EUROPEAN UNION AGENCY
FOR CYBERSECURITY

MANUEL DE L'UTILISATEUR

CADRE EUROPÉEN DES COMPÉTENCES EN MATIÈRE DE CYBERSÉCURITÉ (ECSF)

À PROPOS DE L'ENISA

L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union chargée d'atteindre un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'UE sur la cybersécurité, l'Agence de l'Union européenne pour la cybersécurité contribue à la politique de l'UE en matière de cybersécurité, renforce la fiabilité des produits, services et processus TIC grâce à des schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'UE, et aide l'Europe à se préparer aux cyber défis de demain. Grâce au partage des connaissances, au renforcement des capacités et à la sensibilisation, l'Agence collabore avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, renforcer la résilience des infrastructures de l'Union et, par conséquent, préserver la sécurité numérique de la société et des citoyens européens. De plus amples informations sur l'ENISA et ses travaux sont disponibles à l'adresse suivante : www.enisa.europa.eu.

CONTACT

Pour contacter les auteurs, veuillez écrire à l'adresse euskills@enisa.europa.eu.

REMERCIEMENTS

Ce cadre est le résultat de l'avis et de l'accord des experts du groupe de travail ad hoc sur le cadre des compétences composé d'Agata BEKIER, Vladlena BENSON, Jutta BREYER, Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku KORKIAKOSKI, Csaba KRASZNAY, Haralambos MOURATIDIS, Christina GEORGHIADOU, Erwin ORYE*, Edmundas PIESARSKAS, Nineta POLEMI*, Paresh RATHOD*, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN et Jan HAJNY.

Fabio DI FRANCO et Athanasios GRAMMATOPOULOS ont dirigé cette activité pour l'ENISA.

AVIS JURIDIQUE

AVIS DE DROIT D'AUTEUR

* Rapporteur du groupe de travail ad hoc sur le cadre européen des compétences en matière de cybersécurité

ISBN : 978-92-9204-583-8 – DOI : 10.2824/95989

TABLE DES MATIÈRES

RÉSUMÉ

La pénurie de main-d'œuvre et de compétences dans le domaine de la cybersécurité est une préoccupation majeure tant pour le développement économique que pour la sécurité nationale. En examinant le problème, l'ENISA a identifié la nécessité pour l'Europe d'adopter une approche globale pour définir un ensemble de rôles et de compétences en matière de cybersécurité qui pourraient être mis à profit pour réduire la pénurie et le déficit de compétences. L'ENISA a travaillé à l'élaboration d'un tel cadre et présente le **Cadre Européen des Compétences en matière de Cybersécurité (ECSF),** qui vise à renforcer la culture européenne de la cybersécurité en fournissant un langage européen commun à toutes les communautés, faisant ainsi un pas essentiel vers l'avenir numérique de l'Europe.

L'ECSF fournit un outil pratique pour **soutenir l'identification et l'articulation des tâches, des compétences, des aptitudes et des connaissances associées aux** rôles des **professionnels européens de la cybersécurité.** L'objectif principal du cadre est de **créer une compréhension commune** entre les individus, les employeurs et les prestataires de programmes d'apprentissage dans l'ensemble des États membres de l'UE, ce qui en fait un outil précieux pour combler le fossé entre le lieu de travail professionnel en cybersécurité et les environnements d'apprentissage.

Le cadre décrit les exigences les plus importantes d'un lieu de travail professionnel en matière **de cybersécurité en définissant un ensemble de 12 profils de fonctions professionnels typiques en matière de cybersécurité.** Ces profils fournissent une compréhension commune des principales missions, tâches et compétences en matière de cybersécurité nécessaires dans un contexte professionnel de cybersécurité, ce qui en fait la référence parfaite pour le profilage des compétences et des connaissances nécessaires aux professionnels de la cybersécurité. Le cadre a été conçu pour être facilement compris et suffisamment complet pour fournir des informations approfondies appropriées en matière de cybersécurité ainsi que suffisamment souples pour permettre une personnalisation en fonction des besoins de chaque utilisateur. En intégrant toutes les perspectives des parties prenantes, le cadre s'applique à tous les types d'organisations et soutient le développement de toutes les professions de la cybersécurité.

L'ECSF est le résultat des travaux menés par le groupe de travail ad hoc de l'ENISA sur le cadre européen des compétences en matière de cybersécurité[2] composé d'experts représentant différents points de vue. Le cadre élaboré repose sur une analyse des cadres existants, des résultats et des conclusions de la recherche sur les besoins du marché et de l'accord des experts. Des études de cas d'utilisateurs et des exemples indicatifs, inspirés de divers environnements de travail et d'apprentissage, démontrent la mise en œuvre pratique de ce cadre et soutiennent ce travail.

