CYBERWEEK 2024

LA CYBERSÉCURITÉ POUR LES PETITES STRUCTURES DE LA SANTÉ

16 OCTOBRE 2024

MONS

Agence du Numérique

Cyberwal by digital wallonia

Wallonie Relance

Programme

13h00 : Introduction - Philippe Costard, Santhea & Fabian Céréssia, Unessa.
13h15 : Retour d'expérience : tentatives de cyber-attaques et bonne pratiques mises en place - Gregory Lenoir, MR-MRS "Les Chèvrefeuilles & Les Jardins du Bultia".
13h45 : Présentation du programme Cyberwal by Digital Wallonia et de la Cyber Response Team (CRT) - Nina Hasratyan et Jeremy Grandclaudon, Agence du Numérique.
14h15 : Outils, enseignements et recommandations à l'attention des PME de la santé - Carine Schadeck et Alexandre Hock, WALLONIE SANTE.
14h45 : Pause-café.
15h00 : Démo: utilisation d'un simulateur numérique pour mener une cyber-attaque sur une petite structure de la santé virtuelle - SIA Partners.
15h45 : Témoignage : comment réagir lorsque mon fournisseur de services est compromis ? - Francis Lejeune, CSD Liège.
16h15 : Workshop: comment comprendre et appliquer le Cyber Fundamentals (CyFun) Framework (niveau Basic) - Nina Hasratyan et Jeremy Grandclaudon, Agence du Numérique.
16h45 : Conclusion.
17h00 : Networking & drink.

Cyberwal
by digital
wallonia

santhea

UNESSA

Introduction

Cyberwal
by digital
wallonia

Les Chèvrefeuilles

Les Jardins du Bultia

Gregory Lenoir

MR-MRS "Les Chèvrefeuilles & Les Jardins du Bultia"

Cyberwal
by digital
wallonia

Retour d'expérience

Maisons de repos & Résidences-services

Gregory Lenoir – Direction Technique

Cyberweek 2024 : la cybersécurité pour les petites structures de la santé

Entreprises Familiales

Les Chèvrefeuilles

Havré

- Maison de repos (49 lits)
- Résidence Service (44 appart.)
- Habitats groupés (7 maisons)

Les Jardins du Bultia

Gerpinnes

- Maison de repos (182 lits)
- Résidence service (44 appart.)
- Centre de bien-être et de revalidation

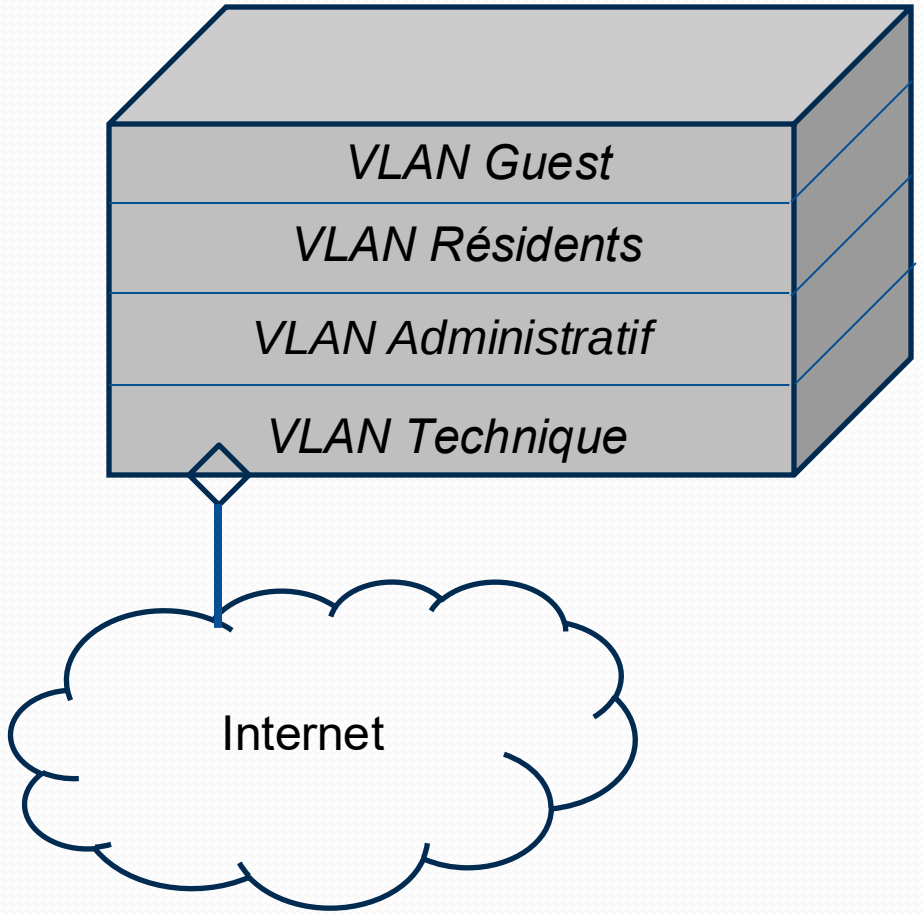
Expériences personnelles:

Directeur Informatique
part&namut

Concepteur
Octapi

200

Maison de repos



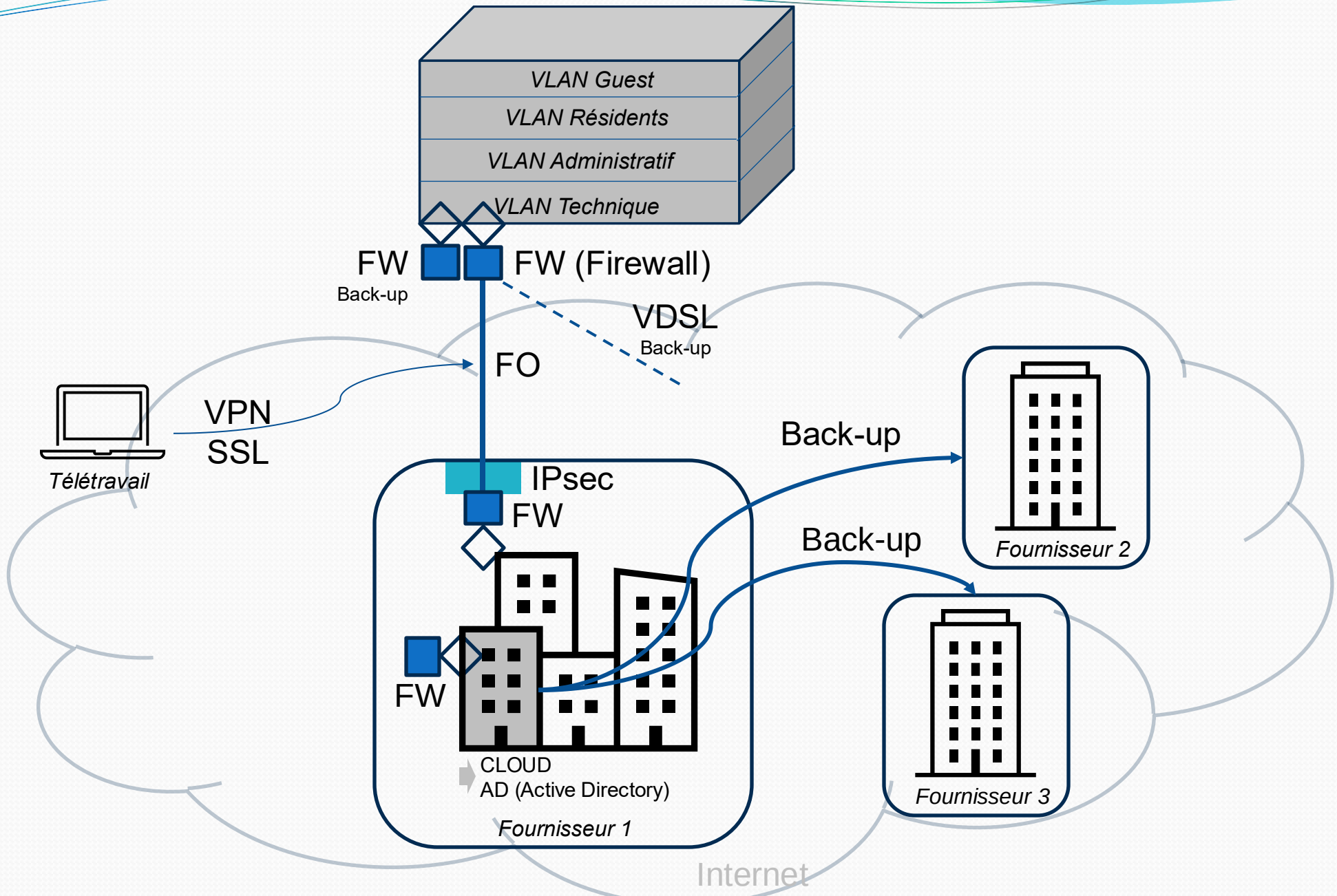
- Chaque media est scanné

Antivirus, IDS,
EDR, NDR…*

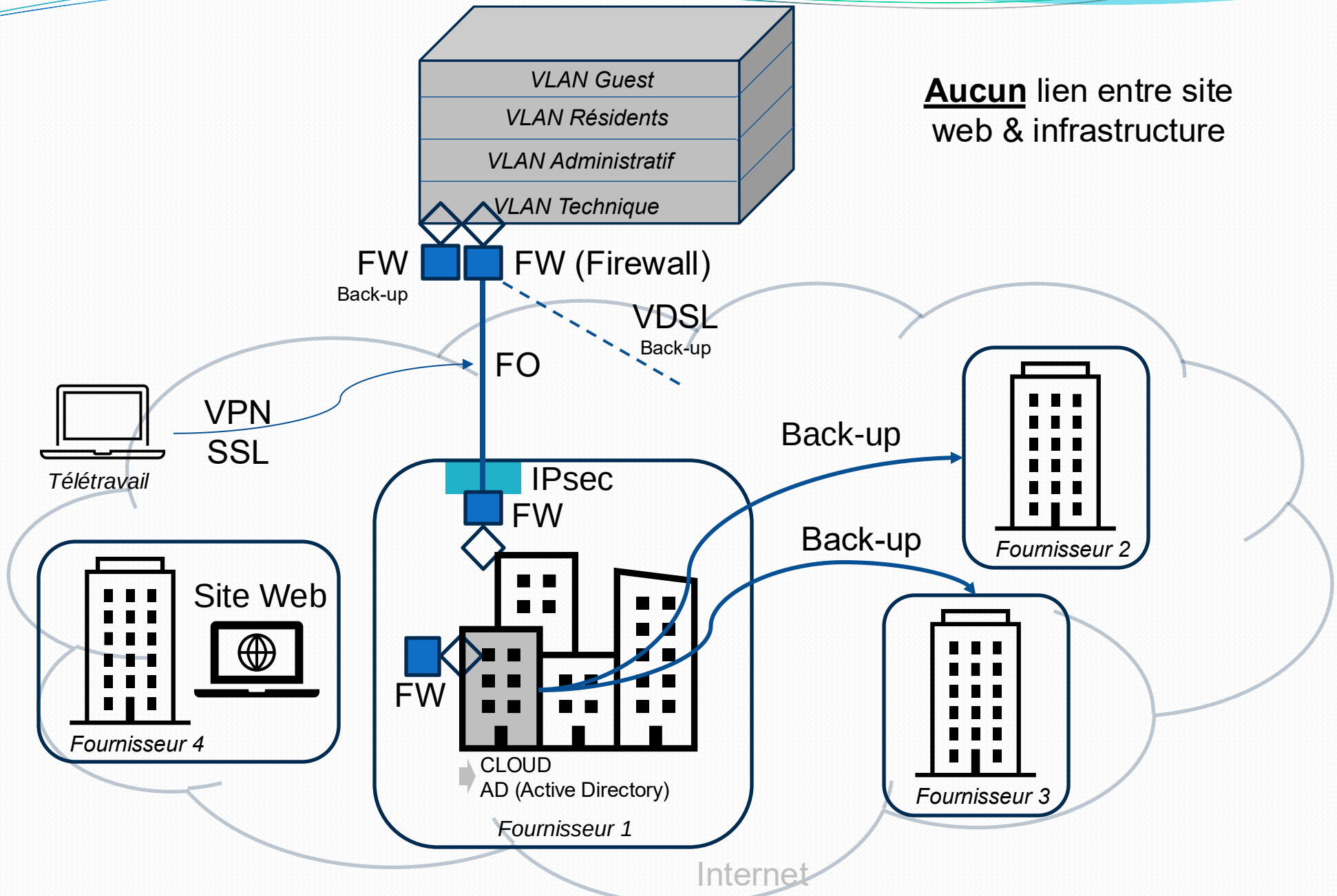
- Matériel à jour
- Formation des collaborateurs
- User <> ~~Admin~~
- MFA
(Authentification à plusieurs facteurs)

*Intrusion Detection System, Endpoint Detection and Response, Network Detection and Response

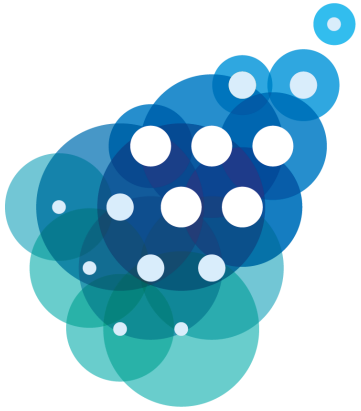
10


VLAN Guest
VLAN Résidents
VLAN Administratif
VLAN Technique
FW
Back-up
FW (Firewall)
VDSL
Back-up
FO
VPN
SSL
Télétravail
IPsec
FW
FW
Back-up
Back-up
Fournisseur 2
Fournisseur 3
CLOUD
AD (Active Directory)
Fournisseur 1
Internet

