CYBERWEEK 2024

LA SÉCURITÉ NUMÉRIQUE POUR LE SECTEUR PUBLIC

15 OCTOBRE 2024

LOUVAIN-LA-NEUVE

Agence du Numérique · Cyberwal by digital wallonia · iMio · Wallonie service public SPW · Solvay Brussels School Economics & Management · Centre for Cybersecurity Belgium · SIAPARTNERS · Cresco. Cybersecurity · Wallonie Relance

Programme

8h30 : Accueil.
9h00 : Introduction - Nina Hasratyan et Jeremy Grandclaudon, responsables du programme Cyberwal by Digital Wallonia à l'Agence du Numérique.
9h05 : La Directive NIS2 et l'arrivée de la loi de transposition avec un focus sur le secteur public - Stéphan André, Legal Officer, Centre for Cybersecurity Belgium (CCB).
10h05 : Bug Bounty : retour d'expérience d'iMio sur un projet en cours - Joël Lambillotte, Directeur Général Adjoint, iMio.
10h35 : Démo: utlisation d'un simulateur numérique pour mener une cyber-attaque sur une entité publique virtuelle - SIA Partners.
11h00 : Pause-café.
11h10 : Active cyber protection : une approche belge, mais pas que, de la cybersécurité - Phédra Clouner, Directrice adjointe, Centre for Cybersecurity Belgium (CCB).
11h30 : La recherche de compétences en cybersécurité dans le secteur public - Georges Ataya, Professeur à la Solvay Business School et Directeur, Ataya & Partners.
12h10 : Renforcer la Cybersécurité des Services Publics grâce à l'Écosystème de Recherche Wallon - Dr Ir Fabian Lapierre, SPW EER.
12h30 : Conclusion : annonce de la Cyber Response Team (CRT) - Stéphane Vince, Directeur. Pôle Technologie et Administration numérique à l'Agence du Numérique.
13h00 : Networking lunch. Animation par Cresco : HackingLab.

Cyberwal
by digital
wallonia

Nina Hasratyan

Agence du Numérique

Jeremy Grandclaudon

Agence du Numérique

Cyberwal
by digital
wallonia

Stéphan André

Centre pour la Cybersécurité Belgique (CCB)

Cyberwal
by digital
wallonia

Transposition de la directive NIS2 en Belgique (Secteur public) - Cyberweek LLN

NIS Team CCB

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Que signifie TLP Green ?

CENTRE FOR CYBERSECURITY BELGIUM

TRAFFIC LIGHT PROTCOL (TLP)

Green (TLP GREEN)

Limited disclosure, recipients can spread this within their community.

Les sources peuvent utiliser **TLP:GREEN** lorsque les informations sont utiles pour accroître la sensibilisation au sein de leur communauté élargie. Les destinataires peuvent partager les informations **TLP:GREEN** avec leurs pairs et les organisations partenaires au sein de leur communauté, mais pas par le biais de canaux accessibles au public (par exemple, sites web, LinkedIn...). Les informations **TLP:GREEN** ne peuvent pas être partagées en dehors de la communauté. Remarque : lorsque le terme "communauté" n'est pas défini, il s'agit de la communauté de la cybersécurité/défense.

CENTRE FOR CYBERSECURITY BELGIUM

NIS 2 : POUR QUI ? POURQUOI ?

QUOI ?

La directive n°2022/2555 (« NIS 2 ») est une révision de la directive n°2016/1148 (« NIS 1 ») (*Network and Information Security*). Il s'agit d'une législation de l'UE en matière de cybersécurité.

QUELLES OBLIGATIONS ?

1. S'enregistrer auprès du CCB (Safeonweb@work).
2. Prendre des mesures de cybersécurité adéquates.
3. Notifier au CCB les cyberincidents significatifs.
4. Effectuer des évaluations régulières de la conformité vérifiées par un organisme de contrôle de la conformité (entités essentielles).

POURQUOI ?

NIS 2 vise à établir un niveau élevé et commun de cybersécurité dans l'UE en imposant des exigences de gestion des risques de cybersécurité et de notification des incidents aux entités actives dans différents secteurs critiques.

POUR QUI ?

Les entités (essentielles ou importantes) établies en Belgique et fournissant des services dans les secteurs repris aux annexes I ou II.

Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 relative à des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union (directive NIS2).

Transposition

Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (loi NIS2)

L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Arrêté royal du 9 juin 2024 portant exécution de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (arrêté royal NIS2).

Acte d'exécution de la Commission établissant les modalités d'application de la directive (UE) 2022/2555 en ce qui concerne les exigences techniques et méthodologiques des mesures de gestion des risques en matière de cybersécurité et précisant davantage les cas dans lesquels un incident est considéré comme significatif

European Commission

La version finale sera bientôt publiée

CyberFundamentals Framework
Recommandation du CCB - Guide de démarrage rapide NIS2
Guide du CCB sur la notification d'incidents (à venir)
Guide du CCB sur la CVD (à mettre à jour)
FAQ

Agenda

CENTRE FOR CYBERSECURITY BELGIUM

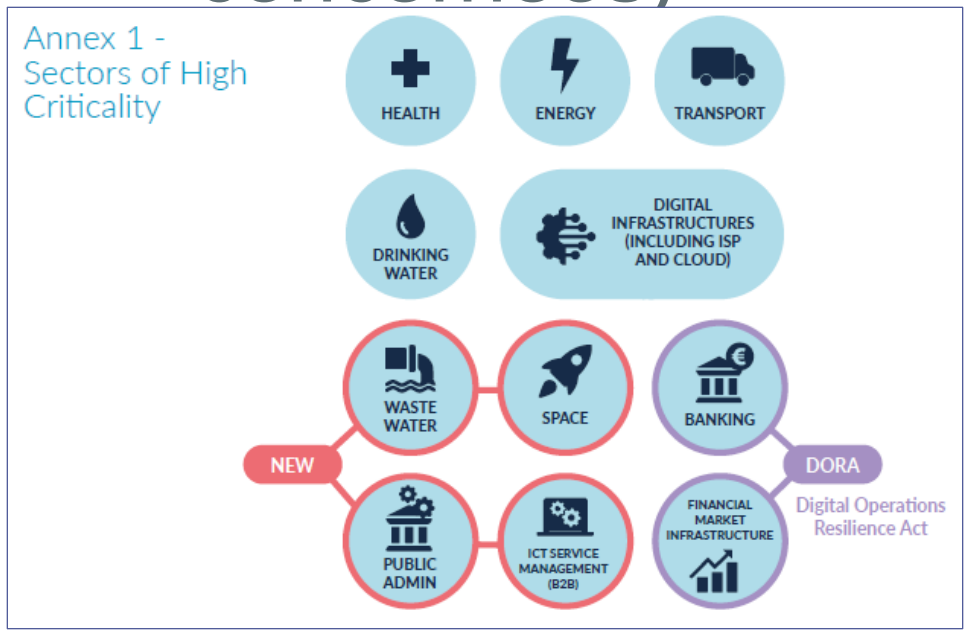
1. Champ d'application (entités concernées)
2. Autorités compétentes
3. Mesures de cybersécurité (cadres de cybersécurité/évaluation des risques)
4. Notification d'incident
5. Supervision
6. Prochaines étapes / Q/A

CENTRE FOR CYBERSECURITY BELGIUM

Champ d'application (entités concernées)

01

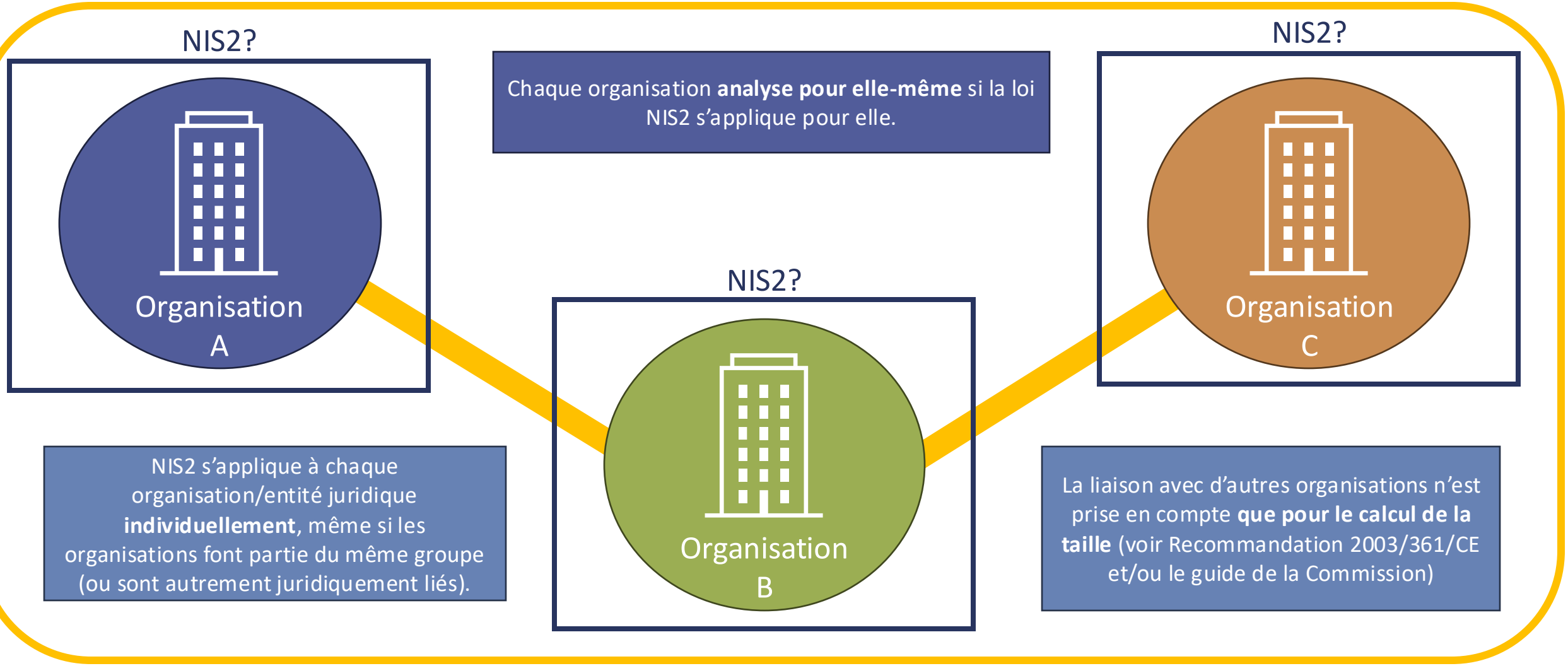
NIS2 Champ d'application (entités concernées)



Source : www.ncsc.gov.ie

- **Fournir un service** (type d'entité) mentionné à l'annexe I ou à l'annexe II + **taille** ("size-cap")
- Exceptions :
  - autre législation de l'UE applicable (*Lex specialis*) : DORA Digital Operations Resilience Act (secteurs financier/bancaire) ou **exclusions spécifiques** (administrations publiques actives dans la sécurité publique).
  - l'identification nationale (CER ou NIS) - **y compris pour les administrations publiques qui dépendent des entités fédérées** ;
  - types d'entité pour lequel la règle du "size-cap" ne s'applique pas

Application individuelle



Groupe ABC

Dans le champ d'application	Hors champ d'application
Entités de l'annexe I et de l'annexe II (+ voir size-cap) **Administrations publiques qui dependent de l'État fédéral** : Y compris : • SPF Justice (avec une exclusion pour la base de données judiciaire) ; • SPF Intérieur (avec une exclusion partielle pour le NCCN) ; • SPF Affaires étrangères (avec une exclusion pour les réseaux et les systèmes d'information des ambassades en dehors de l'UE). **Zones de secours**	**Certaines administrations fédérales** actives dans le domaine de la sécurité nationale et/ou publique (art. 5) (en partie) : • SGRS/ADIV • VSSE • OCAM/OCAD • Ministère de la défense • Inspection de la police et des services généraux de police • CCB DU NCCN **Autorités judiciaires et juridictions** **Parlements** **Banque nationale de Belgique.** **Installations nucléaires - classe I** (à l'exception des parties utilisées pour la production et la distribution d'électricité)
Les administrations publiques fédérées identifiées (régions et/ou communautés).	**Les *administrations locales* et le secteur de l'éducation** (***sauf si fournissent un service mentionné à l'annexe I ou II*** ou sont spécifiquement identifiés).
	Systèmes d'information classifiés ou systèmes de documents nucléaires

Annexe I : secteurs hautement critiques

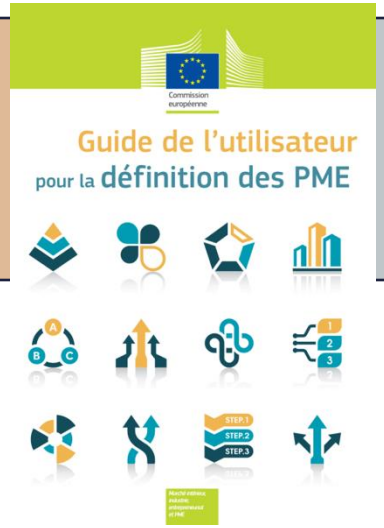
SECTEUR	SOUS-SECTEUR et/ou TYPE D'ENTITÉ		GRANDES ENTREPRISES *effectif d'au moins 250 ETP, ou chiffre d'affaires annuel > € 50 M et bilan annuel total > € 43 M*	MOYENNES ENTREPRISES *effectif d'au moins 50 ETP, ou > € 10 M de chiffre d'affaires annuel / bilan annuel total*	PETITES & MICRO ENTREPRISES
1. Énergie	Électricité	Entreprises d'électricité ; Gestionnaires de réseau de distribution ; Gestionnaires de réseau de transport ; Producteurs ; Opérateurs désignés du marché de l'électricité ; Acteurs du marché ; Exploitants d'un point de recharge	**Essentiel**	Important*	**Seulement si identifié***
	Réseaux de chaleur et de froid	Opérateurs de réseaux de chaleur ou de réseaux de froid			
	Pétrole	Exploitants d'oléoducs ; Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole ; Entités centrales de stockage			
	Gaz	Entreprises de fourniture ; Gestionnaires de réseau de distribution ; Gestionnaires de réseau de transport ; Gestionnaires d'installation de stockage ; Gestionnaires d'installation de GNL ; Entreprises de gaz naturel ; Exploitants d'installations de raffinage et de traitement de gaz naturel			
	Hydrogène	Exploitants de systèmes de production, de stockage et de transport d'hydrogène			
2. Transports	Transports aériens	Transporteurs aériens utilisés à des fins commerciales ; Entités gestionnaires d'aéroports, aéroports, et entités exploitant les installations annexes se trouvant dans les aéroports ; Services du contrôle de la circulation aérienne			
	Transports ferroviaires	Gestionnaires de l'infrastructure ; Entreprises ferroviaires			
	Transports par eau	Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret ; Entités gestionnaires des ports et les entités exploitant des infrastructures et des équipements à l'intérieur des ports ; Exploitants de services de trafic maritime (STM)			
	Transports routiers	Autorités routières chargées du contrôle de la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale ; Exploitants de systèmes de transport intelligents			
3. Secteur bancaire	Établissements de crédit *[DORA Lex specialis]*				
4. Infrastructures des marchés financiers	Exploitants de plates-formes de négociation ; Contreparties centrales *[DORA Lex specialis]*				
5. Santé	Prestataires de soins de santé ; Laboratoires de référence de l'Union européenne ; Recherche et développement dans le domaine des médicaments ; Fabrication de produits pharmaceutiques de base et de préparations pharmaceutiques ; Fabrication de dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique				
6. Eau potable	Fournisseurs et distributeurs d'eaux destinées à la consommation humaine, **seulement si** cette activité est une partie essentielle de leur activité générale				
7. Eaux usées	Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées, **seulement si** cette activité est une partie essentielle de leur activité générale				
8. Infrastructure numérique	Prestataires de services de confiance qualifiés		**Essentiel**		
	Fournisseurs de services DNS [à l'exclusion des opérateurs de serveurs racines de noms de domaine]				
	Registres de noms de domaine de premier niveau				
	Fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public		**Essentiel**		Important*
	Prestataires de services de confiance non-qualifiés		**Essentiel**	Important*	**Seulement si identifié***
	Fournisseurs de points d'échange internet				
	Fournisseurs de services d'informatique en nuage				
	Fournisseurs de services de centres de données				
	Fournisseurs de réseaux de diffusion de contenu				
9. Gestion des services TIC	Fournisseurs de services (de sécurité) gérés				
10. Administration publique (à l'exclusion du pouvoir judiciaire, des parlements, des banques centrales, de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi)	Administrations publiques qui dépendent de l'État fédéral		**Essentiel**		
	Administrations publiques qui dépendent des entités fédérées (après identification suite à une évaluation basée sur les risques de la criticité des services fournis)		**Important***		
	Zones de secours (y compris le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale)				
11. Espace	Exploitants d'infrastructures terrestres qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics		**Essentiel**	Important*	**Seulement si identifié***

CENTRE FOR CYBERSECURITY BELGIUM

Annexe II : autres secteurs critiques

SECTEUR	SOUS-SECTEUR et/ou TYPE D'ENTITÉ	GRANDES ENTREPRISES *effectif d'au moins 250 ETP, ou chiffre d'affaires annuel > € 50 M et bilan annuel total > € 43 M*	MOYENNES ENTREPRISES *effectif d'au moins 50 ETP, ou > € 10 M de chiffre d'affaires annuel / bilan annuel total*	PETITES & MICRO ENTREPRISES
1. Services postaux et d'expédition	Prestataires de services postaux, y compris les prestataires de services d'expédition	Important*		Seulement si identifié*
2. Gestion des déchets	Seulement s'il s'agit de la principale activité économique			
3. Produits chimiques	Fabrication de substances et distribution de substances ou de mélanges ; Production d'articles à partir de substances ou de mélanges			
4. Denrées alimentaires	Activités de distribution en gros, production industrielle ou transformation industrielle de denrées alimentaires			
5. Fabrication	Dispositifs médicaux (in vitro); produits informatiques, électroniques et optiques ; équipements électriques ; machines et équipements n.c.a. ; véhicules automobiles, remorques et semi-remorques ; d'autres matériels de transport (NACE C 26-30)			
6. Fournisseurs numériques	Fournisseurs de places de marché en ligne			
	Moteurs de recherche en ligne			
	Plateformes de services de réseaux sociaux			
7. Recherche	Organismes de recherche, à l'exclusion des établissements d'enseignement			

Annexe I: Secteurs hautement critiques
Types d'entité + seuil*



Annexe II: Autres secteurs critiques
Types d'entité + seuil

Grande entreprise (au moins 250 ETP ou €50M+ de chiffres d'affaires annuel ou €43M+ de bilan annuel)

Entreprise moyenne (au moins 50 ETP ou €10M+ de chiffres d'affaires annuel ou de bilan annuel)

Grande entreprise (au moins 250 ETP ou €50M+ de chiffres d'affaires annuel ou €43M+ de bilan annuel)

Entreprise moyenne (au moins 50 ETP ou €10M+ de chiffres d'affaires annuel ou de bilan annuel)

Entités essentielles

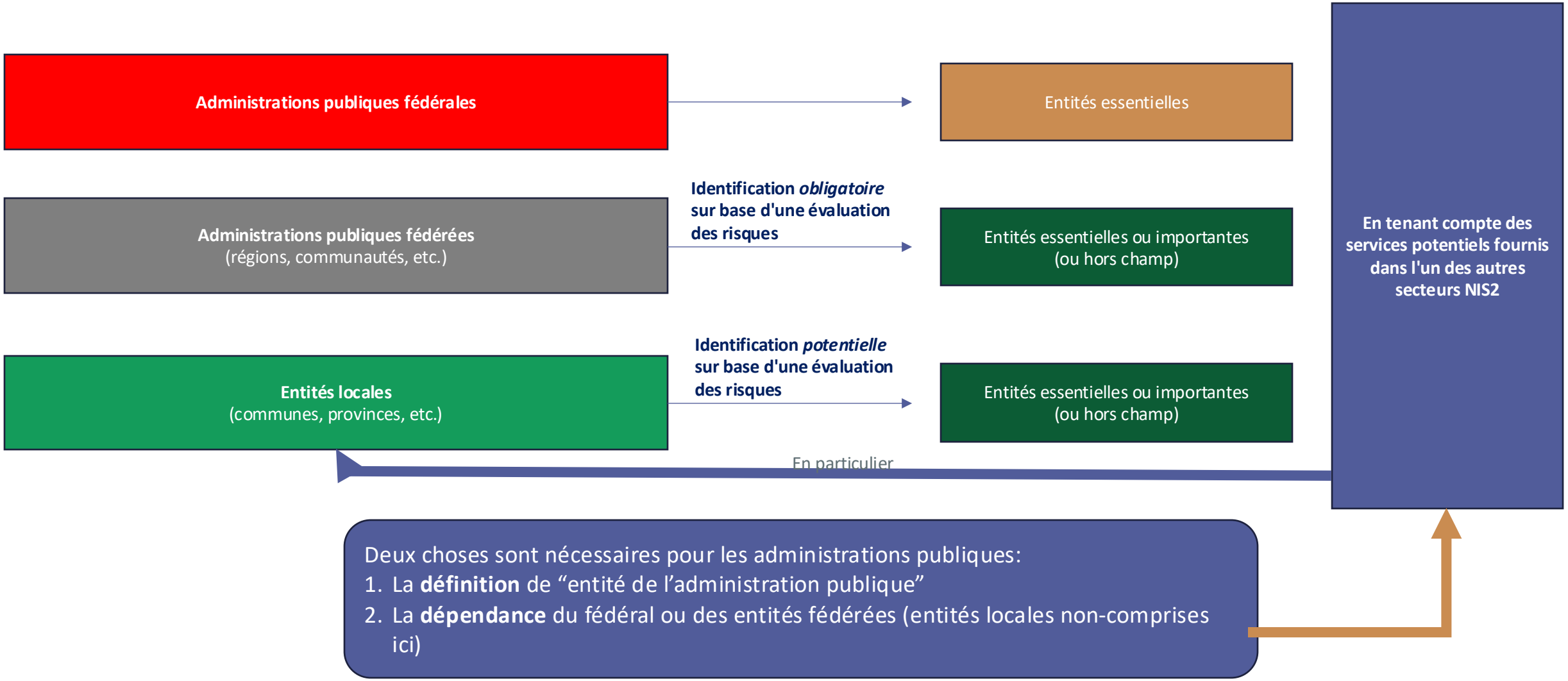
Entités importantes

Entités importantes

Entités importantes

(*) Rappel: il existe des exceptions pour lesquelles les seuils ne s'appliquent pas

Administrations publiques sous NIS2



Pas de condition de taille pour les entités **du secteur** de l'administration publique

La loi s'applique aux entités de l'administration publique, quelle que soit leur taille.
Art. 8, 34° "entité de l'administration publique" :
Une **autorité administrative** visée à l'article 14, § 1er, alinéa 1er, des lois coordonnées sur le Conseil d'État qui satisfait aux critères suivants : a) elle n'a pas de caractère industriel ou commercial ; b) elle n'exerce pas à titre principal une activité énumérée dans la colonne type d'entité d'un autre secteur ou sous-secteur de l'une des annexes de la loi ; c) elle n'est pas une personne morale de droit privé.

Annexe I - Secteurs hautement critiques
10. Administration publique

- Entités de l'administration publique qui dépendent de l'Etat fédéral.

- Entités de l'administration publique qui dépendent des entités fédérées, **identifiées** conformément à l'article 11, § 2 de la loi.

- Les zones de secours au sens de l'article 14 de la loi du 15 mai 2007 relative à la sécurité civile ou le Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale au sens de l'ordonnance du 19 juillet 1990 portant création d'un Service d'incendie et d'aide médicale urgente de la Région de Bruxelles-Capitale.

Dépendance =

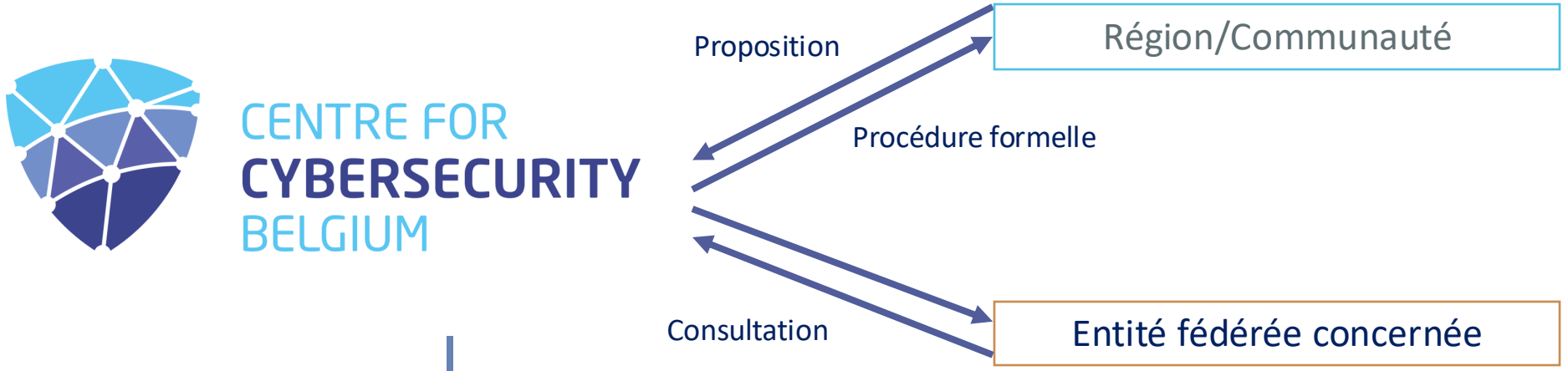
- entités qui font partie du niveau fédéral et du niveau fédéré;
- entités qui ont été créés par ces autorités publiques;
- entités dont l'activité est financée majoritairement par ces autorités publiques;
- entités dont la gestion est soumise à un contrôle de ces autorités ou organismes;
- entités dont plus de la moitié des membres de l'organe d'administration, de direction ou de surveillance sont désignés par ces autorités ou organismes.