Les principaux avantages de l'utilisation de l'ECSF se sont révélés être :

- garantir une **terminologie commune** et une **compréhension commune** des professionnels de la cybersécurité dans l'ensemble de l'UE ;
- recenser l'ensemble **des compétences critiques requises du point de vue de la main-d'œuvre** dans le domaine de la cybersécurité pour soutenir la poursuite de son développement et de son amélioration ;
- promouvoir **l'harmonisation des programmes d'éducation, de formation et de développement de la main-d'œuvre dans le domaine de la** cybersécurité.

Le présent manuel de l'utilisateur de l'ECSF donne un aperçu complet du champ d'application, des principes-cadres et des principales possibilités d'application de l'ECSF. L'objectif principal du manuel est de rendre l'ECSF facilement accessible, compréhensible et utilisable par toutes les parties prenantes jouant un rôle actif ou ayant un besoin de professionnels de la cybersécurité dûment qualifiés.

Le cadre européen de compétences en matière de cybersécurité (ECSF) vise à renforcer la culture européenne de la cybersécurité en fournissant un langage européen commun à toutes les communautés, ce qui constitue une avancée essentielle vers l'avenir numérique de l'Europe.

[2] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

1. INTRODUCTION

La pénurie de compétences en cybersécurité est l'un des principaux défis à relever pour une Union Européenne cyber sécurisée. Plus précisément, il y a un manque de personnel qualifié et compétent sur le marché du travail pour assumer des rôles dans la cybersécurité et qui peut répondre de manière suffisante à l'évolution des cybermenaces et aux défis émergents en matière de cybersécurité. Le manque de compétences en cybersécurité a un certain nombre de facteurs sous-jacents. Il s'agit notamment d'un niveau insuffisant de compréhension des compétences et des aptitudes nécessaires dans la discipline de la cybersécurité entre les différents acteurs du marché des compétences en matière de cybersécurité. Au fil des ans, ce problème est devenu un problème bien documenté[3], qui continue d'affecter de manière significative les pays aux niveaux européen et international.

Afin de réduire le déficit et la pénurie actuels et futurs de compétences, davantage de professionnels de la cybersécurité dotés de compétences appropriées sont nécessaires. À cette fin, la stratégie européenne en matière de compétences[4], le plan d'action en matière d'éducation numérique[5] et le pacte pour les compétences[6] restent des instruments importants pour mobiliser les parties prenantes afin qu'elles travaillent ensemble à la réalisation des objectifs de la décennie numérique[7] en créant des possibilités de formation plus nombreuses et de meilleure qualité.

Dans ce contexte, l'ENISA a lancé un groupe de travail ad hoc sur le cadre européen des compétences en matière de cybersécurité[8] en décembre 2020. Un groupe multidisciplinaire d'experts a été réuni dans le but de promouvoir l'harmonisation des concepts d'éducation, de formation et de développement de la main-d'œuvre en matière de cybersécurité. Le cadre élaboré (ECSF) fournit un outil européen ouvert pour construire une compréhension commune des profils de rôles professionnels en matière de cybersécurité et des cartographies communes avec les aptitudes et compétences appropriées requises. Ces travaux constituent la base pour unir leurs forces dans le cadre d'un programme de renforcement des capacités de la main-d'œuvre européenne dans le domaine de la cybersécurité, en fonction de la demande actuelle du marché.

L'ECSF fournit un outil européen ouvert pour construire une compréhension commune des profils de rôles professionnels en matière de cybersécurité et des cartographies communes avec les aptitudes et compétences appropriées requises.

1.1 AUDIENCE CIBLE

Bien que le champ d'application ultime du contenu du cadre de l'ECSF soit celui des professionnels de base de la cybersécurité, un accent particulier est également mis sur les groupes cibles de l'ECSF constitués d'experts non spécialisés dans la cybersécurité qui ont besoin d'une vue d'ensemble de la discipline. Cette orientation rend le cadre facile à comprendre pour toutes les parties prenantes concernées.

Le public cible de l'ECSF est constitué des équipes dirigeantes des organisations, des ressources humaines (RH) et des fonctions de cybersécurité, des professionnels de la cybersécurité, des nouveaux arrivants et des cyber amateurs, ainsi que des organismes de formation de tous types dans le contexte public et privé, des associations sectorielles, des chercheurs de marché et des décideurs politiques.

Le champ d'application principal du cadre de l'ECSF est celui des professionnels de base de la cybersécurité, mais l'accent est également mis sur les experts non spécialisés en cybersécurité qui ont besoin d'une vue d'ensemble de la discipline.