12



Aucun lien entre site web & infrastructure



Agence
du Numérique

Nina Hasratyan

Agence du Numérique

Jeremy Grandclaudon

Agence du Numérique

Cyberwal
by digital
wallonia

Cyberwal
by digital
wallonia

Cyberweek – 16/10/2024

La cybersécurité pour les petites structures de la santé

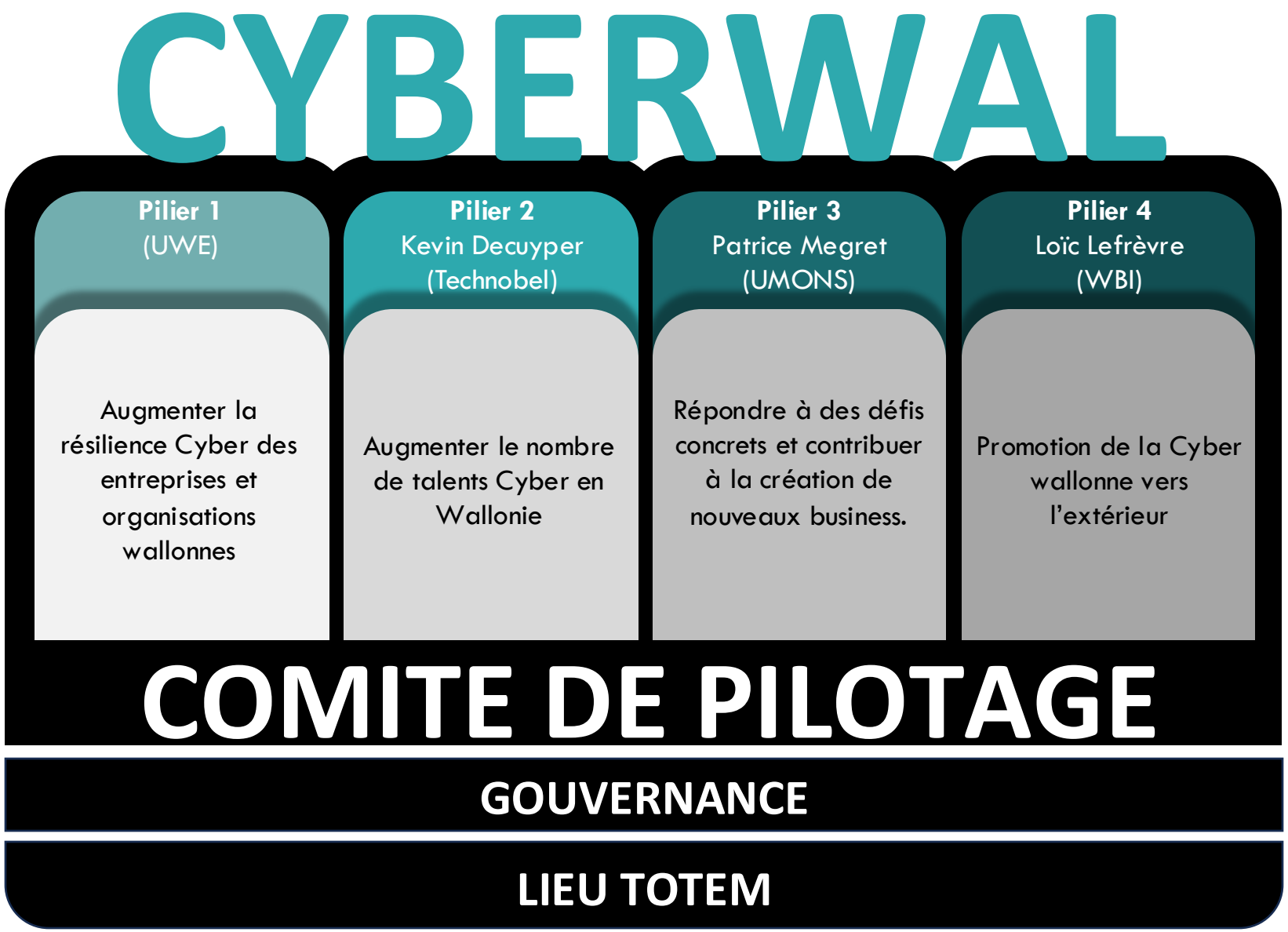
Jeremy Grandclaudon

Nina Hasratyan

Agence
du Numérique


QUATRE
PILIERS

VUE D'ENSEMBLE



RAYONNEMENT

RECHERCHE

COMPETENCES

USAGES

Cyberwal by Digital Wallonia : des actions dédiées aux petites structures de la santé

Cyberwal
by digital
wallonia

Boîte à outils de cybersécurité pour PME

Mobiliser & Accompagner

Objectifs :

- Contribuer à améliorer la cyber-protection des entreprises
- Fournir une vidéo d'introduction, des outils gratuits, et des ressources complémentaires
- Aider les entreprises en matière de cyber-hygiène essentielle

Cyberwal by digital wallonia

- **Partenariat avec le Global Cyber Alliance (GCA)**

1. Identifier vos appareils et applications
   L'Inventaire
2. Mettre à jour vos défenses
   Mettre à jour vos appareils et applications, Chiffrer vos données Sécuriser vos sites web
3. Éviter l'emploi de mots de passe simples
   Mots de passe forts, 2FA
4. Prévenir l'hameçonnage et les logiciels malveillants
   Antivirus, Sécurité DNS (Quad9)
5. Sauvegarder et récupérer
   Configurer et planifier des sauvegardes
6. Protéger vos emails et votre réputation
   DMARC et vérifications du site Web

SCAN ME

Campagne de sensibilisation spécifique

Mobiliser & Accompagner

Objectifs :

- Rappeler l'importance de veiller à la sécurité des données des patients, résidents, pensionnaires

Cyberwal by digital wallonia

Campagne de sensibilisation spécifique

Livre blanc :

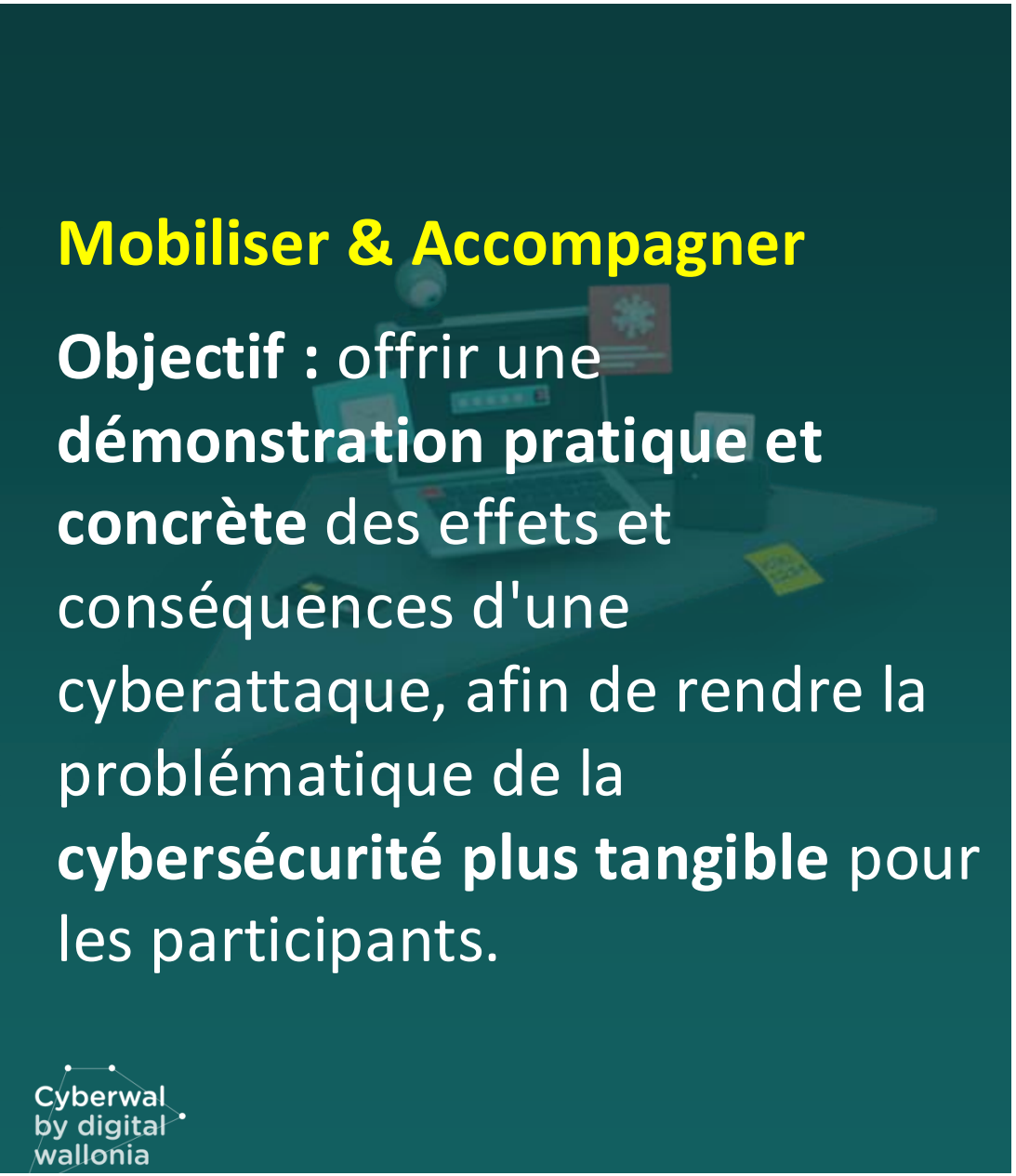
Les défis et les meilleures pratiques de la cybersécurité dans le secteur de la santé

Mobiliser & Accompagner

Cyberwal
by digital
wallonia

- Présenter de manière concrète les **défis et les bonnes pratiques de cybersécurité** dans le secteur de la santé
- Faire prendre consciences des **risques associés aux nouvelles technologies** dans le domaine de la santé
- Propose une **stratégie globale pour renforcer les défenses** en cybersécurité des établissements de santé

Simulateur numérique



Mobiliser & Accompagner

Objectif : offrir une **démonstration pratique et concrète** des effets et conséquences d'une cyberattaque, afin de rendre la problématique de la **cybersécurité plus tangible** pour les participants.

Cyberwal by digital wallonia

- Un **environnement virtuel** offrant différents **scénarios de cyberattaques**.
- Des scénarios avec une variété de processus, de cibles, de vulnérabilités et de conséquences.
- Disponible de manière itinérante **à partir de 2025**.
- Propose **3 niveaux de complexité** dans les scénarios d'attaque

- **Pour qui ?**
  - Preneurs de décision.
  - Tout type de public, technique ou non.
  - Utilisé lors d’événements et de conférences pour les publics cibles.

Cyber Response Team (CRT)

Mobiliser & Accompagner

Objectif : offrir un **support aux demandes d'assistance** des acteurs du secteur de la santé :

- En **accompagnant** dans les premières démarches pendant et/ou après un incident de sécurité
- En **mettant en relation** avec des partenaires pertinents

Cyberwal by digital wallonia

- Constituée après consultation et **accord du CCB et du CERT.be**
- Déploiement **à partir de 2025**
- **Responsabilités :**
  - **Intervenir sur place** en cas de cyberattaque pour **endiguer la menace**.
  - **Aider les acteurs en amont à préparer et gérer** les incidents cyber.
  - Faire le **lien avec les initiatives nationales et internationales** (bonnes pratiques, veille informationnelle, retours d'expérience, …).

