher, and a minimum of 256K RAM. First read and assent to the limited warranty and to the license agreement on the reverse. [If you use this diskette, you will have to pay the mandatory software leasing fee(s).] Then do the following:

*Step 1:* Start your computer (with diskette drive A empty).
*Step 2:* Once the computer is running, insert the Introductory Diskette into drive A.
*Step 3:* At the C> prompt of your root directory type: A:INSTALL and then press ENTER. Installation proceeds automatically from that point. It takes only a few minutes.
*Step 4:* When the installation is completed, you will be given easy-to-follow messages by the computer. Respond accordingly.
*Step 5:* When you want to use the program, type the word AIDS at the C> prompt in the root directory and press ENTER.

**Limited Warranty**

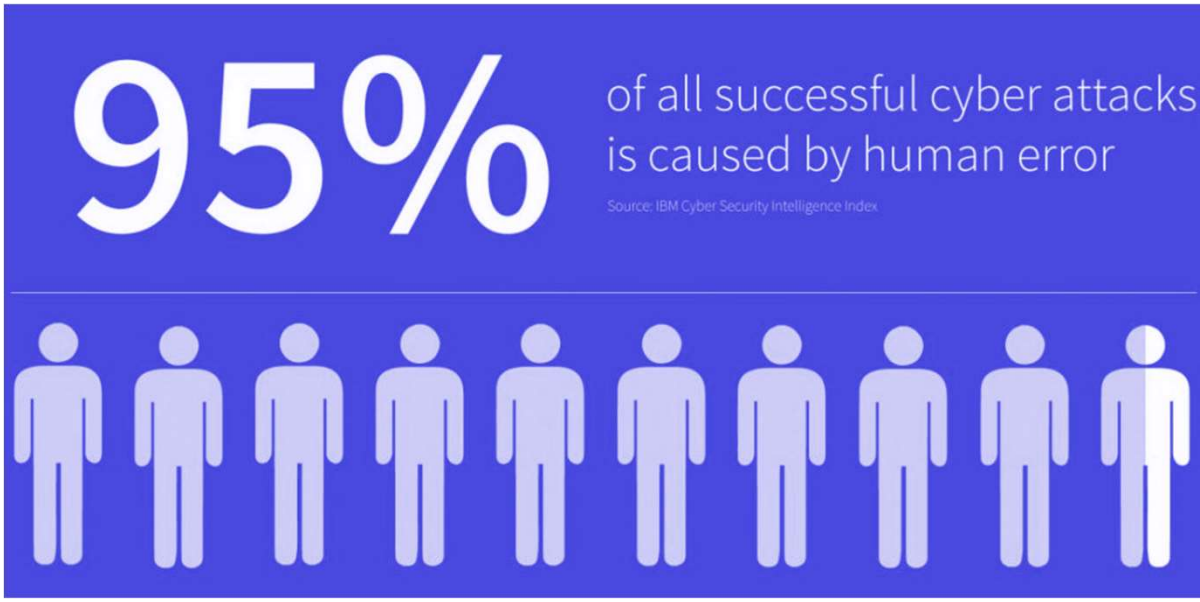
If the diskette containing the programs is defective, PC Cyborg Corporation will replace it at no charge. This remedy is your sole remedy. These programs and documentation are provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the programs is with you. Should the programs prove defective, you (and not PC Cyborg Corporation or its dealers) assume the entire cost of all necessary servicing, repair or correction. In no event will PC Cyborg Corporation be liable to you for any damages, including any loss of profits, lost of savings, business interruption, loss of business information or other incidental, consequential, or special damages arising out of the use of or inability to use these programs, even if PC Cyborg Corporation has been advised of the possibility of such damages, or for any claim by any other party.

**License Agreement**

Read this license agreement carefully. If you do not agree with the terms and conditions stated below, do not use this software, and do not break the seal (if any) on the software diskette. PC Cyborg Corporation retains the title and ownership of these programs and documentation but grants a license to you under the following conditions: You may use the programs on microcomputers, and you may copy the programs for archival purposes and for purposes specified in the programs themselves. However, you may not decompile, disassemble, or reverse-engineer these programs or modify them in any way without consent from PC Cyborg Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the following types of lease (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs; they are not provided to you free of charge. The prices for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of your breach of this license agreement, PC Cyborg Corporation reserves the right to take any legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing these programs with others, unless: the programs are accompanied by all program documentation including this license agreement; you fully inform the recipient of the terms of this agreement; and the recipient assents to the terms of the agreement, including the mandatory payments to PC Cyborg Corporation. PC Cyborg Corporation does not authorize you to distribute or use these programs in the United States of America. If you have any doubt about your willingness or ability to meet the terms of this license agreement or if you are not prepared to pay all amounts due to PC Cyborg Corporation, then do not use these programs. No modification to this agreement shall be binding unless specifically agreed upon in writing by PC Cyborg Corporation.

# Le problème, c'est (souvent) l'humain

- Généralement, vous êtes la cible principale de l'attaque
- Les humains seront toujours vulnérables
- Exemple typique : « Pêche »




https://cyberaware.com/cybercrime-the-human-element-beyond-it/

# La cybersécurité : un problème de perception


# La cybersécurité : opinions subjectives

**La cybersécurité est perçue comme un coût (à mettre en œuvre) :**

- Nous ne serons jamais attaqués
- Cela n'augmente pas la part de marché de l'entreprise/du secteur
- C'est TROP COMPLIQUE.

**Vérité:**

- Toute entité attaquée a perdu plus d'argent que si elle avait investi dans des protections
- Toute entité disposant de matériel informatique est susceptible d'être attaquée
- Le coût indirect des attaques est substantiel
- Les nouvelles directives l'imposeront.

# Quel est le coût (si vous ne le faites pas) ?

Cybercrime Costs. PHOTO: Cybercrime Magazine.

**Cybercrime To Cost The World $10.5 Trillion Annually By 2025**


# Sécurité vs sûreté

- La sûreté ne garantit pas la sécurité.
- Les contrôles de sûreté contribuent à la sécurité.

## Exemple 1

**Sûreté :**
« il n'y a pas d'erreur dans mon code »

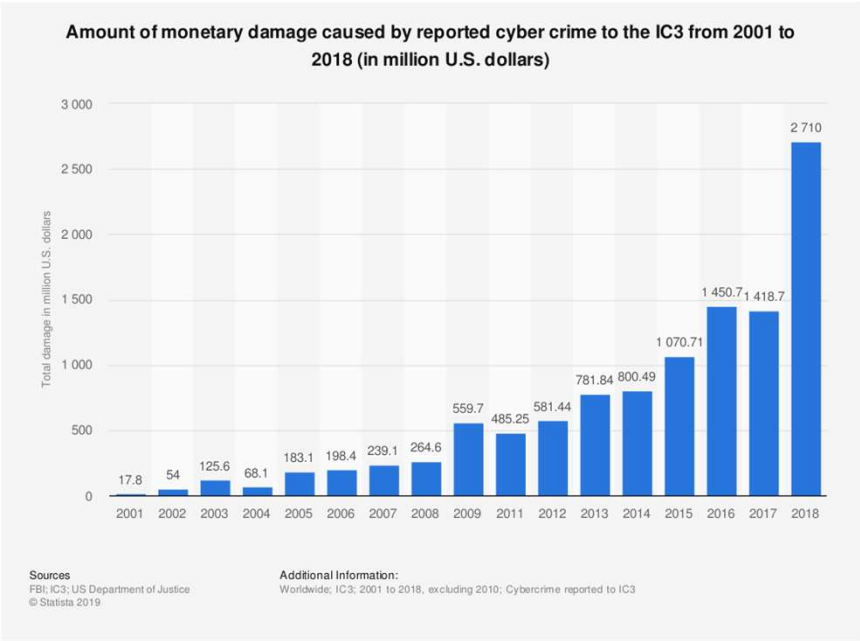
**Sécurité :** ne garantit pas que le code ne soit utilisé que par un employé autorisé

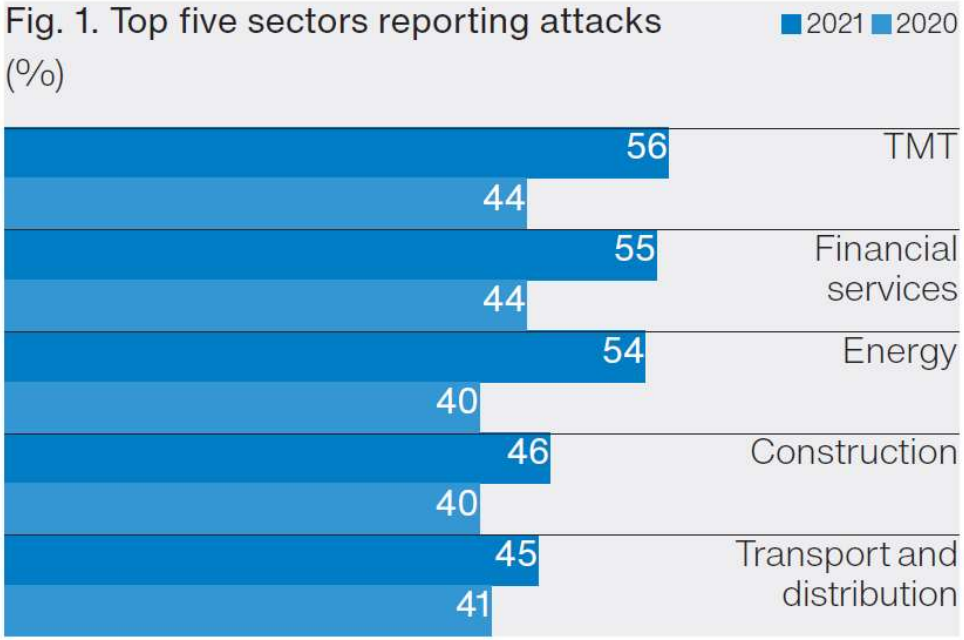
## Exemple 2

**Sûreté :**
« il n'y a pas d'erreur dans le système de contrôle d'accès»

**Sécurité :** ne garantit pas que seuls les employés autorisés ont été ajoutés

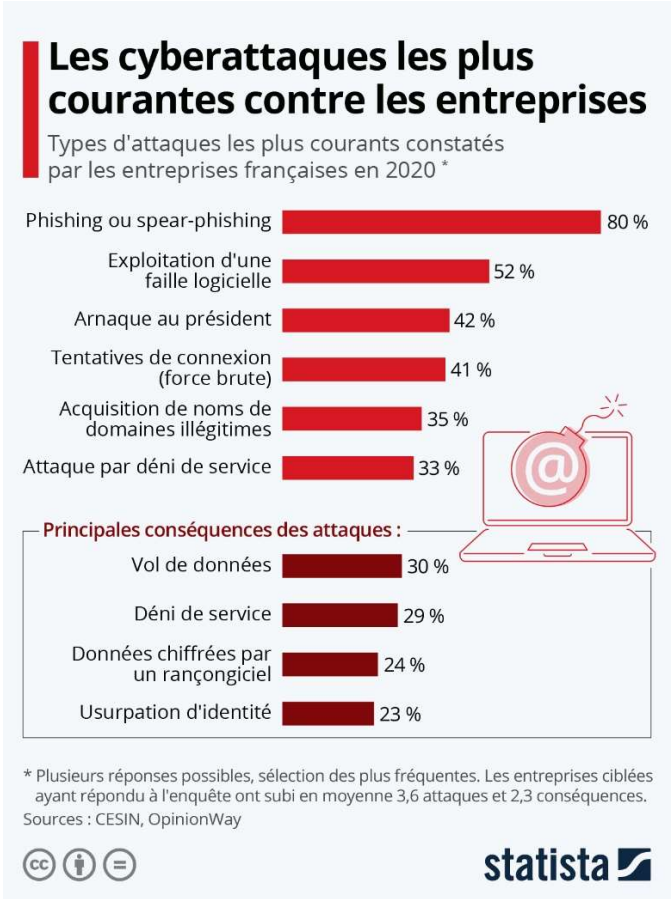
# Les menaces pèsent sur les secteurs vitaux



# Cybersécurité

- Le vol de données n’est pas tout
- Se concentrer sur cela, c’est ignorer le reste
- Regardons la cybersécurité d’une manière plus « globale »
- Pour anticiper toutes les menaces.



# Les menaces évoluent et s'intensifient

- 2 malwares sur 3 restent sous le radar des anti-malwares traditionnels
- +60 % des attaques ne sont pas liées à des malwares
- Augmentation de l'exploitation des vulnérabilités critiques « 0-day » et généralisées
- Log4shell, .. : La situation géopolitique augmente les niveaux de cybermenaces au niveau mondial
- C'est notamment le cas en Belgique (UE + OTAN)

Quels moyens minimums faut-il ?

# Le premier moyen : une volonté politique mondiale

- Sans une politique cohérente, il n'y a pas de direction
- Sans union transfrontalière, il n'y a pas de couverture numérique mondiale
- Structures européennes : ENISA, CCB, CERT, etc.
- Normes : RGPD, NIS, ISO 27001, Loi IA, ...
- Fournisseurs de services disponibles pour déployer des mesures et des protections
- Une police/une justice soutenue et formée.

# Deuxième moyen : une meilleure organisation


Aspects financiers

Impacts sur la réputation

**Sécurité I.S**

Aspects juridiques

Impact sur l'organisation

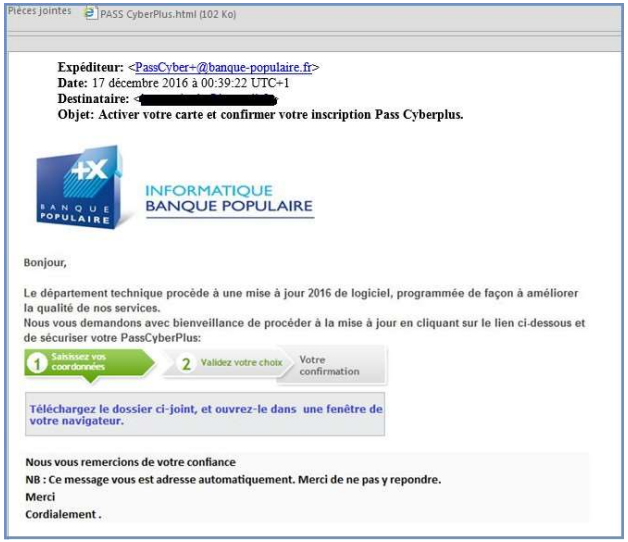
# Troisième moyen : l’éducation

- L’éducation dès le plus jeune âge
- Le numérique est la seule révolution industrielle non enseignée
- Formation continue des employés
- Reconversion des talents
- L’acceptation de l’atypique.