1.2 STRUCTURE DU MANUEL

Le manuel d'utilisation est structuré comme suit :

[3] ENISA, 2020, Cybersecurity Skills Development in the EU https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[4] https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_1196
[5] https://education.ec.europa.eu/focus-topics/digital-education/action-plan
[6] https://ec.europa.eu/commission/presscorner/detail/fr/qanda_20_1197
[7] https://digital-strategy.ec.europa.eu/fr/node/157
[8] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/adhoc_wg_calls

- Le chapitre 1 présente les principaux défis qui mettent en évidence la nécessité de créer un cadre pour les compétences en matière de cybersécurité ainsi que le public cible pour ce travail ;
- Le chapitre 2 présente les principes de conception de l'ECSF ainsi que les principaux avantages de son utilisation
- Le chapitre 3 explique les différentes applications de l'ECSF sous différents angles.

En outre, le document comprend deux (2) annexes qui soutiennent le manuel d'utilisation de l'ECSF et ses objectifs :

- L'annexe A relie l'ECSF à d'autres normes et cadres de l'UE.
  L'objectif de la présente annexe est de relier l'ECSF aux normes et cadres européens reconnus existants qui sont pertinents pour ces travaux.
- L'annexe B énumère les cas d'utilisation de l'ECSF.
  L'objectif de la présente annexe est de fournir des scénarios concrets afin de mettre en évidence la mise en œuvre pratique de ce cadre.

2. COMPRENDRE L'ECSF

L'ECSF est composé d'un ensemble représentatif de **12 profils de rôle pour les professionnels de la cybersécurité** (présentés dans la figure 1) qui sont généralement requis et appliqués au sein des organisations déployant des professionnels de la cybersécurité. Chaque profil est défini par un modèle commun qui intègre des critères clés (titre, titres alternatifs, résumé, mission, tâches principales, compétences clés, connaissances clés, compétences en ligne). Le contenu de chaque critère est adapté à chaque rôle, mais peut être adapté pour permettre une mise en œuvre flexible afin de répondre à des situations et à des exigences spécifiques.

Figure 1 : Les 12 profils de rôle de l'ECSF pour les professionnels de la cybersécurité

L'ECSF introduit un ensemble représentatif de 12 profils de rôle pour les professionnels de la cybersécurité (généralement requis et appliqués au sein des organisations) dans un format convenu au niveau de l'UE et axé sur la pratique, consacré au domaine professionnel de la cybersécurité.

Les 12 profils de rôle pour les professionnels de la cybersécurité sont fournis dans un format convenu au niveau de l'UE et axé sur la pratique, consacré au domaine professionnel de la cybersécurité. Les profils sont faciles à comprendre et offrent des points d'entrée alternatifs en fonction du contexte, de la perspective et des besoins. Grâce à ces profils, l'ECSF peut être utilisé comme un outil de référence et de communication commun qui peut être appliqué dans différentes organisations et différents pays pour une compréhension mutuelle interne et externe commune.

La structure de chaque profil de rôle est décrite dans le tableau 1 ci-dessous.

Tableau 1 : Les composantes de chaque profil de rôle de l'ECSF

Titre du profil	Le nom du profil de rôle professionnel
Titre(s) alternatif(s)	Répertorie les titres alternatifs typiques sous le même profil.
Récapitulatif	Indique l'objectif principal du profil.
Mission	Décrit la raison d'être du profil.
Élément(s) livrable(s)	Une liste des délivrables typiques du profil, expliquant également la pertinence du profil d'un point de vue non expert.
Tâche(s) principale(s)	Une liste des tâches typiques effectuées par le rôle.
Compétence(s) clé(s)	Une liste des capacités nécessaires pour exécuter les fonctions de travail et les tâches du rôle. Les compétences générales et l'éthique sont rendues explicites dans certains cas.
Connaissances clés	Une liste des connaissances essentielles requises pour exécuter les fonctions et les tâches dans le rôle profilé.
Compétences électroniques (EN16234-1 e-CF)	En lien avec le EN16234-1 e-Competence Framework (e-CF) - Un cadre européen commun pour les professionnels des TIC dans tous les secteurs.

Comme le montre le tableau 1, le profil de chaque rôle est complété par un ensemble d'éléments descriptifs conçus pour donner un aperçu du rôle en termes de description, de tâches et de compétences. Les titres et les titres alternatifs typiques peuvent être utilisés comme référence rapide pour guider les utilisateurs de l'ECSF vers les profils de rôle les plus appropriés pour leur application.