« Il convient de préciser que les **autorités locales** (communes, provinces, intercommunales, CPAS, etc.) **ne sont pas des entités de l'administration publique qui dépendent** de l'Etat fédéral ou qui dépendent des entités fédérées » (EdM loi NIS2)

Art. 10 loi NIS2 (Identification) :

§ 2. En ce qui concerne les entités qui dépendent des entités fédérées, l'autorité nationale de cybersécurité identifie les **administrations publiques qui, à la suite d'une évaluation basée sur les risques, fournissent des services dont la perturbation pourrait avoir un impact important sur des activités sociétales ou économiques critiques.**

Processus spécifique pour les entités fédérées



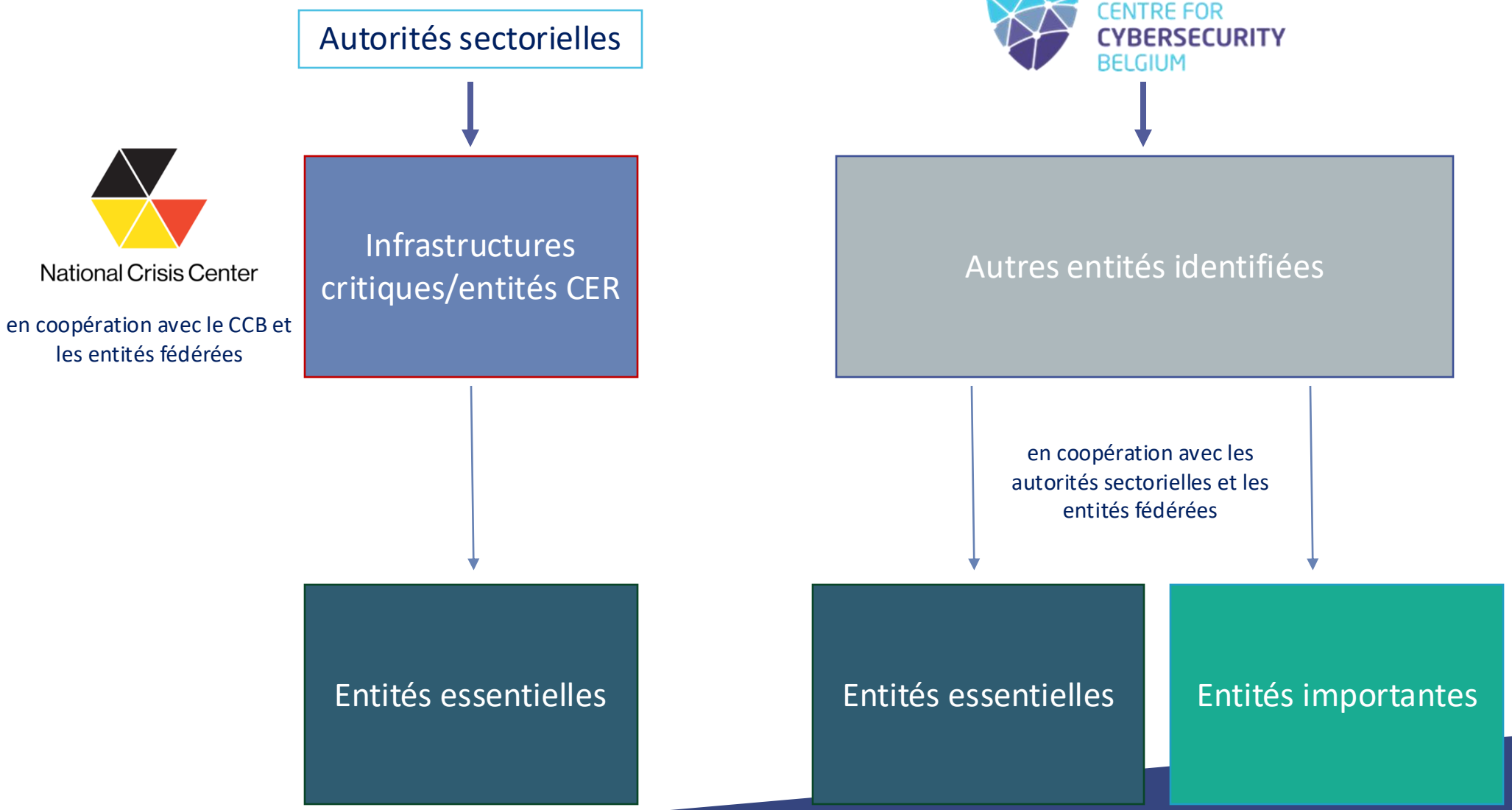
Identification basée sur l'évaluation des risques :

"Les autorités publiques [...] qui fournissent des services dont l'interruption pourrait avoir un impact significatif sur des activités sociétales ou économiques critiques". (art. 11, §2)

- Entité importante
- Entité essentielle

Identification nationale

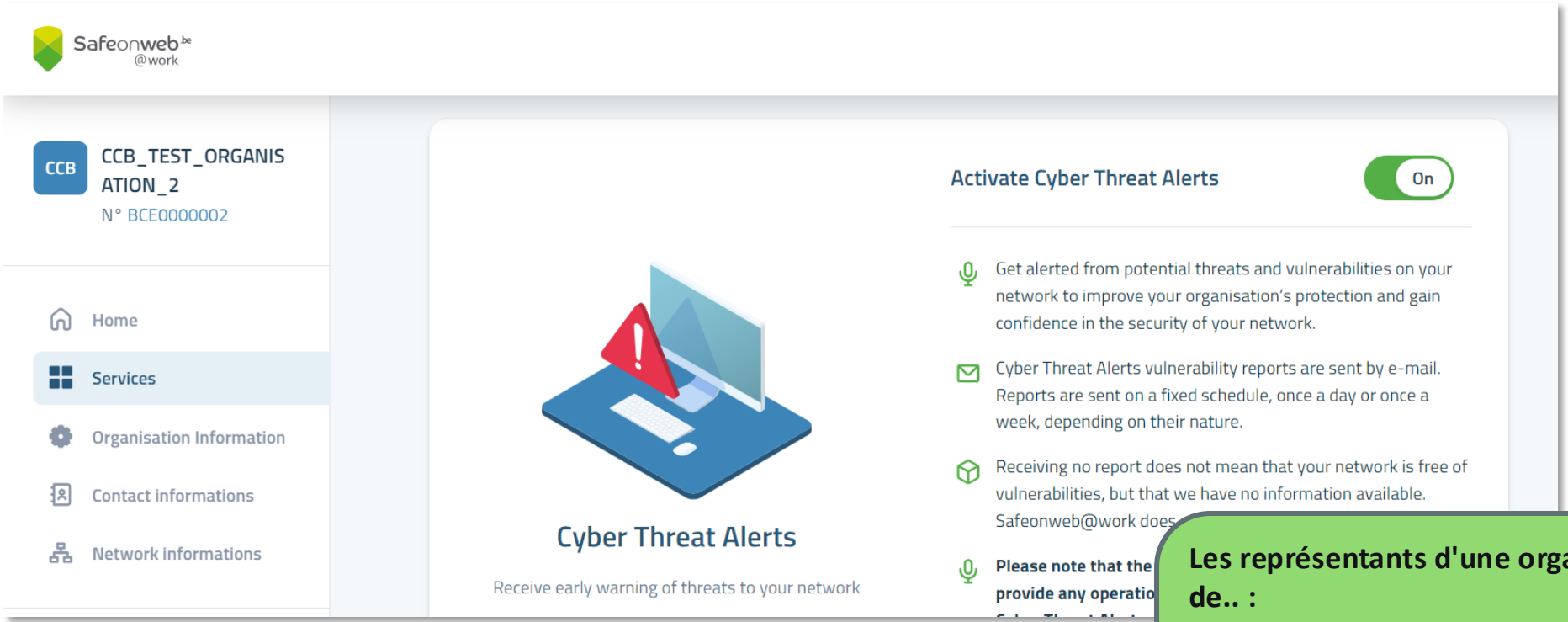
(entités n'entrant pas automatiquement dans le champ d'application)



Enregistrement obligatoire

Date limite 18 mars 2025 (la plupart des entités)

Date limite 18 décembre 2024 (certaines entités des secteurs numériques)



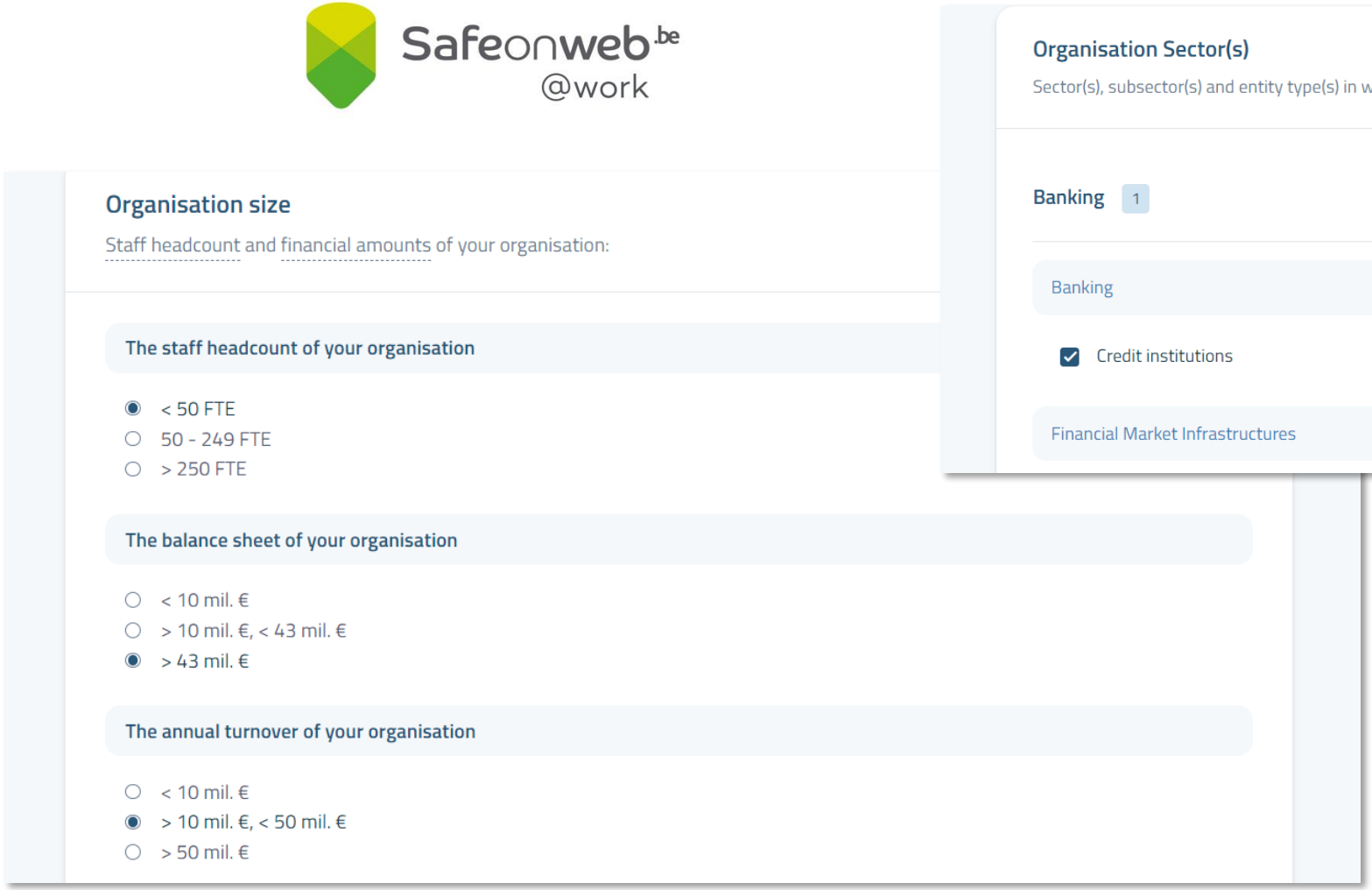
Les représentants d'une organisation seront en mesure de.. :

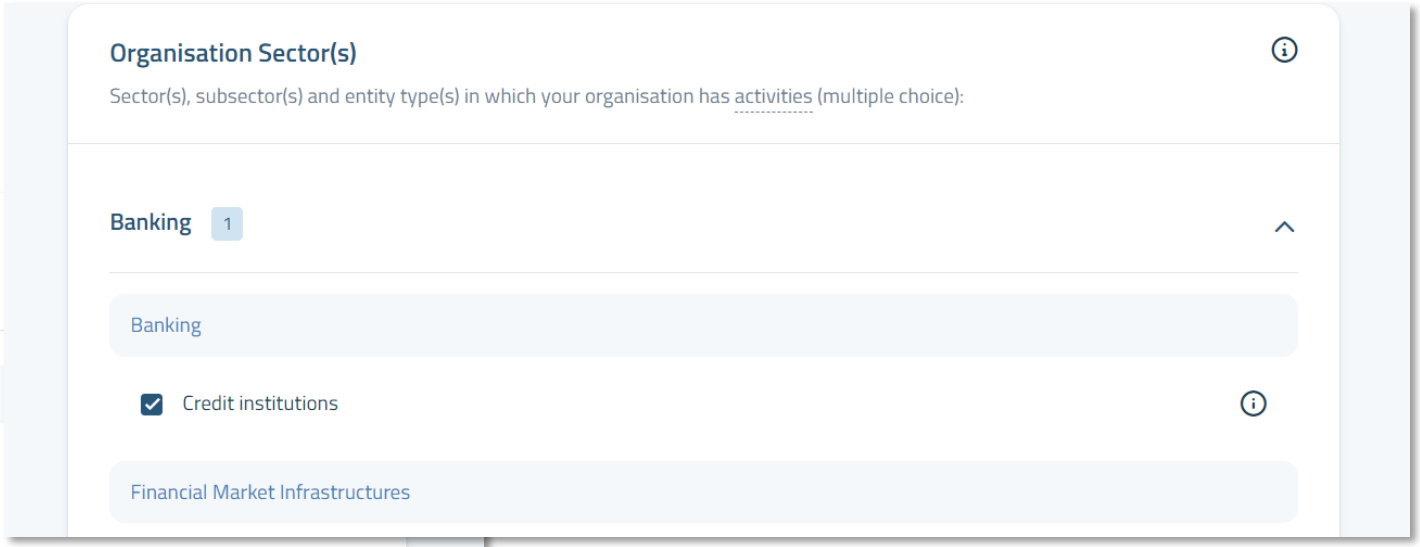
- accéder à Safeonweb@work
- enregistrer les coordonnées des personnes à contacter et les informations sur le réseau
- *s'enregistrer en tant qu'entité NIS2*
- *indiquer le/les secteur(s) d'activité*

Plateforme d'enregistrement

CENTRE FOR CYBERSECURITY BELGIUM

Safeonweb.be @work





➔ Point d'entrée unique pour l'enregistrement des entités NIS2

➔ Test de champ d'application

CENTRE FOR CYBERSECURITY BELGIUM

Autorités compétentes

02

Autorité nationale de cybersécurité

CENTRE FOR CYBERSECURITY BELGIUM

Centre pour la Cybersécurité Belgique (CCB - sous l'autorité du Premier ministre) :

Autorité compétente pour la supervision des entités essentielles et importantes

CSIRT national

Point de contact unique (SPOC) pour la mise en œuvre de la législation NIS2

Représentant BE dans le réseau CSIRT

CSIRTs NETWORK

Représentant BE au sein du groupe de coopération NIS

NIS COOPERATION GROUP

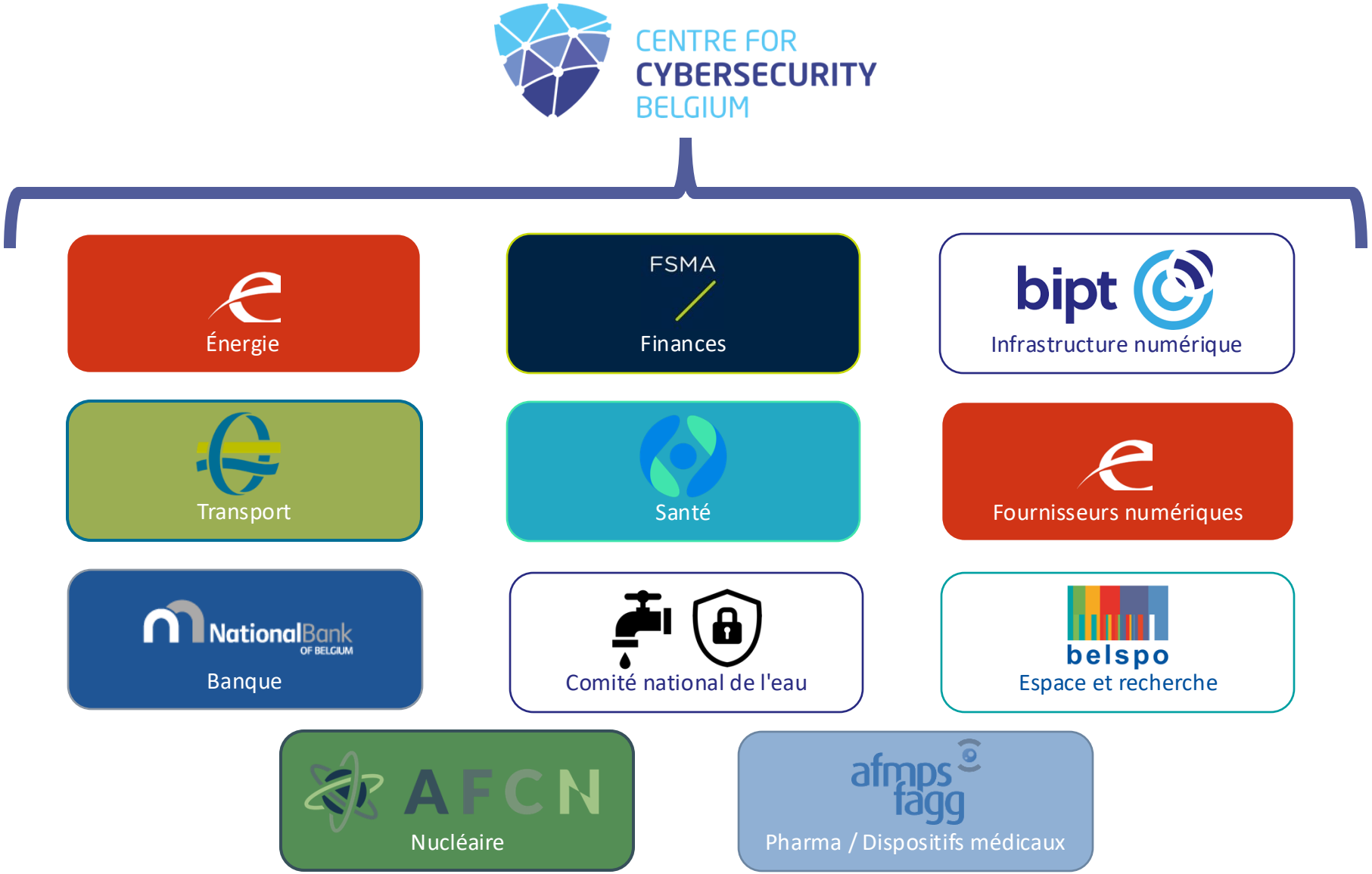
Représentant BE au sein du réseau européen des organisations de liaison en cas de crise cyber (EU-CyCLONe)

CyCLONe
European Cyber Crises Liaison Organisation Network
Powered by ENISA

Nous devons :

- Suivre et coordonner la mise en œuvre de la loi NIS2
- Contrôler la mise en œuvre du NIS2 par les entités essentielles et importantes
- Gérer les crises et les incidents liés à la cybersécurité

NIS2 Autorités sectorielles



NIS2 Autorités sectorielles : Compétences

CENTRE FOR CYBERSECURITY BELGIUM

- Identification supplémentaire
- Enregistrement des entités
- Organisation d'exercices sectoriels
- Analyse et gestion des conséquences d'un incident pour un secteur
- Participation à certains travaux du groupe de coopération NIS
- Sensibilisation des entités de leur secteur
- Coopération au niveau national
- Mesures de gestion des risques en matière de cybersécurité supplémentaires
- Notification d'incident
- Supervision et inspection
- Amendes administratives

Mesures de cybersécurité (cadres de cybersécurité/ Évaluation des risques)

03

Exigences générales en matière de cybersécurité

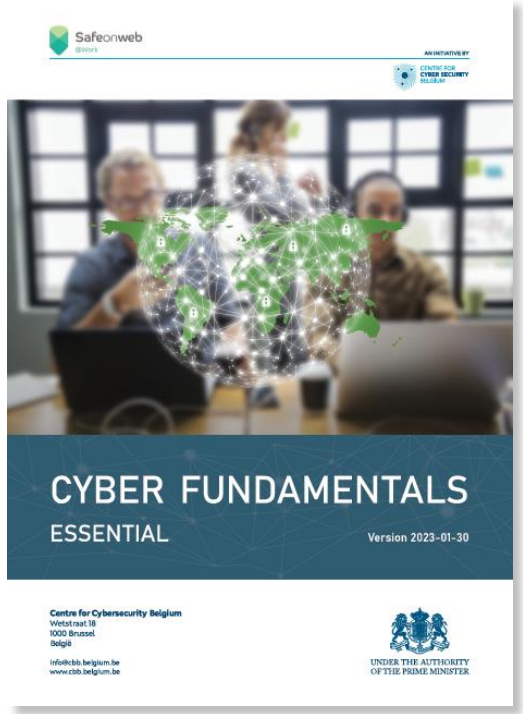
CENTRE FOR CYBERSECURITY BELGIUM

Gouvernance

Mesures de gestion des risques en matière de cybersécurité

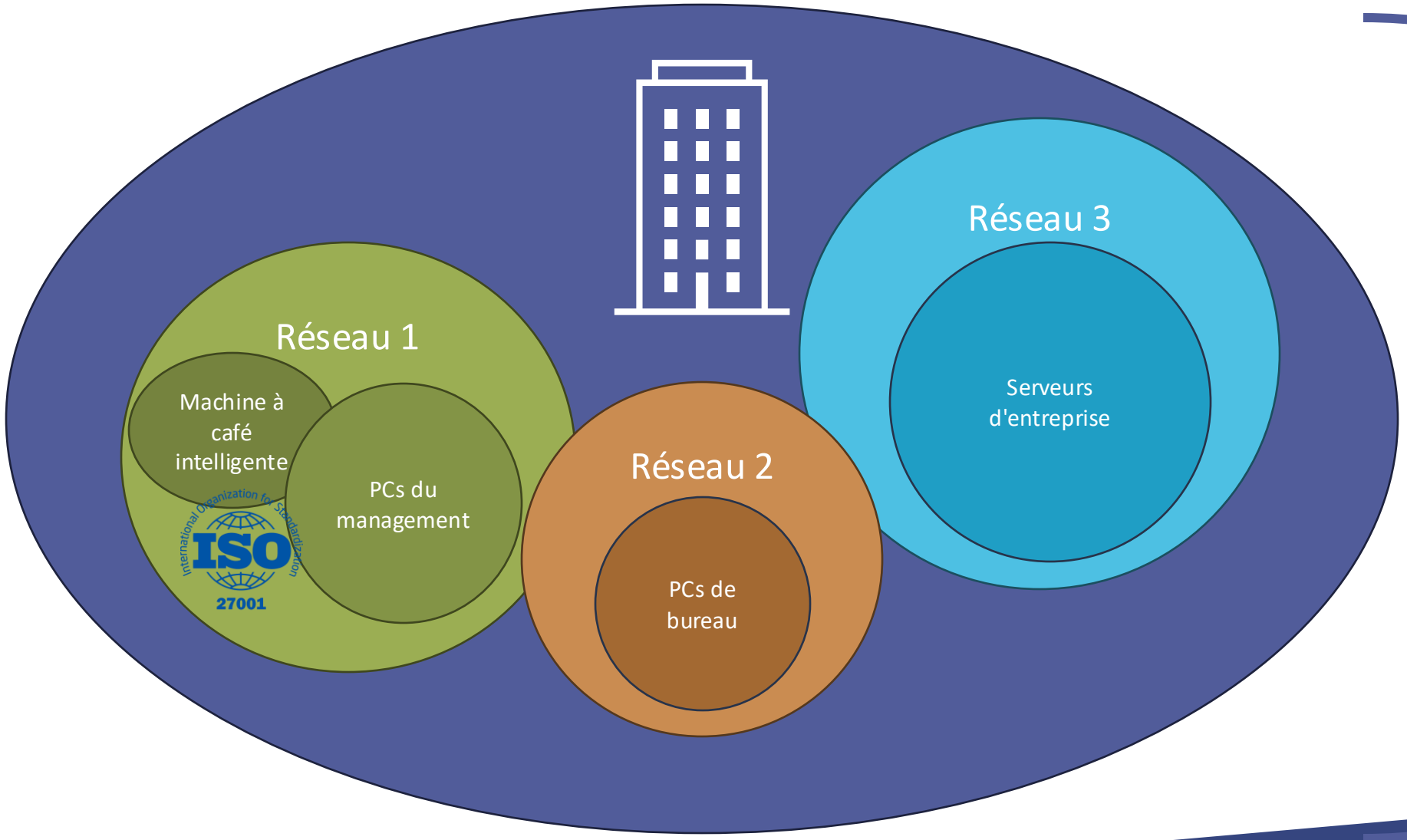
Obligation explicite d'effectuer une **analyse des risques**, d'adopter une **politique de sécurité de l'information** (PSI/IBB) et une politique de **divulgation coordonnée de vulnérabilités** (CVD)

Présomption de conformité en cas de certification CCB CyberFundamentals ou NBN ISO EN 27001 (avec champ d'application pertinent)



ISO 27001

Champ d'application des mesures



Champ d'application NIS2 = entité entière

Responsabilité des organes de direction

CENTRE FOR CYBERSECURITY BELGIUM

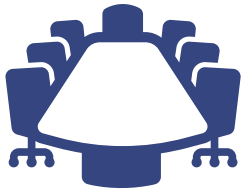
Responsabilité pour les infractions commises par leur entité

Sans préjudice des règles de responsabilité applicables aux institutions publiques, ainsi que de la responsabilité des fonctionnaires et des agents élus ou nommés.

Approuver les mesures de gestion des risques en matière de cybersécurité

Superviser la mise en œuvre des mesures

Suivre une formation et encourager ses employés à suivre une formation similaire



Caractéristiques des mesures de cybersécurité

CENTRE FOR CYBERSECURITY BELGIUM

Mesures **techniques, opérationnelles et organisationnelles**

Appropriées et proportionnées

Gérer les risques qui pèsent sur la sécurité des réseaux et des systèmes d'information que ces **entités utilisent pour leurs activités ou pour la fourniture de leurs services**.

Prévenir ou minimiser l'impact des incidents sur les bénéficiaires de leurs services et sur d'autres services

Tenir compte du **coût de la mise en œuvre**

L'état de l'art et, le cas échéant, les **normes** européennes et internationales pertinentes

Proportionnalité : degré d'exposition de l'entité aux **risques**, sa taille, la probabilité de survenance d'incidents et leur gravité, y compris leur impact sociétal et économique.