# Cas d’étude introductif : le phishing

Séminaire NIS 2

# Le phishing classique


Pièces jointes PASS CyberPlus.html (102 Ko)

**Expéditeur:** <PassCyber+@banque-populaire.fr>
**Date:** 17 décembre 2016 à 00:39:22 UTC+1
**Destinataire:** [redacted]
**Objet: Activer votre carte et confirmer votre inscription Pass Cyberplus.**

INFORMATIQUE BANQUE POPULAIRE

Bonjour,

Le département technique procède à une mise à jour 2016 de logiciel, programmée de façon à améliorer la qualité de nos services.
Nous vous demandons avec bienveillance de procéder à la mise à jour en cliquant sur le lien ci-dessous et de sécuriser votre PassCyberPlus:

1 Saisissez vos coordonnées 2 Validez votre choix Votre confirmation

Téléchargez le dossier ci-joint, et ouvrez-le dans une fenêtre de votre navigateur.

Nous vous remercions de votre confiance
NB : Ce message vous est adresse automatiquement. Merci de ne pas y repondre.
Merci
Cordialement .


**Van:** "Belfius BE" <klantenservice@fitforme.be>
**Onderwerp: Votre compte est suspendu**
**Datum:** 22 november 2022 om 17:41:24 CET
**Aan:**

Belfius

***Belfius mises à jour***

Suite à une vague de phishing le service technique a été mis à jour.

Suite à cette mise à jour certains comptes ciblés ont été verrouillés pour des raisons de sécurité.

Merci de suivre les étapes ci-dessous pour débloquer votre compte.

Pour récupérer l'accès total a votre compte , Il est recommandé de suivre les étapes de vérification.

Pour tout client ayant reçu ce mail et qui n'a pas effectué les étapes de vérification, sous 72h votre compte sera définitivement bloqué.

***Que dois-je faire***

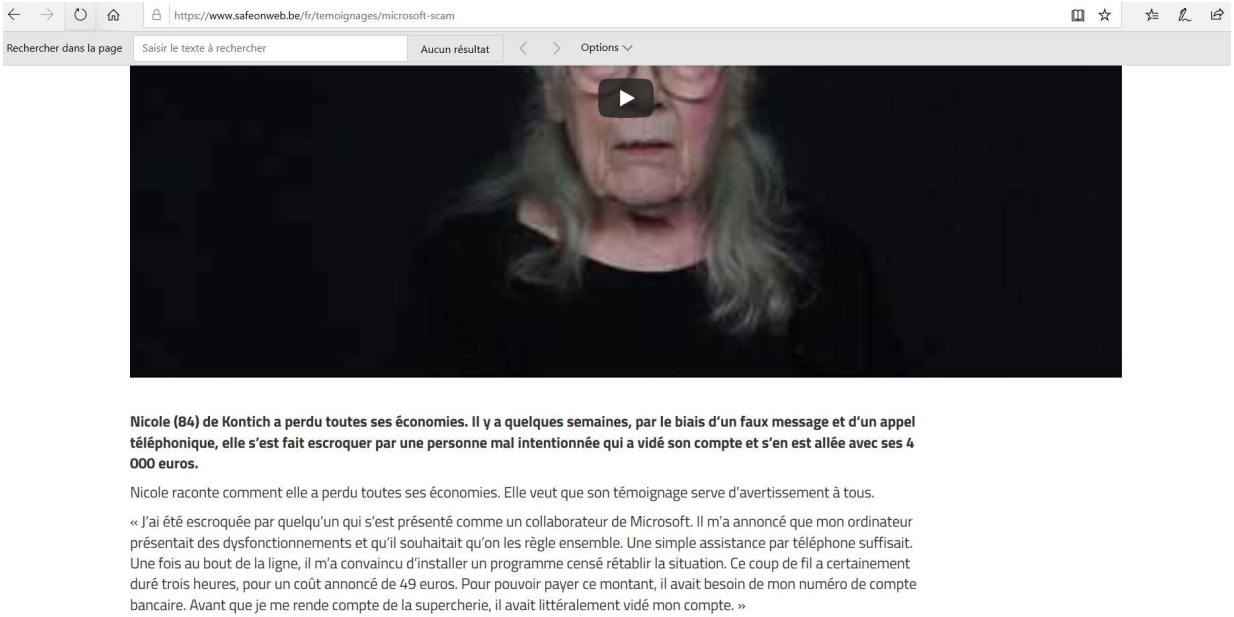
1. Vous trouverez ci-dessous le bouton permettant d'accéder au site Belfius. Vous pouvez vous connecter à vos accès bancaire.
2. Une fois la connexion effectuée, vous recevrez un mail de confirmation.

Cliquez-ici

PHISHING


- Un document de mise à jour d'un logiciel bancaire est proposé
- C'est important : la relation banque/client est désormais électronique (le covid renforce cette situation)
- Dois-je télécharger ce document ?
- Quelle sera la réaction de la banque (négligence grave) ?

# À tout âge et par tout moyen



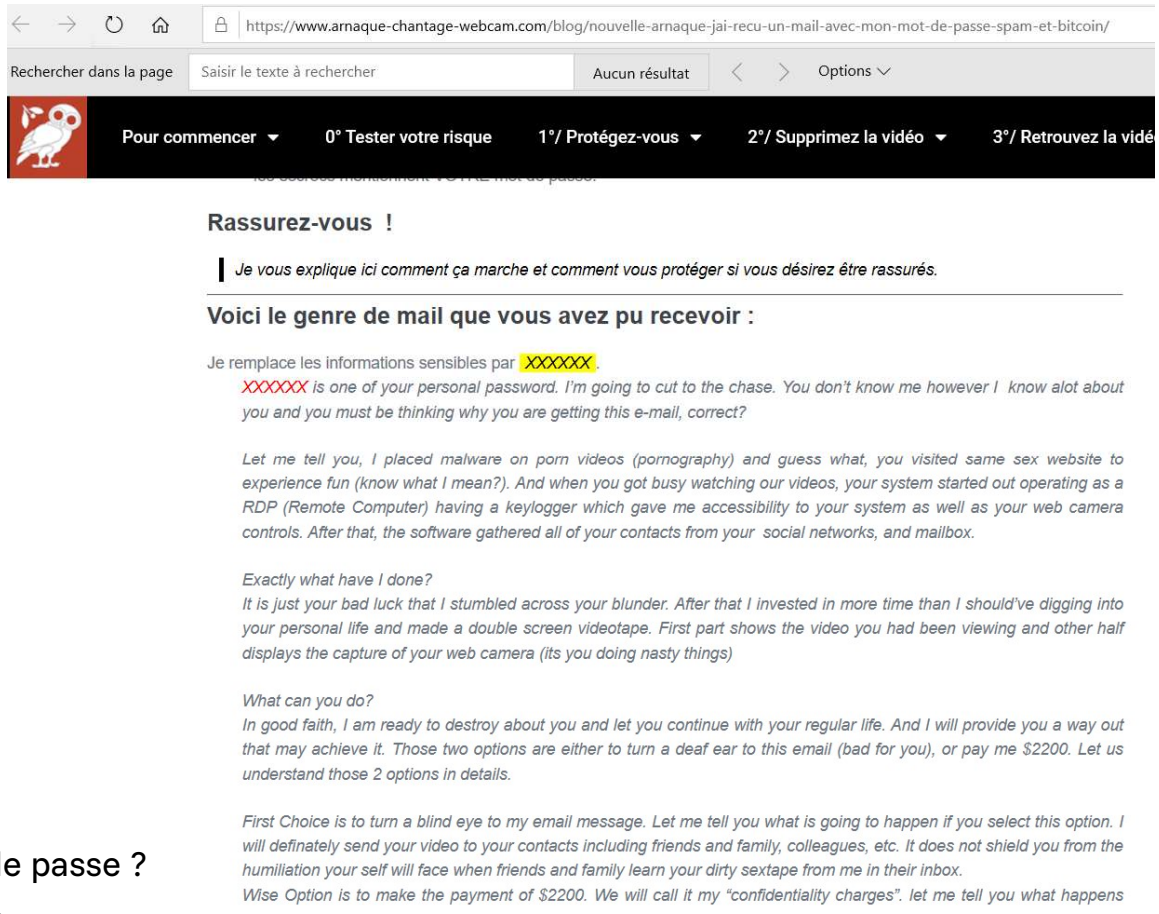

- Microsoft vous téléphone, votre ordinateur va mal,
- Heureusement, Microsoft va vous sauver! Suivez les instructions par téléphone.
- Allez-vous écouter Microsoft, ou ignorer cet appel au risque de perdre l'usage de votre ordinateur?

# Un autre exemple



- Un pirate a pris le contrôle de votre PC et vous a enregistré pendant que vous regardiez un site
- Vous devez payer via le dark web, sinon il diffusera tout
- Votre vie sociale, professionnelle et privée n'en sera pas affectée ! Allez-vous payer ?

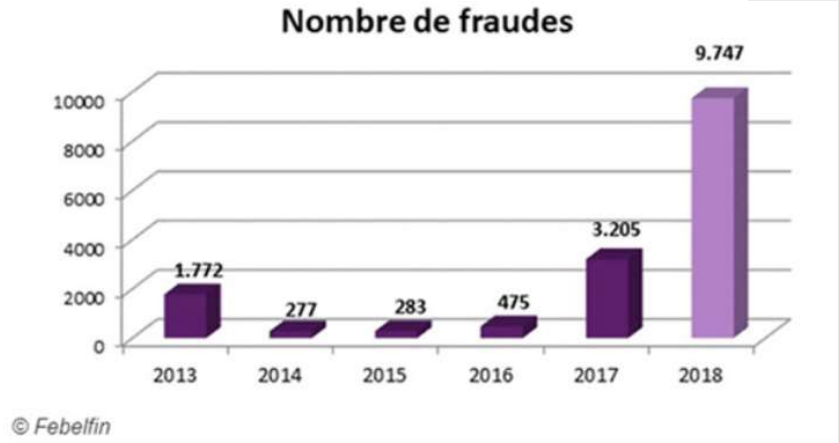
# De plus en plus personnalisé



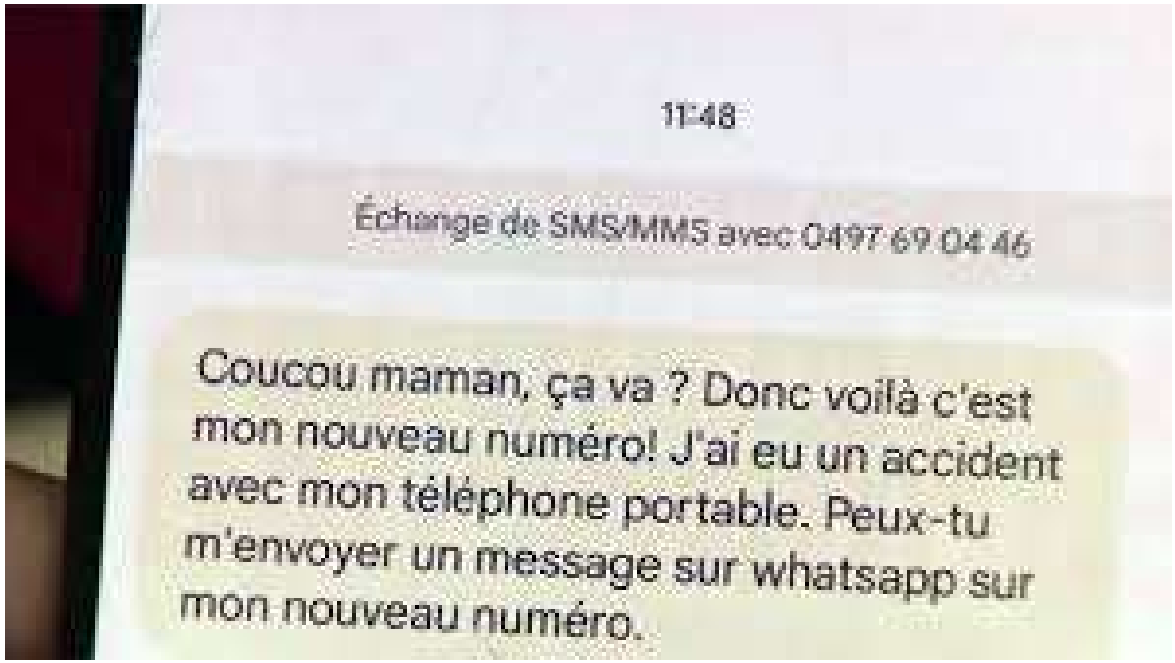

- Comment ont-ils obtenu votre mot de passe ?
- De façon plus générale, vos données