Les composantes des profils de rôle **peuvent être modifiées** pour mieux couvrir les besoins des parties prenantes, et les **profils de rôle** (du ECSF et d'autres cadres) **peuvent être mélangés pour** la même raison. De plus amples informations sur l'application du Fonds européen de stabilité financière sont fournies au chapitre 3.

Les compétences non techniques (également appelées compétences transversales, transférables ou comportementales) sont des composantes nécessaires dans tout ensemble de compétences professionnelles ; par conséquent, ces compétences sont également nécessaires pour les professionnels du domaine de la cybersécurité. Un large éventail de compétences relève des compétences générales telles que la capacité de communiquer, de collaborer avec les autres, de signaler, d'influencer, de penser de manière critique et de gérer le temps et le stress. Les compétences générales clés sont intégrées dans la composante des compétences clés.

Par exemple, le profil de rôle d'un dirigeant principal de la sécurité de l'information (CISO) inclut comme compétences clés les capacités d'influencer, de diriger, de communiquer, de coopérer et de collaborer. Toutes ces compétences sont essentielles pour qu'un CISO puisse accomplir ses missions et tâches. Sur la base des besoins d'une partie prenante, des compétences non techniques supplémentaires peuvent être ajoutées au profil d'un CISO ou une cartographie avec un cadre de compétences non techniques peut être effectuée.

L'éthique est également un élément transversal important qui a une incidence sur tous les aspects de la cybersécurité et constitue donc une composante essentielle des compétences dans le cadre européen des compétences en matière de cybersécurité (ECSF). Dans le contexte de la cybersécurité, l'éthique concerne les décisions qui sont alignées sur nos valeurs et ce qui est moralement acceptable à la fois pour le propriétaire des données et pour l'organisation. Comme les professionnels de la cybersécurité pourraient avoir un accès privilégié à divers types d'informations,

notamment sensibles, la conscience éthique est une valeur importante qu'ils devraient avoir. En dehors de cela, la prise de décision éthique est une compétence importante que les professionnels de la cybersécurité devraient avoir car leurs décisions affectent d'autres personnes. Comme dans le cas des compétences non techniques, l'ECSF a explicitement analysé si le volet éthique du secteur était aligné sur les valeurs et l'éthique européennes.

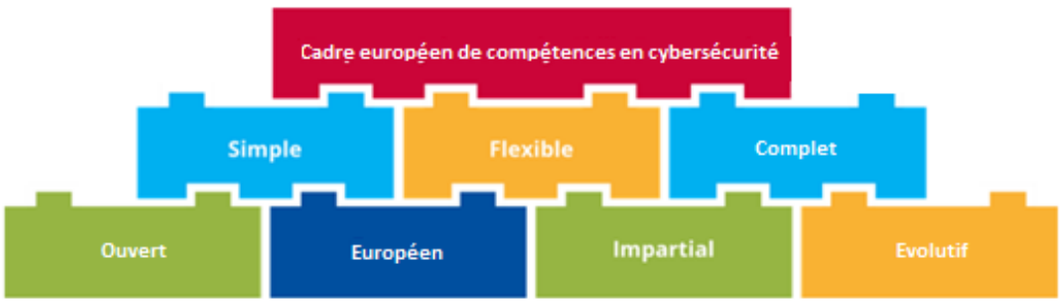
Une analyse plus détaillée des compétences non techniques et éthiques pourrait être effectuée par la partie intéressée, étant donné que le cadre est flexible et adaptable.

2.1 LES PRINCIPES DE CONCEPTION DE L'ECSF

Le cadre européen des compétences en matière de cybersécurité repose sur un certain nombre de principes conçus pour répondre aux besoins des parties prenantes. Cela facilite la compréhension, l'adoption et l'application du cadre tout en maintenant la pertinence et l'impact à court et à long terme.

L'ECSF est basé sur des principes conçus pour couvrir les besoins des parties prenantes, offrant une compréhension, une adoption et une application faciles tout en maintenant la pertinence et l'impact à court et long terme.

Figure 2 : Principes de conception de l'ECSF



2.1.1 Simple mais complet

Le cadre est conçu de manière à être suffisamment général pour être facilement compris et appliqué par un public plus large. Dans le même temps, il comprend suffisamment de détails pour fournir des informations approfondies sur la cybersécurité. Ces attributs facilitent l'utilisation du cadre dans un large éventail d'activités et d'environnements et par des parties prenantes d'horizons divers (par exemple, des organisations de tailles différentes, une expertise technique d'intensité variable et des secteurs d'activité ayant des activités de base différentes).

Cet objectif a été atteint en appliquant le niveau de détail approprié au contenu de l'ECSF, qui n'est ni trop spécifique ni trop abstrait. Offrant 12 profils, l'ECSF couvre un large éventail d'activités de travail diverses, mais maintient un format facile à utiliser.