Évaluation des risques

=> Adapté à la situation concrète de l'entité NIS2

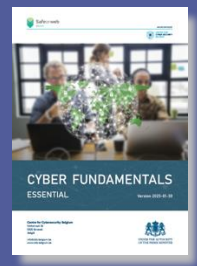
CENTRE FOR CYBERSECURITY BELGIUM

LES MESURES DE CYBERSÉCURITÉ À METTRE EN OEUVRE

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

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

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



ISO 27001

La chaîne d'approvisionnement

CENTRE FOR CYBERSECURITY BELGIUM

Entité NIS2

- Imposer des mesures de gestion des risques en matière de cybersécurité
- Contrôle du respect des mesures

Prendre des mesures de gestion des risques en matière de cybersécurité appropriées et proportionnées.

Fournisseur direct
Prestataire de services

Entité potentiellement non NIS2

La loi NIS2 fait de la sécurité de la chaîne d'approvisionnement une mesure de gestion des risques de cybersécurité minimale, mais ne précise pas comment y parvenir.

Le CCB recommande l'utilisation du CyberFundamentals Framework (CyFun®).

CENTRE FOR CYBERSECURITY BELGIUM

Évaluation périodique de la conformité
Évaluation des risques

Cadres de référence pour l'évaluation de la conformité

Les entités essentielles *se soumettent* à une évaluation périodique de la conformité

Obligatoire

- CyberFundamentals (CyFun®)
- ISO 27001
- Inspection du CCB

Les entités importantes *peuvent* se soumettre à une évaluation périodique de la conformité

Volontaire

- CyberFundamntals (CyFun®)
- ISO 27001

Évaluation de la conformité par un organisme d'évaluation de la conformité (CAB) **accrédité et autorisé** par le CCB

Évaluation des risques spécifiques

L'évaluation des risques est **obligatoire.**

L'évaluation des risques est **au cœur du CyberFundamentals Framework**

BASE - ID.GV-4.1 : Dans le cadre de la gestion globale des risques de l'entreprise, une *stratégie globale de gestion des risques* liés à la sécurité de l'information et à la cybersécurité est élaborée et mise à jour en cas de changement.

BASE - ID.RA-5.1 : L'organisme doit procéder à des *évaluations des risques* dans lesquelles le risque est déterminé par les menaces, les vulnérabilités et l'impact sur les processus et les actifs de l'entreprise.

Aucune méthodologie spécifique n'est imposée pour l'évaluation des risques.

Évaluation du risque par défaut du CCB

Évaluation du risque par défaut par secteur et par taille ➔ niveau approprié CyFun®

CENTRE FOR CYBERSECURITY BELGIUM

Version: 2023-08-03

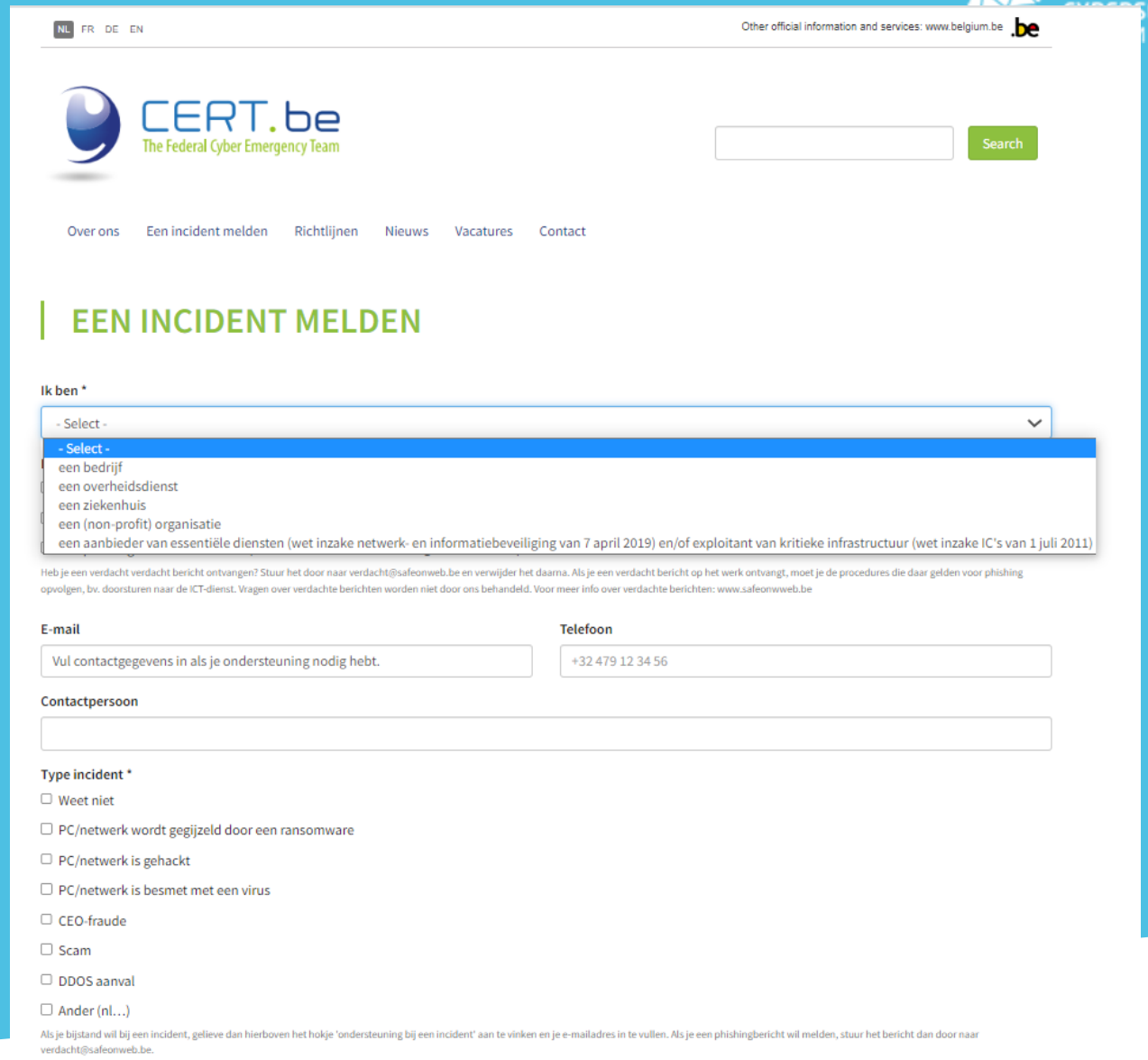
Energy			*Common skills*		*Common skills*		*Common skills*		*Extended Skills*		*Extended Skills*	
Organization Size (L/M/S = 3/2/1)	**3**	*Threat Actor Type*	**Competitors**		**Ideologues Hactivists**		**Terrorist**		**Cyber Criminals**		**Nation State actor**	
Cyber Attack Category	*Global or Targetted*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

Score	CyFun Level
285	**ESSENTIAL**

https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework/choosing-right-cyber-fundamentals-assurance-level-your-organisation

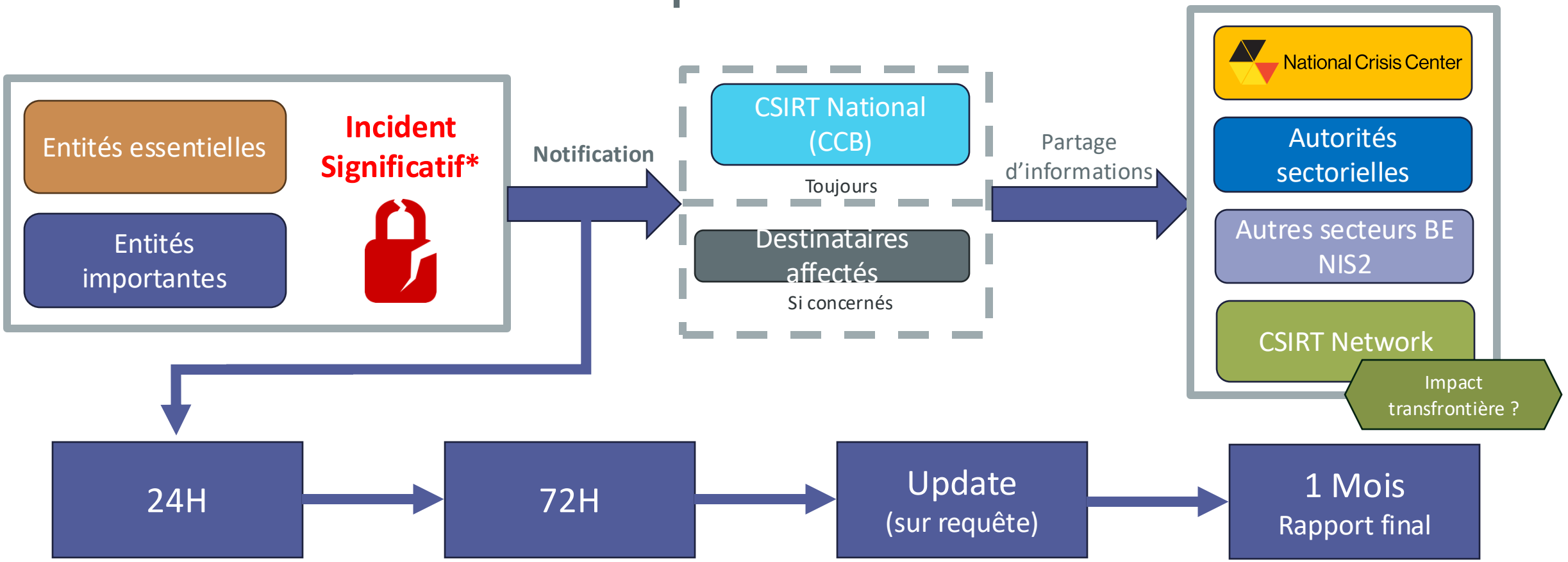
Notification d'incident

04



NB: Les délais sont des délais maximums. En principe, les notifications se font “sans retard injustifié”

Notification - Etapes et délais



Alerte précoce via notification écrite en ligne + info sur potentielle nature malveillante/illicite **+ potentiel impact transfrontière**

- **Evaluation initiale de l’incident**, sa gravité, son impact, si possible, des indicateurs de compromission
- **Mise à jour des informations fournies dans les 24h**

- **description détaillée** de l’incident, sa gravité et son impact
- **type de menace ou cause profonde** qui a probablement déclenché l’incident
- **mesures d’atténuation** appliquées et en cours
- impact transfrontière de l’incident

* susceptibles d'affecter négativement la fourniture de ses services NIS2.

Incident significatif sur les services fournis

"incident" : tout événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles

Un incident est considéré comme **significatif** si :

(a) Il a causé ou est susceptible de causer une perturbation opérationnelle grave de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II ou des pertes financières pour l'entité concernée **ou**;

(b) Il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables

NIS COOPERATION GROUP

Guidance du NIS CG & CCB (à venir)

CENTRE FOR CYBERSECURITY BELGIUM

Supervision

05

Supervision des entités NIS2

Entités importantes

Supervision *ex post* : après un incident ou si une suspicion de possibles manquements

Entités essentielles

Supervision *ex post* et *ex ante*

Mesures de supervision :
- Inspections sur place et à distance
- Audits ad hoc
- Analyses de sécurité
- Demandes d'informations et de preuves

Évaluation régulière et volontaire de la conformité selon CyFun® ou ISO 27001

Évaluation régulière et obligatoire de la conformité selon CyFun® ou ISO 27001, ou inspection obligatoire

Évaluation régulière de la conformité

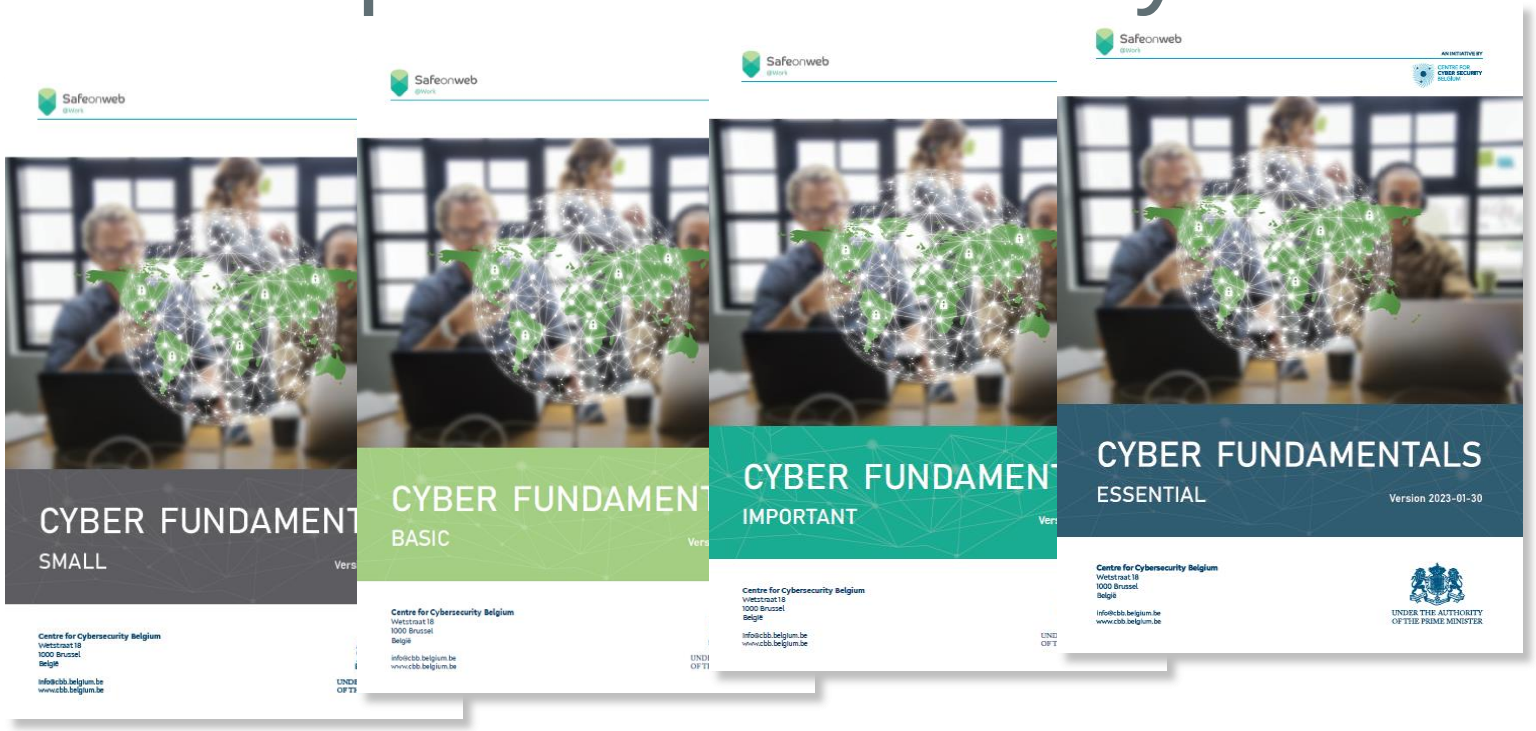
Certification/Vérification : CyberFundamentals par un CAB autorisé (avec le champ d'application pertinent) CyFun®	Exigences sectorielles supplémentaires
Certification : ISO 27001 par un CAB autorisé (avec le champ d'application et statement of applicability pertinent)	Exigences sectorielles supplémentaires
Inspection obligatoire par le CCB (avec retributions à payer pour l'entité)	Exigences sectorielles supplémentaires

Présomption de conformité

CENTRE FOR CYBERSECURITY BELGIUM

Évaluation de la conformité basée sur les CyberFundamentals

Supervision sous CyFun®



Agrément

Accréditation

Organe d'évaluation de la conformité

Certificat et/ou label

Vue d'ensemble CyberFundamentals

	BASIC	IMPORTANT	ESSENTIAL
Type d'évaluation	Vérification	Vérification	Certification
Comment l'évaluation est-elle effectuée ?	Vérification de l'auto-évaluation	Vérification de l'auto-évaluation	Audit de certification basé sur l'auto-évaluation
Évaluation réalisée par	CAB **accrédité** et **agréé**	CAB **accrédité** et **agréé**	CAB **accrédité** et **agréé**
Résultat de l'assurance	Verified Claim	Verified Claim	Certificat
Label (accordé par l'autorité de certification CCB)			

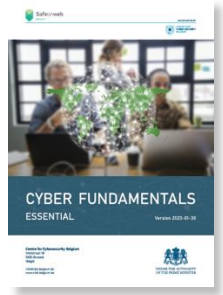
Le rapport d'auto-évaluation CyberFundamentals (Toolbox CyFun®) est la clé (d'entrée) du processus d'évaluation de la conformité.

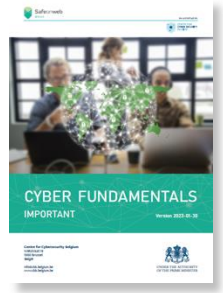
Proportionnalité - Niveaux d'assurance basés sur l'outil d'évaluation des risques CyFun

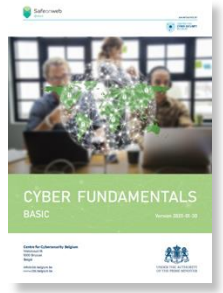
CENTRE FOR CYBERSECURITY BELGIUM

Entités essentielles

Entités importantes







CENTRE FOR CYBERSECURITY BELGIUM

Version: 2023-08-03

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

Score	CyFun Level
285	ESSENTIAL

Champ d'application des évaluations de la conformité

Champ d'application = L'organisation dans son **ensemble**

➔ Sauf si les environnements IT/OT sont physiquement et/ou techniquement séparés

➔ A réaliser de manière à ce que les environnements hors périmètre n'influencent pas les risques de l'environnement dans le périmètre.

➔ A préciser dans le champ d'application de l'évaluation de la conformité

Exclusions *motivées*

BASIC ➔ Maximum 1 mesure CyberFundamentals

IMPORTANT ➔ Maximum 3 mesures CyberFundamentals

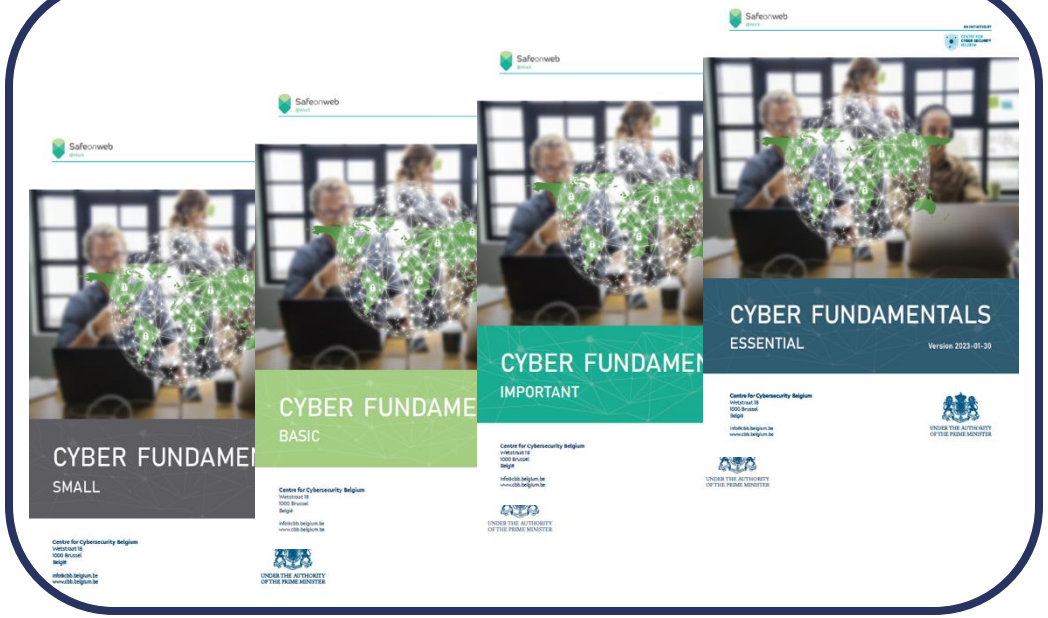
ESSENTIA ➔ Maximum 5 mesures CyberFundamentals

Les mesures clés ne peuvent être exclues

Les mesures liées aux aspects de gestion ne peuvent pas être exclues

L'écosystème CyberFundamentals

CENTRE FOR CYBERSECURITY BELGIUM



CyberFundamentals Conformity Assessment Scheme
Régime d'aide pour les CAB

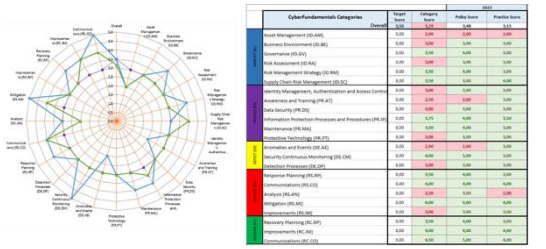
Labels CyberFundamentals

CyFun®
Tableau de concordance

CyFun®
Outil de sélection (risk assessment)

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

CyFun ®
Outil d'auto-évaluation



CyFun® BASIC
Modèles de politiques

La boîte à outils CyberFundamentals est **accessible au public** à l'adresse suivante : ➔ **www.cyfun.eu**

CENTRE FOR CYBERSECURITY BELGIUM

Sanctions

Mesures d'exécution et amendes

Émettre des **avertissements** ou des **instructions contraignantes**		Ordre de **mettre fin à un comportement** ou de mettre en conformité les **mesures de gestion des risques** ou les obligations de déclaration	Ordre d'**informer** la (les) personne(s) physique(s) ou morale(s) à laquelle (auxquelles) ils fournissent des services ou de **rendre publics des** aspects de non-conformité
Désigner un **responsable du suivi**	Ordre de **mise en œuvre des recommandations** fournies	Temp. **suspendre une certification ou une autorisation** concernant une partie ou la totalité des services pertinents fournis par l'entité essentielle	**Interdire** temporairement **l'exercice des fonctions de direction (PDG/Représentant légal)**

500 à 125 000 € pour non-respect des obligations d'information prévues à l'article 12 (processus d'identification)

500 à 200 000 € pour les sanctions à l'encontre d'un membre du personnel d'une entité

5 to la [**entités importantes**].

à 10 000 000 € ou 2 % du chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent par l'entreprise à laquelle l'entité appartient, le montant le plus élevé étant retenu [**entités essentielles**].

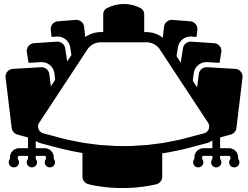
Les amendes administratives ne sont pas applicables pour les entités actives dans le secteur de l'administration publique de l'annexe I.

Mesures administratives spécifiques

Si les mesures correctives demandées ne sont pas prises par une entité essentielle dans le délai fixé, le service d'inspection peut :

a) demander la *suspension temporaire d'une certification ou d'une autorisation* concernant tout ou partie des services pertinents fournis ou des activités menées par l'entité essentielle ;

b) demander d'*interdire temporairement à toute personne physique chargée d'exercer des responsabilités de direction* au niveau du directeur général ou du représentant légal dans l'entité essentielle d'exercer des fonctions de direction dans cette entité.



Sans préjudice des règles de responsabilité applicables aux institutions publiques, ainsi que de la responsabilité des fonctionnaires et des agents élus ou nommés.

Prochaines étapes / Q/A
06

Entrée en vigueur des obligations NIS2 pour les entités importantes et essentielles

Toutes les obligations du NIS2 (loi et arrêté royal) commenceraient à s'appliquer à partir du 18 octobre 2024* :

- Mesures de cybersécurité
- Notification d'incident
- Supervision éventuelle (avec une ligne du temps spécifique pour les premières évaluations périodiques de la conformité pour les entités essentielles - voir diapositive suivante)
- Etc.