# Le phishing : un processus en évolution

- By email
- By social networks
- By whatsapp …




# Sur les thèmes/émotions du moment

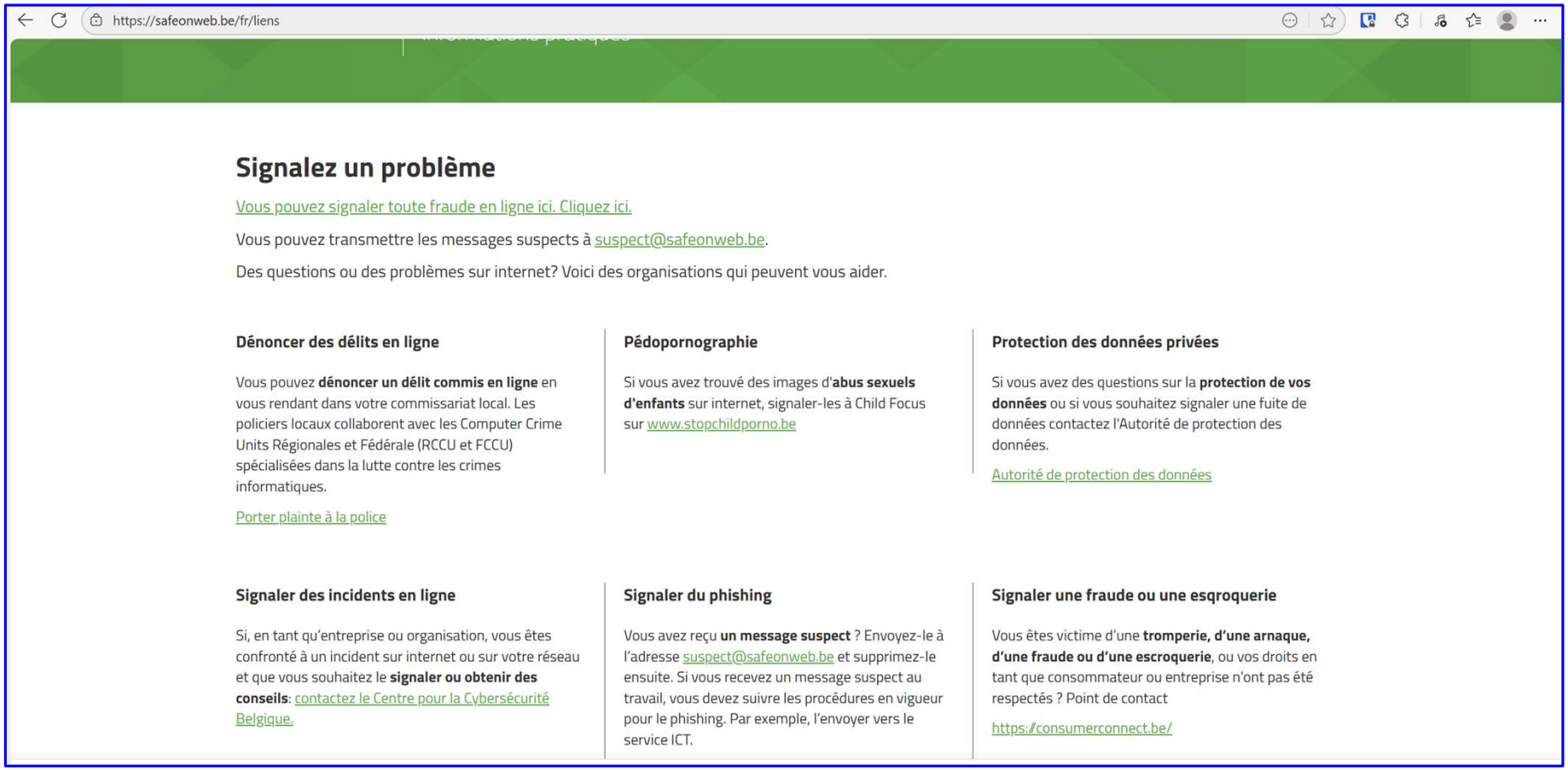
# Que peut-on faire contre le phishing ?

- Former et éduquer les employés sur les techniques de fraude et donner leurs des points de contacts
- Mettez en place des procédures de validation strictes pour les paiements (p. ex., double validation, appel direct au gestionnaire pour confirmation),
- Vérifiez les demandes suspectes en cas d'urgence inhabituelle ou de pression excessive (configurer office 365),
- Sécurisez les communications internes en limitant les informations sensibles accessibles au public.
- Utilisez une authentification forte pour éviter l'usurpation d'identité par e-mail (par exemple, DMARC, SPF, DKIM).
- Implémenter des plans de continuité et de reprise d'activité.

## En cas de doutes/ problèmes :

- Parler à la police
- Utilisation des ressources du CCB

*"Nous n'avons jamais autant besoin d'être humains"*


https://safeonweb.be/fr/liens
Signalez un problème
Vous pouvez signaler toute fraude en ligne ici. Cliquez ici.
Vous pouvez transmettre les messages suspects à suspect@safeonweb.be.
Des questions ou des problèmes sur internet? Voici des organisations qui peuvent vous aider.
Dénoncer des délits en ligne
Vous pouvez dénoncer un délit commis en ligne en vous rendant dans votre commissariat local. Les policiers locaux collaborent avec les Computer Crime Units Régionales et Fédérale (RCCU et FCCU) spécialisées dans la lutte contre les crimes informatiques.
Porter plainte à la police
Pédopornographie
Si vous avez trouvé des images d'abus sexuels d'enfants sur internet, signaler-les à Child Focus sur www.stopchildporno.be
Protection des données privées
Si vous avez des questions sur la protection de vos données ou si vous souhaitez signaler une fuite de données contactez l'Autorité de protection des données.
Autorité de protection des données
Signaler des incidents en ligne
Si, en tant qu'entreprise ou organisation, vous êtes confronté à un incident sur internet ou sur votre réseau et que vous souhaitez le signaler ou obtenir des conseils: contactez le Centre pour la Cybersécurité Belgique.
Signaler du phishing
Vous avez reçu un message suspect ? Envoyez-le à l'adresse suspect@safeonweb.be et supprimez-le ensuite. Si vous recevez un message suspect au travail, vous devez suivre les procédures en vigueur pour le phishing. Par exemple, l'envoyer vers le service ICT.
Signaler une fraude ou une esqroquerie
Vous êtes victime d'une tromperie, d'une arnaque, d'une fraude ou d'une escroquerie, ou vos droits en tant que consommateur ou entreprise n'ont pas été respectés ? Point de contact
https://consumerconnect.be/


https://safeonweb.be/fr/faire-le-test-du-phishing
NL FR DE EN
Autres informations et services du gouvernement: www.belgium.be
Safeonweb be
ACTU BLOG CONSEILS @WORK CAMPAGNES OUTILS ENSEIGNER LIENS CONTACT
Faire le test du phishing
Testez votre connaissance
Chaque jour, nous sommes nombreux à être victimes de faux mails. Par ces mails de phishing, les auteurs tentent de nous extorquer des informations personnelles, des données bancaires ou encore de contaminer notre ordinateur privé ou professionel.
Vous tombez facilement dans le panneau ou, au contraire, vous êtes un as dans l'art de détecter les moindres signes d'une arnaque?
Faire le test du phishing

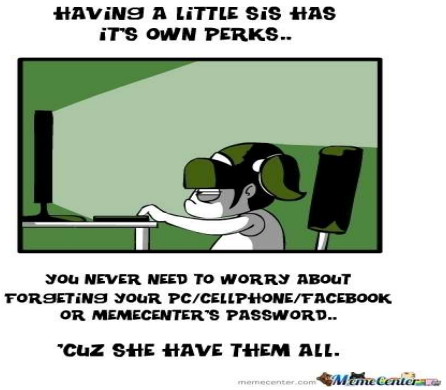

https://safeonweb.be/fr/infecte-par-un-virus
NL FR DE EN
Autres informations et services du gouvernement: www.belgium.be
Safeonweb be
ACTU BLOG CONSEILS @WORK CAMPAGNES OUTILS ENSEIGNER LIENS CONTACT
Infecté par un virus ?
Procédez à un scan en ligne
Vous pensez que votre ordinateur a pu être infecté par un virus ?
Procédez à un scan en ligne gratuit disponible sur l'un des sites antivirus* suivants (uniquement pour les utilisateurs Windows):
F-Secure Online Scanner
Panda Cloud Cleaner
ESET Online Scanner
Si vous disposez déjà d'un logiciel antivirus, utilisez-le sans plus attendre ! S'il détecte un virus, il vous guidera dans le processus de suppression du virus.
Choisissez un antivirus
Si vous n'avez pas encore installé d'antivirus, choisissez-en un dans la liste des antivirus fiables du site neutre de l'institut

# Qui sont les pirates ?

Séminaire NIS 2

# Les pirates ne sont pas toujours méchants !







# Hackers blancs



- White Hat : trouver des vulnérabilités et forcer les entreprises à les corriger
- La correction coûte cher… Les entreprises sont souvent peu réactives ! (un danger pour vous)
- Importance de l’analyse des risques!

# Les vrais méchants (chapeau noir)

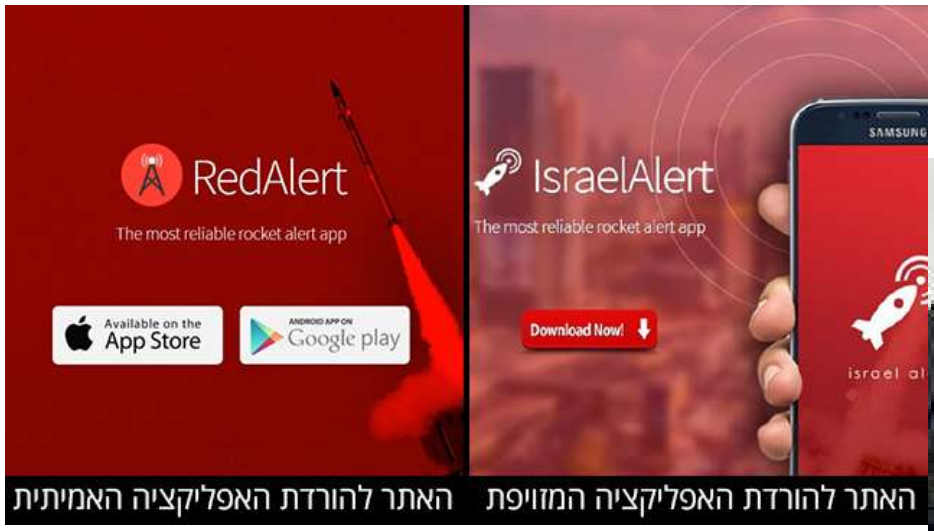
**Objectifs :** détruire, corrompre, manipuler, bloquer, vendre

- Par idéologie ou pour l'argent
- Techniciens et fournisseurs/fournisseurs d'hébergement
- Certains gouvernements/entreprises sont dans cette catégorie !


# Quelle puissance pour les commanditaires ?

- **États-nations** : ressources illimitées, capacités cyber militaires.
- **Groupes affiliés** : expertise avancée, financement discret.
- **Cybercriminels** : réseaux mondiaux, outils sophistiqués accessibles.
- **Hacktivistes** : forte réactivité, influence médiatique.
- **Insiders** : accès direct aux systèmes critiques.

# Un exemple actuel




# Quelques objectifs de pirates/attaquants

## Financial reward (access data, sell data)

- Utilisateurs/e-mails
- Organisation interne
- Clients de données
- Mot de passe, compte bancaire, ...

## Resources

- Bande passante stockage/réseau
- Botnets

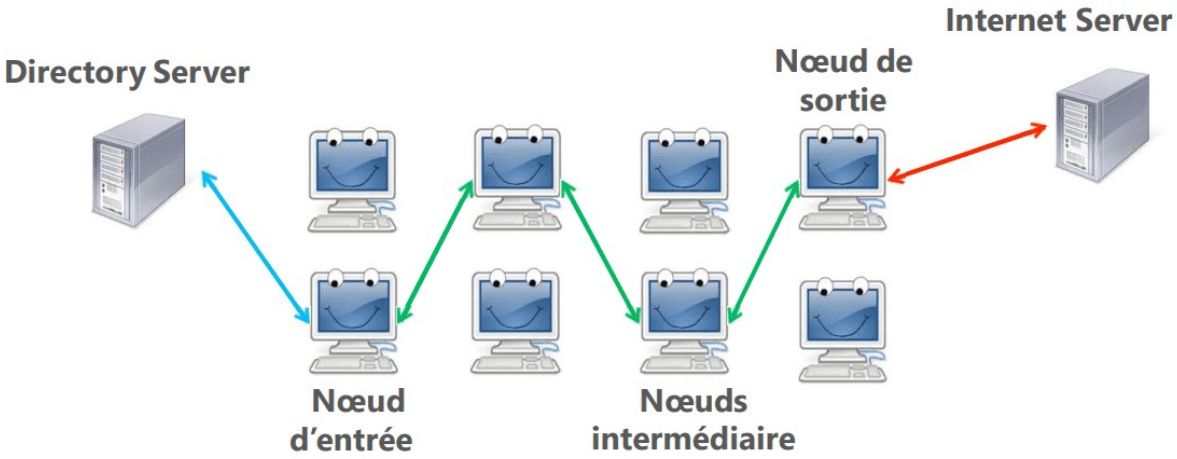
## Blackmail/extorsion

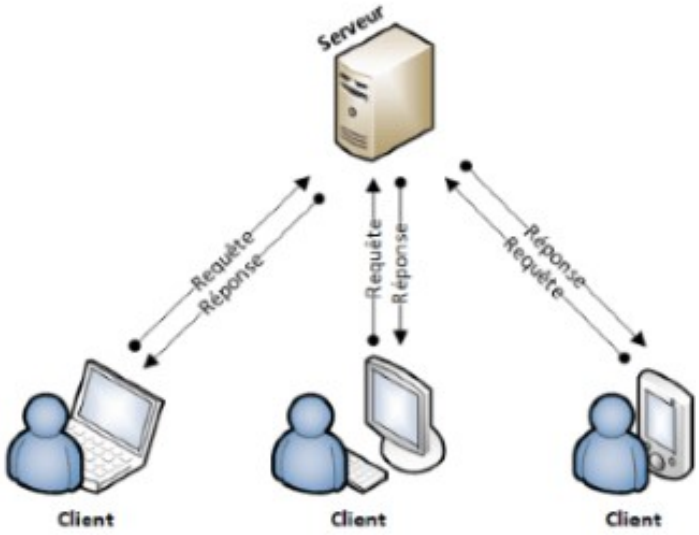
- Refus de service
- Perturbation des données

## Intelligence gathering

- Secteur d'activité/simultané
- Organisation de l'État

# Le Darkweb


Directory Server
Internet Server
Nœud de sortie
Nœud d'entrée
Nœuds intermédiaire


Serveur
Requête
Réponse
Requête
Réponse
Réponse
Requête
Client
Client
Client

# Comment fermer un site du Darkweb ?

- **Enquête judiciaire :** collecte de preuves, identification des administrateurs, et obtention des mandats nécessaires (perquisitions, saisies de serveurs).
- **Travail technique :** souvent, ces sites reposent sur des serveurs classiques (hébergés dans des datacenters connus). L'objectif est d'identifier l'infrastructure réelle derrière le réseau anonymisé.
- **Coopération internationale :** les serveurs étant répartis dans plusieurs pays, il faut la collaboration d'agences étrangères (Europol, Interpol, FBI, etc.).
- **Saisie & redirection :** une fois saisi, le domaine .onion est contrôlé par les autorités. Les utilisateurs qui tentent d'y accéder voient alors une bannière officielle (« ce site a été fermé par… »).
- **Communication publique :** fermeture souvent annoncée pour montrer la capacité d'action des forces de l'ordre et dissuader.

# Réflexions

- **Faut-il toujours lutter contre les hackers ?**
  … Ou s'unir à eux ? Engageriez-vous un hacker (problème de confiance) ?
- **Faits/Idées préconçues :**
  - Often more skilled than certified "experts."
  - Frequently lack formal education in a credential-heavy world.
  - Sometimes have criminal records, raising doubts about change.
- **Observation :**
  - Our society is not ready for this (elitism).