DIGITAL WALLONIA
www.digitalwallonia.be
info@digitalwallonia.be
@digitalwallonia

WE LOVE DIGITAL

AGENCE DU NUMERIQUE
Av. Prince de Liège, 133
5100 Jambes
+32 (0)81 778080
www.adn.be

WE KNOW DIGITAL

STÉPHANE VINCE
Directeur,
Pôle Technologie et
Administration Numérique
Stephane.vince@adn.be

WE MAKE DIGITAL

JEREMY GRANDCLAUDON
Jeremy.grandclaudon@adn.be

NINA HASRATYAN
Nina.Hasratyan@adn.be

AdN

WALLONIE SANTÉ

Carine Schadeck

Wallonie Santé

Alexandre Hock

Wallonie Santé

Cyberwal
by digital
wallonia

WALLONIE SANTÉ

Le FONDS D'INVESTISSEMENT dédié aux acteurs de la santé et de l'action sociale

Partie I : WALLONIE SANTÉ et la cybersécurité
Partie II : Enseignements et recommandations à l'attention des PME de la santé

Partie I : WALLONIE SANTÉ et la cybersécurité

Partie II : Enseignements et recommandations à l'attention des PME de la santé

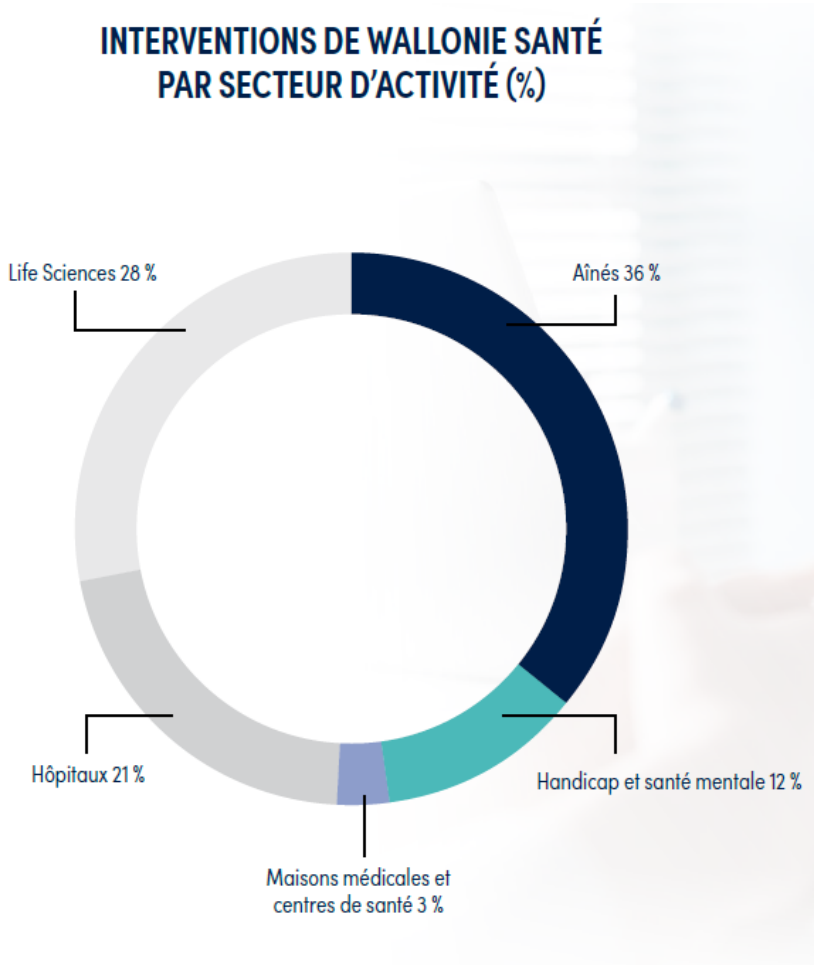
1. WALLONIE SANTÉ – En quelques mots

WALLONIE SANTÉ, créée fin 2018 à l'initiative du Gouvernement wallon, a comme objectif de DÉVELOPPER le Pôle «INVESTISSEMENTS SANTÉ» afin de RELEVER les DÉFIS d'AUJOURD'HUI et de DEMAIN du secteur en matière d'investissements.

WALLONIE SANTÉ est l'unique **FONDS D'INVESTISSEMENT en Belgique** dédié au financement des **acteurs** de **l'Action Sociale et de la Santé.**

WALLONIE SANTÉ fait partie des OUTILS ÉCONOMIQUES WALLONS dont les actionnaires sont la Région Wallonne et Wallonie Entreprendre.

1. WALLONIE SANTÉ – En quelques chiffres (2023)



2. Nos modes d'intervention - Deux effets de levier

FINANCEMENT DES INVESTISSEMENTS

Infrastructure, équipement, informatique, fonds de roulement, ...
dont soutien aux travaux économiseurs d'énergie

TROIS NATURES D'INTERVENTION

- **PRÊTS CLASSIQUES /SPECIFIQUES**
- PARTICIPATIONS EN CAPITAL
- GARANTIES CONVENTION CADRE

SERVICES D'ACCOMPAGNEMENT

► Soutien dans l'élaboration de votre plan financier
► Activation d'un réseau d'opérateurs/experts afin de vous accompagner dans les différents stades de votre entreprise à profit social
► Mise à disposition d'outils de sensibilisation (table ronde cybersécurité p.ex)
► ...

- SMART MONEY
- CRÉATION D'UN ÉCOSYSTÈME INTÉGRÉ (dont partenariat Cyberwal)
- SENSIBILISATION

2. Nos modes d'intervention - Prêts Spécifiques

PRÊTS

SPÉCIFIQUES

LE BESOIN EN TRÉSORERIE

pour les structures ou activités en DÉMARRAGE

TRAVAUX ÉCONOMISEURS D'ÉNERGIE

- LED, POMPE A CHALEUR,…
- PANNEAUX PHOTOVOLTAIQUES
- COGÉNÉRATION
- ….

MESURES D'ADAPTATION AUX ALEAS CLIMATIQUES

CYBER SECURITE

3. Cybersécurité – Démarche de Wallonie SANTÉ

Le paysage de la santé connaît une transformation profonde, caractérisée par un **usage croissant des technologies numériques** et par la **génération d'énormes quantités de données sensibles**. Bien que ces avancées offrent d'incroyables opportunités, elles suscitent également des défis sans précédent en matière de cybersécurité.

Ces dernières années, la Wallonie a en effet connu des cyberattaques visant les établissements de santé, nous rappelant avec force les menaces croissantes auxquelles nous sommes confrontées. **Ces incidents compromettent la vie privée des patients, perturbent les services de santé et même entravent l'innovation médicale.**

3. Cybersécurité – Démarche de Wallonie SANTÉ

C’est dans ce contexte que WALLONIE SANTE a souhaité être précurseur en la matière en adoptant une démarche proactive en vue de renforcer la cybersécurité des établissements de soins et des sociétés actives dans la santé, démarche qui a pour objectif de s’articuler autour de **2 axes:**

- **Le prêt** – via le produit **Cyber Health** proposé par Wallonie Santé (juin 2023)
- **Ecosystème et/ou Sensibilisation** – via
  - *la recherche de partenariats (Cyberwal p.ex), et de collaborations avec des sociétés spécialisées dans la matière et le secteur*
  - *la participation à diverses initiatives (webinaire, vidéo) et l’organisation d’événements (table ronde traitant de sujets spécifiques dédiés aux PME tels que la gestion des fournisseurs et des sous-traitants informatiques)*
  - *la mise à disposition gratuitement d’un outil de scan évaluant la cybermaturité pour les structures du « portefeuille » de Wallonie Santé (depuis septembre 2023)*

3. Cybersécurité – Démarche de Wallonie SANTÉ – Axe prêt CYBERHEALTH

PRÊT CYBERHEALTH

QUELS OBJECTIFS ?

La cybersécurité représente un défi majeur pour toutes les entreprises et plus particulièrement pour le secteur de la Santé et de l'Action Sociale, qui constitue une cible privilégiée en raison notamment du caractère extrêmement sensible des données traitées et du caractère impératif de la continuité des soins.

Vu les risques associés, investir dans la cybersécurité est devenu un enjeu de gouvernance.

WALLONIE SANTÉ fait donc de la cybersécurité une de ses priorités et développe un produit spécifique pour financer les investissements nécessaires.

COMMENT ?

En Encourageant et facilitant **les investissements en matériel et/ou logiciel informatique liés à la cybersécurité** dans le secteur, via un financement à taux réduit.

POUR QUI ?

> À destination des établissements de soins de santé agréés, publics, associatifs ou privés et des entreprises éligibles du secteur de la Santé et de l'Action sociale ;
  - Hôpitaux (généraux et psychiatriques)
  - Établissements pour personnes âgées : MR, MRS, CSJ, Résidences-Services
  - Structures pour personnes handicapées
  - Services et centres en santé mentale
  - Association de Santé Intégrée (ASI) / Maisons médicales ou centres pluridisciplinaires
  - Autres infrastructures liées à la santé
> Ayant leur siège d'exploitation en Wallonie et/ou dont le lieu d'investissement est situé en région wallonne ;

CONDITIONS D'OBTENTION ?

> Validation du plan de financement par les organes de gestion de WALLONIE SANTÉ
> La structure n'est pas considérée « en difficulté »

COMMENT EN BÉNÉFICIER ?

En introduisant votre demande auprès de WALLONIE SANTÉ via notre site Internet (www.walloniesante.be) et en fournissant toutes les informations nécessaires à l'analyse de votre dossier par nos Conseillers.*

CARACTÉRISTIQUES

Montant du prêt
> Jusqu'à maximum 2.000.000€

Durée
> Maximum 5 ans (3 ans pour le software/5 ans pour le hardware)

Taux de référence
> Au maximum le Taux OLO de la période considérée

Remboursements
> Trimestrialités civiles

Garantie
> Sans garantie

Cofinancement
> Pas exigé

Frais de gestion
> Néant

Combinaisons/compatibilités
> Peut se combiner avec des solutions proposées par les partenaires bancaires de l'emprunteur

EXEMPLE

Dans le but de se prémunir contre des attaques potentielles, un hôpital investit 1.000.000€ dans du matériel informatique visant la cybersécurité.

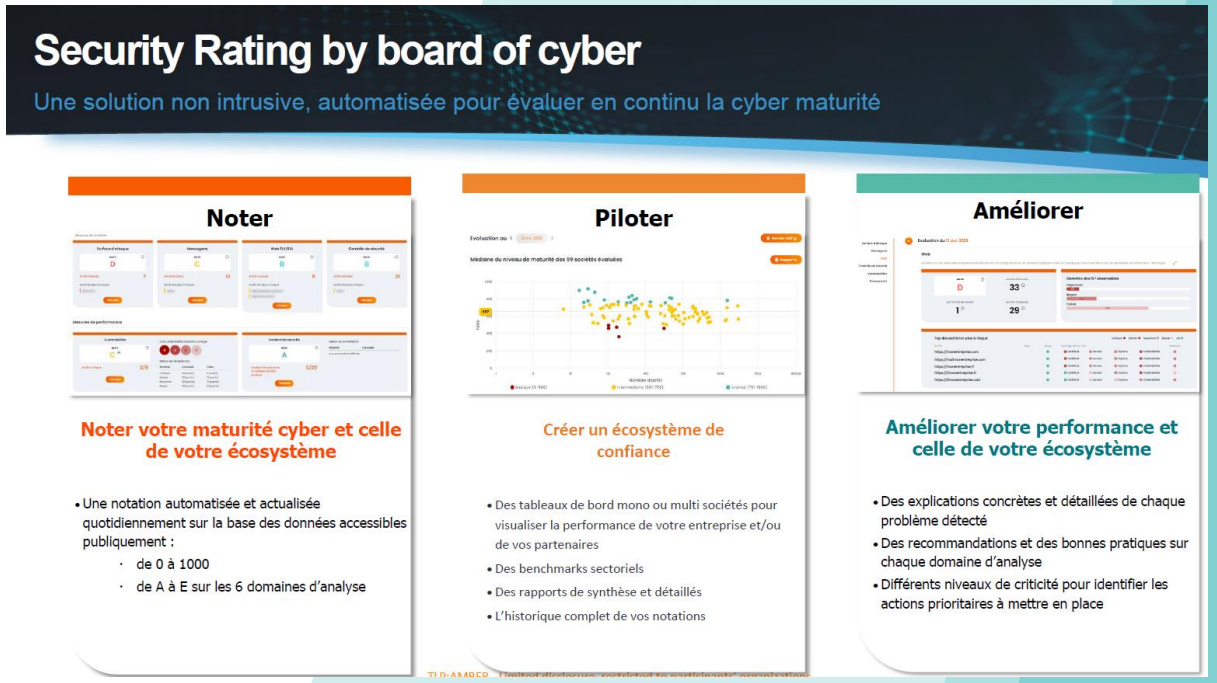
Sur base de l'étude du dossier, WALLONIE SANTÉ prête à l'emprunteur 1.000.000 € sur une durée de 5 ans au taux OLO correspondant (à savoir le 23/06 : 2,85%) et ce sans garantie, ce qui représente un remboursement sur base MENSUELLE de 17.902,11€ pendant 5 ans.

3. Cybersécurité – Démarche de Wallonie SANTÉ – Axe Ecosystème et Sensibilisation

UNESSA

santhea

Cyberwal by digital wallonia



Outil de notation de sécurité en ligne proposé par la société APPROACH pour les structures composant le portefeuille de Wallonie Santé.

Feedback : complémentaire au rapport d'audit, aide au monitoring

=> Expérience Pilote

Partie I : WALLONIE SANTÉ et la cybersécurité

Partie II : Enseignements et recommandations à l'attention des PME de la santé

4. Approach Cyber

Approach Cyber à un coup d'œil

Qui sommes-nous ?

Notre Entreprise

Entreprise privée
Fondée en 2001

Notre positionnement de Pure Player

Votre partenaire de confiance à 360° pour la cybersécurité et la protection de la vie privée

Notre Trajectoire Ascendante

Chiffre d'affaires de 11M+ EUR
100 employés en Belgique et en Suisse

Notre Impact sur la société

Plus de 1000 clients satisfaits dans le monde entier
Contributeur ESG par conception

Nos Certifications

Certifié ISO27001
ISO27701 vérifié

Nos Établissements

Anvers, Louvain-la-Neuve
Lausanne

4. Approach Cyber

Approach Cyber Portefeuille de solutions à 360°

Anticipation

- Évaluations et Audits
- Évaluations Techniques
- Piratage Éthique

Prévention

- Stratégie de Sécurité
- Conseil de Sécurité
- Bureau DPO
- Conformité & Certifications
- Sensibilisation à la Sécurité & Phishing

Protection

- Sécurité des Applications
- Développement Externalisé Sécurisé
- Sécurité des Données
- Solution de Sécurité Cloud
- Gestion des Identités et des Accès

Detection & Réaction

- Managed SOC
- Services de Sécurité Managés
- Intervention aux Urgences /CSIRT

Rétablissement

- Plan de gestion des Incidents
- Planification de la Continuité des Activités

5. Quizz Cyber

Question #1

Quel est l'élement déclencheur le plus fréquent d'une cyberattaque?

1) Une faille dans le serveur

2) Un antivirus non-performant

3) Un employé piégé

5. Quizz Cyber

Question #1

Quel est l'élement déclencheur le plus fréquent d'une cyberattaque?