* à confirmer (en cas d'identification formelle, le délai commence à courir à partir de la notification de la décision administrative)

Ligne du temps de la mise en œuvre *entités essentielles*

CENTRE FOR CYBERSECURITY BELGIUM

2024				2025																				2026												2027			
Jun	Jul	Août	Sep	**Oct**	Nov	**Déc**	Jan	Fév	**Mar**	Apr	Mai	Jun	Jul	Août	Sep	Oct	Nov	Déc	Jan	Fév	Mar	**Avr**	Mai	Jun	Jul	Août	Sep	Oct	Nov	Déc	Jan	Fév	Mar	**Avr**
				18		18			18													18												18

Date limite enregistrement général*

Sur Safeonweb@work

Date limite enregistrement secteur numérique*

*en cas d'identification formelle, le délai commence à courir à partir de la notification de la décision administrative

Mesures de sécurité et notification des incidents

Mesures de gestion des risques en matière de cybersécurité
Notification obligatoire des incidents significatifs
Notification volontaire d'autres incidents, de cybermenaces

Amélioration des mesures à la suite d'incidents
Formation à la cybersécurité

Mise en œuvre et supervision progressives

- Choisissez votre cadre
- Commencer à mettre en œuvre ou à compléter des mesures de cybersécurité

CYBER FUNDAMENTALS ESSENTIAL Version 2023-01-30
CYBER FUNDAMENTALS IMPORTANT Version 2023-01-30
CYBER FUNDAMENTALS BASIC Version 2023-01-30

ISO 27001

Obtenir le label CyFun Basic ou Important (ou inspection équivalente)

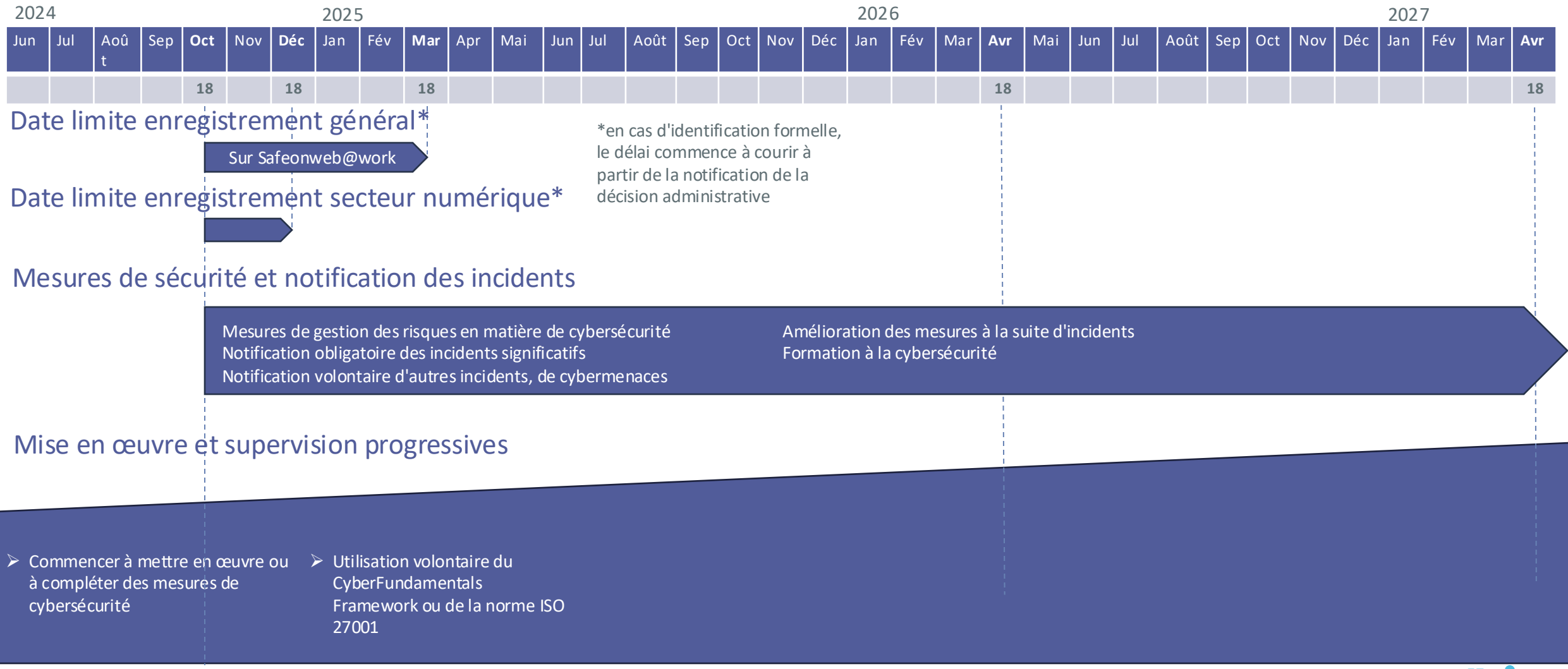
CyFun BASIC Verified
CyFun IMPORTANT Verified

Obtenir le label CyFun Essential (ou inspection équivalente)

CyFun BASIC Verified
CyFun IMPORTANT Verified
CyFun ESSENTIAL Certified

Ligne du temps de la mise en œuvre *entités importantes*

CENTRE FOR CYBERSECURITY BELGIUM



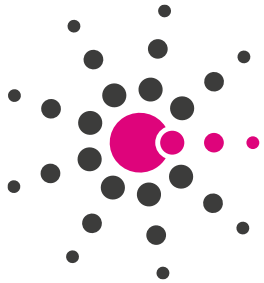
CENTRE FOR
CYBERSECURITY
BELGIUM

NIS Team CCB
nis@ccb.belgium.be

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be



iMio

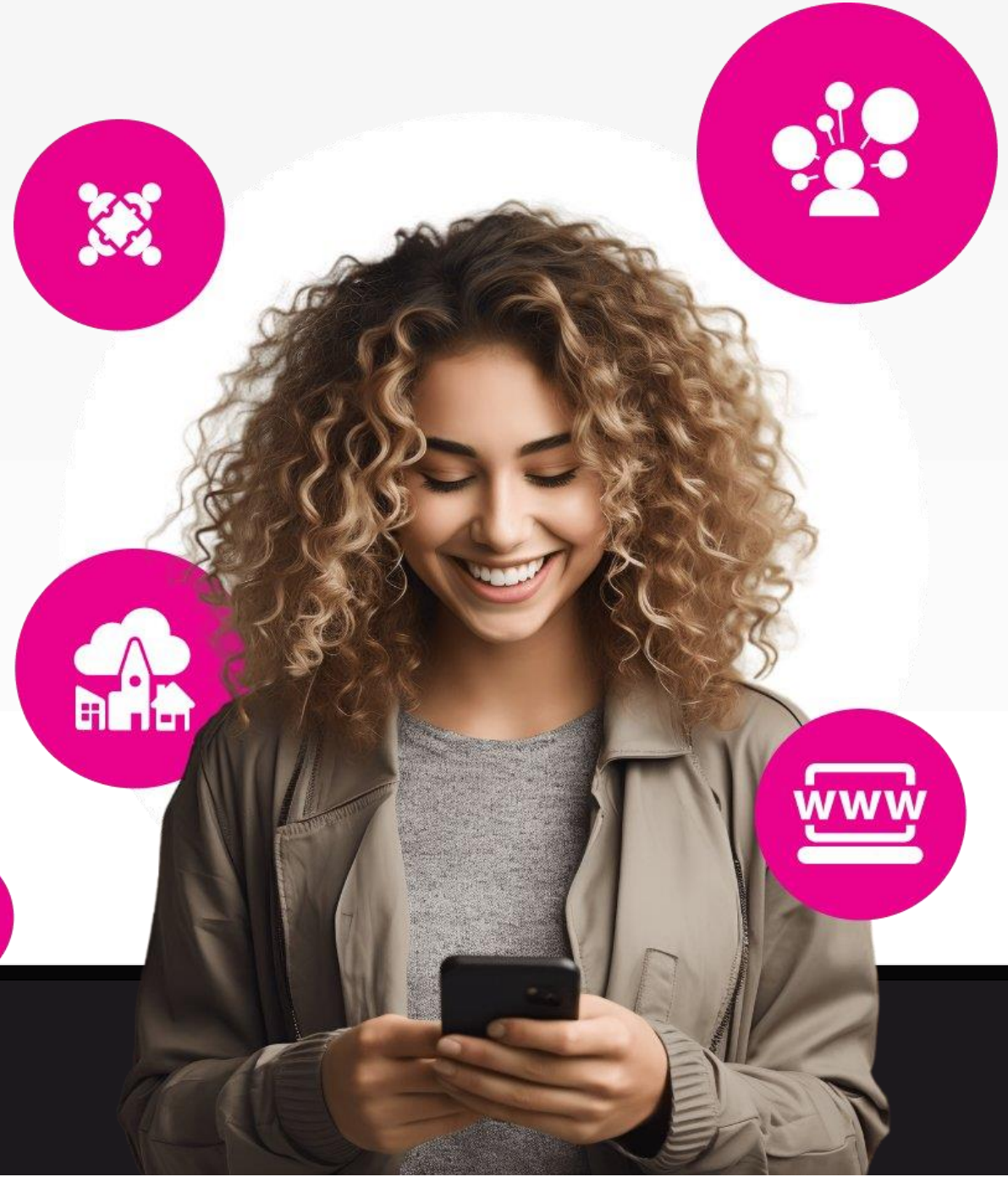
Joël Lambillotte

Directeur Général Adjoint, iMio

Cyberwal
by digital
wallonia

Programme de Bug Bounty

15 octobre 2024



iMio

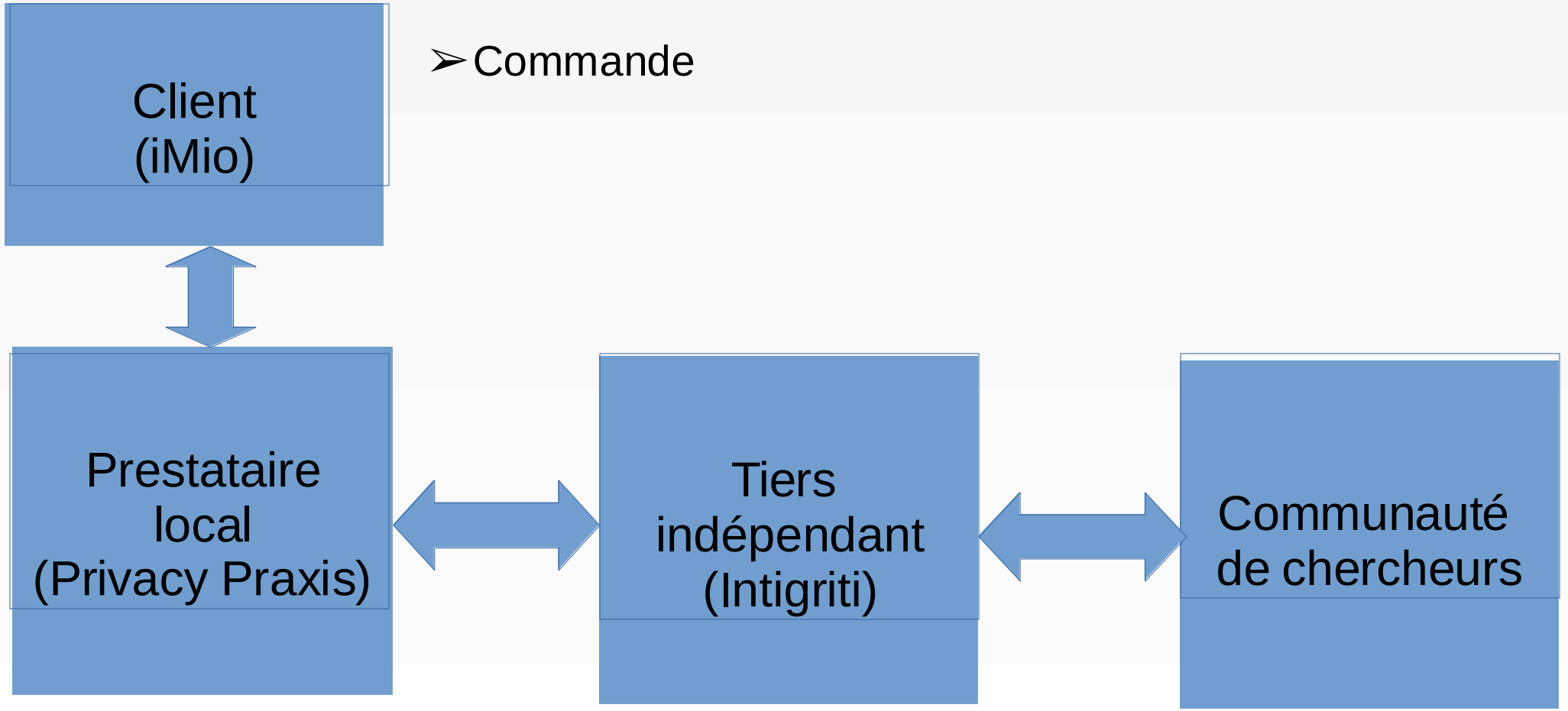
Présentation générale

- **Un programme Bug Bounty** permet de détecter de manière proactive les vulnérabilités et d'améliorer la sécurité des applications web critiques.
- Un **espace test d'une application est mis à disposition de hackers éthiques.**
  Les hackers trouvent des faiblesses et des bugs.
  Ils reçoivent des récompenses proportionnelles à leurs découvertes.
- Une équipe **analyse et valide ou refuse les vulnérabilités.**
  Elle fournit un **rapport** de chaque vulnérabilité trouvée.

Pen Test VS Bug Bounty

	Pen-Test	Bug Bounty
Resources	Une équipe	Plusieurs dizaines d'individus
Méthodologie	Cadré par le client	Encourage la créativité
Durée du test	1 semaine	Répétitif
Facturation	Sur la durée	Sur la durée et les résultats obtenus
Expertise	Limitée à l'équipe	Profils variés
Cible	Infrastructure locale Applications web	Applications web

Acteurs



➢ Commande

➢ Validation

➢ Triage
➢ Qualification

➢ Découverte de failles
➢ Reproduction

Difficultés du bug bounty pour un marché public

- Difficulté d'alignement au fonctionnement de structures internationales
  - Risque d'incompatibilité entre le contrat « standard » et le cahier des charges
  - Modèle financier imposé (location plateforme, facturation, …)
  - Formation imposée pour utiliser la plateforme

→Intervention d'un acteur local (Privacy Praxis) qui a fourni une offre

Difficultés du bug bounty pour un marché public

- Le marché impose
  - Une limite budgétaire
  - Un délai
  - Des critères sur les CV (non connus!)

→ Mise en place d'un programme hybride :

- Rémunération des failles découvertes
- Budget fixé à l'avance

- Programme fonctionnant sous forme de campagnes ponctuelles
- Tarification à la découverte d'une vulnérabilité
- Tests en "grey box"
- Norme CVSS, cadre OWASP
- Certifications (CEH,…)

Poste du cahier des charges	Quantité	
Licence/accès à la plateforme	1	
Vulnérabilité faible	80	
Vulnérabilité moyenne	40	
Vulnérabilité haute	20	
Vulnérabilité critique	5	

Restrictions

- L'installation de logiciels malveillants (virus, vers, chevaux de Troie, etc.).
- Des attaques par déni de service (DdoS).
- Des manœuvres d'ingénierie sociale (social engineering).
- Des tentatives de hameçonnage (phishing).
- L'envoi de courriels indésirables (spam).
- La suppression de données du système informatique.
- La provocation de dommages aux systèmes ou aux données.
- Toute autre infraction (par exemple cambriolage, vol, agression, etc.).

Exemple

Program name	iMio Bug Bounty
Code	XXXXXXX

Specifications

Severity	Medium
CVSS score	6.5
CVSS vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

ATTACK VECTOR (AV)	Network
ATTACK COMPLEXITY (AC)	Low
PRIVILEGES REQUIRED (PR)	None
USER INTERACTION (UI)	None
SCOPE (S)	Unchanged
CONFIDENTIALITY (C)	Low
INTEGRITY (I)	Low
AVAILABILITY (A)	None

Domain type	URL
Domain	https://XXXXX.imio-test.be/
Tier	Tier 2
Endpoint / Vulnerable component	XXXXX.imio-test.be/

Exemple

Impact

It is possible to execute arbitrary JS in a victim's browser if she accesses the history of a document with the XSS payload.

Recommended solution

Sanitize the input or encode the ouput in the history section.

Exemple

Messages

YYYYYYY has created the submission
29/08/2024 13:30:48 — EVERYONE

XXXXX has assigned the submission to XXXX
03/09/2024 09:41:06 — INTERNAL

XXXXXXX has changed the severity from High to Medium
03/09/2024 12:46:32 — EVERYONE

[triage]
03/09/2024 12:47:45 — EVERYONE

Dear @YYYYYY,

First of all, thank you for your submission and the time you are making to look into the security of our programs.

We were able to reproduce your proof of concept and will forward your report.

Métriques

- 9 applications testées
- Budget de 107.000 euros TVAC
- Campagne de 2 mois (fin août→fin octobre) Disponibilité
- de la plateforme : 1 an
- Relevés après 1 mois :
  - Low 7
  - Medium 17
  - High 2
  - Critical 3

Premières conclusions

+ Réactivité
+ Diversité des tests et profils des testers
+ Possibilité de faire une pause pour corriger et relancer le bug bounty
+ Vérification par des tiers
+ Possibilité “hybride”

- Marché public complexe à gérer
- Peu de marge de négociation
- Adapté aux grands comptes

SIAPARTNERS

Démo : Utilisation d'un simulateur numérique pour mener une cyber-attaque sur une entité publique virtuelle

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.

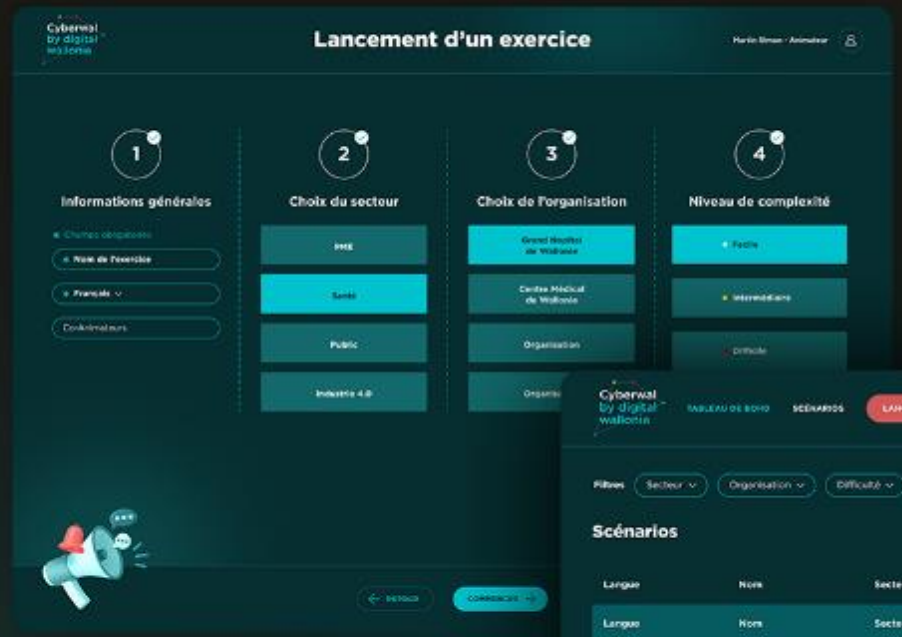
Realistic Cyber Attacks
The scenarios feature a range of proven cyber attacks grounded in real-world experiences.

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.

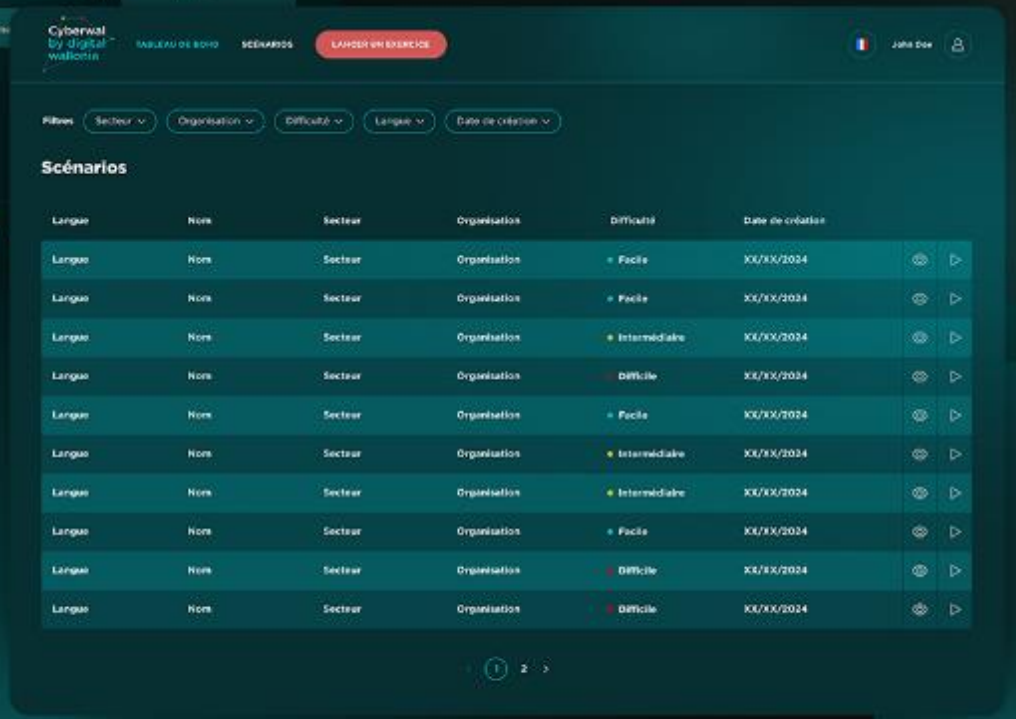

Cyberwal
by digital
wallonia
ANIMATEUR
PARTICIPANT
Identifiant
Mot de passe
Mot de passe oublié ?
Connexion
Se connecter avec
LA SENSIBILISATION SUR LA
cybersécurité pour
la Wallonie
Powered by SIAPARTNERS


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

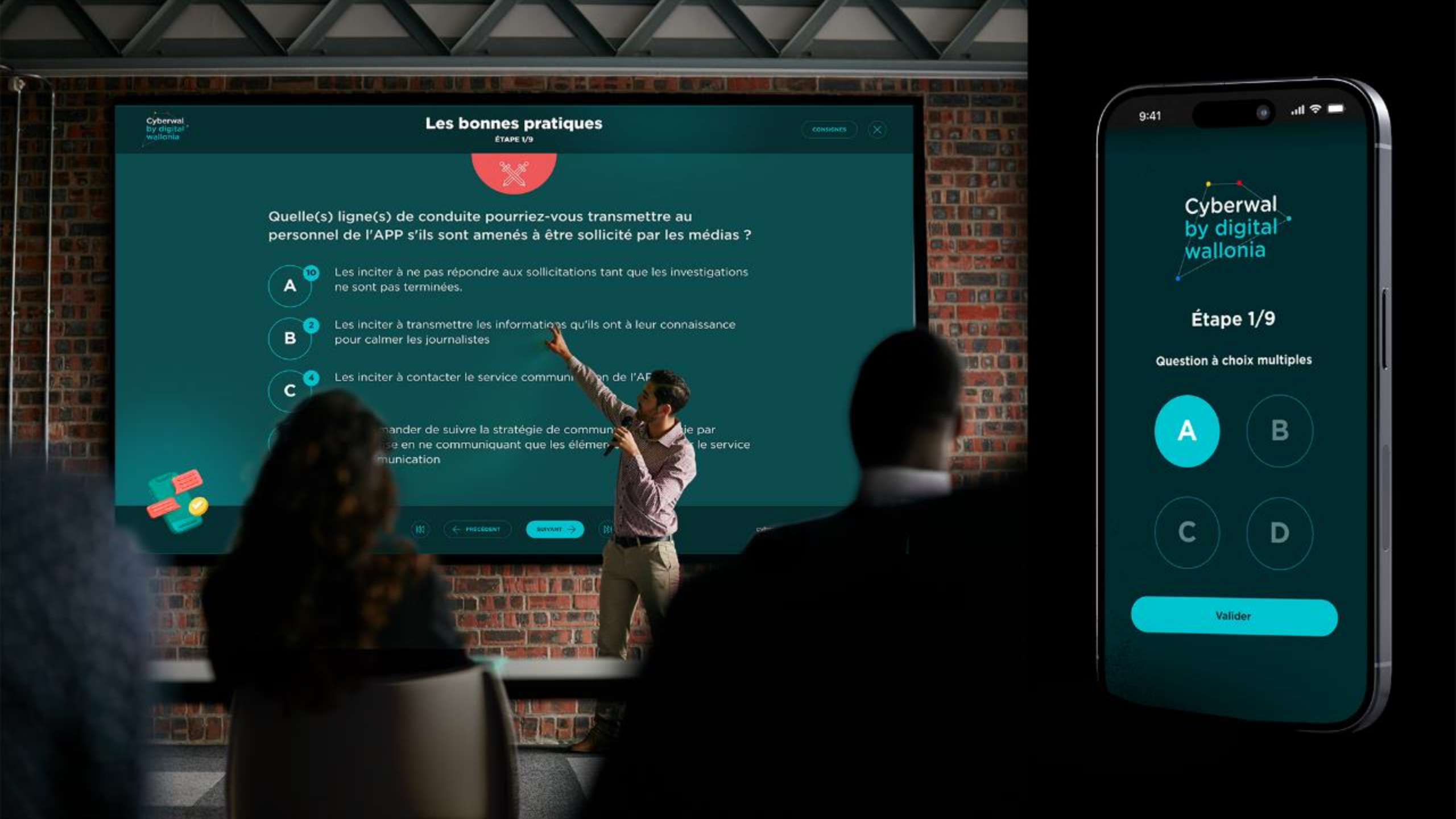

Cyberwal by digital wallonia
LA SENSIBILISATION SUR LA
cybersécurité pour la Wallonie
ANIMATEUR
PARTICIPANT
Code de la session
Accéder
Powered by SIAPARTNERS


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

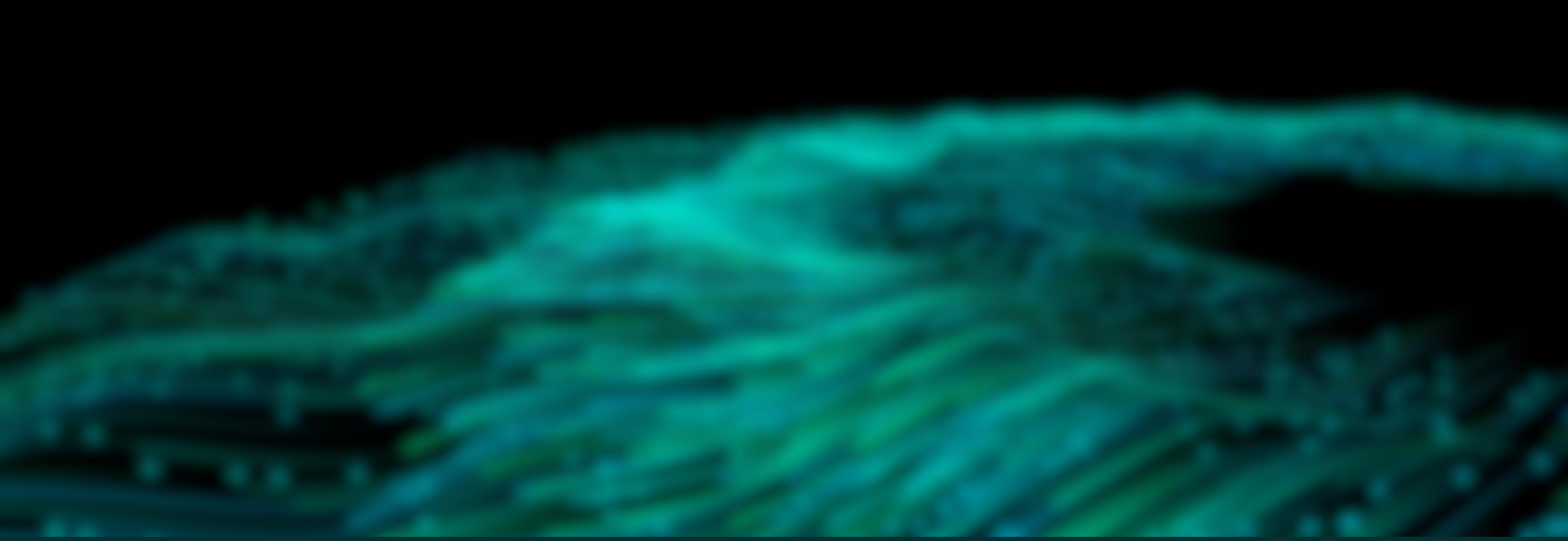
Score

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

Les conférences reprendront dans 10 minutes.