# Exemples de modèles d’attaque

Séminaire NIS 2

# Les attaques « grand public » sont souvent simples

Il existe plusieurs risques majeurs :

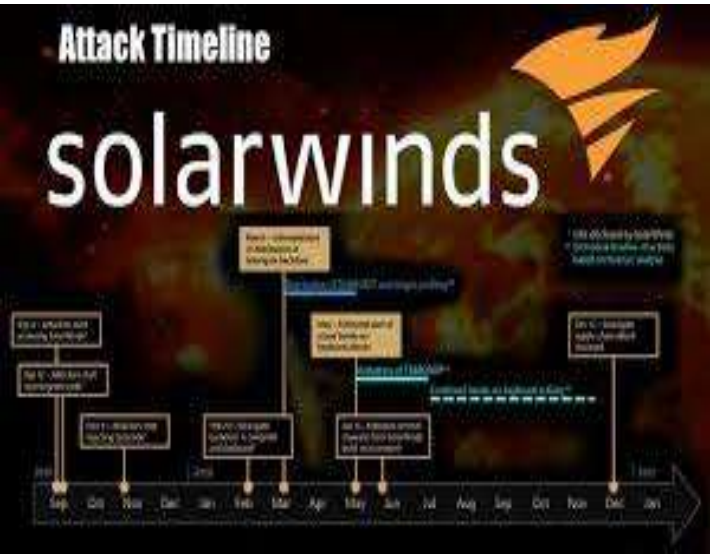
1. Vol ou conservation des données
2. Espionnage
3. Blocage (DDOS)

# Vol de données et rançon

Une ville est victime d'une rançon,
tous les services sont bloqués.

- Comment communiquer sur la situation ?
- Devez-vous payer ?
- Est-ce suffisant pour payer ?
- Comment gérer la continuité de service ?
- Comment pouvons-nous faire en sorte que cela ne se reproduise pas ?
- Dois-je souscrire une assurance ?

# L’espionnage par Orion




**Compromission du logiciel Orion de SolarWinds, un fournisseur de solutions de gestion informatique.**

- **Objectif :** Infiltrer les systèmes gouvernementaux et corporatifs.
- **Victimes :**
  - **Worldwide**: Des organisations des secteurs public et privé, y compris des organismes gouvernementaux, des entreprises technologiques et des fournisseurs de services.
  - **USA**: Des organismes clés tels que le Trésor, le Commerce, les départements de l’Énergie et la National Nuclear Security Administration ont été touchés.
- **Vecteur d’intrusion :** Mise à jour logicielle.

# Attaque DDOS

Mirai


# Vecteurs d’intrusion

# Le cas spécifique des systèmes de distribution d'eau

Séminaire NIS 2

# Dossier de presse de mars 2025 : alerte OTAN

ABONNÉS

## Une experte de l'OTAN met en garde la Belgique quant au risque de cyberattaque : voici le scénario catastrophe le plus redouté !

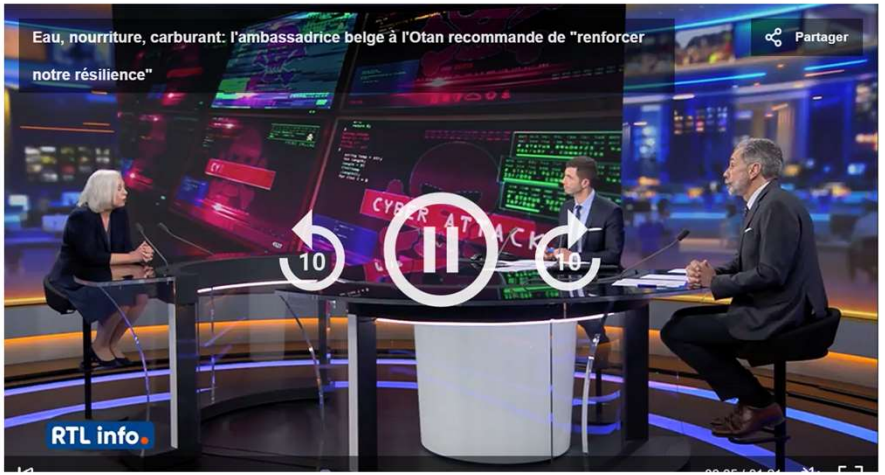
Régulièrement prise pour cible par des hackers, la Belgique craint une cyberattaque de vaste ampleur sur ses infrastructures.

RTL info.

MONDE POLITIQUE SPORTS VOS TÉMOIGNAGES PEOPLE CONSO PRÈS DE CHEZ VOUS DANS L

## "C'est une menace": une cyberattaque russe est probable... et elle pourrait paralyser la distribution d'eau et d'électricité

Publié le 12/03 à 20h27 par RTL info




Cibles : eau, banques, électricité (infrastructures critiques)

# OLDSMAR, Floride

- Un pirate informatique a obtenu un accès à distance non autorisé au système SCADA d'une installation de traitement de l'eau.
- L'attaquant a augmenté les niveaux d'hydroxyde de sodium (lessive) dans l'approvisionnement en eau à des niveaux dangereux.
- Heureusement, un opérateur a repéré l'intrusion en temps réel et a inversé le changement avant qu'un dommage ne se produise.
- L'attaque a mis en évidence les vulnérabilités d'outils d'accès à distance mal sécurisés et d'infrastructures obsolètes.

# Israël - 2020

- Les autorités israéliennes ont fait état de cyberattaques coordonnées visant des stations de traitement et de pompage de l'eau.
- L'origine présumée était l'Iran, avec des attaques visant à perturber les infrastructures critiques.
- Bien que les dégâts aient été minimes, l'événement a incité Israël à riposter par une cyberattaque contre un port iranien.
- L'affaire a souligné l'essor de la cyberguerre en tant qu'outil géopolitique ciblant les services civils.

# Compagnie des eaux du Royaume-Uni

- Plusieurs fournisseurs d'eau britanniques ont été ciblés par des attaques de ransomware.
- Les attaquants ont exigé des paiements en crypto-monnaie pour débloquer l'accès aux systèmes opérationnels.
- Certaines entreprises ont signalé des retards dans les services et des pertes de données, mais la qualité de l'eau et l'approvisionnement n'ont pas été directement affectés.
- L'incident a révélé d'importantes lacunes dans la planification d'urgence et la cyberhygiène dans le secteur.

# Pourquoi cela arrive-t-il ?

Votre secteur est :

- Essentiel pour la santé publique, l'hygiène, l'agriculture et l'industrie
- Fortement numérisé (pensez à l'IA) avec l'automatisation croissante (SCADA, IoT)
- Souvent sous-financé dans les investissements en cybersécurité
- L'interdépendance avec l'énergie et les transports

# Conséquences graves

- Contamination de l’approvisionnement en eau (chimique/biologique)
- Perturbation des opérations de distribution et de traitement
- Panique publique et érosion de la confiance
- Dommages juridiques, réglementaires et de réputation

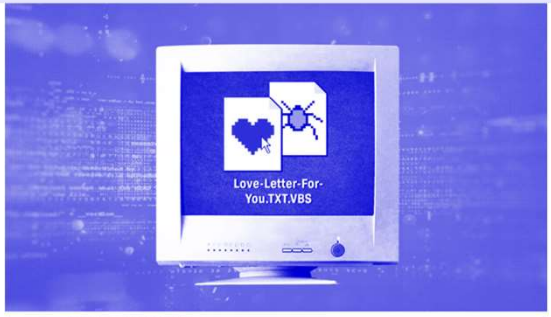
# Réglementation

Séminaire NIS 2

# Les cyberattaques, un crime ?

*« Une cyberattaque est un acte de malveillance contre un appareil informatique via un réseau cyber. »*

- Une cyberattaque est un délit ou même un crime, c'est de la cybercriminalité.




**'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on**

# Crime/délit ne signifie pas punition

- Les « cyberlois » ne sont pas uniformes entre les pays européens
- Et encore moins entre les continents :
  - Pour braquer une banque en France, il faut venir en France
  - Mais vous pouvez pirater une banque française depuis la Chine
  - Quelle loi s'appliquera?

- Le mieux est d'anticiper, après il est souvent trop tard !

# Deux axes principaux

La protection se base sur deux axes principaux :

1. **La protection des données**
(protection juridique)

2. **La protection des infrastructures et des produits**
(protection technique)

# Résumé

| Regulation | Objectif |
|---|---|
| GDPR<br>(General Data Protection Regulation) | Le RGPD régit la collecte, le traitement et le stockage des données personnelles au sein de l'Union européenne |
| Critical Infrastructure Resilience Act | L'objectif de cette directive méconnue de la presse est de protéger physiquement les infrastructures |
| CRA<br>(Cyber Resilience Act) | L'ARC impose des normes de cybersécurité pour les appareils et les logiciels connectés |
| NIS2<br>(Directive on Network and Information Security) | NIS2 renforce la cybersécurité des services essentiels et des fournisseurs de services numériques |

# Les pénalités

## NIS2 vs GDPR – Penalties

| Regulation | Scope | Maximum Penalty |
|---|---|---|
| GDPR | Personal data protection | **€20M** or 4% of global annual turnover |
| Maximum Penalty | **€7M** or 4% of global annual turnover | **€10M** or 2% of global annual turnover (severe breaches) |
| Other Measures | • Temporary processing ban | • Temporary suspension of activities<br>• Binding instructions to management |

# **NIS2** (Directive sur la sécurité des réseaux et de l'information)

## Definition

*NIS2 renforce la cybersécurité des services essentiels et des fournisseurs de services numériques. Les systèmes d'IA utilisés dans les infrastructures critiques doivent être sécurisés contre les violations et les perturbations opérationnelles.*


*Figure 1: NIS2 Pillars (Source IN Groupe)*

# Example NIS2 (Directive on network and inf.security)

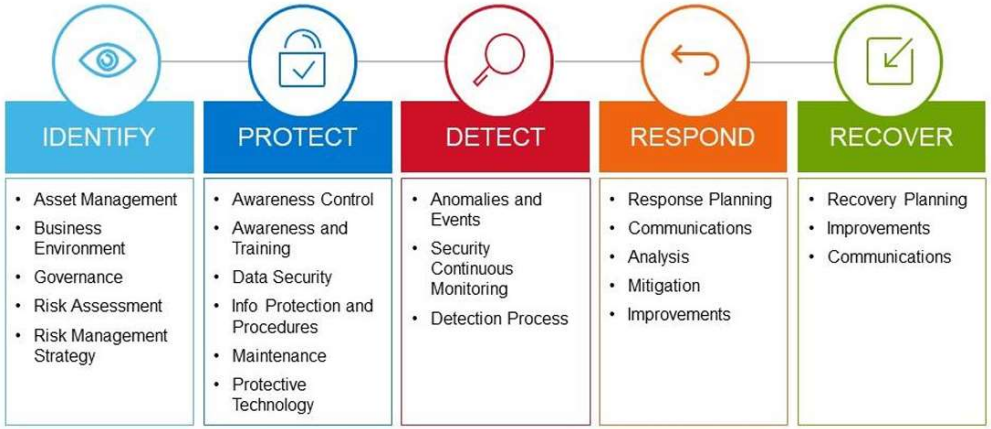
## Example

Le système de gestion de réseau basé sur l'IA d'un fournisseur d'énergie est perturbé par une cyberattaque, ce qui entraîne des pannes régionales.

**Solution pour se mettre en conformité :**

- Établissez des plans de réponse aux incidents robustes, mettez en œuvre une sécurité multicouche pour les systèmes d'IA
- Effectuez régulièrement des tests de résistance pour identifier les vulnérabilités.

# Le cadre du NIST




# Gouvernance et analyse de risque

Séminaire NIS 2

# Mettre en place une gouvernance cyber

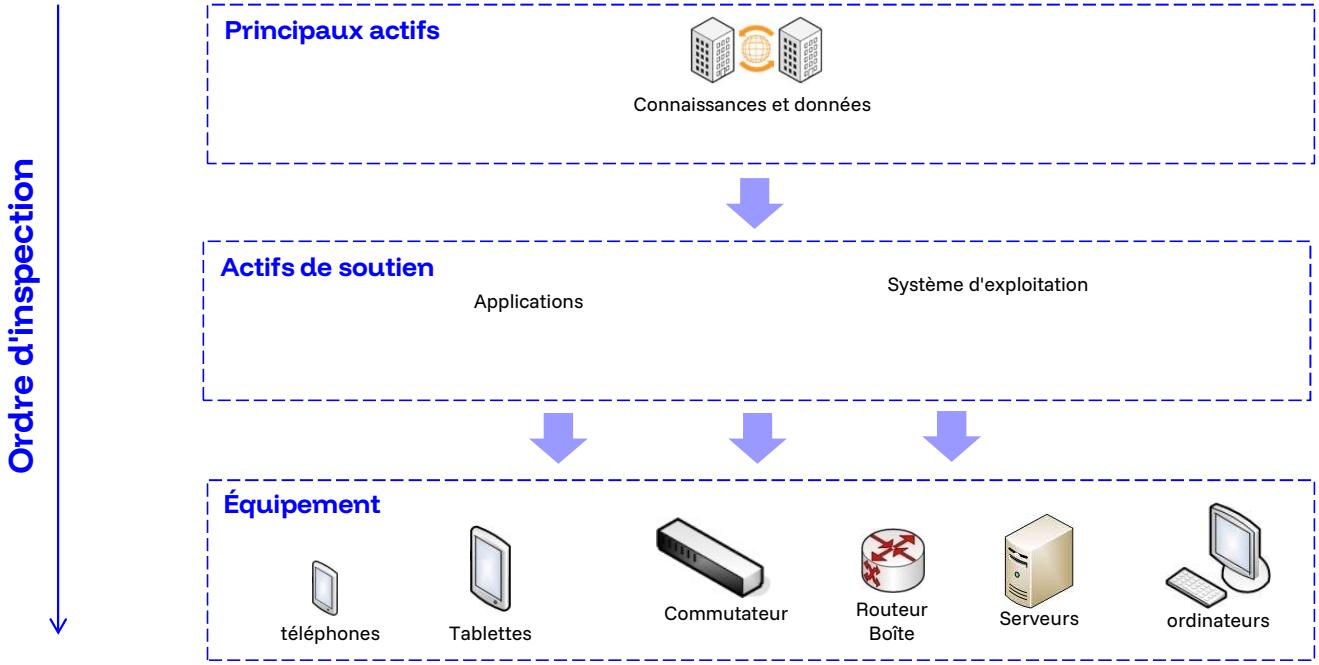
Une cybersécurité robuste combine des dispositifs de prévention, de détection et de réaction face aux menaces.

| Étape | Outil | Objectif | Horizon |
|---|---|---|---|
| 1 | **Analyse de risque** | Identifier les menaces et les vulnérabilités | Prévention |
| 2 | **Mesures de mitigation** | Réduire la probabilité ou l'impact | Réduction du risque |
| 3 | **Plan de continuité (PCA/PRA)** | Garantir la résilience en cas d'incident | Réaction et reprise |
| 4 | **Retour d'expérience (REX)** | Améliorer en continu le dispositif | Amélioration continue |

# Analyse de risques

- Identifier les actifs
- Analysez les menaces et les vulnérabilités
- Évaluer les risques en fonction des impacts possibles
- Traiter les risques (si nécessaire)
- Surveiller et améliorer en permanence

# Connaitre ses actifs




# Analyser les menaces par rapport à des critères

- Critères utilisés pour définir les niveaux de sécurité d'un SI
- Servir de mesure pour évaluer sa sécurité

**Disponibilité :** Peut être accessible en cas de besoin par ceux qui sont autorisés, ceux qui ne sont pas autorisés ne doivent pas interdire l'accès à ceux qui sont autorisés

**Intégrité :** Doit être exact et complet. Ne doit pas être modifié de manière illégale/illégitime, mais seulement par ceux qui sont autorisés

**Confidentialité :** Ne peut être accessible qu'à ceux qui y sont autorisés, et leur interdit de divulguer des informations à ceux qui ne sont pas autorisés à y accéder

# Un critère supplémentaire : la preuve

**Il s'agit de l'évolution de l'actif, principalement de la traçabilité**

- Qui interagit avec l'actif ?
- Comment s'effectue l'authentification de l'utilisateur ?
- Qui est responsable des interactions ?
- La traçabilité devient de plus en plus importante.
- C'est notamment le cas avec le framework NIS2.