1) Une faille dans le serveur

2) Un antivirus non-performant

3) Un employé piégé

5. Quizz Cyber

Question #2

Quel pourcentage d’attaques commence par une erreur humaine?

1) 25%

2) 50%

3) 80%

5. Quizz Cyber

Question #2

Quel pourcentage d’attaques commence par une erreur humaine?

1) 25%

2) 50%

3) 80%

5. Quizz Cyber

Question #3

Quelles structures sont ciblées par des cyber-attaques?

1) Uniquement les entreprises cotées en bourse avec un gros chiffre d'affaires

2) Uniquement les organismes publics

3) Uniquement les entreprises de taille intermédiaire

4) Toutes ces structures sont des cibles potentielles

5. Quizz Cyber

Question #3

Quelles structures sont ciblées par des cyber-attaques?

1) Uniquement les entreprises cotées en bourse avec un gros chiffre d'affaires

2) Uniquement les organismes publics

3) Uniquement les entreprises de taille intermédiaire

4) Toutes ces structures sont des cibles potentielles

6. Enseignements et recommandations

- Sensibilisation des collaborateurs
- Gestion des mots de passe
- Gestion des accès
- Installation d'antivirus
- Gestion des vulnérabilités
- Gestion des backups
- Gestion de crise
- Evaluation de votre posture de sécurité

6.1. Sensibilisation des collaborateurs

Risque élevé d'attaques par **hameçonnage**, **fraude téléphonique**, **hameçonnage ciblé** et **ingénierie sociale**

- Confidentialité des données et l'importance de chaque employé
- Vigilance face aux emails externes
- Prudence lors de paiements
- Séparation usage personnel & professionnel des appareils

La sécurité est la responsabilité de tous: **Chacun a son rôle à jouer**

6.2. Gestion des mots de passe

Risques

- ⚠ Oubli
- ⚠ Partage
- ⚠ Redondance
  - Vol de mot de passe = accès à tous vos comptes
- ⚠ Stockage dans un endroit non sécurisé
- ⚠ Mots de passe facilement devinables ou vulnérables au piratage

Recommandations

- ✓ Créer des mots de passe uniques pour chaque compte
- ✓ Instaurer une politique de mots de passe forts
  - Minimum 8 caractères
  - Recommandation de 15 caractères
  - Possibilité d'utiliser des passphrases avec jusqu'à 64 caractères
- ✓ Stockage sécurisé
- ✓ Mots de passe personnels et confidentiels
- ✓ Utiliser un coffre-fort de mot de passe

6.3. Gestion des accès

Risques

- ⚠ Abus d'accès ou de privilèges (intentionnel ou accidentel)
- ⚠ Dégâts et destructions physiques des équipements critiques
- ⚠ Propagation rapide une fois qu'un attaquant a pénétré le réseau
- ⚠ Sans authentification multifactorielle (MFA), un attaquant n’a besoin que d’un mot de passe pour compromettre un compte

Recommandations

- ✓ Besoin de savoir & moindre privilège
- ✓ Limitation des droits administrateurs
- ✓ Restrictions des accès physique
- ✓ Authentification multifacteur (MFA)

6.4. Installation d'antivirus

Risques

- ⚠ Installation de logiciels malveillants
  - Rançongiciels
  - Logiciels espions
  - Hameçonnage
  - Etc.
- ⚠ Violation de données
- ⚠ Accès non autorisés

Recommandations

- ✓ Installer un antivirus qui répond à vos besoin
- ✓ Favoriser les antivirus "EDR" nouvelle generation (Endpoint Detection and Response)
- ✓ Imposer la mise à jour automatique et régulière de l'antivirus
- ✓ Imposer le scan automatique et régulier des appareils

6.5. Gestion des vulnérabilités

Risques

- ⚠ Exploitation des failles de sécurité
- ⚠ Perte de données
- ⚠ Interruption des services

Recommandations

- ✓ Inventorier le matériel et les logiciels
- ✓ Appliquer les mises à jour disponibles dès que possible
- ✓ Suivre l'actualité
- ✓ Utilisation d'outil de scan automatisés

6.6. Gestion des backups

Risques

- ⚠ Pertes de données (pannes matérielles, cyber-attaques, etc.)
- ⚠ Interruption du service
- ⚠ Corruption des sauvegardes

Recommandations

- ✓ Effectuer des sauvegardes régulières automatisées
- ✓ Appliquer la règle « 3-2-1 »
  - 3 copies des données (original + 2 copies)
  - 2 types de supports différents
  - 1 copie hors site
- ✓ Chiffrer les sauvegardes
- ✓ Réaliser des tests de restauration

6.7. Gestion de crise

Risques

- ⚠ Manque de coordination
- ⚠ Communication inefficace
- ⚠ Aggravation des impacts de l’incident
- ⚠ Interruption prolongée du service

Recommandations

- ✓ Définir un plan de gestion de crise
- ✓ Attribuer des responsabilités spécifiques
- ✓ Définir des canaux de communication d’urgence
- ✓ Tester votre plan régulièrement

6.8. Évaluation de votre posture de sécurité

Risques

- ⚠ Faiblesses non détectées
- ⚠ Surconfiance dans votre niveau de sécurité
- ⚠ Exposition à de nouvelles menaces

Recommandations

- ✓ Surveillance continue des contrôles de sécurité
- ✓ Effectuer des audits réguliers
- ✓ Exécuter des tests de pénétration réguliers

Nous contacter

Jean-Charles Hubert
Manager
Security Strategy & Advisory
APPROACH

jeancharles.hubert@approach-cyber.com

Carine Schadeck
Coordinatrice &
Investment Manager
WALLONIE SANTE

carine.schadeck@wallonie-entreprendre.be

Alexandre Hock
Investment Manager

WALLONIE SANTE

alexandre.hock@wallonie-entreprendre.be

Merci pour votre attention

Les conférences reprendront dans 15 minutes.

Cyberwal
by digital
wallonia

SIAPARTNERS

Démo : Utilisation d'un simulateur numérique pour mener une cyber-attaque sur une petite structure de la santé virtuelle

Sia Partners

Cyberwal
by digital
wallonia

Cyber Crisis Awareness Platform

Digital simulator

Cyberwal by digital wallonia

Wallonie Relance

SIAPARTNERS

Speakers

Nina Hasratyan
Agence du Numérique

nina.hasratyan@adn.be

Jeremy Grandclaudon
Agence du Numérique

jeremy.grandclaudon@adn.be

News

Cyberattaques en Belgique : les sites de services bancaires visés ce jeudi

Une nouvelle salve de cyberattaques a visé des sites internet belges ce jeudi 10 octobre 2024. Cette fois-ci, ce sont ceux de Febelfin (la fédération du service bancaire) et du SPF Economie qui ont été ciblés, confirme le Centre pour la cybersécurité Belgique (CCB).

BELGIQUE

Cyberattaques de sites d'autorités belges : "L'objectif est de décrédibiliser les autorités à quelques jours des élections"

RTL info ACTU SP

Le secteur de la santé belge de plus en plus ciblé par des cyberattaques: "Cela permet de pouvoir négocier une rançon"

Publié le 04/08 à 11h05 Par RTL info avec Cath

LE SOIR

24 Opinions Podcasts Politique Société Monde Économie Vidéos Sports

ACCUEIL • SOCIÉTÉ

Nouvelle cyberattaque en Belgique : plusieurs sites communaux et portuaires visés

Le groupe de hackers qui a attaqué des sites gouvernementaux lundi a visé des ports et des communes ce mardi.

Cyberattaque à l'hôpital d'Armentières : une réouverture des urgences espérée lundi dans la journée

remière fois que
attaque.

Technologie

Belgique : 200 sites gouvernementaux victimes d'une vaste cyberattaque

L'attaque a eu lieu au moment où une commission parlementaire belge, chargée de déterminer s'il convient d'accuser la Chine de génocide à propos du traitement des ouïghours, se réunissait.

DUVEL, LA CHOUFFE: STOPPÉE APRÈS UNE CYBERATTAQUE, LA PRODUCTION DES BIÈRES BELGES REPREND

Data breach CYBERSÉCURITÉ \ DONNÉES PERSONNELLES \ BELGIQUE

Un fournisseur de la ville de Bruxelles visé par une cyberattaque, des données personnelles dérobées

Cyberwal by digital wallonia Wallonie Relance SIAPARTNERS

Presentation of the cyber crisis awareness platform

In a context where cyber threats are omnipresent, awareness of risks and best practices is becoming imperative for organizations. In an environment where cyber threats are omnipresent, organizations must prioritize understanding risks and adopting best practices. To enhance awareness among Walloon institutions and businesses regarding cyber risks and effective IT hygiene, L'Agence du Numérique sought to develop a cyber crisis awareness platform. This innovative tool allows for the simulation of various cyber-related crisis scenarios, by staging incidents, their impacts, and the solutions to address them, thus offering an immersive experience that prepares organizations to face these threats.

48 **Engaging, multidimensional crisis scenarios crafted to enhance cybersecurity awareness in a crisis context.**

4 **strategic sectors of activity representative of the Walloon economic and social fabric: Health , Industry 4.0 , Public Sector , SMEs .**

3 **levels of complexity that involve more or less sophisticated attacks.**

An immersive platform promoting dynamic interactions

Dynamic interactions
Participants can engage in real-time through their smartphones, promoting active participation and interaction..

Knowledge development
Open to all participants, regardless of their cybersecurity knowledge level, this enriching experience allows everyone to enhance their skills.

Diversity of questions
Questions are tailored to various participant profiles based on their expertise, including legal teams, human resources, information security, communications, and specific professions.

“Coach” facilitator
The facilitator guides discussions, shares feedback and provides context and a broader perspective on the events unfolding in the scenario.

Chronological consistency
The scenarios progress chronologically, presenting realistic situations, diverse stimuli, and a mini-informant that offers insights into key concepts.

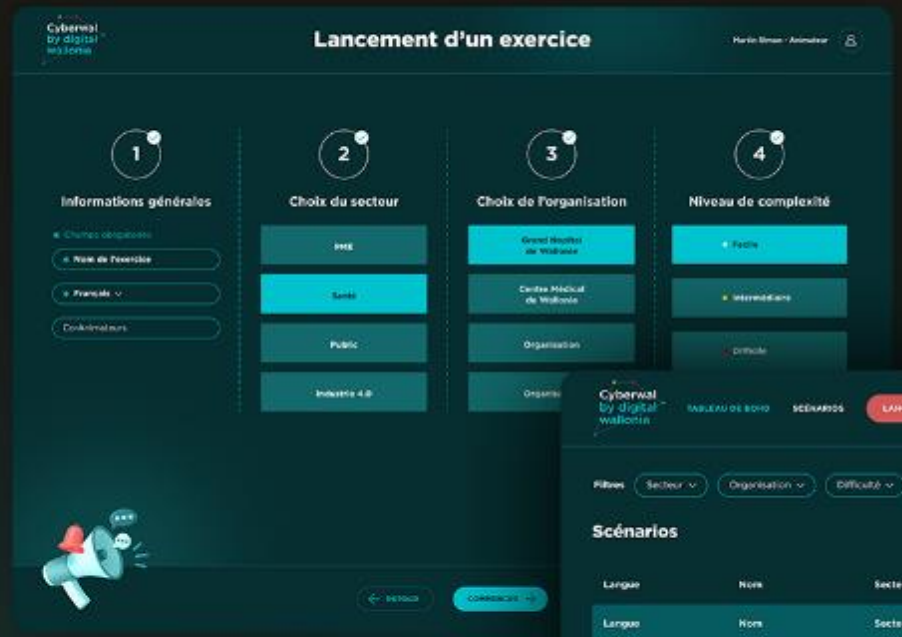
Realistic Cyber Attacks
The scenarios feature a range of proven cyber attacks grounded in real-world experiences.

Collaborative scenarios

With a **scripted approach**, the platform is tailored to different audiences, providing a clear and contextualized understanding of **cybersecurity** issues relevant to each specific sector.

During the simulation, participants **engage actively** through a variety of stimuli that encourage deeper thinking by answering both multiple-choice and open-ended questions. **Facilitated discussions** will emphasize best practices and incorporate feedback, providing participants with a practical perspective that is directly relevant to their professional environments.