Cyberwal
by digital
wallonia

CENTRE FOR
CYBERSECURITY
BELGIUM

Phédra Clouner

Directrice adjointe, Centre for Cybersecurity Belgium (CCB)

Cyberwal
by digital
wallonia

ACTIVE CYBER PROTECTION - UNE APPROCHE BELGE, MAIS PAS QUE, DE LA CYBERSÉCURITÉ

Phédra Clouner, Directrice générale adjointe

Cyberweek- 15/10/2024

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

CENTRE FOR CYBERSECURITY BELGIUM

1 The CCB : Who are we?

2 Our approach: Active Cyber Protection

CENTRE FOR CYBERSECURITY BELGIUM

THE CENTRE FOR CYBERSECURITY BELGIUM

The national cybersecurity agency

CENTRE FOR CYBERSECURITY BELGIUM

A government body operating under the authority of the Prime Minister:

- Created in **2014** by Royal Decree
- Acts as Computer Security Incident Response Team (**CSIRT/CERT**)
- Coordinates the implementation of the **National Cybersecurity Strategy**
- Competent authority for coordinating the implementation of the **NIS2 Directive** on the cybersecurity of important and essential entities.

But also:

- The **National Coordination Centre** (NCC-BE) tasked with centralising EU and national funding opportunities to support investments in cybersecurity projects since 2021,
- The **National Cybersecurity Certification Authority** (NCCA) in the context of European certification schemes since 2022.

Our legal mission

CENTRE FOR CYBERSECURITY BELGIUM

High-level mission: Make Belgium one of the least vulnerable countries in the cyber domain

A coordination role at strategic level…

- Drafting the National Cybersecurity Strategy in cooperation with other government departments
- Coordinating implementation of the Strategy at national level
- Supporting national crisis management for cyber aspects
- Monitoring and updating the legal framework on cybersecurity
- Representing Belgium in international cybersecurity forums

... and at operational level

- Issuing alerts and advisories on the latest cyber threats
- Monitoring notifications and reports of cyber incidents at national and international level
- Supporting organisations in responding to cyber incidents
- Developing standards and practical guides on cyber security, etc.

Our constituents

CENTRE FOR CYBERSECURITY BELGIUM

The population as a whole:
Educate & involve individuals in their own security

@Home

@Work

Organisations:
Large companies, SMEs, associations…

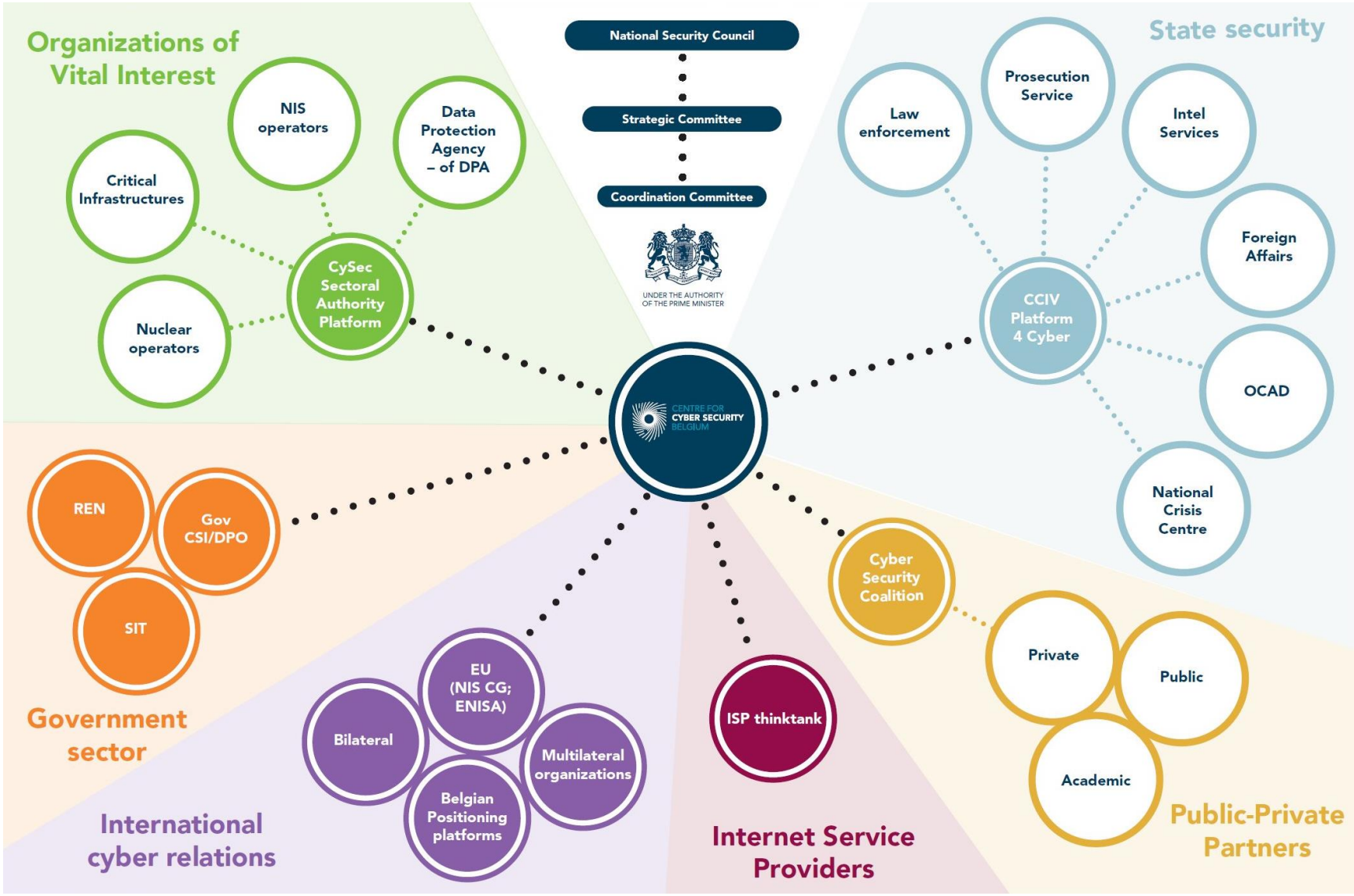
Organisations of vital interest:
Critical infrastructures, etc.

@OIV

@Gov

Public authorities:
Federal, but also regional and local

Belgian Cybersecurity Governance



CENTRE FOR CYBERSECURITY BELGIUM

Active Cyber Protection

What is Active Cyber Protection (ACP)?

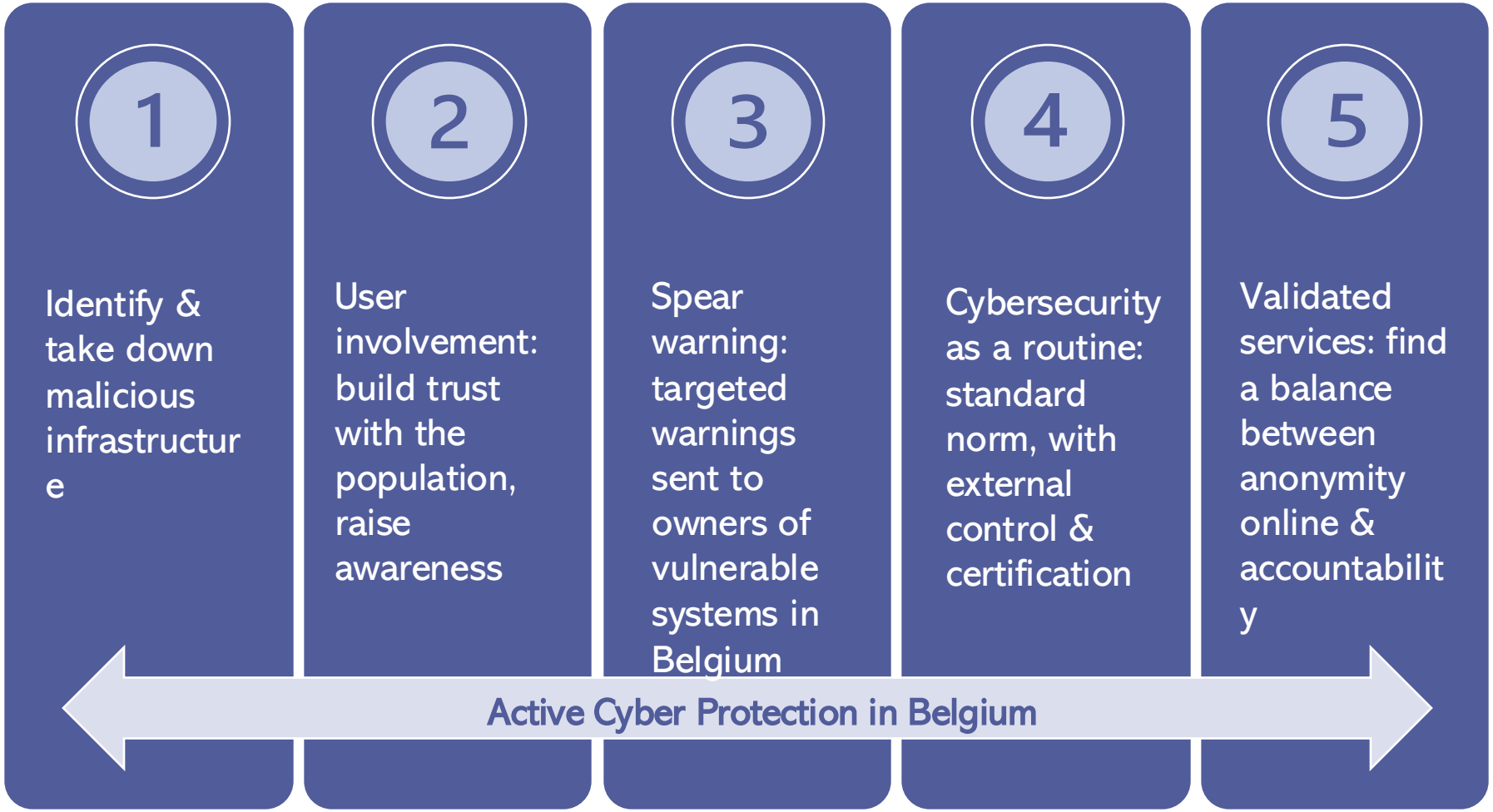
CENTRE FOR CYBERSECURITY BELGIUM

A proactive, tailored, automated ad participative approach to cybersecurity:

proactive	rather than just reacting to attacks, a **proactive search** for potential threats and vulnerabilities to support preparedness and prevent cybersecurity breaches
tailored	Because there is no “one size fits all” solution, customised solutions needed to take into account the **different needs** of stakeholders
automated	In a rapidly changing cybersecurity landscape, speed is essential & **automated solutions** are needed to protect systems from increasingly automated attacks
participative	**Active involvement** of all actors, from individuals to small and large organisations, in identifying and fixing vulnerabilities

Active Cyber Protection in Belgium

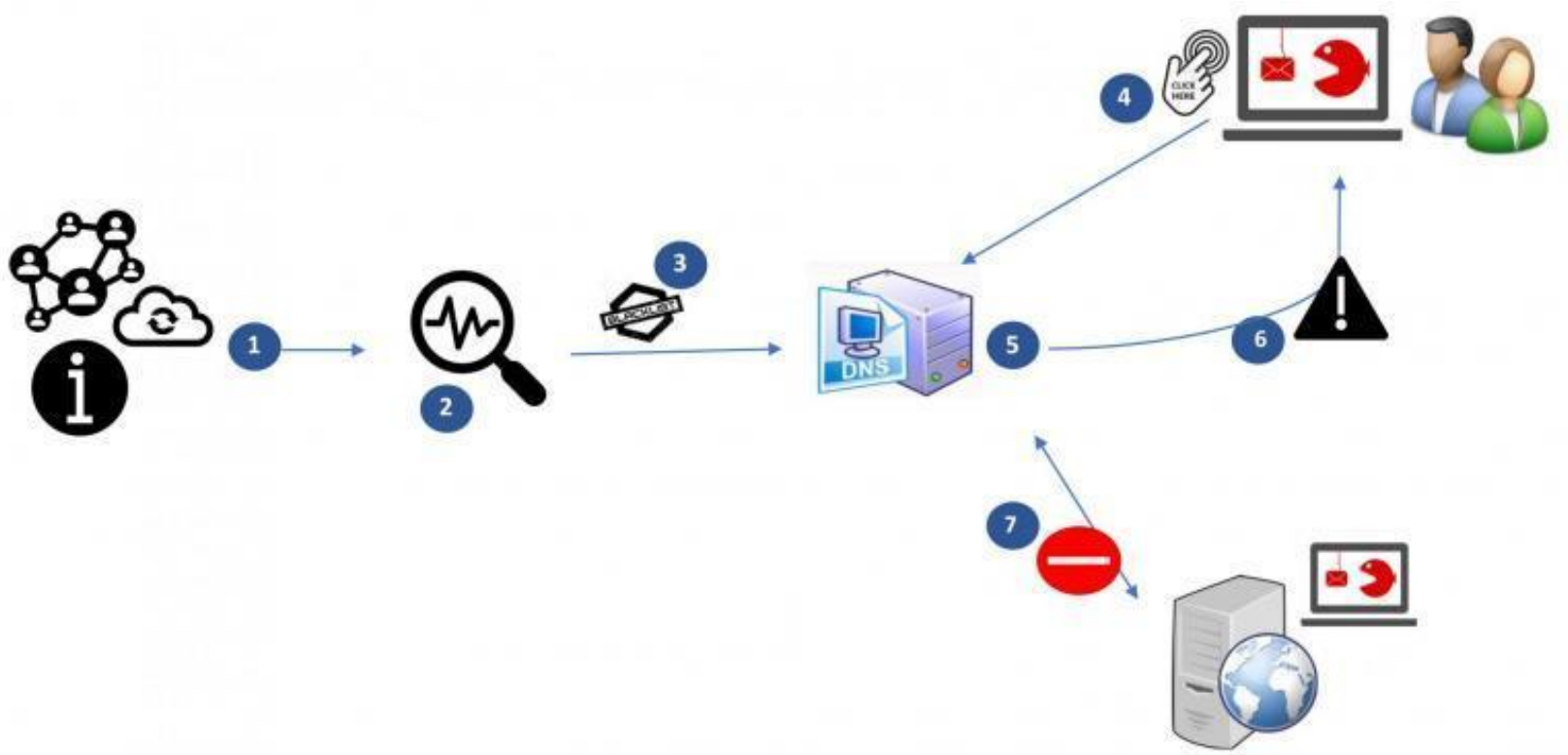
CENTRE FOR CYBERSECURITY BELGIUM



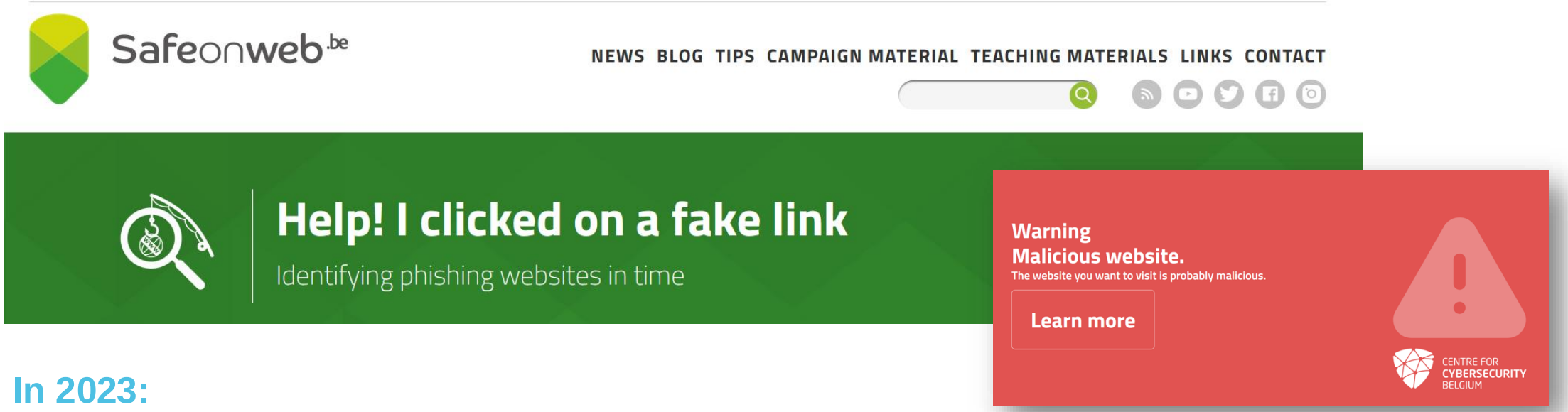
Addressing malicious infrastructure

CENTRE FOR CYBERSECURITY BELGIUM

The Belgian Anti-Phishing Shield (BAPS)



User involvement: Safeonweb



In 2023:

- Close to **10 million messages** were sent to suspect@safeonweb.be
- **1.2 million suspicious hyperlinks** detected thanks to these notifications.
- Fraudulent sites were neutralised thanks to a **warning page** displayed via the Belgian Anti-Phishing Shield (BAPS).

For more details: **safeonweb.be**

Spear warning

CENTRE FOR CYBERSECURITY BELGIUM

A targeted, timely & specific alert

Non-technical description of the risk, technical details & recommended action(s)

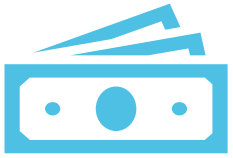
Email notification, letter or phone call (in the most urgent cases)

Credential Leak

Infection

Vulnerability

Pre-Ransomware notification



Compromised assets

Cybersecurity as a routine

CENTRE FOR CYBERSECURITY BELGIUM

A reference **framework with 4 levels**, freely available:

- **ESSENTIAL :** 144 key measures to address the risk of advanced cyber-attacks by actors with extensive skills and resources
- **IMPORTANT :** 107 key measures to minimise the risks of targeted cyber-attacks by actors with common skills and resources
- **BASIC:** 34 key measures based on readily available tools
- **SMALL:** basic recommendations in non-technical language for micro-organisations

The Cyberfundamentals framework integrates **NIS2 requirements**, thereby helping important and essential entities in their compliance efforts..

Cybersecurity as a routine

CENTRE FOR CYBERSECURITY BELGIUM

The Cyberfundamentals **mapping** facilitates compliance with international cybersecurity standards:

The NIST Cybersecurity Framework

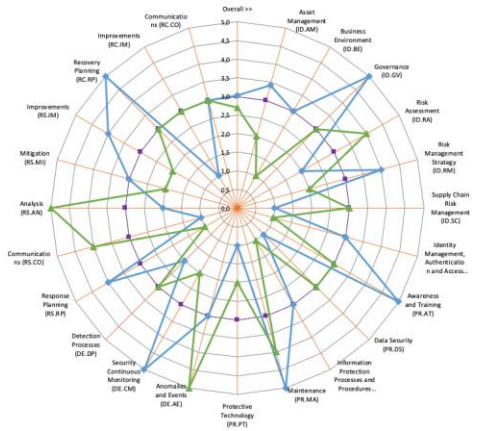
CIS Controls

Information Security Management System ISO 27001 Certified

IEC 62443
OT standards

Mor details at: **cyfun.be**

A **self-assessment tool:**



	CCB Cyberfundamentals Framework	Target Score	2023 Policy Score	2023 Practice Score
	Overall >>	3,00	3,02	2,70
IDENTIFY (ID)	Asset Management (ID.AM)	3,00	3,42	2,00
	Business Environment (ID.BE)	3,00	3,00	1,00
	Governance (ID.GV)	3,00	5,00	3,00
	Risk Assessment (ID.RA)	3,00	2,00	4,00
	Risk Management Strategy (ID.RM)	3,00	4,00	2,00
	Supply Chain Risk Management (ID.SC)	3,00	1,00	3,00
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC)	3,00	3,00	1,00
	Awareness and Training (PR.AT)	3,00	5,00	3,00
	Data Security (PR.DS)	3,00	1,00	3,00
	Information Protection Processes and Procedures (PR.IP)	3,00	3,00	1,00
	Maintenance (PR.MA)	3,00	5,00	4,00
	Protective Technology (PR.PT)	3,00	1,00	2,00
DETECT (DE)	Anomalies and Events (DE.AE)	3,00	3,00	5,00
	Security Continuous Monitoring (DE.CM)	3,00	5,00	2,00
	Detection Processes (DE.DP)	3,00	2,00	3,00
RESPOND (RS)	Response Planning (RS.RP)	3,00	4,00	1,00
	Communications (RS.CO)	3,00	1,00	4,00
	Analysis (RS.AN)	3,00	2,00	5,00
	Mitigation (RS.MI)	3,00	3,00	2,00
	Improvements (RS.IM)	3,00	4,00	2,00
RECOVER (RC)	Recovery Planning (RC.RP)	3,00	5,00	3,00
	Improvements (RC.IM)	3,00	1,00	3,00
	Communications (RC.CO)	3,00	3,00	3,00

Cybersecurity as a routine

CENTRE FOR CYBERSECURITY BELGIUM

Safeonweb@work: A dedicated portal with a full set of free **tools & services** available to all organisations registered in Belgium :

Self-Assessment
Questionnaire to assess your level of cyber maturity & obtain recommendations

Policy templates
Customisable documents e.g. Identity and Access Management Policy, Incident Management, etc.

Cyberfundamentals
4-level guide, mapping, self-assessment tool…

Coordinated Vulnerability Disclosure Policy
How to design a reward program for ethical hackers

Videos & Webinars
Latest information on the threat landscape, best practices…

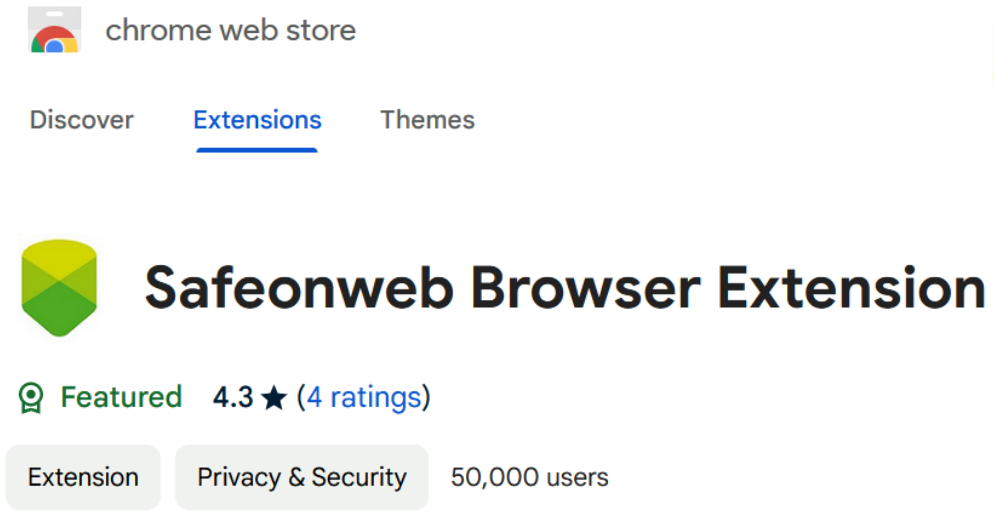
Information on cybersecurity subsidies
e.g. EU & Belgian calls for proposals

… and much more !

For more details: **atwork.safeonweb.be**

Validated services

An example: the Safeonweb browser extension



Green (OK) – 4/4: website owner has an Extended Validation Certificate issued by a Certificate Authority or the site owner is registered on Safeonweb@work (BE organisations only)

Amber (!) – 1 to 3/4: he website owner has an Organisation Validation Certificate, or a Domain Validation Certificate
→ risk if sharing personal data

Red (X) – 0/4: website lacks basic security features or is known as malicious.
→ high risk when browsing & sharing data

Going the last mile

CENTRE FOR CYBERSECURITY BELGIUM

We think big, but start small:

- Several iterations often needed: explore & learn
- Stay realistic & focus on concrete results

Change is easier in small steps!

CENTRE FOR
CYBERSECURITY
BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

Georges Ataya

Professeur à la Solvay Business School et Directeur, Ataya & Partners

Cyberwal
by digital
wallonia

La sécurité numérique pour le secteur public

La recherche de compétences en cybersécurité dans le secteur public

Georges Ataya,
Professeur, Solvay Business School
Associé, Ataya & Partners
Vice-Chair, Belgian Cybersecurity Coalition

Georges Ataya

Professor, founder and Academic Director of Digital and information security management at SBS-EM
Co-Fouder of the Belgian Cybersecurity Coalition
Co-founder DPO Circle
Member of the Advisory Board: Agoria, BECI, CIONET, ISACA, Belgian Cybersecurity Coalition
Founder at Ataya & partners, advisory firm (atayapartners.com)
Founded IT Management Academy
Past International Vice President at ISACA
Past Partner Ernst & Young
Past Deputy International CIO ITT World Directories
Previously Project Manager and Senior IT Auditor

Linkedin: ataya

Academy.atayapartners.com/fintech-sessions

Involvement in EU funded projects in Cybersecurity

CyberHubs

Involved in the CyberHubs project launched by Digital EUROPE, co-funded by the Erasmus+ Programme of the European Union and leaded by Agoria at the Belgian level. It aims to improve the quality and relevance of education and training programmes in cybersecurity and to provide an innovative methodology for anticipating skills needs.

Digital4Security

Digital4Security, a €20 million EU-funded project launched in October 2023, equips European SMEs with cybersecurity expertise through collaboration among 35 partners from 14 EU countries. The program focuses on protecting economic prosperity by offering academic accreditation and industry certification to professionals, managers, and business leaders, aligning with ENISA's European Cybersecurity Skills Framework (ECSF) to enhance the security and success of European businesses.

cocyber

COcyber is a 2-year project that aims to enhance the exchange, coordination, and collaboration between the cybersecurity civilian and defence spheres. COcyber will maximise the project impact by developing toolkits, ready-to-use material, and flagship events and engaging a group of ambassadors and renowned experts on its advisory board.

Cyber Incident Responder

Chief Information Security Officer (CISO)

Cybersecurity Educator

Cybersecurity Auditor

Cybersecurity Implementer

Cybersecurity Architect

Cyber Legal, Policy and Compliance Officer

Cyber Threat Intelligence Specialist

Penetration Tester

Cybersecurity Researcher

Cybersecurity Risk Manager

Digital Forensics Investigator

INTENDED AUDIENCE

1

Intended Audience

CHIEF INFORMATION SECURITY MANAGER (CISO)

Decision making and relations with the General Management; Security Architecture and its impact on cybersecurity and business strategy; Cybersecurity operations and its impact on business activity; certification and accreditation in line with industry standards and regulatory requirements; the risk profiles in relation to budget priorities and protection targets.

2

Intended Audience

CYBERSECURITY IMPLEMENTATION MANAGER

Cybersecurity project and program management; Security Architecture and its impact on targeted protections; impact of implementation projects and architecture on Cybersecurity operations; Capabilities and technology requirements for reaching intended industry standards and regulatory requirements; the residual risks in relation to program and project delivery as well as business risks related to delivered capabilities.