# Les besoins en matière de sécurité doivent être évalués

- Souvent une évaluation basée sur le niveau (faible, moyen, fort, ...)
- Permet de mesurer l'impact en cas de succès d'une attaque
- Cela a un impact sur le niveau de protection.
- Très important : Dépend des contraintes internes et externes (ex : loi)
- Exemple :


**Niveau de disponibilité :** très fort

**Niveau d'intégrité :** Moyen

**Niveau de confidentialité :** très élevé

**Niveau d'épreuve :** faible

# Equation du risque

**RISQUE = Attaquants*VULNERABILITE*IMPACT**

« Attaquants * Vulnérabilité » se lit comme :
« la probabilité qu'un attaquant exploite la vulnérabilité »

| Niveau | Exemple | Interprétation |
|---|---|---|
| **Faible** | Une faille mineure sur un serveur interne isolé, connue seulement en interne, et nécessitant un accès physique. | L'exploitation est **peu probable** car les attaquants n'ont ni accès ni intérêt. |
| **Élevé** | Une faille critique non corrigée sur un serveur web exposé à Internet, déjà exploitée dans le monde par des groupes APT. | L'exploitation est **hautement probable** car la vulnérabilité est connue, accessible et attractive pour un attaquant puissant. |

# Plan de traitement des risques

On crée une matrice d'acceptance par vulnérabilité, puis on décide :

- Réduire (p. ex., appliquer un correctif)
- Transfert (p. ex., assurance)
- Accepter (risque résiduel)
- Éviter (abandonner un projet ou un actif)

| Impact \ Likelihood | Low | Medium | High |
|---|---|---|---|
| Low | Accepted | Accepted | Caution |
| Medium | Accepted | Caution | Not Accepted |
| High | Caution | Not Accepted | Not Accepted |

# Les mesures de mitigation

Des actions destinées à **réduire la probabilité ou l'impact** d'un risque lorsqu'il ne peut être totalement supprimé.

| Risque | Objectif de mitigation | Exemples de mesures concrètes | Effet attendu |
|---|---|---|---|
| **Intrusion** | Empêcher ou retarder l'accès non autorisé aux systèmes | Pare-feu, segmentation réseau, authentification multifactorielle | Réduction de la probabilité d'accès illégitime |
| **Vulnérabilité** | Empêcher l'exploitation d'une faille connue | Gestion proactive des patchs, surveillance des versions logicielles | Réduction du risque d'exploitation |
| **Vol de données** | Limiter l'impact d'une compromission | Chiffrement des données, contrôle des accès, sauvegardes sécurisées | Protection de la confidentialité et restauration rapide |
| **Phishing** | Réduire la probabilité de compromission humaine | Filtrage des courriels, simulation de phishing, sensibilisation du personnel | Diminution du taux de clic sur des liens malveillants |

# Plan de continuité et de retour (PCA/PRA)

| Objectif | Type de plan | Exemple de mesure | Effet attendu |
|---|---|---|---|
| **Assurer la disponibilité** | PCA | Hébergement redondant, site de secours | Activité maintenue sans interruption critique |
| **Protéger les données** | PRA | Sauvegardes automatisées et externalisées | Restauration rapide après incident |
| **Coordonner la crise** | PCA | Cellule de crise et procédures de communication | Réaction rapide et ordonnée |
| **Redémarrer les systèmes** | PRA | Plans de restauration testés, images système prêtes | Retour à la normale contrôlé |
| **Améliorer la résilience** | PCA & PRA | Tests annuels, retours d'expérience | Renforcement continu des dispositifs |

# Exemple virtuel

**Entreprise :** AquaCity Utilities

**Secteur :** Gestion publique de l'eau et des eaux usées

**Actifs clés :** systèmes SCADA, ERP, capteurs IoT, applications mobiles

AQUACITY
Utilities

# 1. Identification des actifs

- Réseau SCADA : contrôle des pompes et du traitement
- Facturation client et systèmes ERP
- Capteurs IoT pour la pression et la qualité de l'eau
- Applications mobiles et serveurs internes pour les techniciens

AQUACITY Utilities

# 2. Menaces et vulnérabilité

- **Menaces :** ransomware, hameçonnage, compromission de la chaîne d'approvisionnement, exposition des API
- **Vulnérabilités :** systèmes hérités, authentification faible, informations d'identification partagées, antivirus obsolète

# 3. Evaluation des risques

- Scénario : Accès par hameçonnage → SCADA → manipulation du chlore
- Impact : Critique – Risque pour la santé publique
- Probabilité : Moyenne – Filtrage des e-mails faible
- Niveau de risque : ÉLEVÉ

# 4. Plan de traitement des risques

- SCADA : Réduire – sensibilisation, filtrage, segmentation
- API IoT : Réduire – Rotation des clés API, accès VPN
- Informations d'identification : à éviter : RBAC unique, pas d'administrateur partagé
- Vol de mobile : Transfert – Cyberassurance

AQUACITY Utilities

# Quelques mots sur les contre-mesures

Séminaire NIS 2

# Contre-mesures de cybersécurité

# Exemples de contre-mesures

- **Celles que vous connaissez :**
  - Aucun @ dans les URL
  - Vérifier le nom du domaine : Facebook et non facbook
  - Certificats (n'acceptez pas un certificat non fiable)
  - Anti-spam
  - Mise à jour logicielle
  - Anti-virus (logiciel, web, ..)
  - …
- **Plus techniques :**
  - Intelligence artificielle
  - Protections de la pile/du tas/du compilateur
  - Outils de validation statiques et dynamiques
  - …

# Est-ce plus sûr ?

Les contre-mesures aident à percevoir le système comme étant plus sûr. Mais ce n'est pas toujours le cas, et une contre-mesure peut être vulnérable.

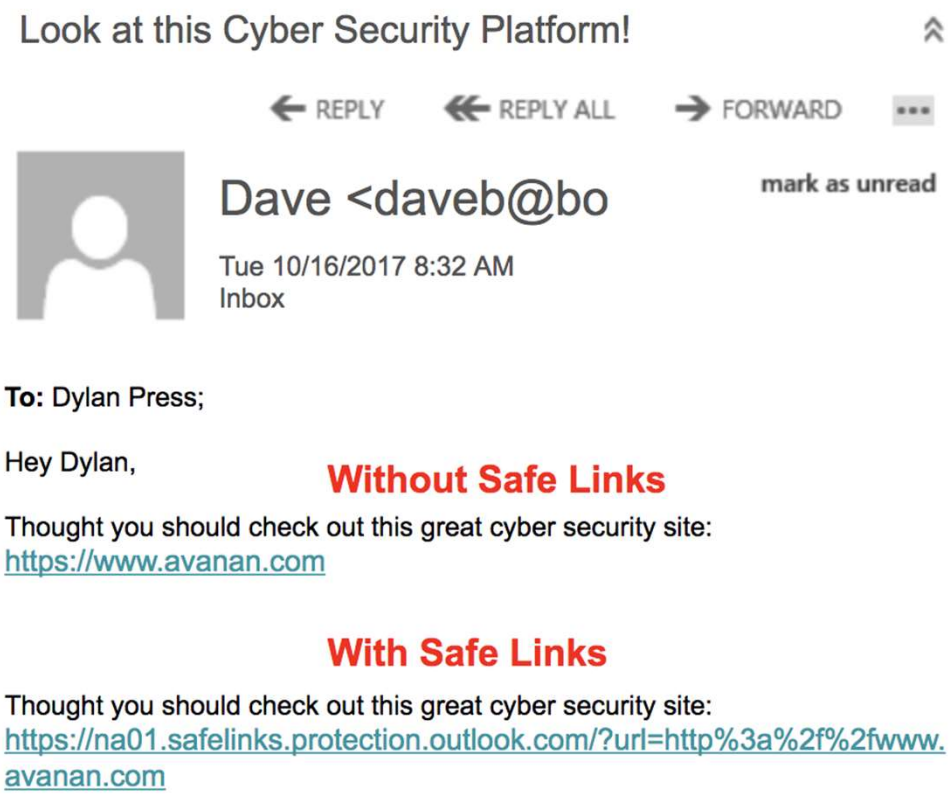
EXAMPLE:

- **Sécurité :** « Si vous perdez votre mot de passe, veuillez cliquer ici, un code vous sera envoyé par SMS »
- **Problème :** Pendant des années, il était possible de rediriger le numéro de téléphone par appel téléphonique vers l'opérateur

# Exemple d'antivirus (statique) : liens fiables (1)

- Illustrations de : https://www.avanan.com/blog/microsoft-atp-safe-links
- Lorsqu'une personne clique sur une URL dans un e-mail, la fonctionnalité Liens fiables vérifie si elle est malveillante ou sûre avant d'afficher la page Web dans le navigateur de l'utilisateur.
- Cela se fait par comparaison statique avec la base de données Microsoft
- Si l'URL est identifiée comme non sécurisée, l'utilisateur est redirigé vers une page affichant un message d'avertissement lui demandant s'il souhaite continuer vers la destination non sécurisée.

# Exemple d'antivirus (statique) : liens fiables (2)

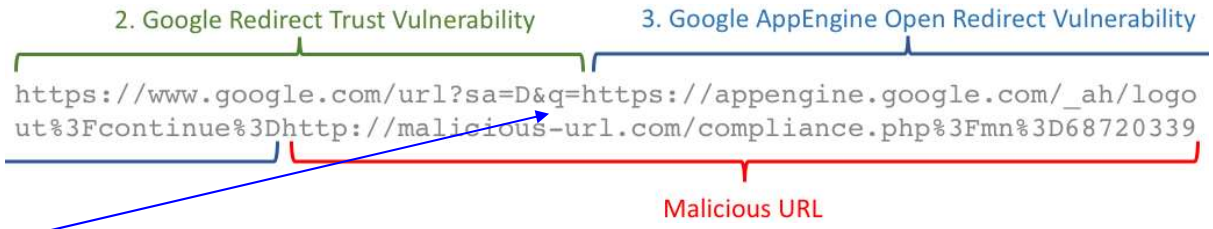


# Dangereux !

- La NSA pourrait collaborer avec Microsoft (porte dérobée intentionnelle)
- Safe Links n'analyse pas dynamiquement les URL : il vérifie uniquement si l'URL figure sur des listes noires connues de sites malveillants.
- Il a du mal à détecter les URL inconnues de type zero-day.
- L'analyse des liens fiables ne s'applique pas de liens fiables aux domaines qui sont ajoutés à la liste blanche de Microsoft.