2.1.2 Flexible et évolutif

En adoptant une approche modulaire et une structure flexible, le cadre permet à chaque composant d'être extensible ou utilisé indépendamment. Ces caractéristiques permettent d'étendre davantage l'ECSF et/ou d'établir des liens avec d'autres cadres pour étendre ses applications.

En appliquant cette flexibilité, les profils et leurs composants, tels que définis par l'ECSF, peuvent être appliqués module par module permettant à chacun d'être adapté pour répondre à des besoins spécifiques. Cette flexibilité garantit la pertinence du cadre au fil des ans et permettra également de simples mises à jour du cadre à l'avenir.

2.1.3 Ouvert et impartial

Le cadre a été élaboré avec la contribution d'un groupe de travail important et diversifié composé d'experts professionnels en cybersécurité. Afin de développer un cadre impartial, l'ENISA a créé ce groupe à partir d'une variété d'experts d'horizons divers. En impliquant des experts d'horizons différents, le processus d'élaboration du cadre a suivi une approche multidimensionnelle éliminant tout biais en faveur de domaines d'intérêt spécifiques. En outre, en tant que publication de l'ENISA, le cadre est disponible publiquement, accessible et ouvert. Les profils et composantes de l'ECSF ont

été élaborés sur la base d'une perspective multipartite, en mettant l'accent non seulement sur le point de vue de l'emploi dans le domaine de la cybersécurité, mais aussi du point de vue des prestataires de programmes d'apprentissage. En outre, la véracité du cadre a été renforcée par l'engagement et les examens d'une variété d'intervenants supplémentaires.

2.1.4 Européen

Poussé par l'exigence de réduire au minimum les lacunes en matière de compétences en cybersécurité et les pénuries de main-d'œuvre dans toute l'Europe, l'ECSF devait être conforme aux exigences européennes spécifiques, afin de permettre une adoption et une utilisation faciles par les organisations européennes. Cette orientation a été guidée par le respect des normes et cadres européens existants.

L'ECSF se connecte bien avec le paysage professionnel européen actuel des TIC pour assurer une adoption facile et une large reconnaissance. L'ECSF tire le meilleur parti des expériences et structures existantes et établit des liens cohérents avec les normes et cadres professionnels pertinents de l'UE en matière de TIC. Les profils définis par le cadre sont conçus pour être conformes et complémentaires aux lois et réglementations européennes et pour améliorer les approches de l'éthique européenne telles qu'identifiées sur le marché européen. L'ECSF prend en considération les exigences de protection des données et de la vie privée fixées par la réglementation européenne, les rôles communs demandés par le marché européen et les normes et cadres européens utilisés dans le secteur des TIC.

2.2 LES PRINCIPAUX AVANTAGES FOURNIS PAR L'ECSF

L'ECSF est un outil facile à utiliser mais complet. Il est basé sur des études de marché récentes, la collaboration d'experts en cybersécurité et une analyse du paysage plus large de la cybersécurité et des cadres TIC. Il exprime ainsi les besoins pertinents du marché européen. Il se compose de 12 rôles professionnels typiques en matière de cybersécurité, accompagnés d'un résumé, d'une mission principale, de résultats observables (livrables), de tâches, de compétences, d'aptitudes, de connaissances et de niveaux de compétences, selon les besoins et appliqués dans le contexte du travail en Europe, à comprendre et à utiliser dans toute l'Europe.

L'ECSF fournit une référence sans ambiguïté pour identifier et réduire les pénuries et les lacunes actuelles et futures en matière de compétences en cybersécurité.

L'ECSF fournit une référence sans ambiguïté pour identifier et réduire les pénuries et les lacunes actuelles et futures en matière de compétences en cybersécurité. Il est générique, mais en même temps suffisamment précis pour donner au marché de l'UE une taxinomie claire des aptitudes, des compétences et des professions au sein de la main-d'œuvre dans le domaine de la cybersécurité. En outre, il peut être facilement relié à d'autres structures et cadres existants dans des domaines connexes.

L'utilisation de l'ECSF comme langage européen commun pour les rôles, les aptitudes, les connaissances et les compétences professionnelles en matière de cybersécurité offre de nombreux avantages, dont certains sont énumérés ci-dessous.