3

Intended Audience

CYBERSECURITY MANAGEMENT ADVISOR

Capabilities to deliver CISO services, strategy, and architecture advisory and management counselling; Risk prioritisation and business impact analysis; Auditing; Risk assessment and maturity improvement projects; Review and assistance with external services, with the reliance on technology solutions, and with personnel maturity.

4

Intended Audience

DIGITAL TRANSFORMATION PROFESSIONAL

Managing portfolio, programs or projects involve adequate knowledge of Cybersecurity issues related to business, technology and implementation constraints. Cybersecurity Architecture, Business needs, risk, and compliance issues drive todays transformation initiatives.

5

Intended Audience

Chief Information officer (CIO)

Lead Information and Cybersecurity activities vertically or liaise with horizontal cybersecurity activities in an enterprise; Understand the business capabilities; technical requirements and process implementation while leading the implementation of cybersecurity protections. Develop a technology savvy business management to support cybersecurity maturity in services and products and within technology and business personnel.

6

Intended Audience

SECURITY OPERATIONS PROFESSIONAL

Understanding the business requirements and managing cybersecurity related operations; Build adequate capabilities to support incident and crisis situations; manage the organisation capabilities including architecture, configuration, operations, and services.

7

Intended Audience

RISK MANAGER

Translate cybersecurity risks into business impact and formulate protection targets and priorities; understand the financial returns on cybersecurity investments and advice general managers in their decision making; assess risks of cybersecurity related projects and acquired external services.

8

Intended Audience

COMPLIANCE PROFESSIONAL

Management of compliance activities in relation to cybersecurity laws, regulations, and industry requirements. Implementation of and project activities related to implementing selected controls. Support in the accreditation and the certification of operations and systems. Support in reaching relevant maturity levels to build control layers towards reaching intended cybersecurity protection.

9

Intended Audience

HUMAN RESOURCES MANAGER

Understand cybersecurity skills and roles that are required to support recruiting, upskilling, reskilling and promoting cybersecurity, IT and business personnel. Apply innovative methods to build cybersecurity maturity.

10

Intended Audience

AUDIT PROFESSIONAL

Review of lines of defence related to Cybersecurity services, risk evaluation, compliance activities, maturity improvement projects, and cybersecurity governance and monitoring activities. Review of external services and evaluation of technology components and cybersecurity profile of business operations.

11

Intended Audience

BUSINESS MANAGER

Use cybersecurity capabilities as a competitive advantage and integrate security protections in developed products and services; Actively use cybersecurity capabilities in FINTECH, technology start-ups, and innovative products and services.

12

Intended Audience

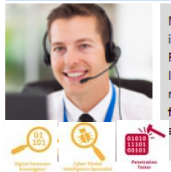
SENIOR EXECUTIVE

Apply cybersecurity management methods while managing human resources, leading finance operations, directing operations and business processes, and selling products and services.

13

Intended Audience

Cybersecurity technical experts



Manage Technical cybersecurity activities including Digital Forensics investigators, Penetration testers, and Cyber Threat Intelligence specialist. Apply management methods while determining relevant actions to face related risks. Manage technical teams accordingly.

14

Intended Audience

Cybersecurity Architect

Use full knowledge of risks and mitigation actions in building layers of protection. Ensure that built architecture is capable of implementing targeted protection strategy. Align building blocks with cybersecurity operations and foreseen future needs.

15

Intended Audience

Cybersecurity Academics

Get updated on most recent management practices, frameworks and standards in relation to cybersecurity. Re-use advanced education practices to promote awareness, management knowledge and

16

ROLE → Skills

INTRUSION ANALYST

PESA	Testing and conducting Simulated Attack Exercise
PESA	Management, Incident Investigation & Response
PESA	Intrusion Detection and Analysis
PESA	Legal & Regulatory Environment and Compliance
PESA	Information Risk Strategy
PESA	Research
PESA	Threat Intelligence, Assessment and Threat Mo
PESA	Specialist Advice
PESA	Research
PESA	Management, Incident Investigation & Response

IMPACT

ROLE QUALIFICATION REPORT

Skillsbeam | Role Qualification Report | KEVIN CLAES | INTRUSION ANALYST
Created on 6 February 2022 | Name | Role Assessed

ROLES' SKILLS LEVELS

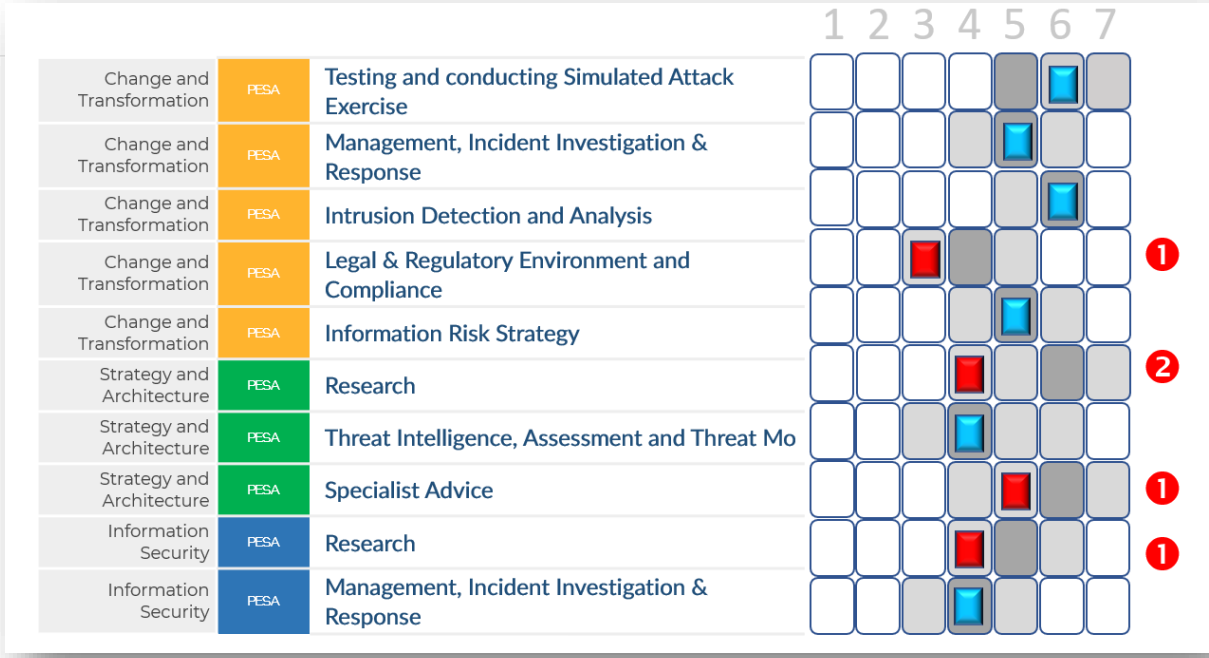
	ROLE	Average GAP	Assessment date/type	Skills #	Max / Min levels	Recommendations
1.	Intrusion Analyst	1.00	2022-02-01 Self Assessed	10	6 / 2	Still Current

Summary statement
Intrusion Analysts identify, track and discover sophisticated malicious cyber activity targeting systems and networks.

Mission
An Intrusion Analyst plans, coordinates and conducts proactive cyber threat discovery activities to identify potential intrusion or anomalous behaviour based on cyber threat intelligence. An Intrusion Analyst assesses and evaluates cyber threat intelligence for indicators of compromise, and provides detailed planning, analysis and reporting on current and emerging threats to information systems.

Main task/s

- Plan, coordinate and conduct network and system activity
- Understand and apply cyber threat models
- Assess and evaluate cyber threat intelligence
- Communicate technical findings and recommendations
- Design and develop complex technical and procedural systems



© Copyright 2022, Georges Ataya and Atayapartners.com

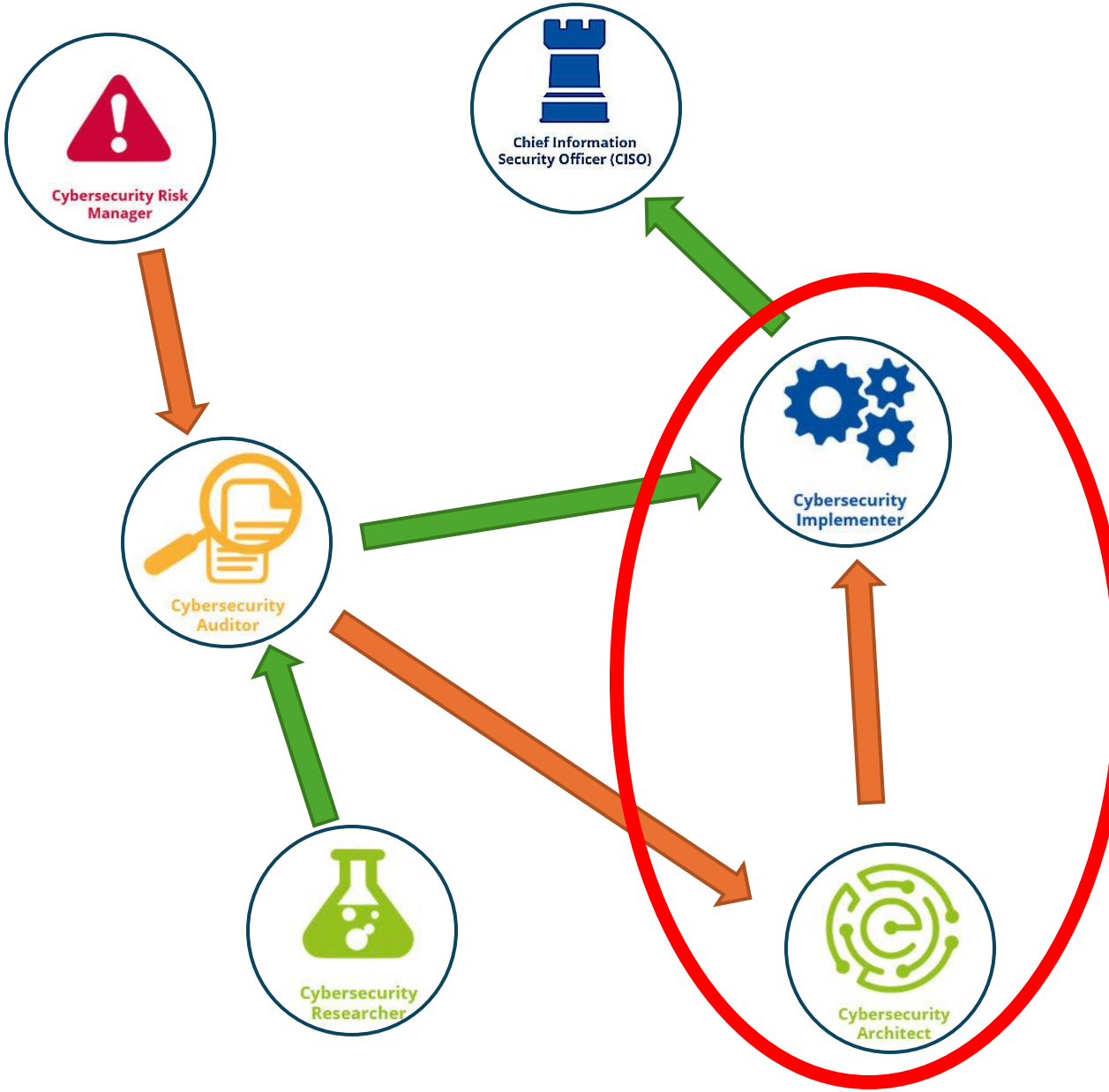

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK
ECSF
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK
SEPTEMBER 2022


Cybersecurity Risk Manager
Chief Information Security Officer (CISO)
Cybersecurity Implementer
Cybersecurity Auditor
Cybersecurity Researcher
Cybersecurity Architect


Intended Audience
Cybersecurity Architect
Use full knowledge of risks and mitigation actions in building layers of protection. Ensure that built architecture is capable of implementing targeted protection strategy. Align building blocks with cybersecurity operations and foreseen future needs.


enisa
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK
ECSF
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK
SEPTEMBER 2022


Intended Audience
CYBERSECURITY IMPLEMENTATION MANAGER
Cybersecurity project and program management; Security Architecture and its impact on targeted protections; impact of implementation projects and architecture on Cybersecurity operations; Capabilities and technology requirements for reaching intended industry standards and regulatory requirements; the residual risks in relation to program and project delivery as well as business risks related to delivered capabilities.

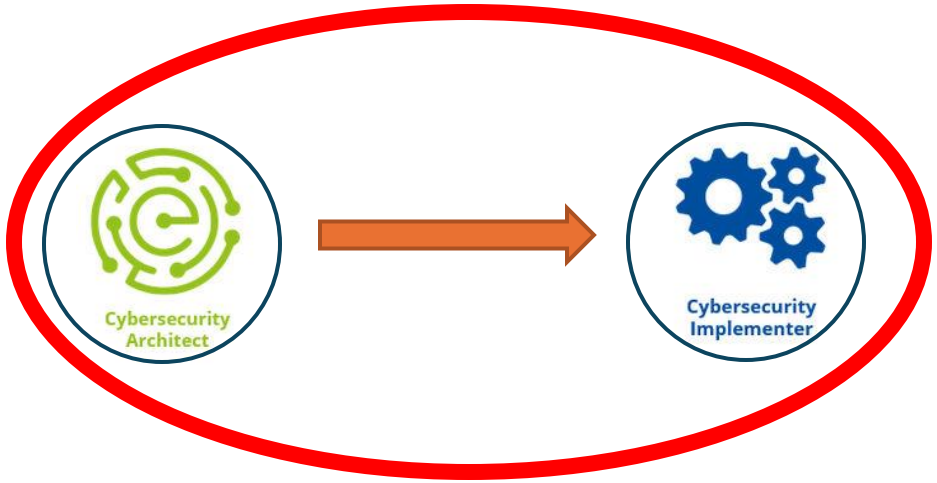

Cybersecurity Risk Manager
Chief Information Security Officer (CISO)
Cybersecurity Implementer
Cybersecurity Auditor
Cybersecurity Researcher
Cybersecurity Architect

CYBERSECURITY ARCHITECT

- Principal Security Architect — 6
- Lead Security Architect — 5
- Senior Security Architect — 4

CYBERSECURITY IMPLEMENTER

- Principal Cyber Security Analyst — 6
- Lead Cyber Security Analyst — 5
- Senior Cyber Security Analyst — 4
- Cyber Security Analyst — 3



A.5. Architecture Design - 5
A.6. Application Design - 3
B.1. Application Development - 3
B.3. Testing - 3
B.6. ICT Systems Engineering - 4

A.5. Architecture Design - 5
A.6. Application Design - 5
B.1. Application Development - 4
B.3. Testing - 3
B.6. ICT Systems Engineering - 3

Operates at the highest organizational level, determines overall organizational vision and strategy, and assumes accountability for overall success	**SET STRATEGY, INSPIRE, MOBILISE**	7
Has significant organizational influence, makes high-level decisions, shapes policies, demonstrates leadership, fosters organizational collaboration, and accepts accountability in key areas	**INITIATE, INFLUENCE**	6
Accountable for achieving workgroup objectives and managing work from analysis to execution and evaluation. Provides authoritative guidance in their field and works under broad direction.	**ENSURE, ADVISE**	5
Performs diverse complex activities, supports and supervises others, works autonomously under general direction, and contributes expertise to deliver team objectives.	**ENABLE**	4
Performs varied tasks, sometimes complex and non-routine, using standard methods and procedures. Works under general direction, exercises discretion, and manages own work within deadlines.	**APPLY**	3
Provides assistance to others, works under routine supervision, and uses their discretion to address routine problems.	**ASSIST**	2
Performs routine tasks under close supervision, follows instructions, and requires guidance to complete their work	**FOLLOW**	1

CYBERSECURITY ARCHITECT

- Principal Security Architect — 6
- Lead Security Architect — 5
- Senior Security Architect — 4

CYBERSECURITY IMPLEMENTER

- Principal Cyber Security Analyst — 6
- Lead Cyber Security Analyst — 5
- Senior Cyber Security Analyst — 4
- Cyber Security Analyst — 3

Requirements definition and management	REQM	Change and transformation	4
Vulnerability assessment	VUAS	Delivery and operation	5
Database design	DBDS	Development and implementation	4
Data modelling and design	DTAN	Development and implementation	4
User experience design	HCEV	Development and implementation	4
Network design	NTDS	Development and implementation	6
Programming/software development	PROG	Development and implementation	4
Software design	SWDN	Development and implementation	4
Testing	TEST	Development and implementation	5
Continuity management	COPL	Strategy and architecture	5
Information systems coordination	ISCO	Strategy and architecture	6

Requirements definition and management	REQM	Change and transformation	6
Penetration testing	PENT	Delivery and operation	5
Database design	DBDS	Development and implementation	5
Data modelling and design	DTAN	Development and implementation	5
User experience design	HCEV	Development and implementation	6
Network design	NTDS	Development and implementation	4
Programming/software development	PROG	Development and implementation	6
Software design	SWDN	Development and implementation	6
Testing	TEST	Development and implementation	6
Information systems coordination	ISCO	Strategy and architecture	6
Enterprise and business architecture	STPL	Strategy and architecture	7
Enterprise and business architecture	STPL	Strategy and architecture	7

CYBERSECURITY ARCHITECT

Organisation design and implementation	ORDI	Change and transformation	7
Requirements definition and management	REQM	Change and transformation	4
Vulnerability assessment	VUAS	Delivery and operation	5
Database design	DBDS	Development and implementation	4
Systems design	DESN	Development and implementation	6
Data modelling and design	DTAN	Development and implementation	4
User experience design	HCEV	Development and implementation	4
Hardware design	HWDE	Development and implementation	6
Network design	NTDS	Development and implementation	6
Programming/software development	PROG	Development and implementation	4
Software design	SWDN	Development and implementation	4
Testing	TEST	Development and implementation	5
Solution architecture	ARCH	Strategy and architecture	6
Continuity management	COPL	Strategy and architecture	5
Information systems coordination	ISCO	Strategy and architecture	6
Information security	SCTY	Strategy and architecture	5

CYBERSECURITY IMPLEMENTER

Organisation design and implementation	ORDI	Change and transformation	7
Requirements definition and management	REQM	Change and transformation	6
Penetration testing	PENT	Delivery and operation	5
Database design	DBDS	Development and implementation	5
Systems design	DESN	Development and implementation	6
Data modelling and design	DTAN	Development and implementation	5
User experience design	HCEV	Development and implementation	6
Hardware design	HWDE	Development and implementation	6
Network design	NTDS	Development and implementation	4
Programming/software development	PROG	Development and implementation	6
Software design	SWDN	Development and implementation	6
Testing	TEST	Development and implementation	6
Solution architecture	ARCH	Strategy and architecture	6
Information systems coordination	ISCO	Strategy and architecture	6
Information security	SCTY	Strategy and architecture	5
Enterprise and business architecture	STPL	Strategy and architecture	7
Enterprise and business architecture	STPL	Strategy and architecture	7

CYBERSECURITY ARCHITECT

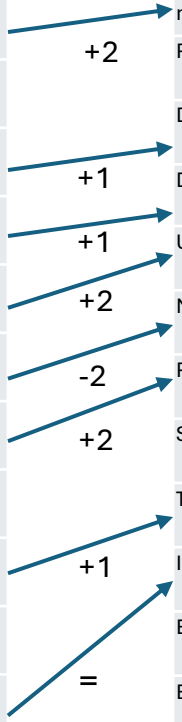
Requirements definition and management	REQM	Change and transformation	4
Vulnerability assessment	VUAS	Delivery and operation	5
Database design	DBDS	Development and implementation	4
Data modelling and design	DTAN	Development and implementation	4
User experience design	HCEV	Development and implementation	4
Network design	NTDS	Development and implementation	6
Programming/software development	PROG	Development and implementation	4
Software design	SWDN	Development and implementation	4
Testing	TEST	Development and implementation	5
Continuity management	COPL	Strategy and architecture	5
Information systems coordination	ISCO	Strategy and architecture	6

CYBERSECURITY IMPLEMENTER

Requirements definition and management	REQM	Change and transformation	6
Penetration testing	PENT	Delivery and operation	5
Database design	DBDS	Development and implementation	5
Data modelling and design	DTAN	Development and implementation	5
User experience design	HCEV	Development and implementation	6
Network design	NTDS	Development and implementation	4
Programming/software development	PROG	Development and implementation	6
Software design	SWDN	Development and implementation	6
Testing	TEST	Development and implementation	6
Information systems coordination	ISCO	Strategy and architecture	6
Enterprise and business architecture	STPL	Strategy and architecture	7
Enterprise and business architecture	STPL	Strategy and architecture	7

CYBERSECURITY ARCHITECT

Requirements definition and management	REQM	Change and transformation	4
Vulnerability assessment	VUAS	Delivery and operation	5
Database design	DBDS	Development and implementation	4
Data modelling and design	DTAN	Development and implementation	4
User experience design	HCEV	Development and implementation	4
Network design	NTDS	Development and implementation	6
Programming/software development	PROG	Development and implementation	4
Software design	SWDN	Development and implementation	4
Testing	TEST	Development and implementation	5
Continuity management	COPL	Strategy and architecture	5
Information systems coordination	ISCO	Strategy and architecture	6



CYBERSECURITY IMPLEMENTER

Requirements definition and management	REQM	Change and transformation	6
Penetration testing	PENT	Delivery and operation	5
Database design	DBDS	Development and implementation	5
Data modelling and design	DTAN	Development and implementation	5
User experience design	HCEV	Development and implementation	6
Network design	NTDS	Development and implementation	4
Programming/software development	PROG	Development and implementation	6
Software design	SWDN	Development and implementation	6
Testing	TEST	Development and implementation	6
Information systems coordination	ISCO	Strategy and architecture	6
Enterprise and business architecture	STPL	Strategy and architecture	7
Enterprise and business architecture	STPL	Strategy and architecture	7


Intended Audience
RISK MANAGER
Translate cybersecurity risks into business impact and formulate protection targets and priorities; understand the financial returns on cybersecurity investments and advice general managers in their decision making; assess risks of cybersecurity related projects and acquired external services.


enisa
ECSF
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK
SEPTEMBER 2022


Intended Audience
CHIEF INFORMATION SECURITY MANAGER (CISO)
Decision making and relations with the General Management; Security Architecture and its impact on cybersecurity and business strategy; Cybersecurity operations and its impact on business activity; certification and accreditation in line with industry standards and regulatory requirements; the risk profiles in relation to budget priorities and protection targets.

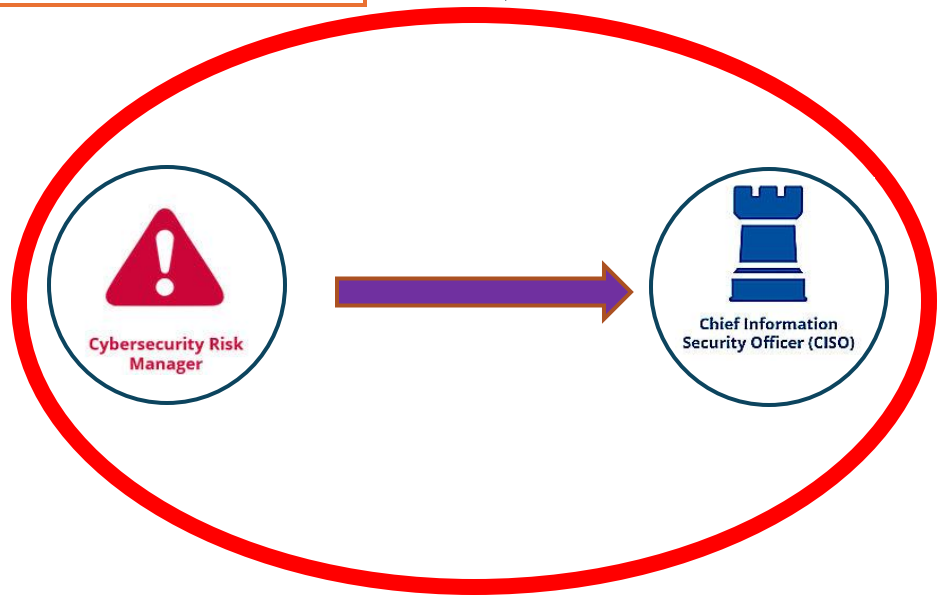

Cybersecurity Risk Manager
Chief Information Security Officer (CISO)
Cybersecurity Auditor
Cybersecurity Implementer
Cybersecurity Researcher
Cybersecurity Architect

CYBERSECURITY RISK MANAGER

- Head of Cyber Risk and Assurance — 6
- Lead Cyber Risk Analyst — 5
- Senior Cyber Risk Analyst — 4
- Cyber Risk Analyst — 3

CHIEF INFORMATION SECURITY OFFICER (CISO)

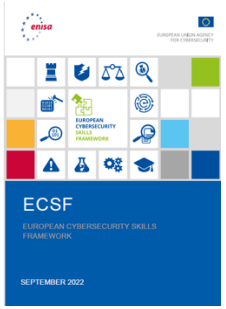
- Chief Information Security Officer — 7
- Head of Cyber Security — 6
- Cyber Security Manager — 5



E.3. Risk Management - 4
E.5. Process Improvement - 3
E.7. Business Change Management - 4
E.9. IS-Governance - 4
E.3. Risk Management - 4

A.7. Technology Trend Monitoring - 4
D.1. Information Security Strategy Development - 5
E.3. Risk Management - 4
E.8. Information Security Management - 4
E.9. IS-Governance - 5

CYBERSECURITY RISK MANAGER



- Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards
- Analyse and consolidate organisation's quality and risk management practices
- Enable business assets owners, executives and other stakeholders to make risk-informed decisions to manage and mitigate risks
- Build a cybersecurity risk-aware environment
- Communicate, present and report to relevant stakeholders
- Propose and manage risk-sharing options

CHIEF INFORMATION SECURITY OFFICER (CISO)

Assess and enhance an organisation's cybersecurity posture
- Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks
- Analyse and comply with cybersecurity-related laws, regulations and legislations
- Implement cybersecurity recommendations and best practices
- Manage cybersecurity resources
- Develop, champion and lead the execution of a cybersecurity strategy
- Influence an organisation's cybersecurity culture
- Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing
- Review and enhance security documents, reports, SLAs and ensure the security objectives
- Identify and solve cybersecurity-related issues
- Establish a cybersecurity plan
- Communicate, coordinate and cooperate with internal and external stakeholders
- Anticipate required changes to the organisation's information security strategy and formulate new plans
- Define and apply maturity models for cybersecurity management
- Anticipate cybersecurity threats, needs and upcoming challenges
- Motivate and encourage people