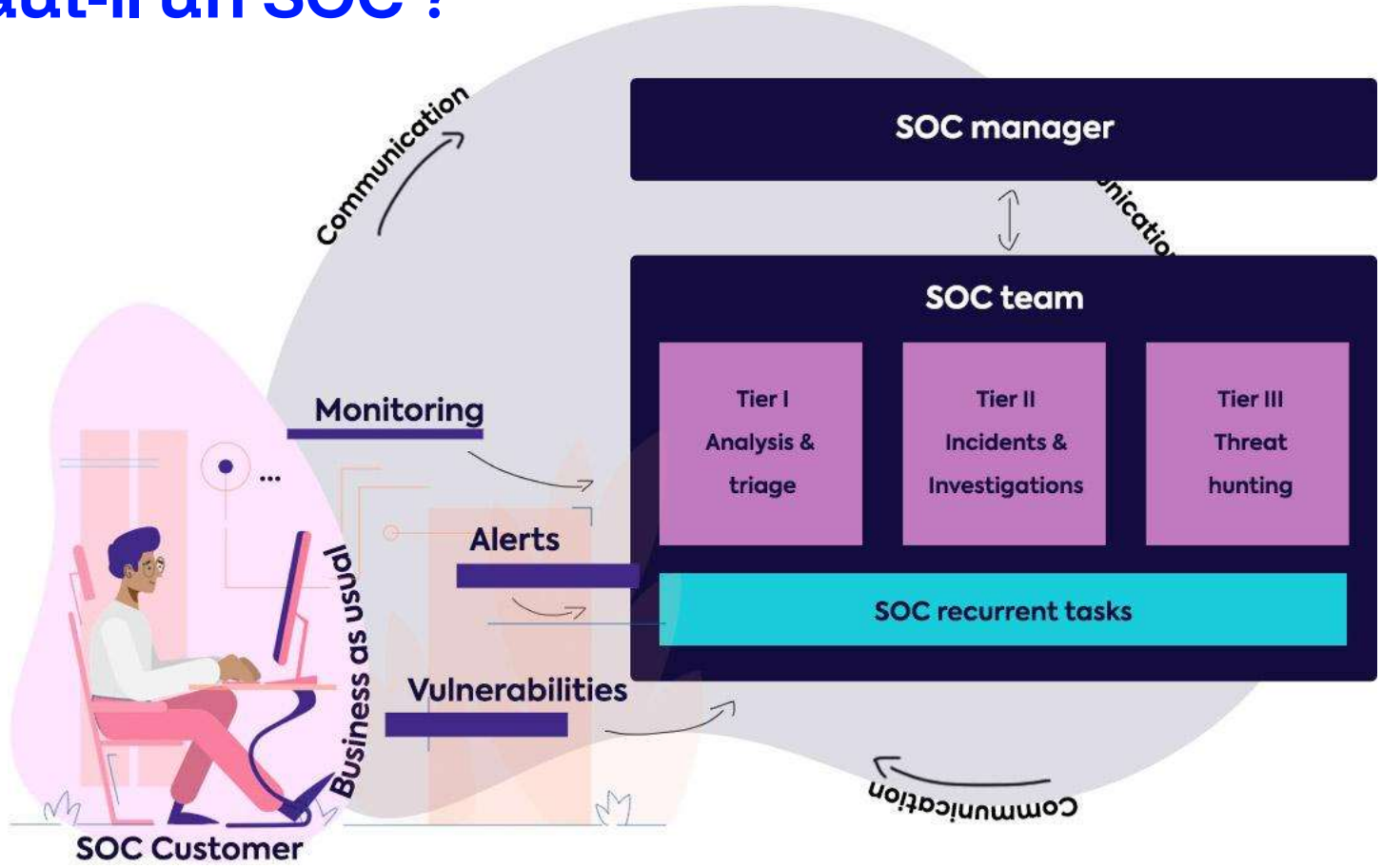
# Redirection Google (2018)

- Google est mis sur liste blanche par Safe Links.
- Problèmes : Google n'a jamais dit qu'il vérifierait les liens de redirection
- Vulnérabilité de redirection Google : envoyez un mail à votre secrétaire avec le lien suivant




- q= est une redirection
- Si vous effectuez une redirection en dehors de Google, vous recevrez un avertissement
- Rien ne se passera si vous restez à l'intérieur du domaine Google
- Il suffit de placer votre malware sur un domaine Google

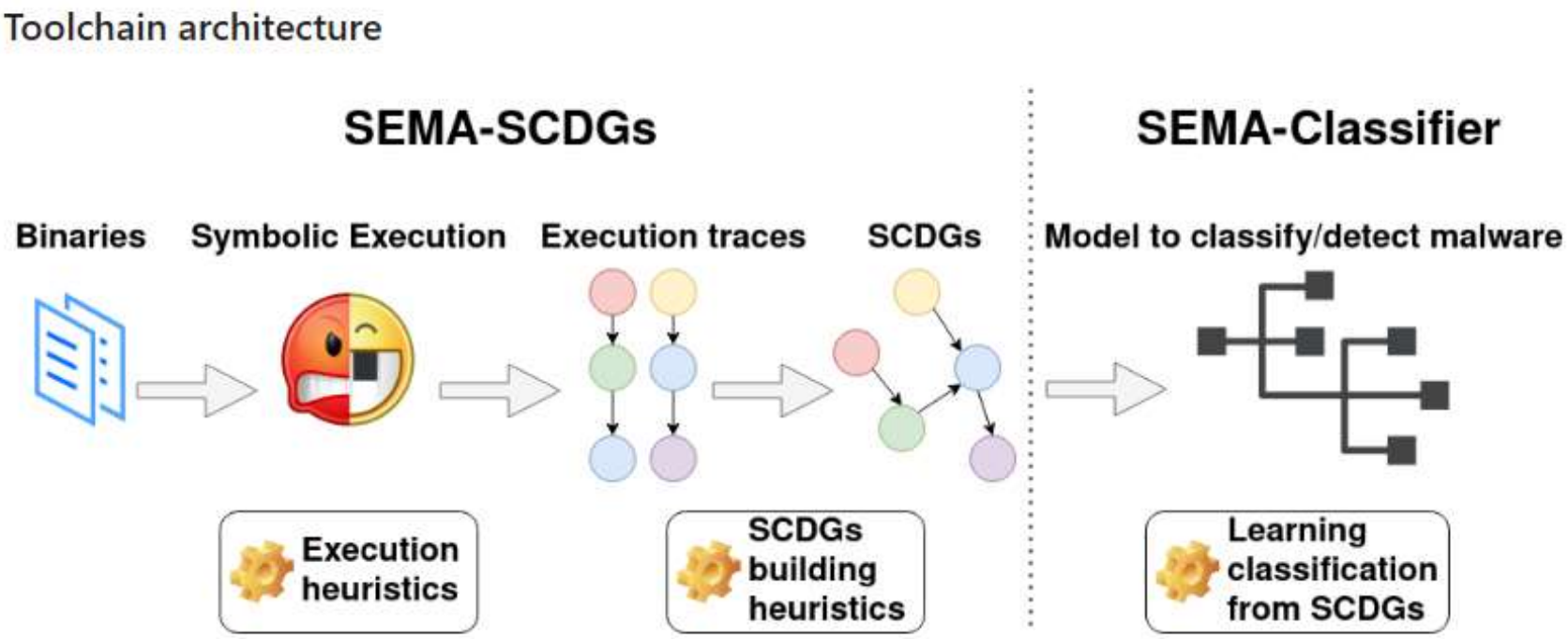
# Me faut-il un SOC ?



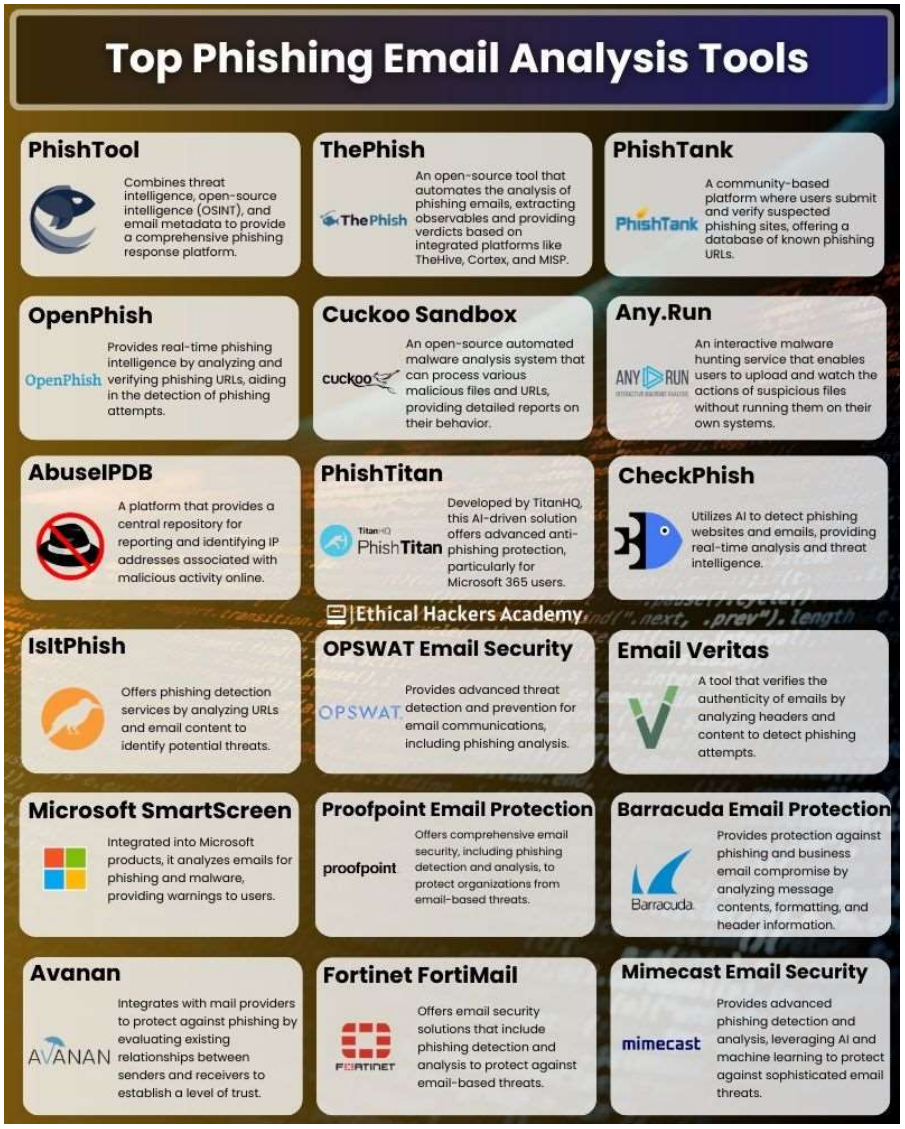
# L’IA peut-elle aider la cybersécurité ?

Séminaire NIS 2

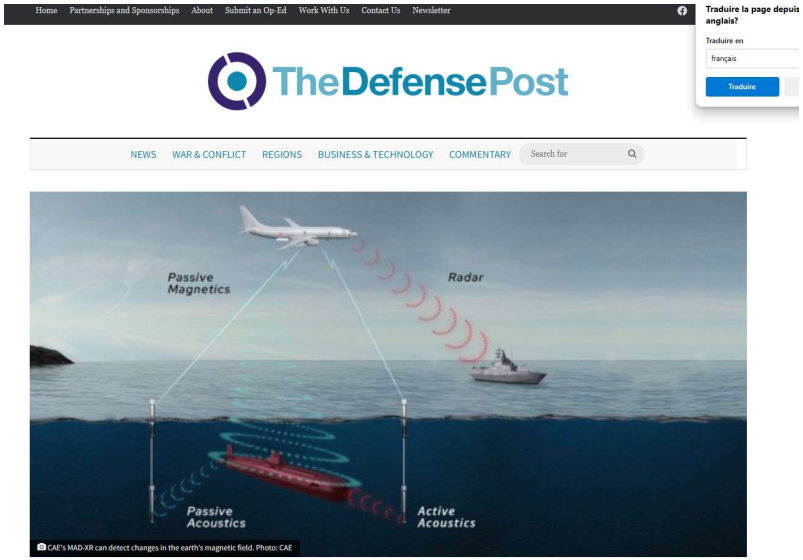
# Analyse des logiciels malveillants/virus

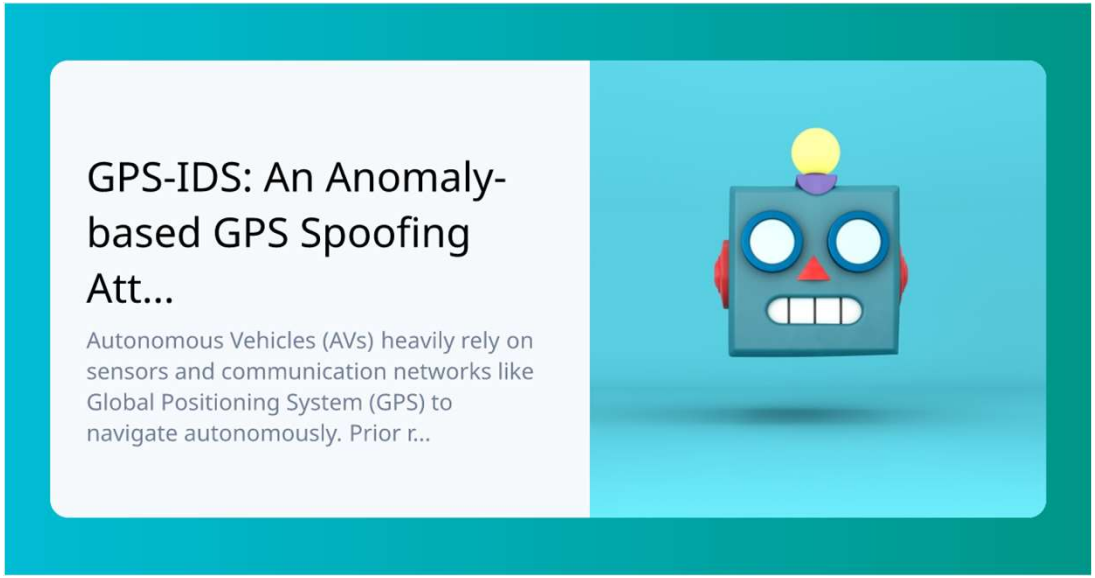


# Outils


Top Phishing Email Analysis Tools
PhishTool
Combines threat intelligence, open-source intelligence (OSINT), and email metadata to provide a comprehensive phishing response platform.
ThePhish
An open-source tool that automates the analysis of phishing emails, extracting observables and providing verdicts based on integrated platforms like TheHive, Cortex, and MISP.
PhishTank
A community-based platform where users submit and verify suspected phishing sites, offering a database of known phishing URLs.
OpenPhish
Provides real-time phishing intelligence by analyzing and verifying phishing URLs, aiding in the detection of phishing attempts.
Cuckoo Sandbox
An open-source automated malware analysis system that can process various malicious files and URLs, providing detailed reports on their behavior.
Any.Run
An interactive malware hunting service that enables users to upload and watch the actions of suspicious files without running them on their own systems.
AbuseIPDB
A platform that provides a central repository for reporting and identifying IP addresses associated with malicious activity online.
PhishTitan
Developed by TitanHQ, this AI-driven solution offers advanced anti-phishing protection, particularly for Microsoft 365 users.
CheckPhish
Utilizes AI to detect phishing websites and emails, providing real-time analysis and threat intelligence.
Ethical Hackers Academy
IsItPhish
Offers phishing detection services by analyzing URLs and email content to identify potential threats.
OPSWAT Email Security
Provides advanced threat detection and prevention for email communications, including phishing analysis.
Email Veritas
A tool that verifies the authenticity of emails by analyzing headers and content to detect phishing attempts.
Microsoft SmartScreen
Integrated into Microsoft products, it analyzes emails for phishing and malware, providing warnings to users.
Proofpoint Email Protection
Offers comprehensive email security, including phishing detection and analysis, to protect organizations from email-based threats.
Barracuda Email Protection
Provides protection against phishing and business email compromise by analyzing message contents, formatting, and header information.
Avanan
Integrates with mail providers to protect against phishing by evaluating existing relationships between senders and receivers to establish a level of trust.
Fortinet FortiMail
Offers email security solutions that include phishing detection and analysis to protect against email-based threats.
Mimecast Email Security
Provides advanced phishing detection and analysis, leveraging AI and machine learning to protect against sophisticated email threats.