1. L'utilisation de l'ECSF garantit une terminologie commune et une compréhension partagée entre la demande professionnelle en matière de cybersécurité (lieu de travail, recrutement) et l'offre (qualification, formation, évaluation et reconnaissance) dans l'ensemble de l'UE.
2. L'ECSF soutient l'identification des exigences essentielles en matière de compétences du point de vue de la main-d'œuvre. Il permet aux prestataires de programmes d'apprentissage de soutenir le développement des compétences essentielles et aux décideurs politiques de soutenir des initiatives ciblées visant à atténuer les lacunes recensées en matière de compétences.
3. L'ECSF aide à comprendre les rôles professionnels en matière de cybersécurité et les compétences essentielles requises, ainsi que la législation pertinente. En particulier, les non-experts et les départements RH sont en mesure de mieux comprendre les exigences en matière de planification des ressources, de recrutement et de planification de carrière en matière de cybersécurité.
4. L'ECSF promeut l'harmonisation en matière d'éducation, de formation et de développement de la main-d'œuvre dans le domaine de la cybersécurité. En outre, l'utilisation d'un langage européen

commun dans les compétences et les rôles en matière de cybersécurité concerne directement l'ensemble du domaine professionnel des TIC.

5. L'ECSF contribue à améliorer la résilience face aux cyberattaques et à garantir la sécurité des systèmes TIC dans l'ensemble de la société. Il fournit une structure standard et donne des conseils sur la manière de renforcer les capacités de la main-d'œuvre européenne dans le domaine de la cybersécurité.

L'ECSF offre des avantages supplémentaires en fonction du type de partie prenante. Un exemple des principales parties prenantes et des principaux avantages associés est présenté au point 3.

Figure 3 : Exemple des principaux bénéficiaires du ECSF exprimant la nécessité d'une définition commune du gestionnaire des risques

Le tableau 2 présente une liste détaillée des applications et des avantages potentiels de l'utilisation de l'ECSF, sur la base des parties prenantes.

Tableau 2 : Applications et avantages potentiels de l'ECSF pour les parties prenantes

Partie prenante	Avantages de l'utilisation de l'ECSF

Organisations	• soutient le développement d'une stratégie et d'une structure d'organisation en matière de cybersécurité;
	• soutient le développement de la planification des ressources humaines en matière de cybersécurité;
	• apporte un soutien dans le processus de recrutement, en particulier:
	  ○ l'identification des exigences relatives au rôle en matière de cybersécurité;
	  ○ l'évaluation des candidats à la cybersécurité
	• fournit une analyse du rôle de la cybersécurité et des lacunes en matière de compétences, ce qui permet de prévoir les besoins au niveau de l'individu, de l'équipe ou de l'organisation
	• définit des plans de développement et de formation au niveau individuel, en équipe ou organisationnel
	• soutient l'évaluation des rôles en matière de cybersécurité en contribuant à la mise en place de services personnalisés modèles pour les rôles en matière de cybersécurité
	• fournit un langage commun et facile à comprendre pour les appels d'offres en matière de cybersécurité marchés publics, postes vacants et audits

Fournisseurs de programmes d'apprentissage	• soutient la conception, la refonte et la maintenance de programmes d'apprentissage et de programmes d'études • offre une collaboration interinstitutionnelle et une mobilité dans le cadre de programmes d'apprentissage, par ex. programmes d'apprentissage transeuropéens de plusieurs institutions • encourage l'offre de programmes d'apprentissage et sensibilise • positionne les acquis d'apprentissage dans un contexte de travail réel • soutient les processus d'évaluation et de reconnaissance • fournit une orientation professionnelle aux étudiants

Particulier	• aide les individus à faire des choix de carrière professionnels et à se positionner eux-mêmes • élargit les perspectives d'apprentissage, ouvre de nouveaux chemins de carrière et favorise le développement professionnel afin de soutenir la requalification et l'amélioration des compétences • aide à comprendre les exigences pratiques du lieu de travail et les attentes professionnelles dans plus détail • identifie les parcours d'apprentissage formels et non formels • fournit un soutien dans la construction de cheminements de carrière
Associations professionnelles	• permet la consolidation des communautés de parties prenantes pour soutenir le partage des connaissances, les nouveaux développements, les améliorations et la poursuite de la mise en œuvre dans les États membres de l'UE • fournit un soutien dans la réalisation d'analyses de marché et la présentation des résultats dans un langage partagé • aide à fournir des conseils professionnels complets dans le secteur de la cybersécurité
Les décideurs politiques et les parties prenantes gouvernementales	• soutient une compréhension commune dans le domaine de la cybersécurité • stimule la planification des priorités et le renforcement des capacités en matière de cybersécurité • permet de cartographier de nombreuses initiatives en matière de cybersécurité sur la base des profils de l'ECSF • soutient les initiatives politiques fondées sur l'analyse des données;
Tous	• offre un langage commun à toutes les parties prenantes • accélère la collaboration en fournissant un point de départ de référence commune • fournit une référence partagée pour rassembler et présenter les professionnels de la cybersécurité liés information et besoins à tous les niveaux, national, européen et international

3. DEMANDES DE L'ECSF

Ce chapitre montre comment le cadre européen des compétences en matière de cybersécurité (ECSF) peut être appliqué de manière modulaire et flexible en fonction des besoins des différentes parties prenantes.