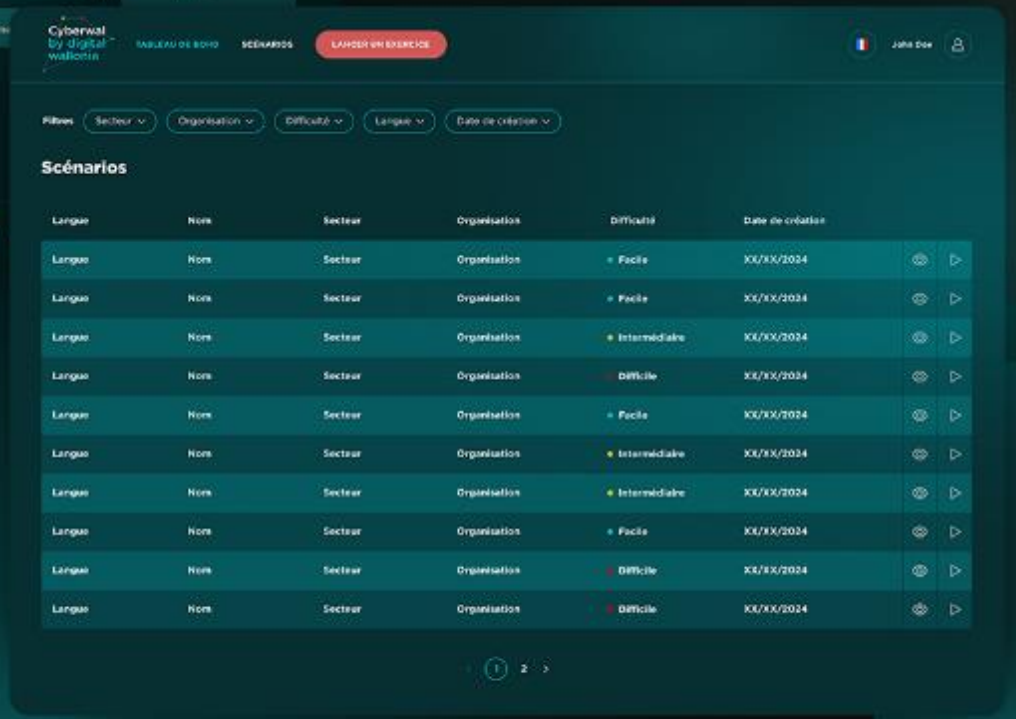

Cyberwal
by digital
wallonia
ANIMATEUR
PARTICIPANT
Identifiant
Mot de passe
Mot de passe oublié ?
Connexion
Se connecter avec
LA SENSIBILISATION SUR LA
cybersécurité pour
la Wallonie
Powered by SIAPARTNERS


Cyberwal by digital wallonia
Lancement d'un exercice
1
Informations générales
2
Choix du secteur
3
Choix de l'organisation
4
Niveau de complexité


Nom de l'exercice
SECTEUR PUBLIC.
Cible privilégiée des attaquants :
Les PME, vecteur d'attaque de grands organismes

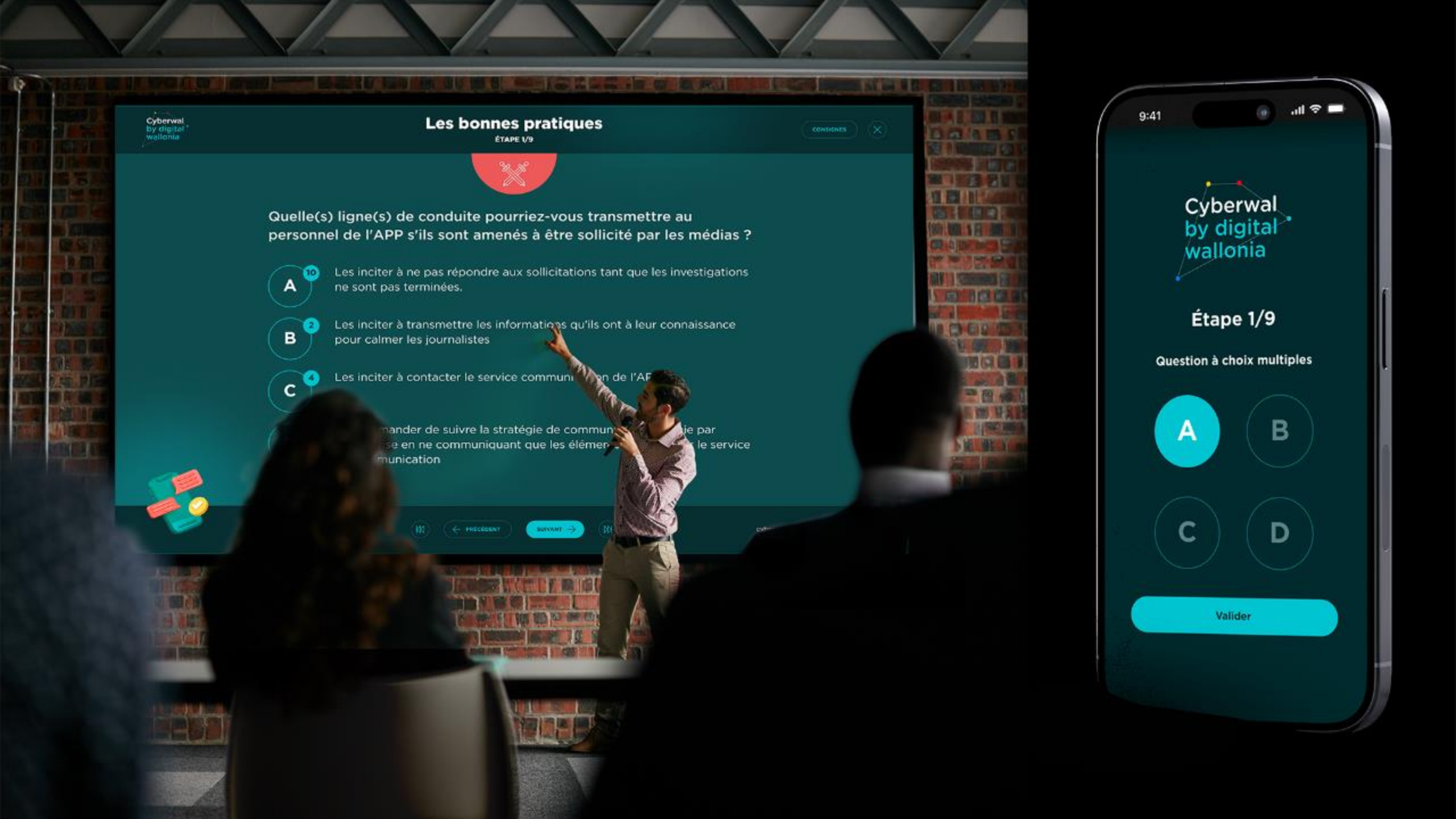

Cyberwal by digital wallonia
LA SENSIBILISATION SUR LA
cybersécurité pour la Wallonie
ANIMATEUR
PARTICIPANT
Code de la session
Accéder
Powered by SIAPARTNERS


Cyberwal by digital wallonia
Étape 1/9
Question ouverte
Vous pouvez soumettre 3 réponses !
Exemple 1
Réponse
Réponse
Valider


Cyberwal by digital wallonia
TABLEAU DE BORD
SCÉNARIOS
LANCER UN EXERCICE
John Doe
Filtres
Secteur
Organisation
Difficulté
Langue
Date de création
Scénarios
Langue
Nom
Secteur
Organisation
Difficulté
Date de création
Facile
Intermédiaire
Difficile
XX/XX/2024


Êtes-vous sûr de vouloir quitter ?
Attention, vous ne pourrez pas reprendre la session en cours.


Nom de l'exercice
ÉTAPE 1/9
Un des magasiniers a contacté les médias afin de les alerter des conditions de travail déplorables. Plusieurs journalistes se sont donc déplacés sur les lieux et tentent de s'introduire dans les locaux pour obtenir des informations et des séquences vidéo.


Cyberwal by digital wallonia
Les bonnes pratiques
ÉTAPE 1/9
CONSIGNES
Quelle(s) ligne(s) de conduite pourriez-vous transmettre au personnel de l'APP s'ils sont amenés à être sollicité par les médias ?
A
Les inciter à ne pas répondre aux sollicitations tant que les investigations ne sont pas terminées.
B
Les inciter à transmettre les informations qu'ils ont à leur connaissance pour calmer les journalistes
C
Les inciter à contacter le service communi on de l'AP
mander de suivre la stratégie de commun ie par
e en ne communiquant que les élémen le service
munication
PRÉCÉDENT
SUIVANT
9:41
Cyberwal by digital wallonia
Étape 1/9
Question à choix multiples
A
B
C
D
Valider

Cyberwal by digital wallonia

TABLEAU DE BORD SCÉNARIOS LANCER UN EXERCICE

Martin Simon - Animateur

Filtres Date Secteur (Santé) Difficulté Statut Langue EXPORTER

Vos scénarios par secteur

Évolution du score moyen/niveau

2024

Total de participants

379

15 animateurs

Total d'exercices

13

3 4 6

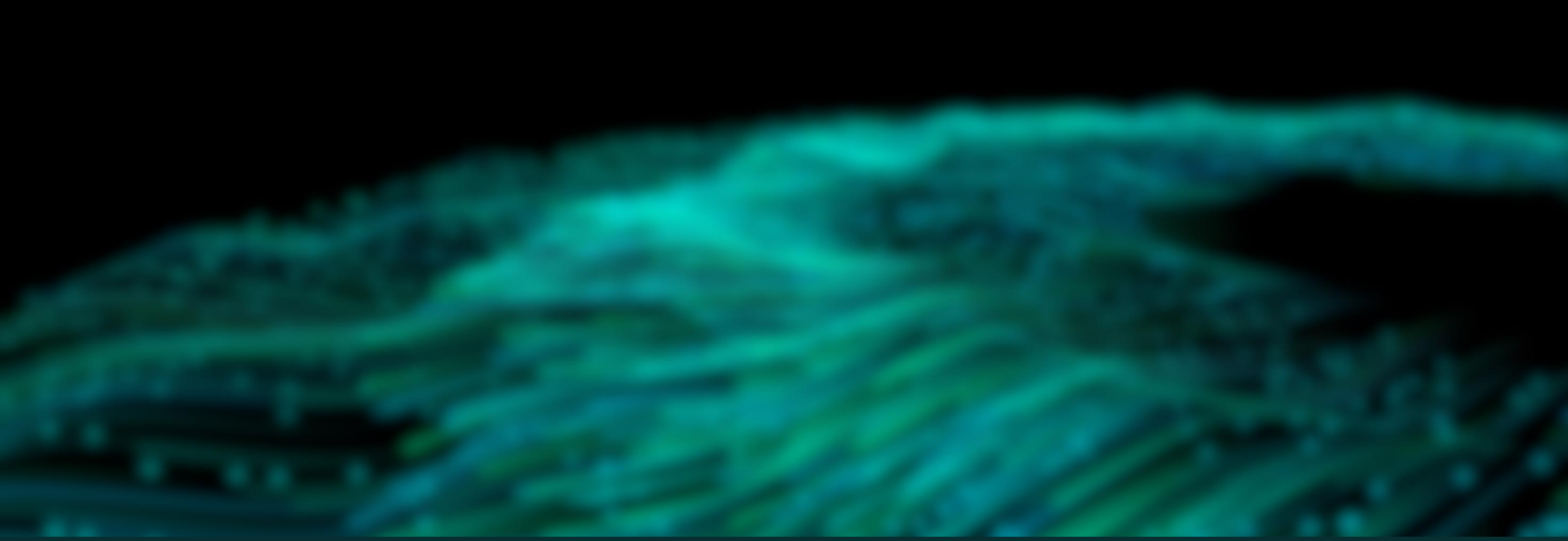
Score

50%

Min 35%
Max 65%

Vos exercices

Nom	Participants	Date	Difficulté	Scénarios	Statut
Nom	Participants	XX/XX/2024	Facile	Scénarios	REPRENDRE



Any questions?

Cyberwal by digital wallonia

Wallonie Relance

SIAPARTNERS

réseau Solidaris

Francis Lejeune

CSD Liège

Cyberwal
by digital
wallonia

CYBERWEEK

16/10/2024

La Centrale de Services à Domicile est **membre du réseau Solidaris**.

La CSD à vos côtés

Notre mission est de procurer rapidement aux personnes l'aide dont elles ont besoin en cas d'accident, de maladie, de handicap ou tout simplement lorsque les limites de l'âge se font sentir. Cet accompagnement leur permet de rester à leur domicile, dans le **respect de leurs choix de vie**.

Une offre pluridisciplinaire

Aide familiale, Soins infirmiers, Garde à domicile, Garde répit, Garde enfants malades, Ergothérapie, Livraison de repas, Transport collectif, Location de matériel médical, Télévigilance, Centre de coordination, Partenaires indépendants…

Sur la route

- → Nous couvrons toute la **Province de Liège**
- → Nous comptons **1200 travailleurs**
- → Nous aidons plus de **10.000 familles**

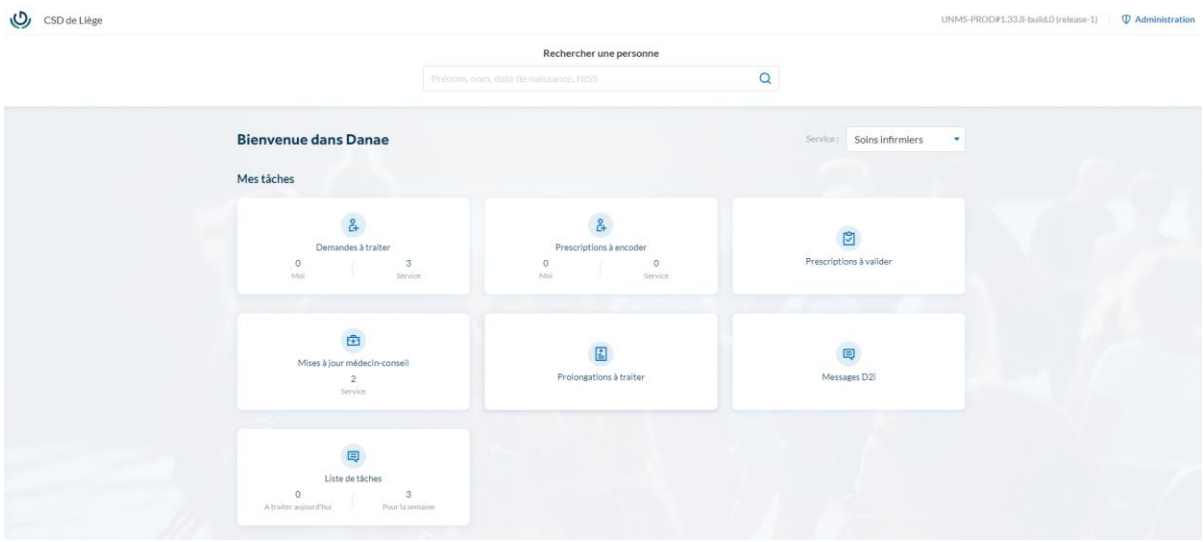
Quelques **chiffrés-clés** de notre activité en 2023 →