# Anomalies dans les transmissions



# Conclusions

Séminaire NIS 2

# Bonne nouvelle

# Le cyber range de l'ADN

# Conclusion

- Les menaces évoluent, mais notre résilience grandit.
- En anticipant, nous réduisons les risques.
- En réfléchissant, nous faisons les bons choix.
- En agissant, nous assurons la continuité.

**La cybersécurité, c'est avant tout une affaire de préparation et de confiance.**

Digit'Eaux

Société Digitale des Eaux de Wallonie

# Séminaire sectoriel NIS2

12.12.2025, Namur

**Notre expertise numérique**
**au Service de l'Eau**

# Stratégie Digitale: 4 axes

## Digitalisation des processus

**Outiller voire automatiser les processus métiers dans une logique *fit-to-standard.***

- Optimisation des processus métiers
- Configuration d'outils commerciaux
- Production de données de qualité
- Adoption des processus standards et configurations Out-Of-The-Box
- Accompagnement au changement
- Transformation digitale en mode « projet » et par « Cycles en V »
- Partenariats stratégiques avec éditeurs de logiciels « socles » (SAP, Esri, 3P, Microsoft…)

## Valorisation de la donnée

**Exploiter la donnée comme levier de performance et de décision.**

- Capture, stockage, traitement, gouvernance et exploitation de la donnée
- Génération de rapports analytiques
- Développements d'applications spécifiques basées sur un écosystème stable et cohérent
- Intégration de l'IA
- Développement agile de « produits » plutôt que réalisation de « projets »
- Investissement sur une plateforme de donnée et d'intégration cohérente

## Sécurisation

**Renforcer la protection des systèmes, des données et des utilisateurs.**

- Sécurisation opérationnelle
- Gouvernance et processus
- Gestion des risques
- Gestion des incidents
- Sensibilisation et formation continue
- Continuité d'activité
- Sécurité de la supply chain
- *Security by design*

## Optimisation des coûts

**Réduire les coûts et simplifier la gestion via une mutualisation des moyens.**

- Gestion centralisée, harmonisée et standardisée des serveurs, bases de données, réseaux et workplace
- Externalisation des activités vers prestataires optimisés sur le coût
- Centralisation et standardisation des processus de support (helpdesk, incidents, changes, services)

Digit'Eaux
Société Digitale des Eaux de Wallonie

# Sécurité : Une approche sectorielle

Nous travaillons au niveau du secteur pour établir des **fondations communes** :

- Modèles de gouvernance
- Bonnes pratiques
- Processus standardisés
- Documentation réutilisable
- Référentiels de sécurité mutualisés

Objectif : **accélérer la maturité globale du secteur**, plutôt que multiplier des efforts isolés.

Digit'Eaux
Société Digitale des Eaux de Wallonie


None of us is as smart as all of us.
Kenneth H. Blanchard
quotefancy

# Mutualiser : un levier de performance

**Unir les experts, partager les moyens,**
**renforcer la résilience**

Grâce à la mutualisation :
Des compétences spécialisées deviennent accessibles à tous
Des outils avancés (SOC, SIEM, gestion des vulnérabilités, …) sont partagés
La conformité NIS2 devient plus simple et moins coûteuse
Les incidents sont mieux anticipés et résolus

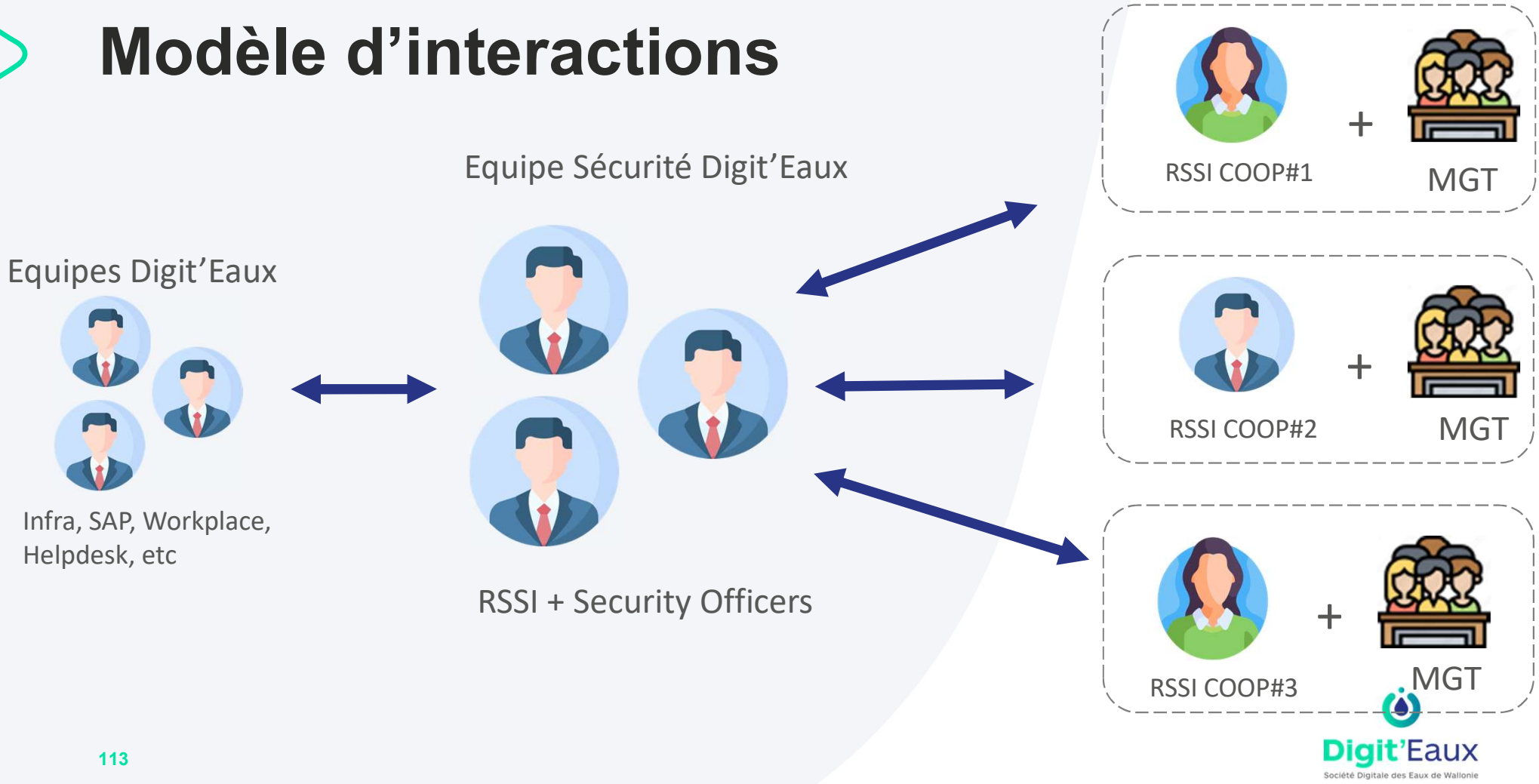
**Ensemble → un niveau de sécurité impossible à atteindre individuellement.**

Digit'Eaux
Société Digitale des Eaux de Wallonie

# Interactions et services

Digit'Eaux
Société Digitale des Eaux de Wallonie

# Modèle d'interactions



# Nos principaux services en Sécurité

**Gouvernance cyber**
- Partage de bonnes pratiques et mise en place de processus

**Audits**
- Audit Sécurité, Tests de pénétration, Security Footprint, analyse d'architecture, Suivi des recommandations

Projets / Services

**Monitoring & incidents**
- Mise en place d'un service SOC
- Processus de suivi d'incidents
- Suivi des incidents

**Sécurité opérationnelle**
- Protection des réseaux et des systèmes d'information (contrôles d'accès, antivirus, sauvegardes, etc.)
- Gestion du workplace et règles de sécurité associées (0365)



Digit'Eaux
Société Digitale des Eaux de Wallonie

# Conclusion

## Construire un secteur de l'eau plus résilient, ensemble

- Notre **volonté** : être un partenaire engagé à vos côtés
- Notre **objectif** : **sécuriser, harmoniser, professionnaliser**
- Nos **forces** : expertise, mutualisation, proximité terrain

**Ensemble, nous pouvons atteindre un niveau de sécurité supérieur et durable**

Digit'Eaux
Société Digitale des Eaux de Wallonie

Digit'Eaux

Société Digitale des Eaux de Wallonie

# Merci

**Notre expertise numérique**
**au Service de l'Eau**

# PRÉSENTATION
## 12 DÉCEMBRE 2025

SPGE
Société Publique de Gestion de l'Eau

IDELUX
Pour vous

# IDELUX

IDELUX
Pour vous

# ENVIRONNEMENT

# ÉCONOMIE

IDELUX ENVIRONNEMENT

**Gestion des déchets solides**

IDELUX EAU

**Valorisation de l'eau**

IDELUX PROJETS PUBLICS

**Projets communaux**


IDELUX DÉVELOPPEMENT

**Développement économique**

IDELUX FINANCES

**Financement**

# 6 secteurs prioritaires






# PÔLE SPATIAL
## REDU-TRANSINNE

IDELUX
Pour vous

# Stratégiquement situé au cœur de l'Europe

# Pôle spatial Redu-Transinne

- 2 sites

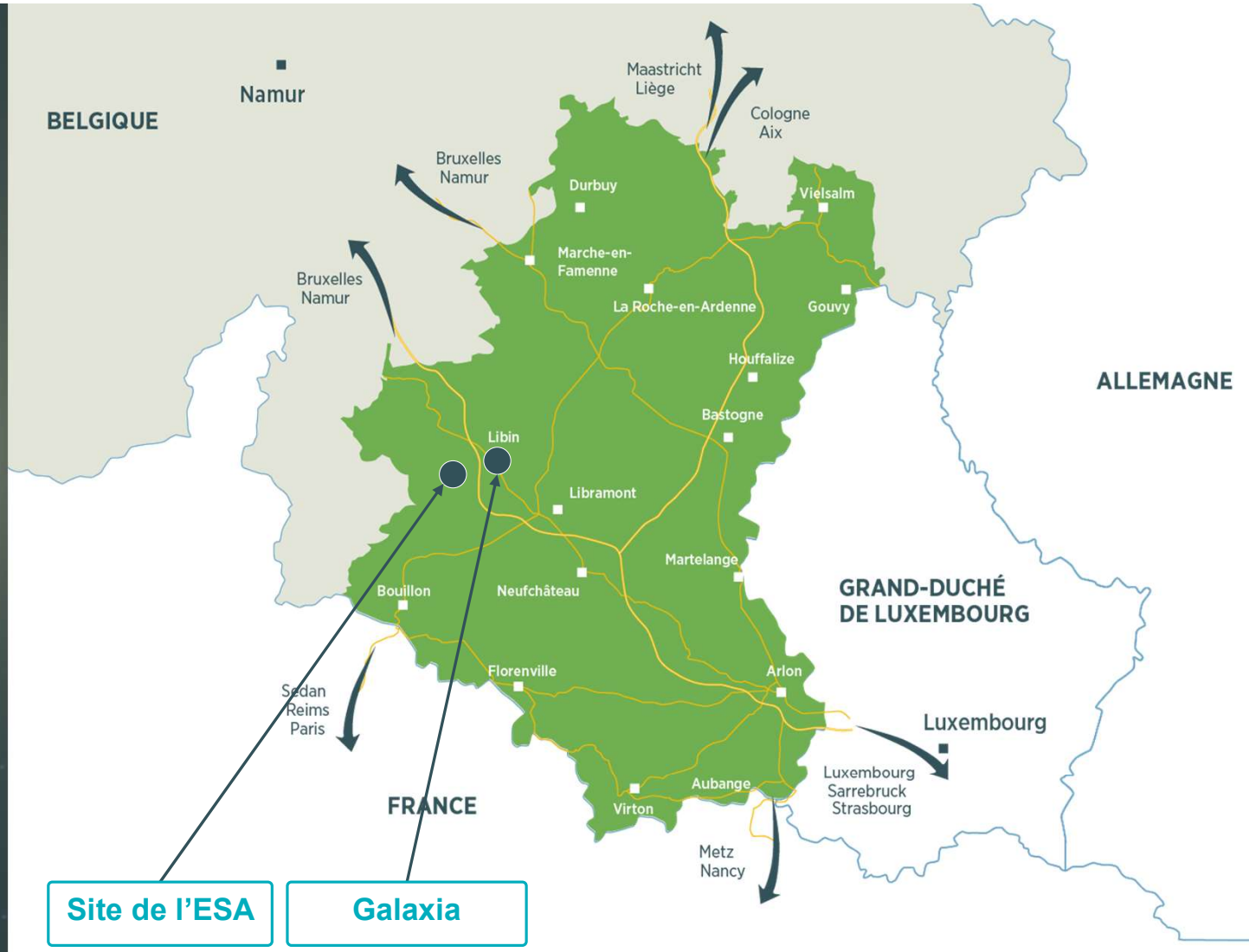


- 3 piliers

**Institutionnel** | **Éducatif** | **Entrepreneurial**

## Dans la province de Luxembourg, un pôle composé de deux sites reliés par fibre optique :

- **À Redu**, le centre de l'Agence Spatiale Européenne (ESA)
- **À Transinne**, le parc d'activités économiques Galaxia de 20 hectares développé par IDELUX



# Pôle spatial Redu-Transinne : 3 piliers

## Institutionnel

- ESA
- EUSPA (UE)

## Éducatif

- Euro Space Center
- ESEC Galaxia

Outils portés par le Plan de relance de la Wallonie

Centre Cybersécurité IDELUX

- Laboratoire Gilles Brassard de cryptographie quantique
- Cyber Range
- École de cybersécurité