L'utilisation spécifique et l'application pratique dépendent de nombreux facteurs tels que la perspective du marché, la taille de l'organisation, le contexte d'une performance particulière et l'objectif global.

Les 12 profils de rôle pour les professionnels de la cybersécurité définis par l'ECSF sont un outil flexible et une référence européenne standard pour une utilisation personnalisée dans un contexte particulier.

Le guide général en cinq étapes suivant fournit une orientation de base :

Les 12 profils de rôles définis par l'ECSF sont un outil flexible et une référence européenne standard pour une utilisation personnalisée dans un contexte particulier.

Figure 4 : Un guide modulaire en cinq étapes pour l'application de l'ECSF

1. **Analyser** la situation de l'environnement cible.
   Recueillir et traiter les informations appropriées nécessaires sur l'état lié à la cybersécurité de l'environnement cible (par exemple, une organisation) afin de créer une base de référence. Identifier les parties impliquées et l'objectif à atteindre.

2. **Identifier** les objectifs spécifiques à atteindre.
   Examiner l'état de l'environnement cible et recenser toute exigence spécifique liée à la cybersécurité à couvrir ou tout objectif à atteindre par l'environnement ciblé. En fonction de la situation, il peut être possible d'utiliser l'ECSF comme taxonomie pour identifier les objectifs en question.

3. **Sélectionner** les composantes appropriées de l'ECSF.
   Examiner les profils ECSF et sélectionner les profils pertinents pour une situation particulière. Ensuite, sélectionnez les composants qui aident à couvrir les besoins ou à atteindre les objectifs requis de l'environnement ciblé.

4. **Adaptez** les composants sélectionnés en fonction de vos besoins.
   Apporter les modifications appropriées aux composants sélectionnés pour mieux s'adapter à une situation particulière et/ou à un environnement ciblé. Les profils ECSF et/ou leurs composantes peuvent être mélangés, scindés ou intégrés dans un contexte sectoriel spécifique en fonction des besoins de chaque situation.

5. **Appliquez** les composants personnalisés à l'environnement cible.
   Prendre des mesures en utilisant les composantes adaptées du FSCE pour couvrir les objectifs liés à la sécurité nécessaires pour améliorer la situation de l'environnement cible et atteindre l'objectif organisationnel.

Le tableau 3 présente quelques exemples indicatifs d'applications du ECSF suivant les cinq étapes présentées ci-dessus.

Tableau 3 : L'approche modulaire de l'ECSF dans la pratique

EXEMPLE	ETAPE	DESCRIPTION
EMPLOYER DES PROFESSIONNELS DE LA CYBERSÉCURITÉ DANS UNE ORGANISATION	1. Analyse	Analyser l'état actuel de l'organisation en matière de cybersécurité.
	2. Identifier	Identifier le manque de personnel pour gérer l'augmentation des problèmes de cybersécurité.
	3. Sélectionner	Sélectionnez la tâche appropriée à partir d'un profil ECSF qui articule une pénurie ou une lacune identifiée dans des compétences spécifiques.
	4. Adapter	Combiner les profils de l'ECSF avec les tâches présentant un intérêt pour l'organisation et structurer les nouveaux rôles avec les tâches, les compétences et les connaissances actualisées afin de répondre à l'évolution des besoins organisationnels et de créer des rôles modifiés en matière de cybersécurité.
	5. Appliquer	Utilisez le profil nouvellement créé pour créer des offres d'emploi ciblées sur les besoins spécifiques de l'organisation.
AMÉLIORER LES COMPÉTENCES DES PROFESSIONNELS DE LA CYBERSÉCURITÉ	1. Analyse	Comprendre les objectifs commerciaux et la stratégie de l'organisation.
	2. Identifier	Identifier tout manque d'expertise et de personnel dans les domaines liés à la cybersécurité.
	3. Sélectionner	Utilisez le(s) profil(s) de l'ECSF pour identifier les compétences et connaissances associées qui font défaut à l'organisation.
	4. Adapter	Analyser certaines compétences et connaissances de l'ECSF afin d'identifier les besoins de formation d'un professionnel de la cybersécurité pour répondre aux besoins de l'organisation.
	5. Appliquer	Identifier les interventions de formation visant à renforcer les compétences de la main-d'œuvre de l'organisation.
FAIRE SES PROPRES CHOIX DE CARRIÈRE	1. Analyse	Choisissez un cheminement de carrière qui vous intéresse.
	2. Identifier	Identifiez votre manque de compétences et les connaissances requises pour vous lancer dans le secteur de la cybersécurité.
	3. Sélectionner	Identifiez le(s) profil(s) de l'ECSF que vous jugez utile(s) du point de vue de l'évolution de carrière et utilisez les aptitudes, connaissances et compétences connexes comme lignes directrices pour la reconversion et le perfectionnement professionnels.
	4. Adapter	Améliorer les profils ECSF sélectionnés en y incluant des compétences et des connaissances supplémentaires en fonction des besoins individuels.
	5. Appliquer	Identifier un programme de formation intégrant la majorité du développement de compétences et de connaissances nécessaires pour se reconvertir ou se perfectionner pour le profil.