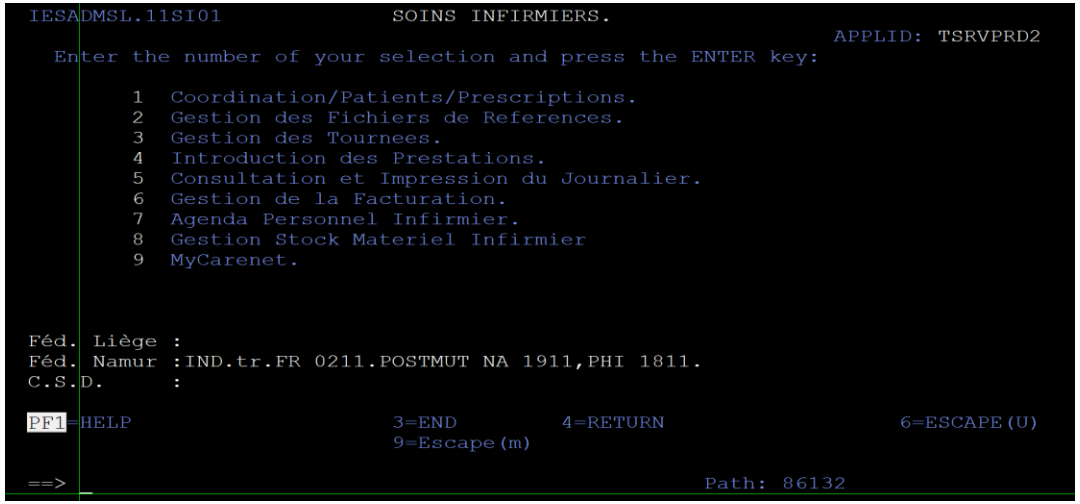
Contexte informatique

Migration en 2021 des systèmes informatiques

- La CSD réalise une migration d'envergure de son informatique mainframe vers un système mixte développé par NRB
- Le cœur métier est redéveloppé et complété par des logiciels existants sur le marché.
- Les solutions du marché sont utilisées pour :
  - Gestion du temps de travail
  - Comptabilité
  - Salaire
  - Impression
  - …

Au 1er février 2023, la CSD passe en production avec ses deux plus grands services « Aide familiale » et « Soins infirmiers ».





Focus sur le hacking

Le logiciel de temps de travail est un logiciel du marché avec un hébergeur externe .

- → Données travailleurs
  - → Nom-Prénom-N° de matricule
  - → Adresse
  - → Contrat
- → Cycles des travailleurs
- → Planning réel
- → API avec historique de 30 jours dans Danae

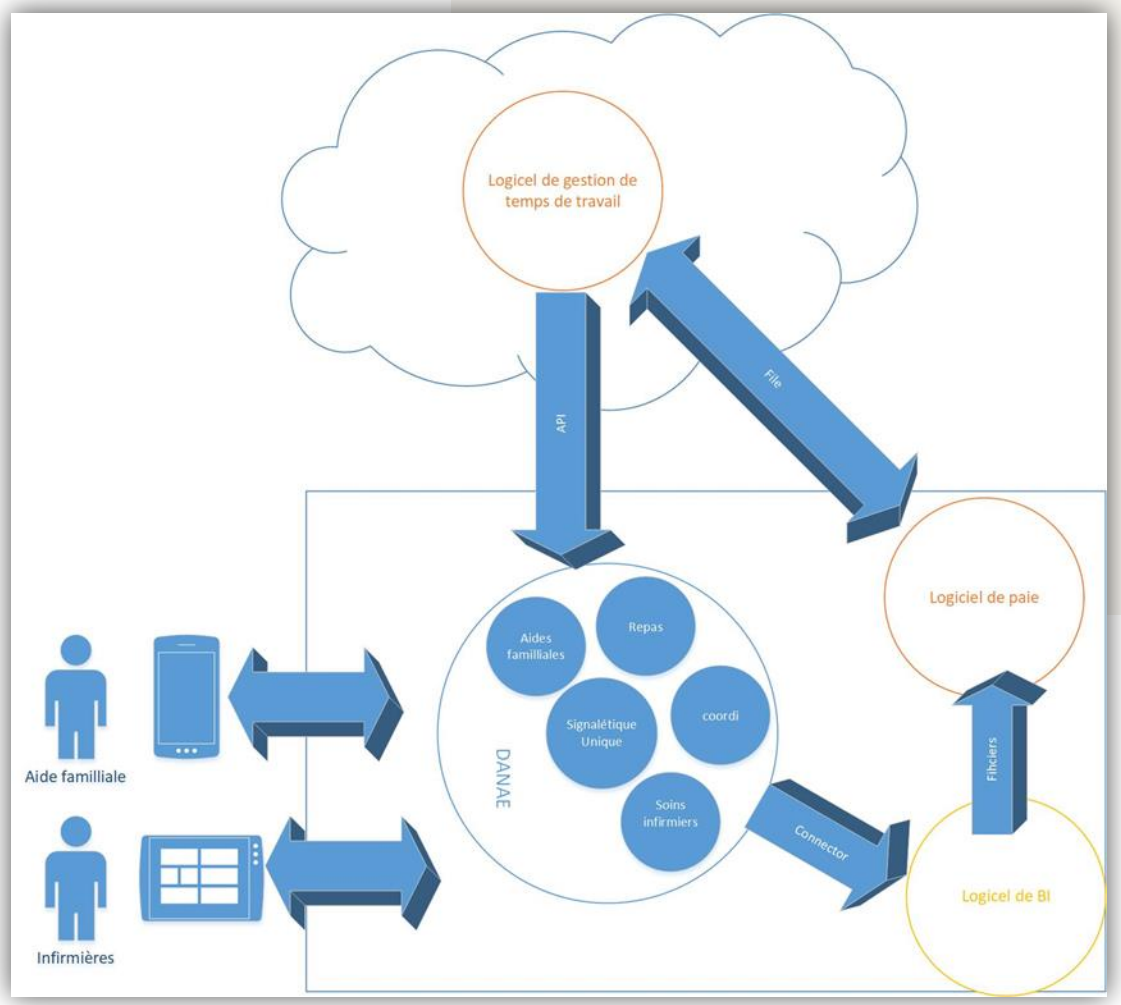
Logiciel Danae

- → Logiciel métiers propres aux CSD
- → Données bénéficiaires
- → Génération des tournées (AF, SI…)

Logiciel de BI

- → Consolidation des données opérationnelles

Logiciel de paie



Gestion de la crise

4 domaines d'actions prioritisés

RGPD

Mise en place des réunions de crise avec les interlocuteurs concernés :

- Responsables
- Key user
- Fournisseurs

AIDE FAMILIALE

- Gestion des absences
- Génération des horaires à 1 semaine

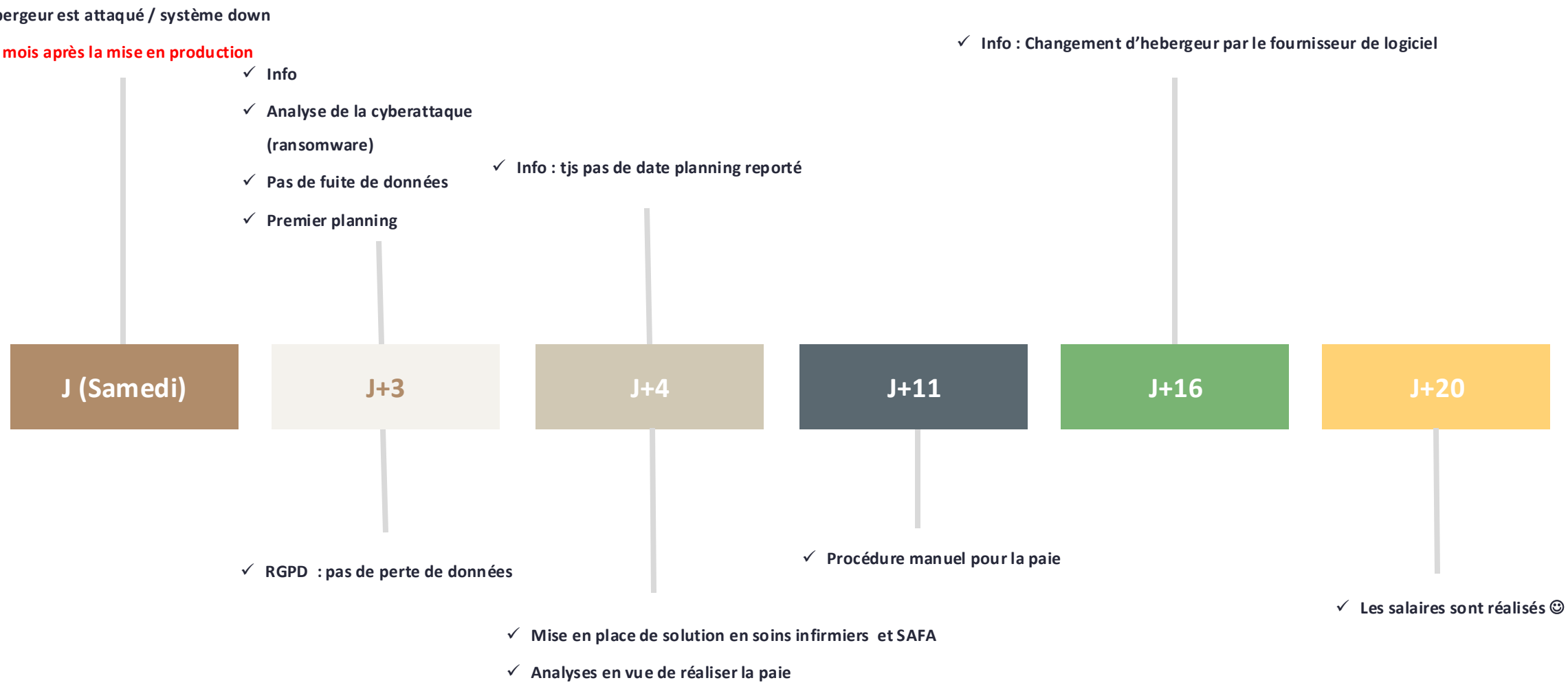
SOINS INFIRMIERS

- Gestion des absences
- Attribution de tournée à 72h

RESSOURCES HUMAINES (SALAIRE)

- Gestion des absences
- Génération des interfaces salaires au 1 du mois

Historique du problème



Historique du problème

✓ Le produit est accessible ***avec le backup de J-1***

J+ 27

J+28

✓ **Organisation du réencodage des du DELTA**

✓ **Retour à la normal**

J+40

Rendre confiance dans l'outil informatique.

Conclusion

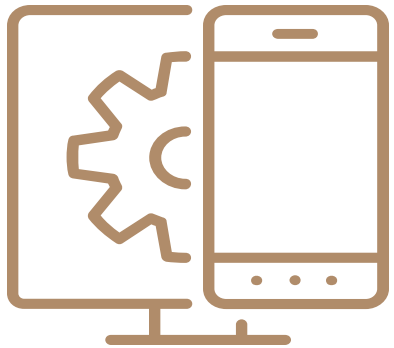
La gestion de la crise IT est gérée par des compétences techniques spécifiques dans un temps indéterminé, mais au sein de la CSD il faut gérer l'opérationnel, le personnel, la communication…

Nos bénéficiaires ne doivent pas être pénalisés par une crise IT.

Exigences dans les contrats

→ Qualité de l'hébergeur

→ Politique de sauvegarde



Anticiper l'opérationnel

→ Avoir une vue sur les procédures et les flux opérationnels (plan de continuité)

→ Avoir une équipe établie avec des utilisateurs de référence

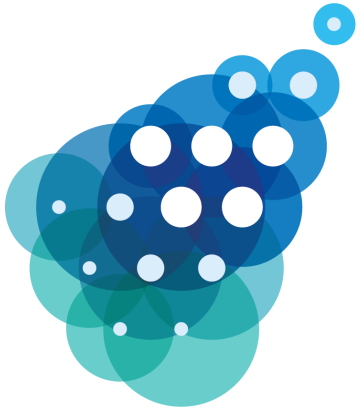
→ Prévoir des solutions alternatives dès la mise en place des solutions

→ Ne pas oublier de communiquer en interne

Rendre confiance dans l'outil informatique.

DES QUESTIONS?