## Entrepreneurial

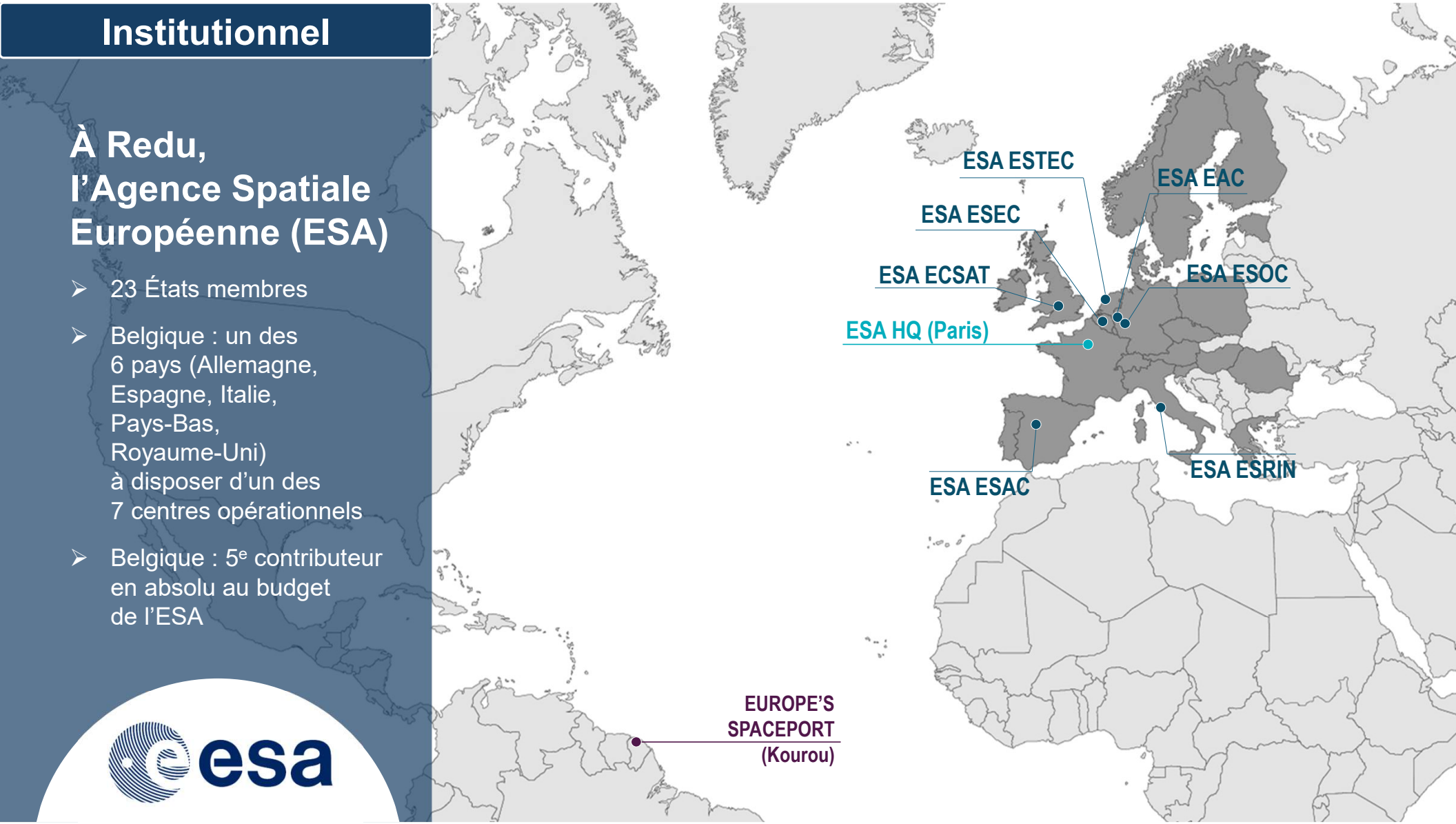
Entreprises de renom dans le spatial

- Telespazio Belgium
- Nexova/Starion

# Institutionnel

## À Redu, l'Agence Spatiale Européenne (ESA)

- 23 États membres
- Belgique : un des 6 pays (Allemagne, Espagne, Italie, Pays-Bas, Royaume-Uni) à disposer d'un des 7 centres opérationnels
- Belgique : 5e contributeur en absolu au budget de l'ESA



## Institutionnel

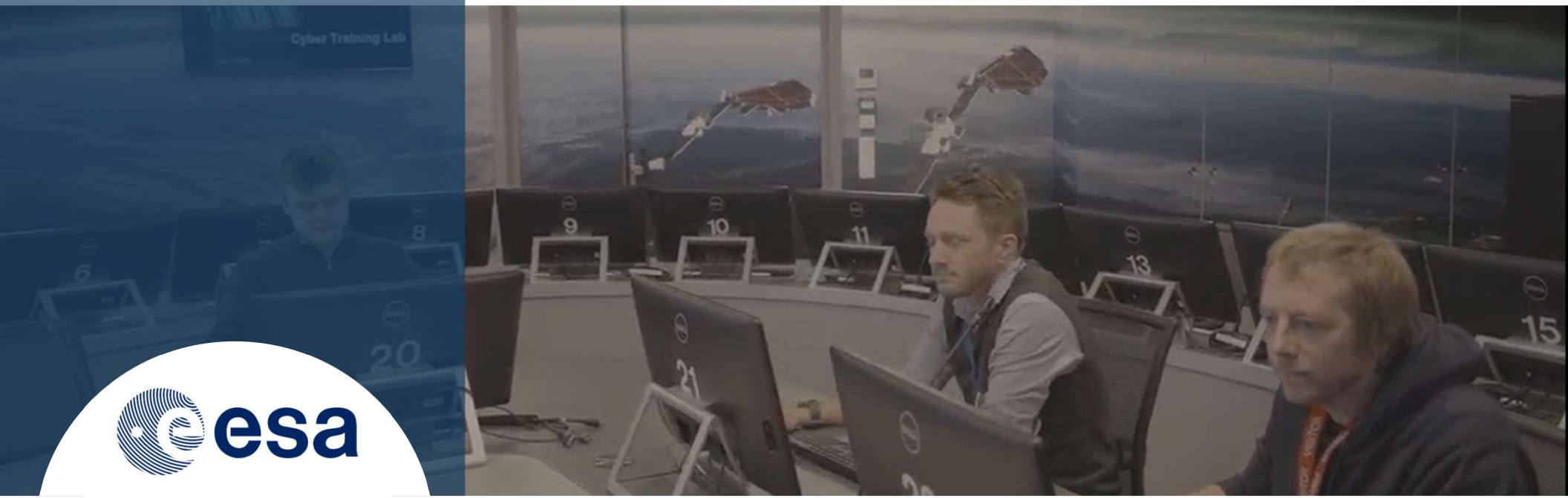
# À Redu, l'Agence Spatiale Européenne (ESA)

- **Implantation à Redu en 1968**
- **Missions historiques :**
  - Télécommunications
  - Observation de la Terre et du Soleil
  - Navigation par satellite

## Institutionnel

# À Redu, l'Agence Spatiale Européenne (ESA)

- **En 2019, « la station de Redu » devient l'ESEC (European Space Security and Education Centre)**
- **2 spécialisations : cybersécurité et éducation**
  - Un centre d'excellence en cybersécurité (SCCoE – Security Cyber Centre of Excellence)
  - Un centre des opérations de sécurité spatiale (CSOC - Space Security Operations Centre)

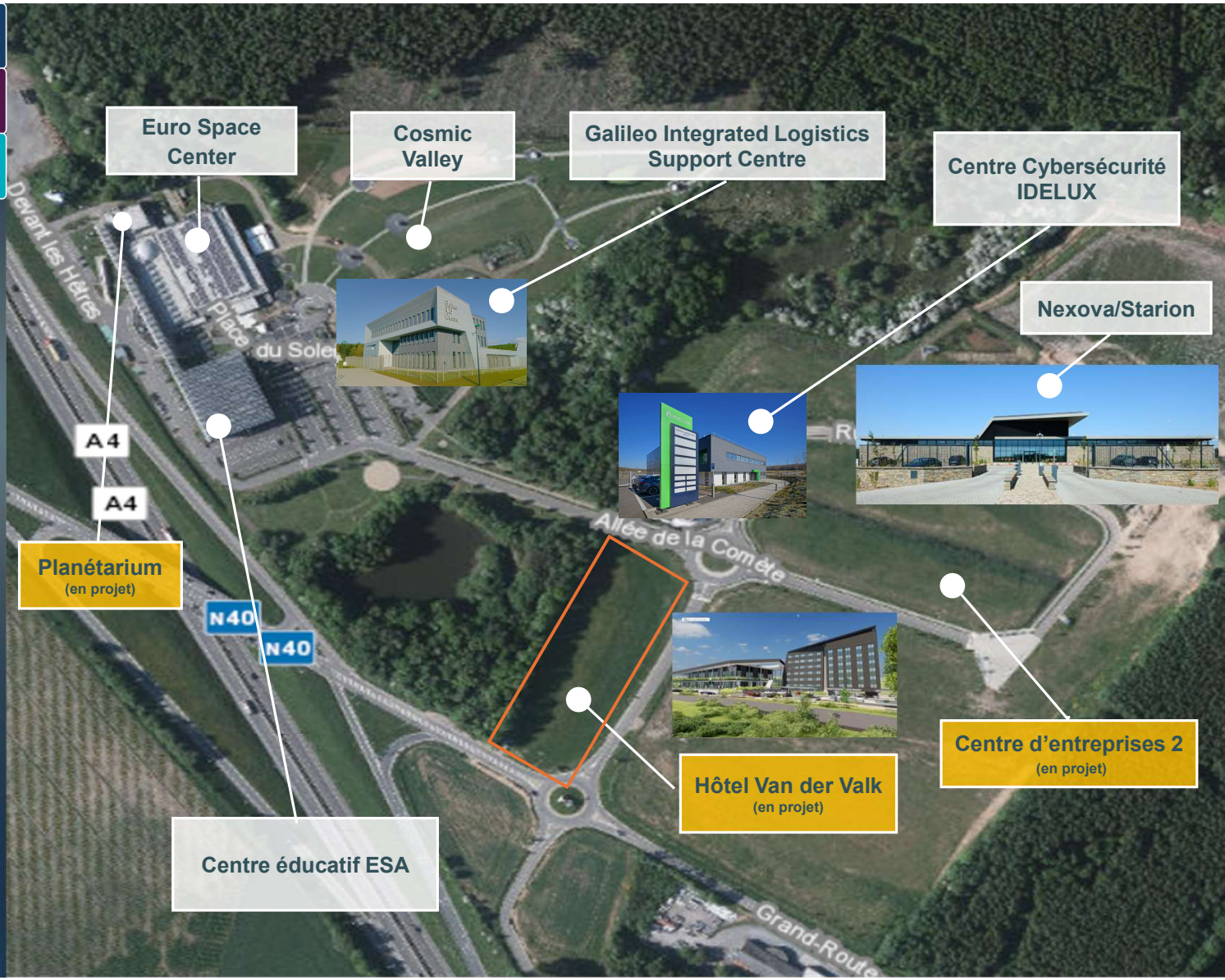


**Institutionnel**

**Éducatif**

**Entrepreneurial**

**À Transinne, Galaxia, parc d'activités économiques (20 ha) dédié au spatial et à la cybersécurité**




European Space Applications Park
GALAXIA

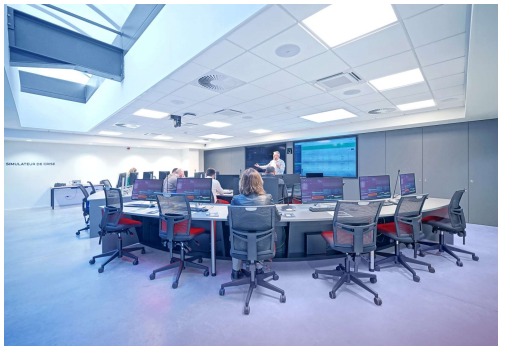
## Éducatif

# 3 outils de cybersécurité

- Investissements portés par le Plan de relance de la Wallonie
- Investissements déployés par IDELUX Développement

**École de cybersécurité**


**Laboratoire Gilles Brassard de cryptographie quantique**



**Cyber Range**

**Centre Cybersécurité IDELUX**

IDELUX DÉVELOPPEMENT

digital wallonia .be

Wallonie Relance

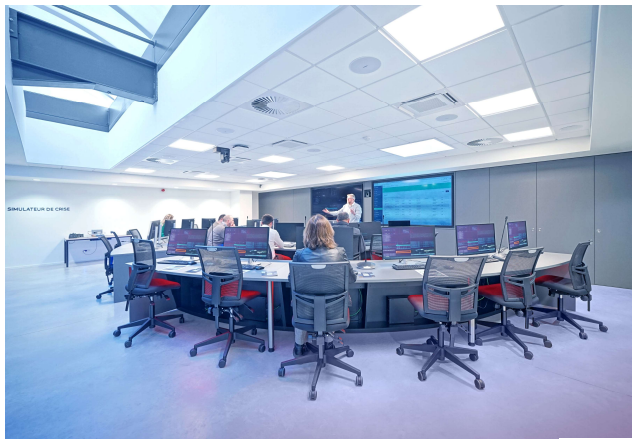
Avec le soutien de la Wallonie

## Éducatif

# Cyber Range

# Simulateur de crise

- En partenariat avec Nexova Group, installation d'une nouvelle infrastructure pour répondre aux besoins en formation en cybersécurité, notamment en lien avec l'IA
- Application des concepts théoriques de cybersécurité sous la forme de travaux pratiques dans un Cyber Range équipé de 20 postes
- Création du jumeau numérique de l'infrastructure IT et simulation d'une attaque cyber et de ses réponses
- À l'usage des experts et des professionnels IT, des chercheurs et des étudiants



IDELUX DÉVELOPPEMENT

digital wallonia .be

Wallonie Relance

Avec le soutien de la Wallonie

Nexova

**Éducatif**

# Cyber Range

## 3 formations en cybersécurité

| **Module 1**<br>Introduction à la cybersécurité | **Module 2**<br>Formation à la cybersécurité | **Module 3**<br>Formation des formateurs |
|---|---|---|
| Formation basique | Formation avancée | Formation des futurs formateurs et développeurs de scénarios sur cyber range |
| 2 heures | 6 heures | 2 jours |
| 1 exercice pratique sur cyber range | 2 exercices pratiques sur cyber range | Travaux pratiques sur cyber range |
| Introduction à la cybersécurité | Le cadre général de la cybersécurité | Introduction et approche de la formation |
| Panorama des menaces actuelles | Les principales contre-mesures et la réponse à incident | Architecture de haut niveau du CITEF |
| Le cadre législatif | Les bonnes pratiques | Administration, organisation et bibliothèque numérique |
| Profils des attaquants | | Introduction au développement de scénarios |
| Modèles d'attaque | | |
| Les contre-mesures essentielles | | |

IDELUX DÉVELOPPEMENT

Nexova

Éducatif

# Cyber Range

## 3 formations en cybersécurité

# L’Agence de développement économique durable de la province de Luxembourg

www.investinluxembourg.be

IDELUX
Pour vous

# Séminaire NIS2

Eaux de Wallonie

MERCI et

BON APPETIT!

12 décembre 2025

Alliance des opérateurs publics de l'eau