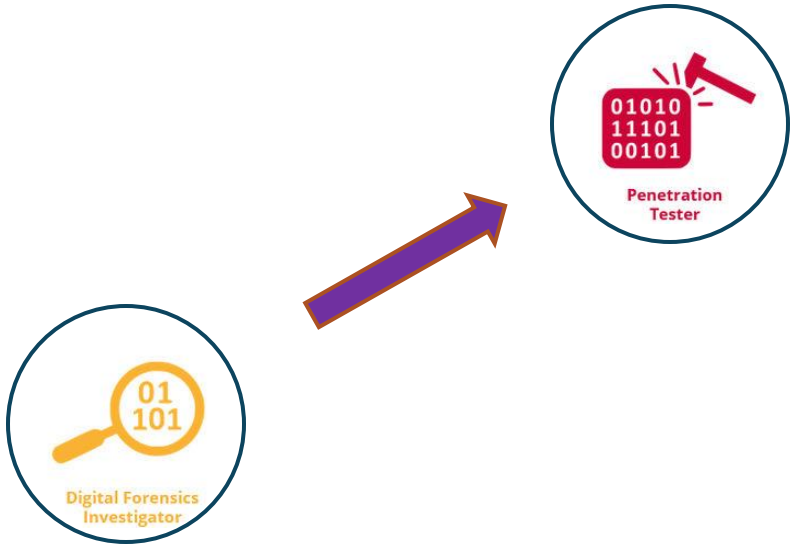
CYBERSECURITY RISK MANAGER

Benefits management	BENM	Change and transformation	6
Organisational change management	CIPM	Change and transformation	6
Programme management	PGMG	Change and transformation	6
Project management	PRMG	Change and transformation	6
Portfolio, programme and project support	PROF	Change and transformation	6
Availability management	AVMT	Delivery and operation	4
Stakeholder relationship management	RLMT	Relationships and engagement	6
Audit	AUDT	Strategy and architecture	5
Risk management	BURM	Strategy and architecture	6
Continuity management	COPL	Strategy and architecture	6
Demand management	DEMM	Strategy and architecture	6
Governance	GOVN	Strategy and architecture	6
Information assurance	INAS	Strategy and architecture	5
Information systems coordination	ISCO	Strategy and architecture	6
Measurement	MEAS	Strategy and architecture	4

CHIEF INFORMATION SECURITY OFFICER (CISO)

Acceptance testing	BPTS	Change and transformation	6
Programme management	PGMG	Change and transformation	7
Portfolio, programme and project support	PROF	Change and transformation	6
Availability management	AVMT	Delivery and operation	6
Capacity management	CPMG	Delivery and operation	6
Digital forensics	DGFS	Delivery and operation	6
Penetration testing	PENT	Delivery and operation	6
Security operations	SCAD	Delivery and operation	6
Safety assessment	SFAS	Development and implementation	6
Stakeholder relationship management	RLMT	Relationships and engagement	7
Risk management	BURM	Strategy and architecture	6
Continuity management	COPL	Strategy and architecture	6
Emerging technology monitoring	EMRG	Strategy and architecture	6
Governance	GOVN	Strategy and architecture	7
Information assurance	INAS	Strategy and architecture	6
Information management	IRMG	Strategy and architecture	6
Information systems coordination	ISCO	Strategy and architecture	6
Information security	SCTY	Strategy and architecture	7


enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK
ECSF
EUROPEAN CYBERSECURITY SKILLS FRAMEWORK
SEPTEMBER 2022


01
101
Digital Forensics Investigator
01010
11101
00101
Penetration Tester

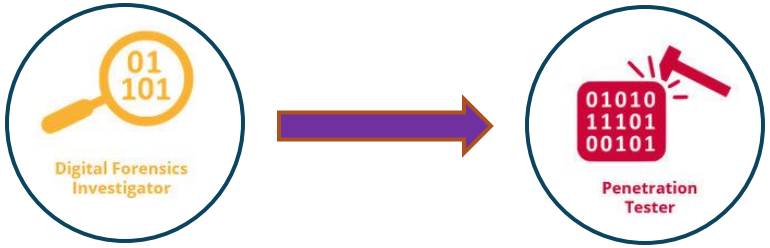
DIGITAL FORENSICS INVESTIGATOR

- Manager Digital & Forensic Investigations — 5
- Senior Digital Forensics Investigator — 4
- Digital Forensics Investigator — 3

PENETRATION TESTER

- Lead Penetration Tester — 5
- Senior Penetration Tester — 4
- Penetration Tester — 3

A.7. Technology Trend Monitoring - 3
B.3. Testing - 4
B.5. Documentation Production - 3
E.3. Risk Management - 3



B.2. Component Integration - 4
B.3. Testing - 4
B.4. Solution Deployment - 2
B.5. Documentation Production - 3
E.3. Risk Management - 4

DIGITAL FORENSICS INVESTIGATOR

PENETRATION TESTER

- Work ethically and independently; not influenced and biased by internal or external actors
- Collect information while preserving its integrity
- Identify, analyse and correlate cybersecurity events
- Explain and present digital evidence in a simple, straightforward and easy to understand way
- Develop and communicate, detailed and reasoned investigation reports

- Develop codes, scripts and programmes
- Perform social engineering
- Identify and exploit vulnerabilities
- Conduct ethical hacking
- Think creatively and outside the box
- Identify and solve cybersecurity-related issues
- Communicate, present and report to relevant stakeholders
- Use penetration testing tools effectively
- Conduct technical analysis and reporting
- Decompose and analyse systems to identify weaknesses and ineffective controls
- Review codes assess their security

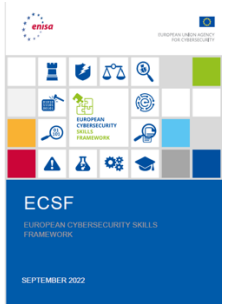
DIGITAL FORENSICS INVESTIGATOR

Portfolio, programme and project support	PROF	Change and transformation	4
Requirements definition and management	REQM	Change and transformation	4
Digital forensics	DGFS	Delivery and operation	5
Database design	DBDS	Development and implementation	4
Testing	TEST	Development and implementation	6
Risk management	BURM	Strategy and architecture	4
Continuity management	COPL	Strategy and architecture	4
Emerging technology monitoring	EMRG	Strategy and architecture	4
Information systems coordination	ISCO	Strategy and architecture	6

PENETRATION TESTER

Portfolio, program, and project support	PROF	Change and transformation	6
Requirements definition and management	REQM	Change and transformation	4
Penetration testing	PENT	Delivery and operation	5
Release and deployment	RELM	Delivery and operation	3
Vulnerability assessment	VUAS	Delivery and operation	5
Database design	DBDS	Development and implementation	4
Network design	NTDS	Development and implementation	6
Real-time/embedded systems development	RESD	Development and implementation	6
Systems integration and build	SINT	Development and implementation	6
Software design	SWDN	Development and implementation	6
Testing	TEST	Development and implementation	6
Risk management	BURM	Strategy and architecture	6
Continuity management	COPL	Strategy and architecture	6
Information systems coordination	ISCO	Strategy and architecture	6
Specialist advice	TECH	Strategy and architecture	4

CYBERSECURITY ARCHITECT



CYBERSECURITY IMPLEMENTER

- Conduct user and business security requirements analysis
- Draw cybersecurity architectural and functional specifications
- Decompose and analyse systems to develop security and privacy requirements and identify effective solutions
- Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles
- Guide and communicate with implementers and IT/OT personnel
- Communicate, present and report to relevant stakeholders
- Propose cybersecurity architectures based on stakeholder's needs and budget
- Select appropriate specifications, procedures and controls
- Build resilience against points of failure across the architecture
- Coordinate the integration of security solutions

- Communicate, present and report to relevant stakeholders
- Integrate cybersecurity solutions to the organisation's infrastructure
- Configure solutions according to the organisation's security policy
- Assess the security and performance of solutions
- Develop code, scripts and programmes
- Identify and solve cybersecurity-related issues
- Collaborate with other team members and colleagues

Skillsbeam.io

Career companion

ROLES

Skills

Business
- Business Information Manager
- Chief Information Officer
- Data Scientist
- Operations Manager

Design
- Business Analyst
- Data Specialist
- Enterprise Architect
- Solution Designer
- Systems Analyst
- Systems Architect

Development
- Developer
- Digital Media Specialist
- Test Specialist

Service & Operation
- Data Administrator
- Network Specialist
- Service Support
- Systems Administrator
- Technical Specialist

Support
- Account Manager
- Digital Consultant
- Digital Educator
- Information Security Specialist

Process Improvement
- DevOps Expert
- Digital Transformation Leader
- Product Owner
- Scrum Master

Technical
- Information Security Manager
- Project Manager
- Quality Assurance Manager
- Service Manager

Digital Roles

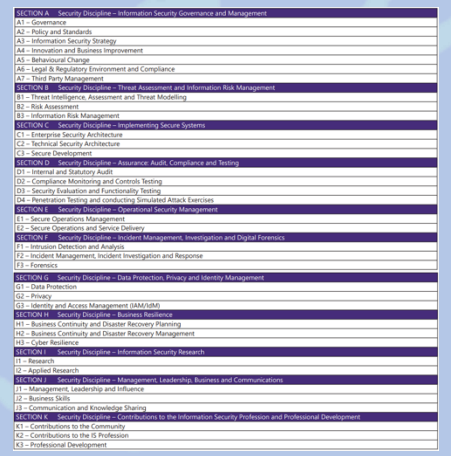
European e-Competence Framework

COBIT 2019

- Chief Information Security Officer
- Cyber Advisor
- Cyber Threat Analyst
- Incident Responder
- Intrusion Analyst
- Malware Analyst
- Operations Coordinator
- Penetration Tester
- Security Architect
- Vulnerability Assessor
- Vulnerability Researcher

Cyber Roles

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

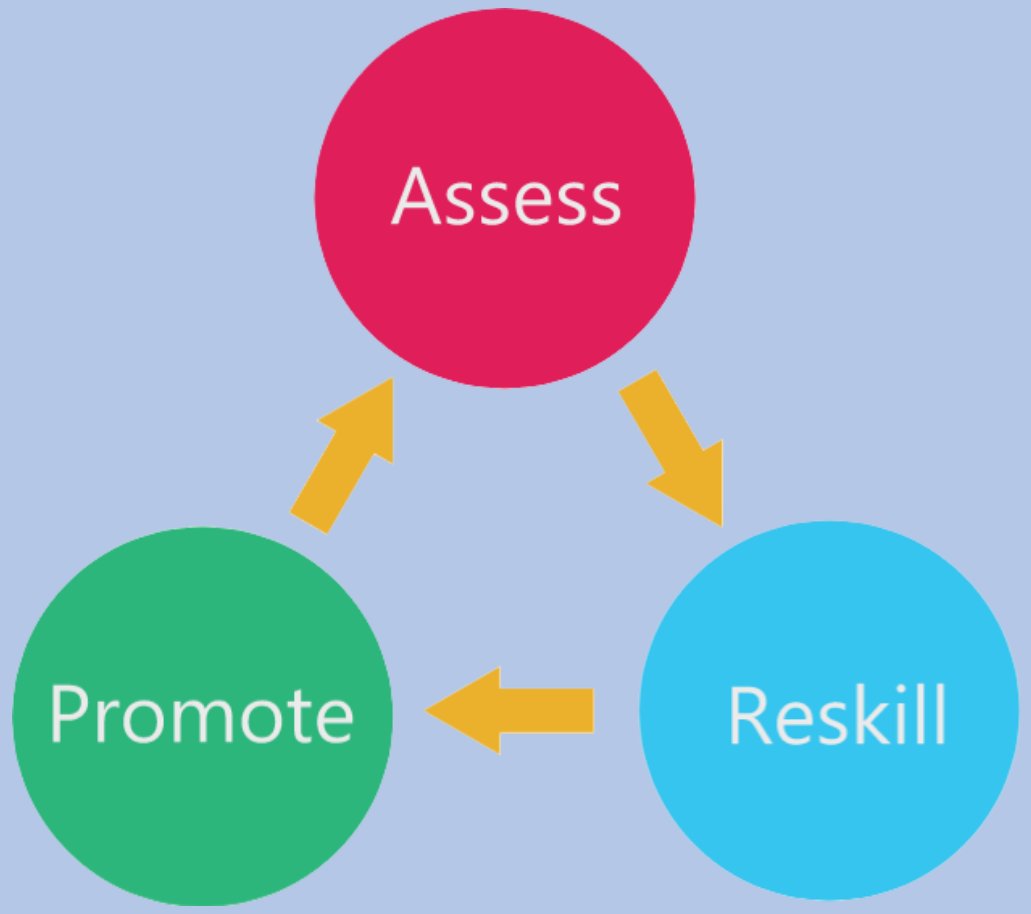


Chartered Institute of Information Security

SFIA

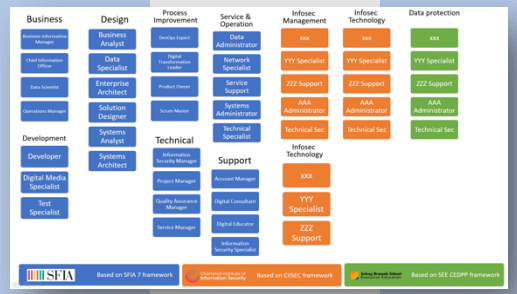
DIGITAL PROFESSIONAL

Take control of your career as from today and define your next actions to focus on essential skills leading to target roles. Become your enterprise's digital gem.

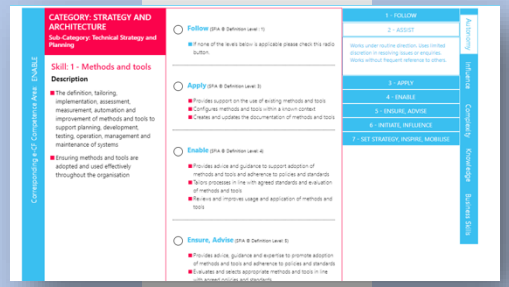


Detailed slides

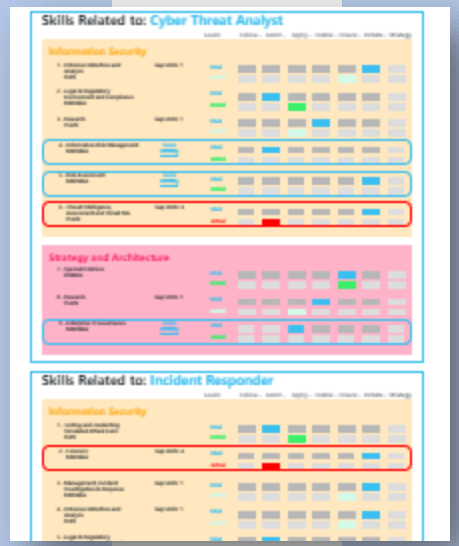
Skillsbeam.io

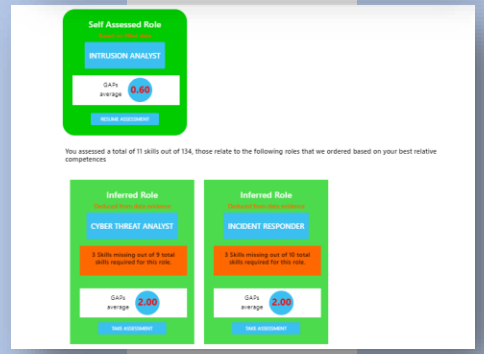


SELECT ROLE TO ASSESS



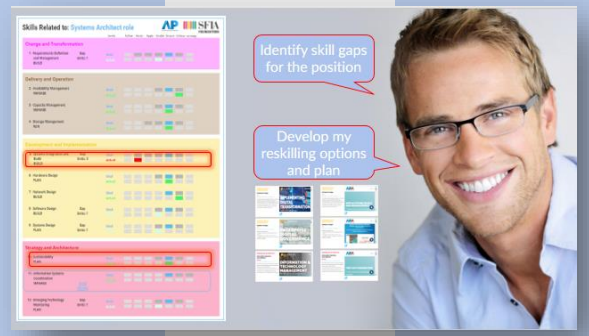
ASSESS ALL SKILLS FOR THAT ROLE





OBTAIN RESULTS AND IDENTIFY OTHER RELEVANT ROLES

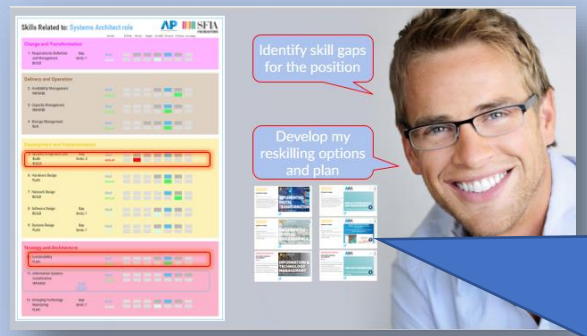
Reference Strong skills



BUILD UPSKILLING PLAN

OBTAIN THE ROLE QUALIFICATION AND UPSKILLING REPORTS

Skillsbeam.io



Upskilling options are recommended based on the skills gaps that are identified.

Participants may add personally identified offerings. Those shall be proposed to others.

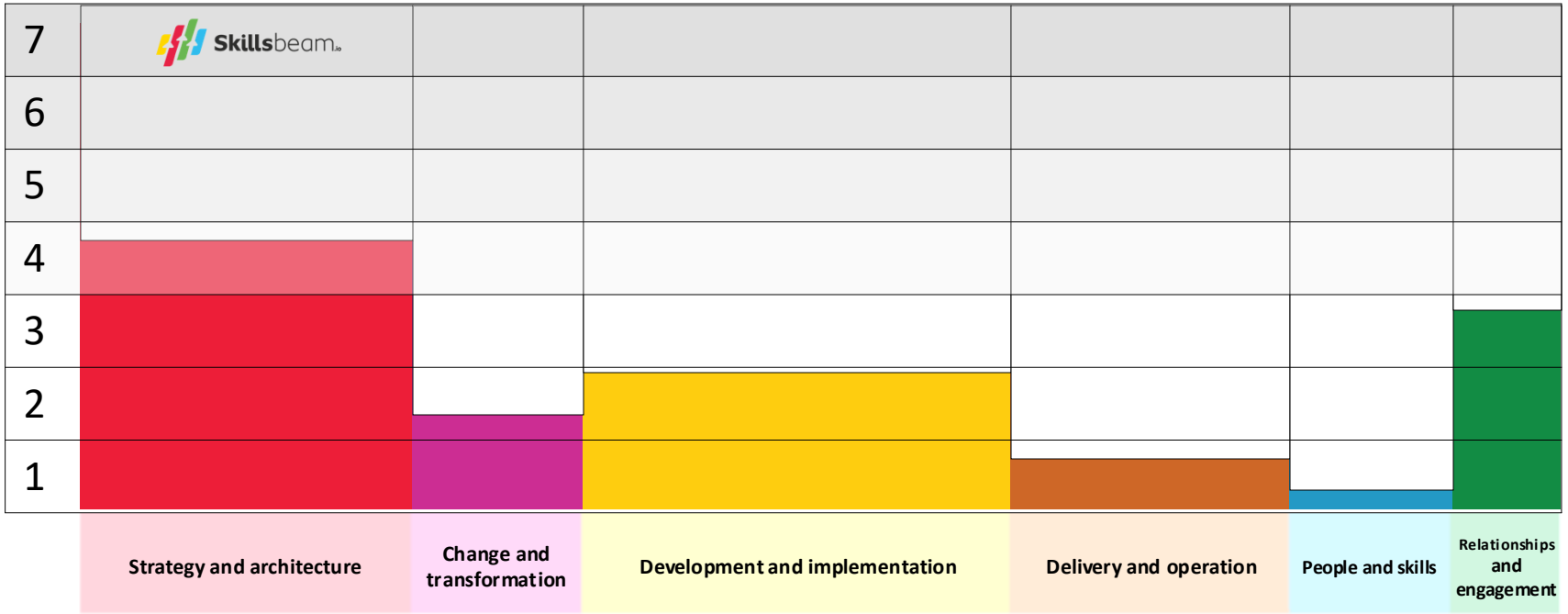
A ranking model allows to promote and grade the upskilling options (à la Booking.com)

Skillsbeam

IMPACT

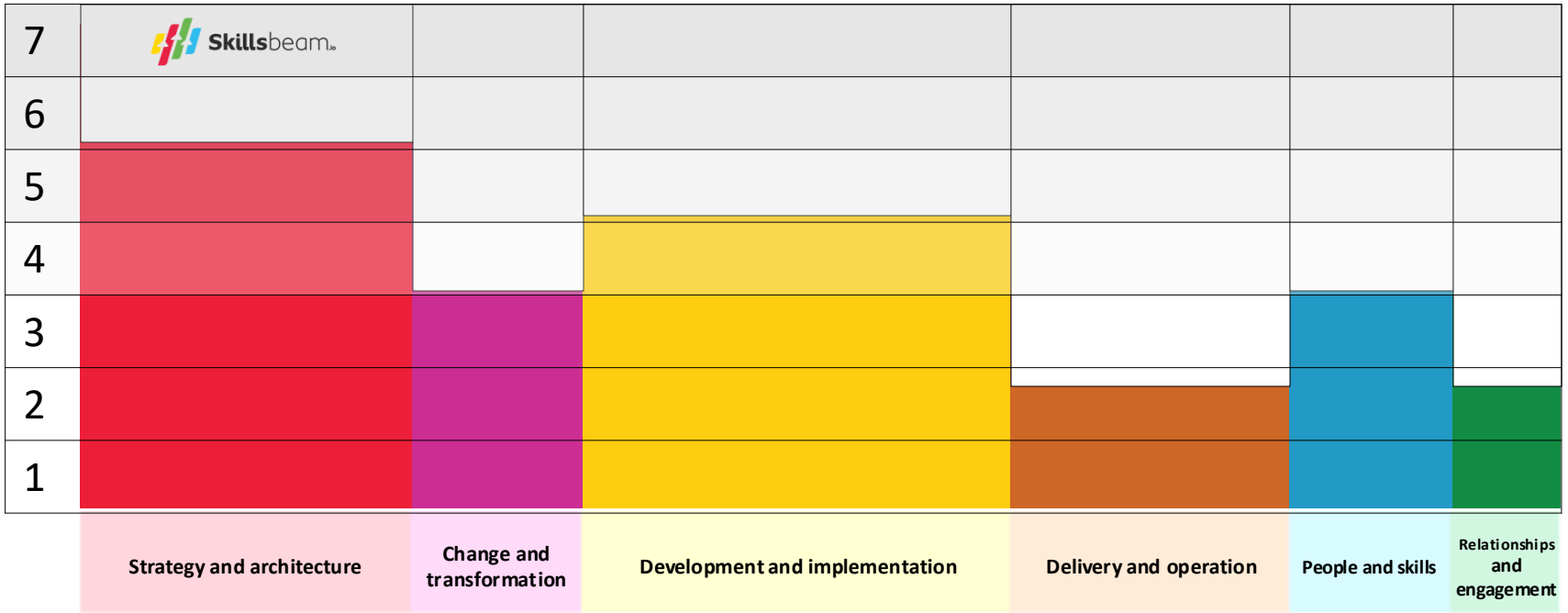
SKILLS MAP

JOHN DOE

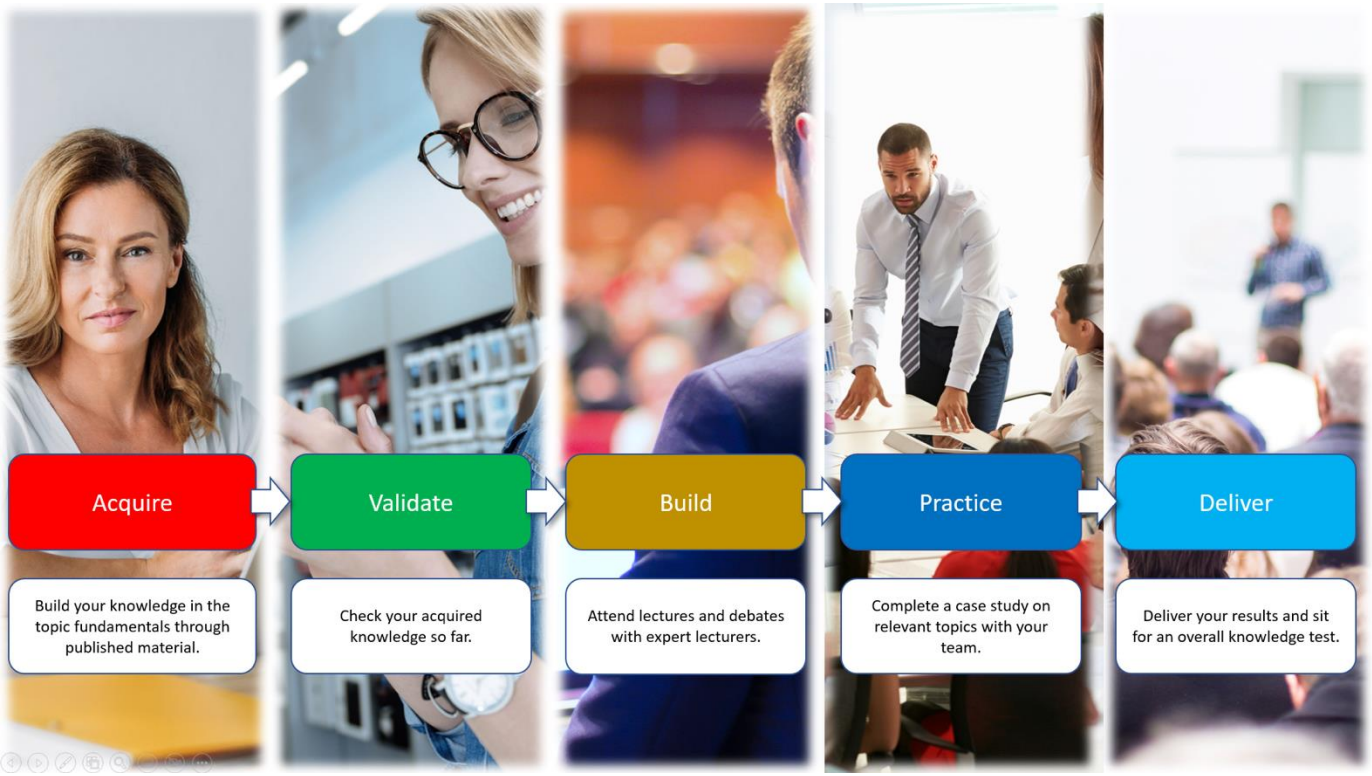


RECOMMENDED LEVELS OF SKILLS CATEGORIES FOR ROLE:

CHIEF INFORMATION OFFICER




ULB
Solvay Lifelong Learning
BRUSSELS SCHOOL OF ECONOMICS & MANAGEMENT
EXECUTIVE MASTER IN
CYBERSECURITY
MANAGEMENT
Solvay.edu/cybersecurity
APPLY NOW



Part 1 (Acquire in an offline learning mode): Plan for a minimum of 12 hours of self-learning where participants obtain self-study resources.