Merci de votre attention



Agence
du Numérique

Nina Hasratyan

Agence du Numérique

Jeremy Grandclaudon

Agence du Numérique

Cyberwal
by digital
wallonia

Cyberwal by digital wallonia

Cyberweek Workshop :

Comment comprendre et appliquer le CyberFundamentals Framework (niveau Basique)

Agence du Numérique

16/10/2024

Contexte de la menace cyber pour les PME

31,8 % des PME belges ont rencontré un **incident de sécurité informatique** en 2023

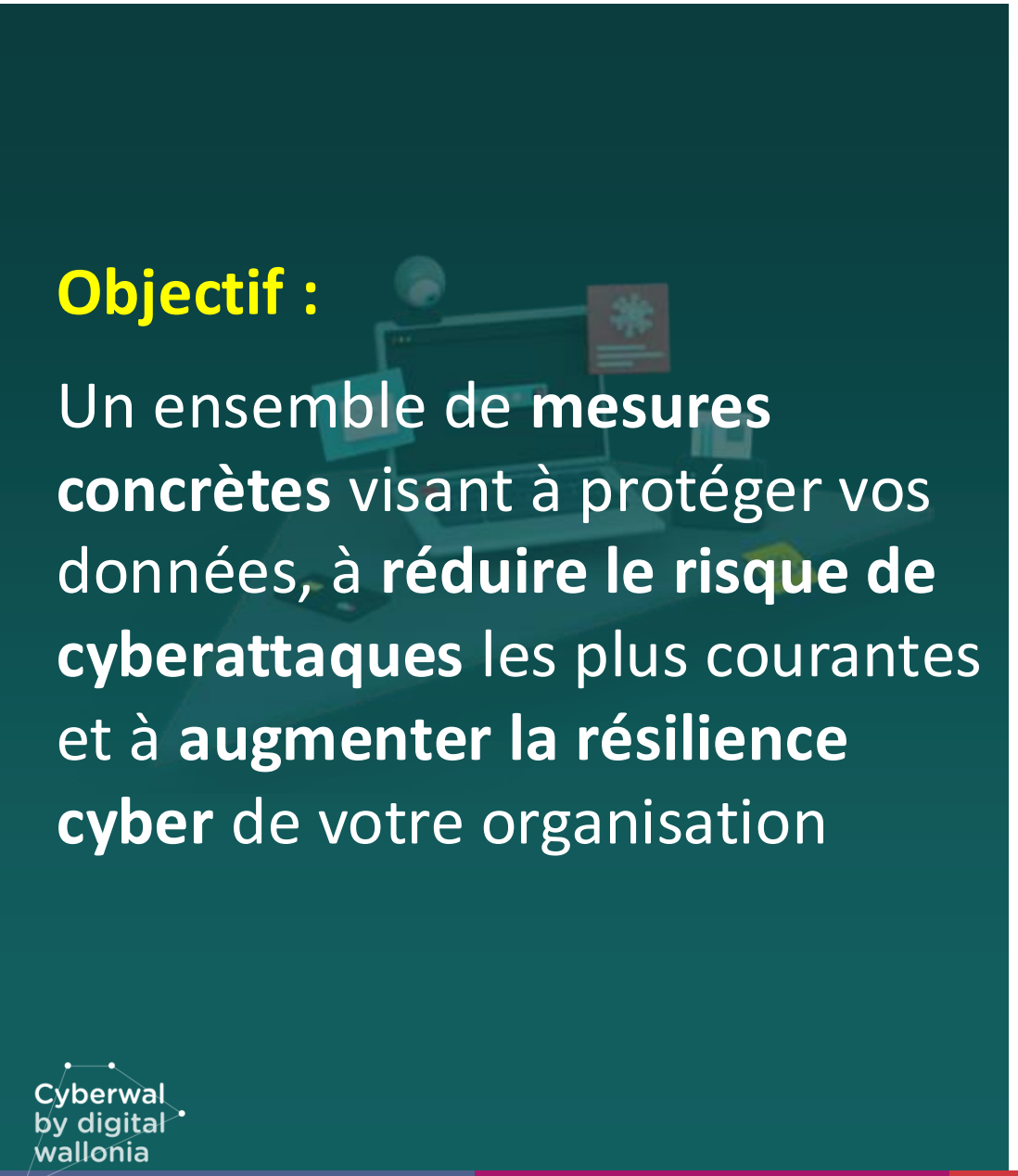
18 % des PME belges n'ont **aucune mesure de sécurité informatique** en place

40 Mio € Montant dérobé par les **attaques de phishings** en 2023

+24% Augmentation du **nombre d'attaques par ransomware** entre 2022 et 2023

Cyberwal by digital wallonia

Qu'est-ce que le CyberFundamentals Framework ?



Objectif :

Un ensemble de **mesures concrètes** visant à protéger vos données, à **réduire le risque de cyberattaques** les plus courantes et à **augmenter la résilience cyber** de votre organisation

- Cadre basé sur **4 frameworks de cybersécurité** :
  - NIST CSF
  - ISO 27001 / ISO 27002
  - CIS Controls
  - IEC 62443
- Propose des **données historiques anonymisées** de cyberattaques réussies
- Echelle à 4 niveaux :
  - Small
  - **Basic**
  - Important
  - Essential

Cyberwal by digital wallonia

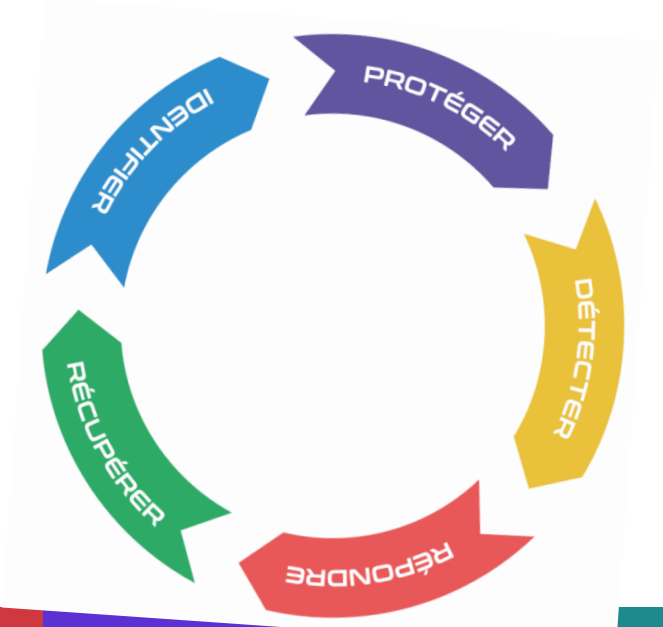
Composition du CyFun niveau Basique

Principes :

Contient les **mesures de sécurité de l'information standards** pour toutes les organisations. Celles-ci fournissent une valeur de sécurité efficace avec des **technologies et des processus qui sont généralement déjà disponibles**

- **34 contrôles**, répartis en différentes mesures, dont **13 clés**

- Mesures s'articulent autour de **5 fonctions essentielles** :
  - **Identifier** : Connaitre les principales cybermenaces
  - **Protéger** : Elaboration et mise en œuvre des mesures de protection
  - **Détecter** : Assurer la détection en temps utile des évènements de cybersécurité
  - **Répondre** : Contenir l'impact d'un cyber-incident
  - **Rétablir** : Maintenir la résilience et restaurer les services



Cyberwal by digital wallonia

Glossaire

Système d'information	L'ensemble organisé des ressources de votre organisation qui permettent de collecter, stocker, traiter, et distribuer de l'information, en général grâce à un réseau d'ordinateurs.
Vulnérabilité	Faille de sécurité. Elle peut servir de porte d'entrée pour des acteurs malveillants s'ils parviennent à l'exploiter.
Menace	Terme générique pour désigner toute intention hostile de nuire dans le cyber espace.
Risque	Ensemble des risques liés à l'usage des technologies numériques. En particulier, toute atteinte potentielle à la confidentialité, l'intégrité ou la disponibilité des données et systèmes d'informations.
Authentification multi-facteurs (MFA)	Méthode d'authentification nécessitant la combinaison de plusieurs facteurs : "quelque chose que je connais", "quelque chose que j'ai", "quelque chose que je suis". *Exemple* : Se connecter avec un mot de passe et un code reçu sur son gsm.

Glossaire

Principe de moindre privilège	Les utilisateurs ne doivent être autorisés qu'à accéder uniquement aux données dont ils besoin pour accomplir leurs missions.
Pare-feu	Outil permettant de protéger un ordinateur connecté à un réseau ou à l'Internet. Le pare-feu filtre les échanges et peut empêcher des attaques externes ou des connexions illégitimes.
Données au repos	Désigne les données stockées de manière persistante, par exemple sur un disque dur.
Données en transit	Données qui sont transmises sur un réseau de communication entre deux endroits.
Segmentation et ségrégation réseau	Désigne le fait de diviser son système d'information en plusieurs zones. Seules les personnes autorisées doivent pouvoir accéder à une zone. Cela permet d'avoir une protection supplémentaire si un utilisateur d'une zone est piraté, il ne pourra pas infecter les autres zones.
Logs	Les logs sont les fichiers qui enregistrent les évènements dans un système d'informations. Ils permettent de faire l'historique des actions effectuées.

Cyberwal
by digital
wallonia

1. Identifier

Agence
du Numérique

Mesures **Identifier** - Catégorie **Gestion d'actifs**

4 contrôles demandent de cataloguer vos actifs :

Vous devez cataloguer :

1. Les dispositifs et systèmes physiques utilisés (ordinateurs, gsms, machines, serveurs, etc.)
2. Les plateformes et applications logicielles utilisées
3. Les informations que l'organisation stocke et utilise
4. Les systèmes d'information externes

Une fois vos actifs catalogués, vous devez les **organiser par ordre de priorité :**

- En fonction de leur **classification**, leur **criticité** et de leur **valeur opérationnelle**.

Mesures **Identifier** - Catégorie **Gouvernance**

Les mesures liées à la gouvernance vous demandent de **documenter les mesures mises en place et votre conformité**.

3 contrôles sont à mettre en place pour prouver votre bonne gouvernance cyber.

Votre organisation doit :

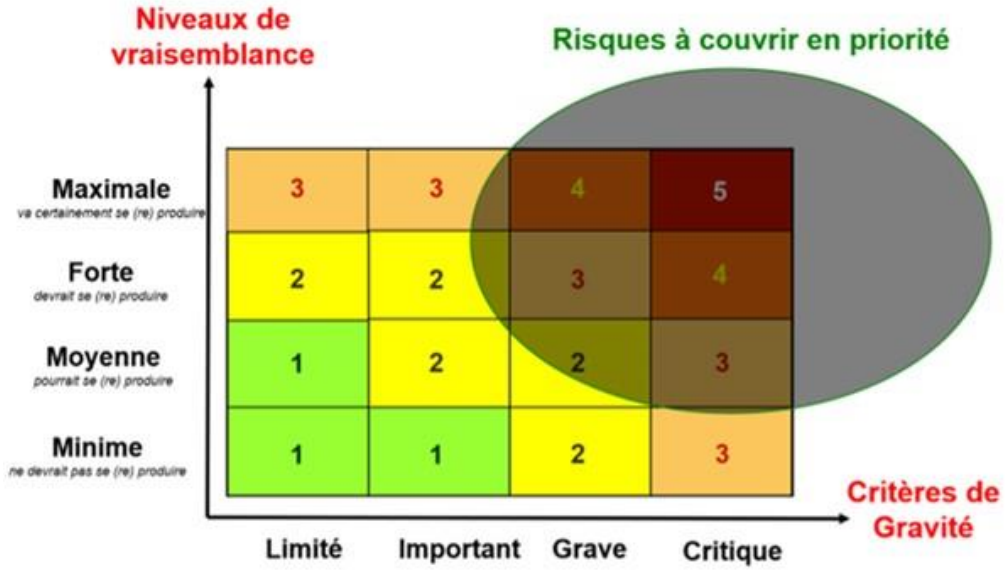
1. Avoir une **politique de cybersécurité** établie et communiquée
2. **Respecter les exigences légales et réglementaires** en matière de cybersécurité
3. Avoir une **stratégie complète** de gestion des risques liés à la sécurité de l'information et à la cybersécurité

Mesures **Identifier** - Catégorie **Evaluation des risques**

L'organisation **comprend le risque de cybersécurité** pour les opérations de l'organisation, ses actifs et les individus

Le travail d'évaluation des risques doit aboutir à la mise en place de **2 contrôles :**

1) Identifier et documenter les menaces et les vulnérabilités.
2) Utiliser les menaces, les vulnérabilités, les probabilités et les impacts pour déterminer les risques



Il est conseillé d'utiliser une **matrice de risques** pour identifier ceux à couvrir en priorité.

Cyberwal
by digital
wallonia

2. Protéger

Agence
du Numérique

Mesures **Protéger** - Catégorie **Gestion des identités, authentification et contrôle d'accès**

La gestion des accès est essentielle à mettre en place, pour garantir que **seuls les utilisateurs autorisés aient accès aux ressources strictement nécessaires**.

Dans le CyFun, cet aspect se divise en **5 contrôles**, qui représentent **10 mesures, dont 8 clés**. L'organisation **comprend le risque de cybersécurité** pour les opérations de l'organisation, ses actifs et les individus

Les **2 mesures complémentaires** sont :

- Gestion des accès physique à l'installation, aux serveurs et aux composants du réseau.
- Les points d'accès sans fil de l'organisation doivent être sécurisés.

Mesures clés : Gestion des identitiés, authentification et contrôle d'accès

8 mesures clés à mettre en place pour le niveau Basique :

1) Il doit y avoir une **gestion des identités et identifiants** des dispositifs et utilisateurs.
2) Les réseaux de l'organisation doivent être sécurisés, notamment par le **MFA.**
3) Les **autorisations d'accès** des utilisateurs aux systèmes doivent être définies et gérées.
4) Les personnes ayant accès aux informations et aux technologies critiques sont identifiées.
5) Le principe de **moindre privilège** doit être mis en place.
6) Personne ne doit avoir de privilège administrateur pour les tâches quotidiennes.
7) Des pares-feux doivent être installés et activés.
8) Les **systèmes critiques doivent être segmentés et ségrégués** du reste du réseau de l'organisation.

Mesures **Protéger** - Catégorie **Sensibilisation et formation**

1 seul contrôle concerne la sensibilisation et la formation : les **employés doivent être formés et informés** de manière appropriée.