Part 2 (Evaluate): A short self-evaluation survey to test the readiness to attend the F2F classes.

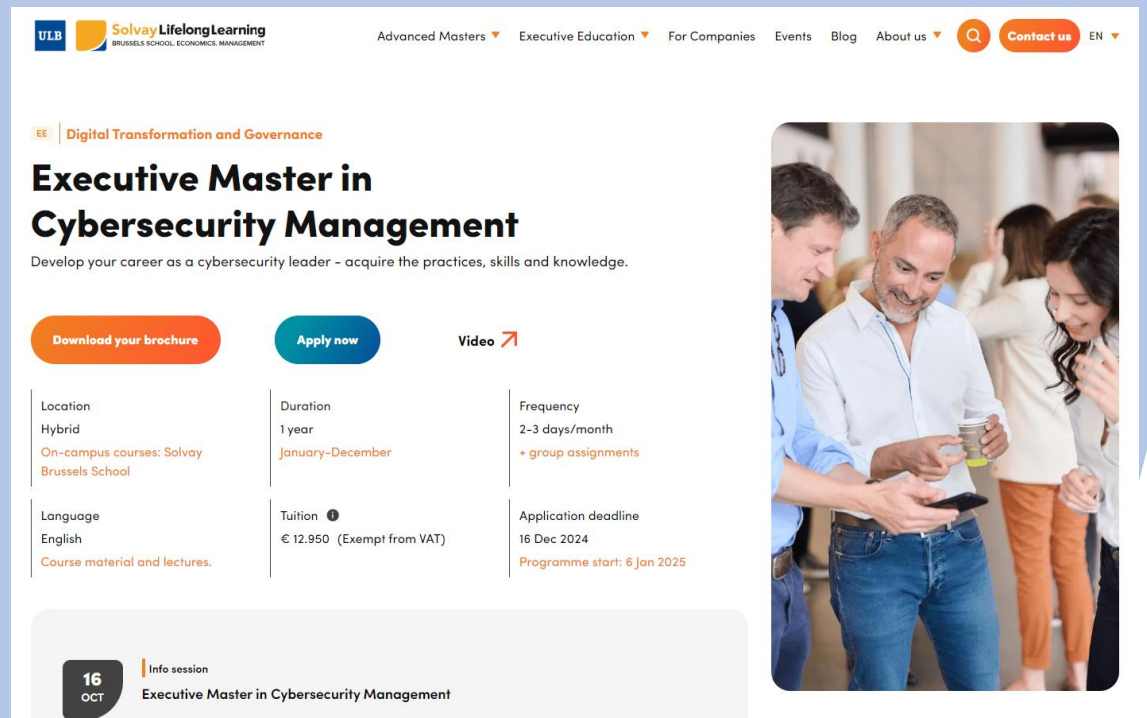
Part 3 (Build expertise): Attend onsite classes and workshops that are also available remotely.

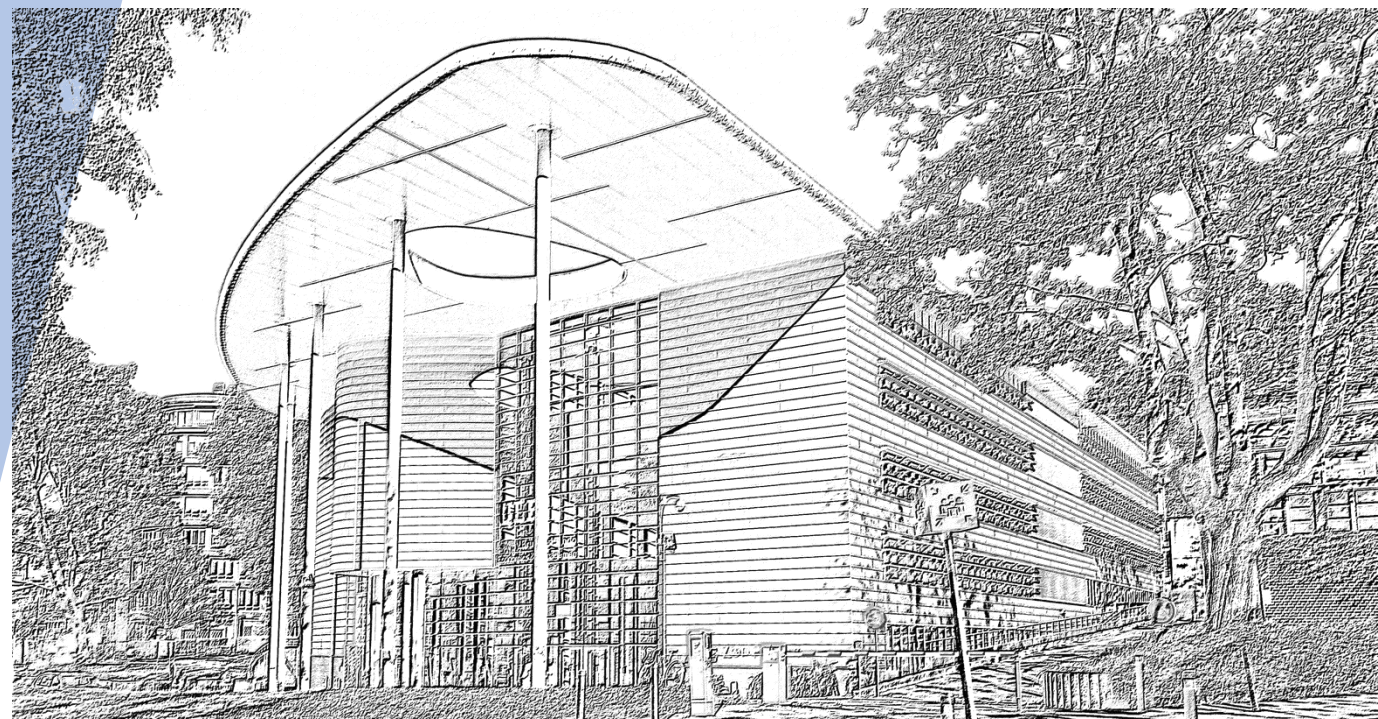
Part 4 (Group Case study): Groups of participants remotely address specific cases related to each module.

Part 5 (Final delivery): Participants present the deliverables of their case study to a jury. This is followed with knowledge-based examination.

SIX LEADERSHIP AREAS

- CISO FUNDAMENTALS
- GRC AND CERTIFICATION
- SECURITY ARCHITECT
- CONTINUITY AND CRISIS MANAGER)
- CYBER SECURITY LEADER
- GENERAL MANAGEMENT





Georges Ataya

gataya@solvay.edu

linkedin.com/in/ataya/

Wallonie
service public
SPW

Fabian Lapierre

SPW EER

Cyberwal
by digital
wallonia

07/11/2024

Wallonie recherche SPW

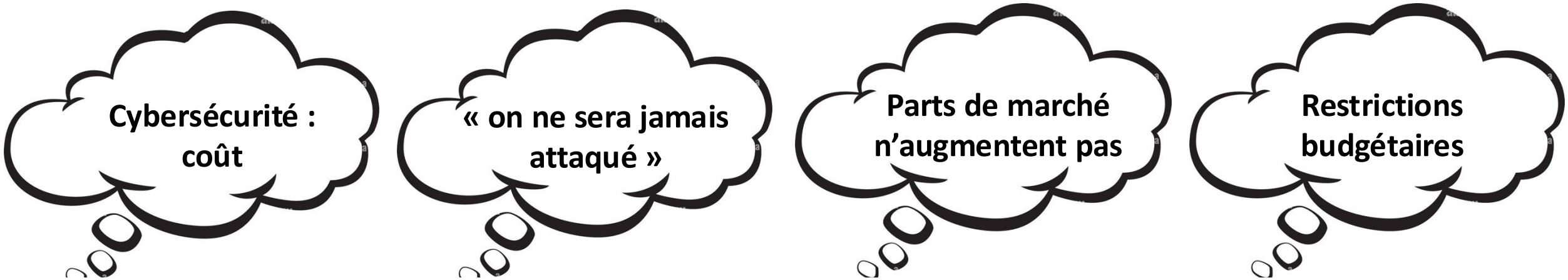
CyberWeek

Renforcer la Cybersécurité grâce à l'Écosystème de Recherche Wallon

Service public de Wallonie économie emploi formation recherche

Démystifier la Cybersécurité

- Idées reçues



- Les cyberattaques ont un coût
  - Méthode proposée par Deloitte : analyser les coûts sur 14 facteurs ;
  - Deux types de coûts pour les facteurs : **directs et indirects**.

Démystifier la Cybersécurité

Facteurs	Type de coût	Description du facteur
Investigation technique	Direct ✓	Analyse des impacts de la cyberattaque sur les systèmes (comment/ pourquoi)
Notification aux clients de l'attaque	Direct ✓	Gestion/ information des clients impactés
Protection des clients après l'attaque	Direct	Services pour détecter et protéger les clients contre les tentatives d'utilisation frauduleuse de leurs données
Mise en conformité	Direct ✓	Frais ou amendes liées à la non-conformité aux réglementations
Relations publiques	Direct ✓	Gestion de la communication externe
Frais juridiques et litiges	Direct ✓	Conseil juridique, litiges (vs SLA et garanties), etc
Amélioration de la cybersécurité	Direct ✓	Coûts R&D pour l'amélioration de l'infrastructure, monitoring, contrôles de sécurité, etc.
Augmentation de la police d'assurance ("malus")	Indirect ✓	Acquisition ou renouvellement d'une assurance risque cybersécurité

Démystifier la Cybersécurité

Coûts liés à la dette	Indirect	Augmentation des taux d'intérêt
Impact opérationnel	Indirect ✓	Gestion opérationnelle, réparations, développement d'une infrastructure temporaire, dériver une partie des ressources pour supporter les solutions alternatives, etc
Perte de valeur dans la relation client	Indirect	Valeur d'acquisition d'un client et de sa contribution aux revenus
Perte de revenus liés à la perte de contrats	Indirect	Perte de revenus et d'opportunités associées à des contrats annulés ou non renouvelés
Impact sur l'image de marque	Indirect ✓	Perte de valeur de la marque entreprise
Perte en Propriété Intellectuelle	Indirect ✓	Perte du contrôle exclusif de secrets d'affaires, copyrights, plans d'investissements et autres informations confidentielles

Contexte actuel

- Respect des législations sur la cybersécurité
  - NIS2;
  - RGPD;
  - Cyber Resilience Act;
- Risques accrus en Belgique (OTAN, Europe, etc)
- Attaques de plus en plus pointues :
  - Activités de R&D nécessaires
- Services Publics :
  - Digitalisation accrue des démarches administratives + approche « Data-centric »
    - Augmentation des risques d'attaques
  - Contexte budgétaire tendu dans le secteur public.

Solution : Créer un « écosystème wallon »

- Créer une **stratégie** pour la cybersécurité en Wallonie :

Cyberwal by Digital Wallonia

- Plusieurs axes :
  - Sensibilisation & accompagnement
  - Formation
  - Recherche (CyberExcellence) : **28 MEUR**
  - Internationalisation
- Valorisation « socio-économique » des résultats par les entreprises wallonnes

Objectifs du programme CyberExcellence

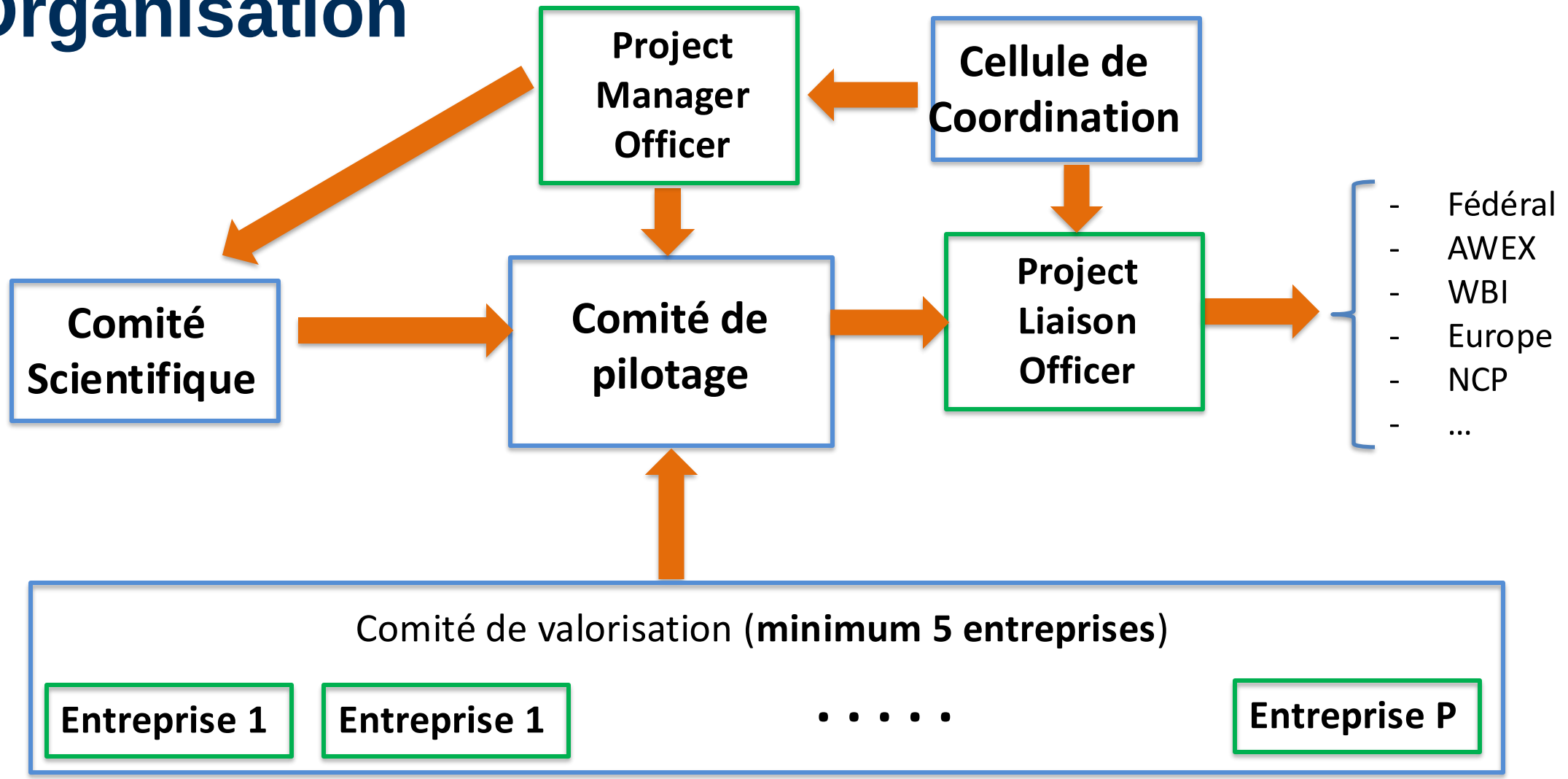
- **Objectif 1** : inciter les Universités à collaborer de manière forte entre elles sur **des projets de grande ampleur dans des technologies jugées prometteuses** en termes de retombées économiques pour la Wallonie. Le projet se doit d'être **structurant** pour les acteurs académiques concernés;

- **Objectif 2 :** réaliser de la recherche de **haut niveau scientifique** et répondant à des **besoins industriels collectifs** du secteur concerné.

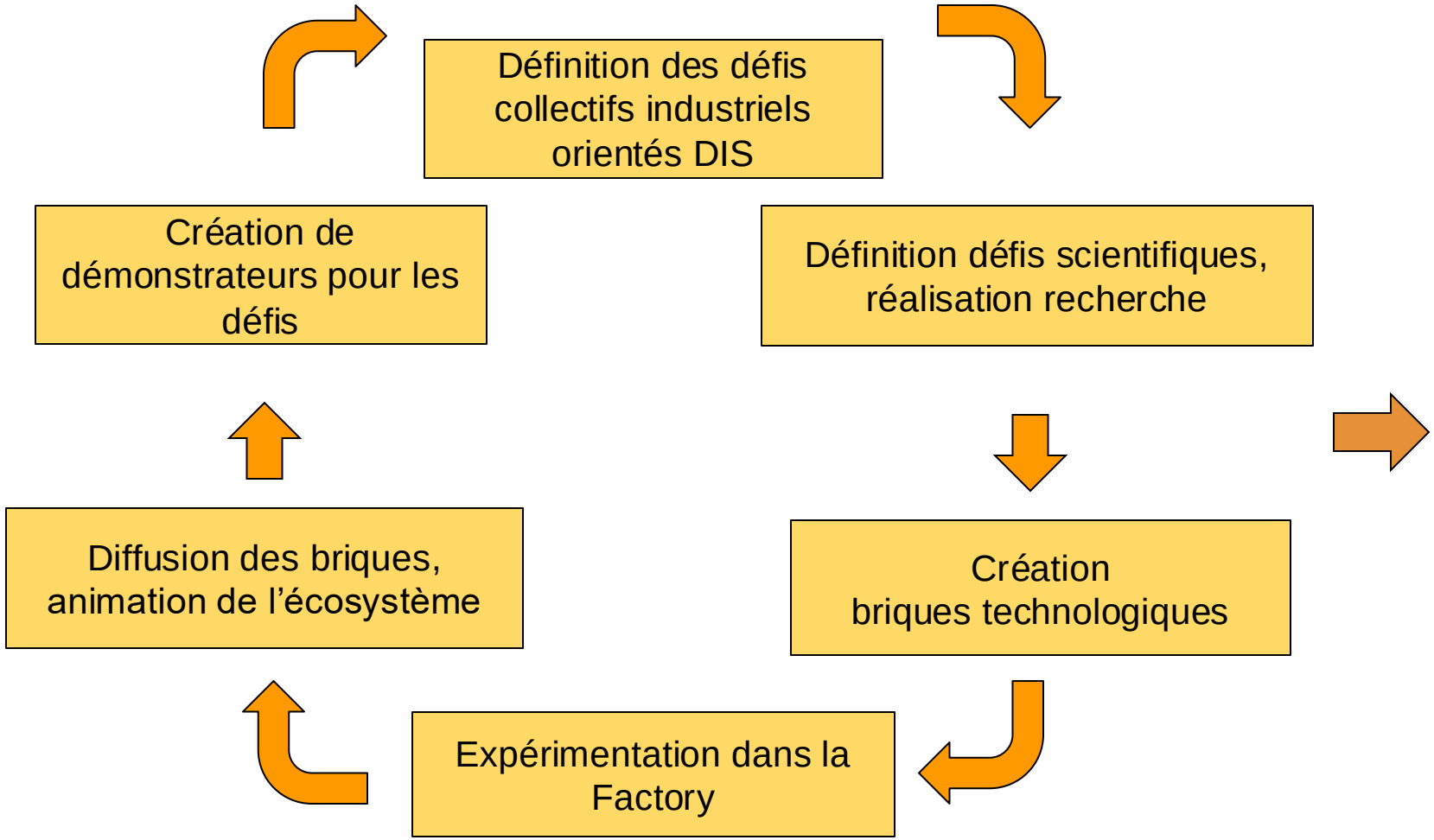
- **Objectif 3 :** augmenter le **rayonnement à l'international** des acteurs du secteur concerné via la création d'un Pôle d'excellence de renommée internationale et d'accroître la participation (et le taux de succès) des acteurs wallons dans les programmes internationaux.

- **Objectif 4** : **former des experts scientifiques et technologiques** (**doctorats**) en phase avec le tissu économique dans le secteur concerné.

Organisation



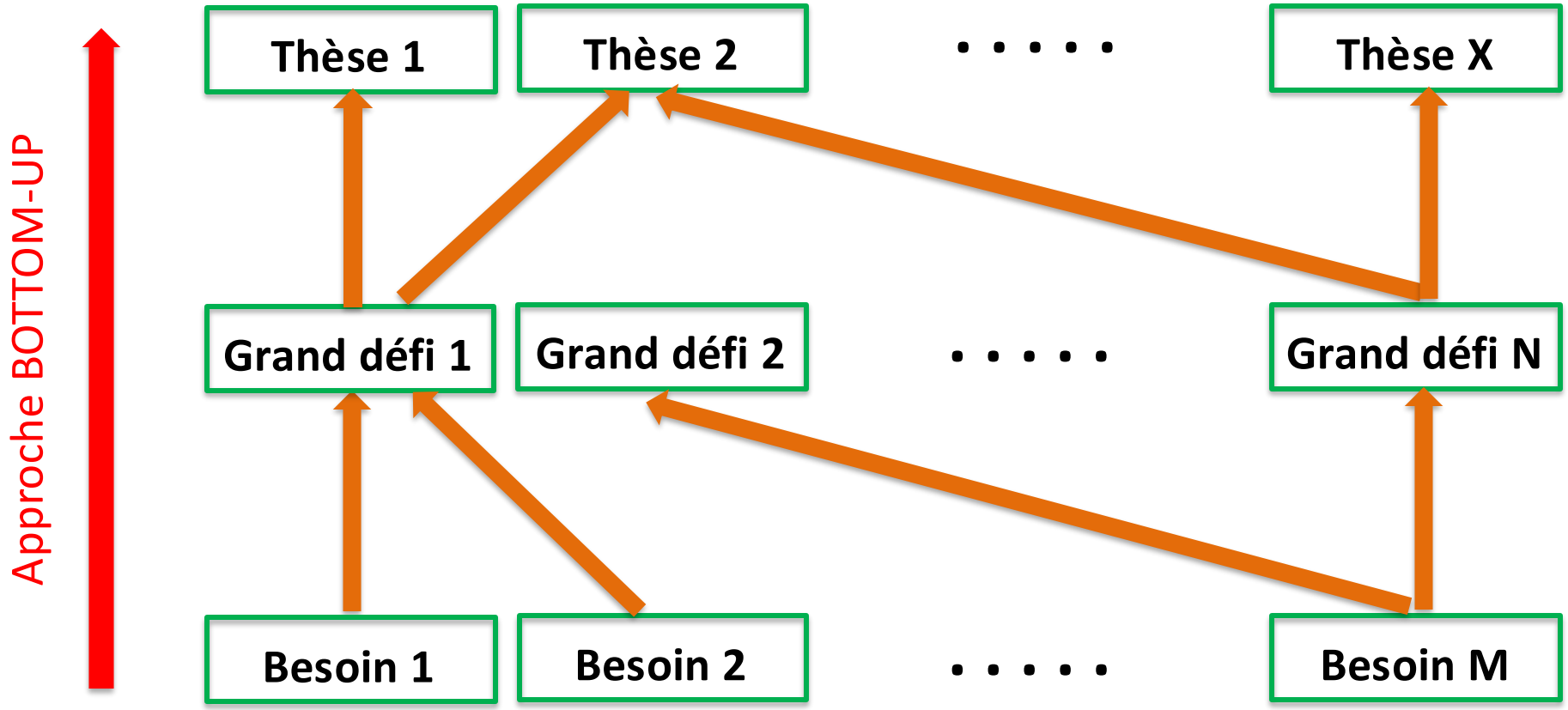
Grands défis



Impacts

- Cyber souveraineté
- Infrastructure plus résiliente
- Baisse du risque de cyberattaques
- Baisse de l'impact des attaques

Liens avec le tissu économique wallon



Cybersécurité et Services Publics

Cyberwal by Digital Wallonia

- **Sensibilisation et accompagnement** : accompagnement personnalisé aux organisations publiques pour les aider à comprendre et à gérer les risques liés à la cybersécurité.
- **Formation** : combler la pénurie de talents en cybersécurité et renforcer les compétences des employés des services publics
- **Recherche et innovation** : collaborer avec des institutions académiques et des entreprises pour développer de nouvelles solutions et technologies.
- **Internationalisation** : se connecter avec des initiatives internationales en cybersécurité, favorisant ainsi l'échange de bonnes pratiques.

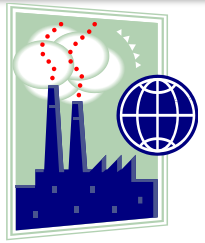
Recherche et Innovation vs Tissu Economique

Financement d'activités de recherche dans les Universités et les Centres de recherche

Wallonie recherche SPW

Transfert des résultats (PI)

Valorisation des résultats de la recherche par le tissu économique wallon



Commercialisation

Entreprises privées ← **Clients** → **Secteur Public**

Axe 1 : Cyber Factory

- « Cyber Factory » :
  - Les travaux de recherche permettent de créer des **briques hardware / software**;
  - Ces briques sont déposées dans une « **Factory** »:
    - Plateforme « Web » permettant d'héberger les briques développées;
    - Ces briques sont téléchargeables et utilisables par tous;
  - « Factory » similaire à une « AppStore » dans le domaine de la Cyber;
  - La « Factory » contient aussi des briques logicielles IA (TRAIL).

Services Publics :

- Evaluer le potentiel des briques de la Factory pour une application dans le Secteur Public.

Axe 2 : Grand Défi

- « Grands défis » :
  - Répondre à des besoins collectifs du tissu économique;
  - Transformer ces besoins en recherche « collective » :
  - Pas de Grand Défi orienté « Besoins collectifs des Services Publics »

Services Publics :

- Evaluer les besoins collectifs des Services Publics
- Evaluer la pertinence de créer un Grand Défi orienté « Secteur Public »
- Evaluer l'intérêt du tissu économique de valoriser les résultats dans le Secteur Public

Axe 3 : Démonstrateurs

- « Démonstrateurs » sur le site de Galaxia (Redu):
  - Cyber Range;
  - Communication quantique.

Services Publics :

- Evaluer la possibilité d'utiliser le Cyber Range par le Secteur Public
- Evaluer la pertinence de créer un Démonstrateur orienté Secteur Public

Services Publics : Economies d'échelle

- Objectif global : réaliser des économies d'échelle
  - Récolte de besoins collectifs ;
  - Développements génériques ;
  - Formation de talents pour créer une expertise interne
    - Experts techniques : infra / software
    - Experts « Traducteurs » : lien entre les axes techniques et non-techniques

Merci pour votre attention

Stéphane Vince

SPW EER

Cyberwal
by digital
wallonia

Plus d’infos sur

digitalwallonia.be/cyber

Cyberwal by digital wallonia

Wallonie Relance