Il convient que la formation et la sensibilisation soit dès l'embauche et continuellement mise à jour.

Mesures **Protéger** - Catégorie **Sécurité des données**

L'organisation doit **garantir la confidentialité, l'intégrité et la disponibilité** des informations.

Il est attendu de l'organisation de :

1. **Protéger les données au repos**
2. **Protéger les données en transit**

Le CyFun laisse l'organisation libre de procéder comme elle souhaite.
Il est tout de même attendu de l'organisation qu'elle **chiffre ses données**, au repos et en transit.

L'organisation doit aussi :

3. **Eliminer de manière sûre** les actifs et supports qui ne sont plus utilisés.
4. **Séparer les environnements** de développement et de test de l'environnement de production.

Mesures **Protéger** - Catégorie **Processus et procédures de protection de l'information**

Il est attendu de l'organisation de mettre en place des **politiques de sécurité** pour gérer la protection des systèmes d'information et des actifs.

L'organisation doit donc mettre en place **2 contrôles :**

1) (**Mesure clé**) Des **sauvegardes** des informations sont effectuées, maintenues et testées.
   - Les sauvegardes doivent avoir lieu sur un système différent de celui sur lequel se trouvent les données originales.

2) La cybersécurité est incluse dans les **pratiques des ressources humaines.**
   - Quand du personnel part, son compte est désactivé et/ou supprimé.
   - Le personnel ayant accès aux informations les plus critiques doit être vérifié.

Mesures **Protéger** - Catégorie **Maintenance**

L'organisation doit respecter cette **mesure clé :**

L'**entretien et la réparation des actifs sont effectués et consignés**, avec des outils approuvés et contrôlés.

Il est donc essentiel que les **correctifs et mises à jour de sécurités soient installés**.

Mesures **Protéger** - Catégorie **Technologie de protection**

L'organisation doit mettre en place des **solutions de sécurité technique**, afin de garantir la sécurité et la résilience des systèmes et des actifs.

Cela repose sur **2 contrôles :**

1) (**Mesure clé**) Les **logs** sont maintenus, documentés et examinés.
   - Les logs doivent être sauvegardés et conservés pendant une période prédéfinie.
   - Les logs doivent être analysés pour déceler des évènements inhabituels.

2) Des **filtres web et email** sont installés et utilisés.
   - Cela permet de détecter et empêcher les courriers électroniques malveillants et/ou le spam.

Cyberwal
by digital
wallonia

3. Détecter

Agence
du Numérique

Mesures **Détecter** - Catégorie **Anomalies et évènements**

L'organisation met en place des mesures pour **détecter les activités anormales**.

Il est essentiel pour l'organisation de vérifier les activités suspectes. C'est pour cela qu'il s'agit d'une **mesure clé** :

L'organisation doit **collecter et corréler les données d'évènements** (logs) de sources et capteurs multiples (pare-feu, anti-virus, etc.).

Mesures **Détecter** - Catégorie **Surveillance continue de la sécurité**

Le système d'information et les actifs sont surveillés pour **identifier les évènements** de cybersécurité et **vérifier l'efficacité des mesures** de protection.

Pour respecter cette exigence, l'organisation doit mettre en place **3 contrôles :**

1) **Surveiller le réseau** pour détecter les évènements potentiel de cybersécurité.
   - Des pares-feux doivent être installés et exploités.
2) **L'activité du personnel est surveillée** pour détecter les évènements potentiels.
3) (**Mesure clé**) Le **code malveillant est détecté**.
   - Des **programmes contre les virus** et autres programmes malveillants doivent être installés et mis à jour.
   - Ces programmes doivent être installés aussi sur les ordinateurs à domicile ou les appareils personnels utilisés pour le travail professionnel.

Cyberwal
by digital
wallonia

4. Répondre

Agence
du Numérique

Mesures **Répondre** - Catégorie **Planification de la réponse**

L'organisation doit **prévoir en amont et documenter** comment répondre aux incidents de sécurité.

1 mesure à mettre en place :

- Un **processus de réponse aux incidents**, comprenant les **rôles**, les **responsabilités**, et les **pouvoirs** doit être exécuté pendant ou après un évènement lié à l'information ou à la cybersécurité sur les systèmes critiques de l'organisation.
  - Les rôles, responsabilités, et pouvoir doivent être précis
  - Il est nécessaire de prévoir les coordonnées des personnes à prévenir

Mesures **Répondre** - Catégorie **Communications**

Les activités de réponse sont coordonnées avec les parties prenantes internes et externes (par ex : forces de l'ordre).

1 contrôle à mettre en place :

- Les informations relatives aux incidents de cybersécurité doivent être **communiquées** et **partagées** avec les employés de l'organisation dans un **format qu'ils peuvent comprendre**

Mesures **Répondre** - Catégorie **Améliorations**

Les activités de réponse de l'organisation sont améliorées par l'intégration des enseignements tirés des activités de détection/réponse actuelles et précédentes.

1 contrôle à mettre en place :

- L'organisation doit effectuer des **évaluations post-incident** afin d'analyser les **enseignements tirés** de la réponse à l'incident et du rétablissement, et par conséquent améliorer les processus / procédures / technologies pour renforcer sa cyber-résilience.

Cyberwal
by digital
wallonia

5. Rétablir

Agence
du Numérique

Mesures **Rétablir** - Catégorie **Planification du rétablissement**

Des processus et des procédures de rétablissement sont exécutés et maintenus pour assurer la restauration des systèmes ou des actifs touchés par des incidents de cybersécurité.

1 contrôle à mettre en place :

- Un processus de rétablissement en cas de catastrophes et d'incidents liés à l'information et à la cybersécurité est élaboré et exécuté selon les besoins.
  - Le processus doit considérer les cas d'incendie, d'urgence médicale, de vol, de catastrophe naturelle ou de cyber-incident.

Cyberwal
by digital
wallonia

Rappel des mesures clés

Agence
du Numérique

13 Mesures clés (1/2)

1) Il doit y avoir une **gestion des identités et identifiants** des dispositifs et utilisateurs.

2) Les réseaux de l'organisation doivent être sécurisés, notamment par le **MFA.**

3) Les **autorisations d'accès** des utilisateurs aux systèmes doivent être définies et gérées.

4) Les personnes ayant accès aux informations et aux technologies critiques sont identifiées.

5) Le principe de **moindre privilège** doit être mis en place.

6) Personne ne doit avoir de privilège administrateur pour les tâches quotidiennes.

7) Des pares-feux doivent être installés et activés.

8) Les **systèmes critiques doivent être segmentés et ségrégués** du reste du réseau de l'organisation.

13 Mesures clés (2/2)

9) Des **sauvegardes** des informations sont effectuées, maintenues et testées

10) L'**entretien et la réparation des actifs sont effectués et consignés**, avec des outils approuvés et contrôlés.

11) Les **logs** sont maintenus, documentés et examinés.

12) L'**entretien et la réparation des actifs sont effectués et consignés**, avec des outils approuvés et contrôlés.

13) Le **code malveillant est détecté**.

Cyberwal
by digital
wallonia

Les questions à se poser ?

Agence
du Numérique

Des exemples de questions à se poser

- Ai-je une documentation qui indique à quels logiciels et données chaque employé peut accéder ?
- De quand date la dernière mise à jour de ma documentation ?
- Ai-je mis en place l'authentification à plusieurs facteurs ? En particulier, pour accéder aux actifs critiques ?
- Ai-je la liste du personnel ayant accès aux actifs critiques ?
- Est-ce que les comptes administrateurs ne sont utilisés que le temps d'effectuer une tâche précise ?
- Lorsqu'un compte administrateur n'est pas nécessaire, est-il désactivé ?
- Est-ce que chaque membre du personnel n'a accès qu'aux informations nécessaires à l'exécution de ses tâches ?

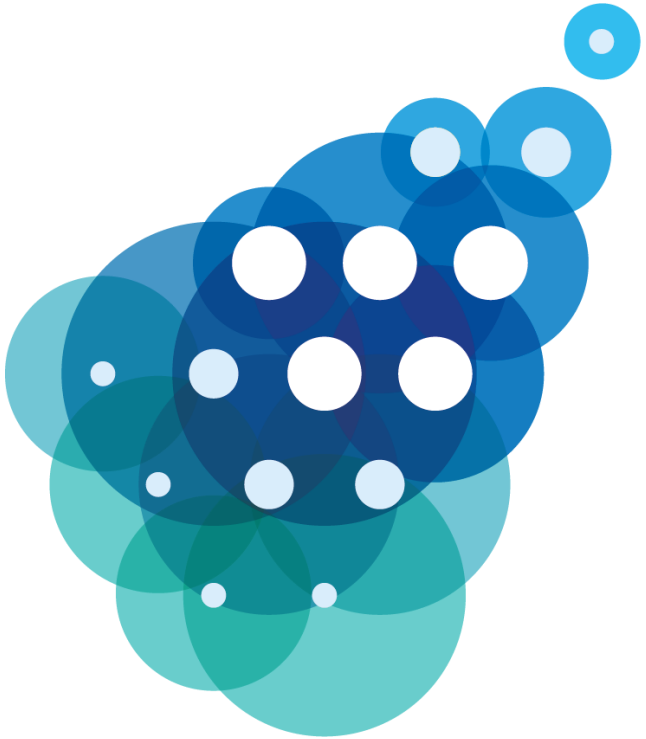
Des exemples de questions à se poser

- Est-ce que les systèmes critiques sont séparés du reste du réseau ? Si oui, est-ce que les accès à ces derniers sont plus stricts ?
- Est-ce que j'effectue régulièrement des sauvegardes ?
- Le rétablissement des sauvegardes a-t-il déjà été testé ?
- Ai-je mis en place des pares-feux ? Des anti-virus ? D'autres solutions de protection ?
- Ai-je activé l'enregistrement des logs pour les composants de mon système ? Sont-ils conservés pour une durée suffisante ?
- Mes actifs et logiciels sont-ils mis à jour régulièrement ? Ces MàJ sont-elles consignées ?

Cyberwal by Digital Wallonia à l'AdN

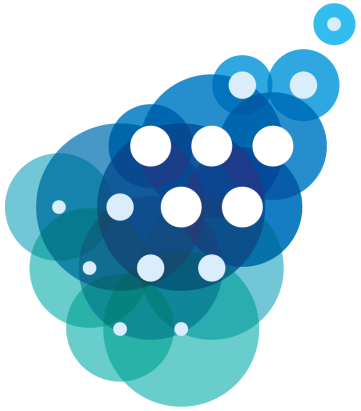
Cyberwal
by digital
wallonia

- **Stéphane Vince**
  stephane.vince@adn.be
- **Jeremy Granclaudon**
  jeremy.grandclaudon@adn.be
- **Nina Hasratyan**
  nina.Hasratyan@adn.be



Agence
du Numérique

We **love** digital | We **know** digital | We **make** digital



Agence
du Numérique

Marie-Pierre Van Dooren

Agence du Numérique

Cyberwal
by digital
wallonia

Programme DigitalEES

Le programme vise à promouvoir l'utilisation des technologies numériques dans les entreprises de manière à optimiser leurs activités au service de leur finalité sociale.

DigitalEES
by digital wallonia

Cibles
DigitalEES

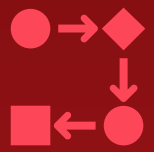
Baromètre de maturité numérique
DigitalEES

Infrastructure.

Connexion, cloud, logiciels…

Organisation.

Mode organisationnel de travail, compétences, formation, etc. et la formation du capital humain.



Processus.

L’automatisation des processus métiers à l’aide des technologies numériques.

Stratégies.

L’intégration des usages des technologies numériques dans la stratégie globale de l’entreprise

Focus EES sur la maturité numérique

DigitalEES

Infrastructure.

18%

ont une politique sécurité informatique.

Organisation.

89%

profil du dirigeant qui est impliqué dans le projet. Il est le sponsor.

Processus.

61%

ont formalisé une politique RGPD

63%

ont créé la fonction de data protection officer (DPO)

Stratégies.

28%

des EES (de + 10 travailleurs) développent de nouveaux produits grâce au digital

Le dirigeant et la stratégie de transformation numérique

DigitalEES

50%

des dirigeants EES sont des convaincus des opportunités du numérique.

47%

des entreprises wallonnes ont mené un projet de digitalisation entre 2020 et 2022.

20%

des EES ayant conduits des projets numériques ont formalisé une stratégie globale de transformation numérique.

Acquisition de nouveaux logiciels

Numérisation des processus de travail

Numérisation des processus avec les partenaires (liaisons)

DigitalEES
by digital
wallonia

DigitalEES

. Axe 1.	. Axe 2 .	. Axe 3 .	. Axe 4 .	. Axe 5 .
Sensibiliser	**Former**	**Outiller**	**Innover**	**Stimuler**





DigitalEES by digital wallonia

DigitalEES

En partenariat et en collaboration avec

Concertes

Agence du Numérique

UNIPSO

Wallonie familles santé handicap AVIQ

W.ALTER

Wallonie service public SPW

santhea

InitiativES

UNESSA

¡ES! Réinventons l'économie

WALLONIE SANTÉ

WE Wallonie Entreprendre

DigitalEES
by digital
wallonia

Restons en contact !

Nous sommes à votre disposition.

Marie-Pierre Van Dooren
mariepierre.vandooren@adn.be

Un networking drink vous attend dans le hall.

Cyberwal
by digital
wallonia

Plus d’infos sur

digitalwallonia.be/cyber

Cyberwal by digital wallonia

Wallonie Relance