3.1 PROFESSIONNELS DE LA CYBERSÉCURITÉ EN MATIÈRE D'EMPLOI – APPLIQUER L'ECSF EN TANT QU'ORGANISATION

L'ECSF peut être utilisé comme guide et feuille de route fournissant une compréhension commune entre les parties concernées en ce qui concerne les rôles au sein d'une organisation en matière de cybersécurité.

L'ECSF fournit un ensemble de référence standard de 12 rôles typiques exécutés par les professionnels de la cybersécurité d'un point de vue organisationnel, couvrant les besoins de cybersécurité des organisations et les processus de cybersécurité qui doivent être suivis afin de sécuriser leurs activités, leurs produits, leurs services et leurs chaînes d'approvisionnement. **Le cadre fournit ainsi un guide et une feuille de route précieux non seulement pour la création, l'expansion et l'exploitation de fonctions liées à la cybersécurité au sein d'une organisation, mais aussi pour s'assurer que sa mission, sa vision et ses objectifs liés à la cybersécurité sont atteints.** Ainsi, une organisation peut utiliser l'ECSF comme point de départ ou comme guide pour accéder rapidement et facilement aux rôles principaux nécessaires pour gérer ses risques de cybersécurité et développer son approche de la cybersécurité. Dans le même temps, les profils de l'ECSF fournissent une compréhension commune entre les parties concernées en ce qui concerne les rôles d'une organisation en matière de cybersécurité.

Trois exemples indicatifs, qui sont présentés plus loin dans le présent chapitre, visent à mettre en évidence la mise en œuvre pratique du cadre dans les domaines suivants :

I. l'amélioration des pratiques en matière de cybersécurité d'une petite entreprise;
II. processus de recrutement d'une grande entreprise avec des exigences de conformité croissantes;
III. planification des ressources de cybersécurité dans une grande organisation.

Exemple I : *L'amélioration des pratiques de cybersécurité d'une petite entreprise* présente l'application de l'ECSF pour répondre aux besoins d'une petite entreprise qui cherche à améliorer sa structure et ses pratiques en matière de cybersécurité. Il montre comment une entreprise pourrait utiliser l'ECSF pour soutenir l'élaboration d'une stratégie de cybersécurité, y compris la planification des ressources humaines pour la cybersécurité et la planification des achats de cybersécurité.

En utilisant l'ECSF comme point de départ ou comme guide, l'entreprise n'a pas besoin d'inventer ou de rechercher les rôles de base nécessaires pour améliorer sa posture de cybersécurité. Les rôles peuvent être attribués à différentes personnes ou peuvent être fusionnés pour être assumés par une seule ou seulement quelques personnes en fonction de la stratégie, des exigences, des besoins et du budget.

L'exemple montre également comment l'ECSF peut soutenir l'organisation dans le processus de recrutement en identifiant les rôles et responsabilités en matière de cybersécurité qui sont nécessaires au sein d'une petite entreprise. Dans cet exemple, une analyse du rôle de la cybersécurité et du déficit de compétences et une prévision conséquente des besoins au niveau organisationnel sont également fournies. En plus de soutenir les processus de ressources humaines dans le recrutement, l'ECSF fournit également un langage commun pour l'achat de services de cybersécurité.

Exemple I : Améliorer les pratiques de cybersécurité d'une petite entreprise

Une petite entreprise de services cloud a connu le succès en quelques mois à peine après que les fondateurs, Alicia et Max, ont mis en œuvre leur idée d'une solution innovante. Alicia était le génie expert de la « technologie », tandis que Max était un génie du marketing. Malheureusement, aucun d'entre eux n'avait d'expérience dans la gestion ou la construction d'une entreprise. Après un an, l'entreprise a commencé à décoller et ils ont donc déménagé dans leur propre bureau et employé du personnel pour développer l'entreprise. Au cours de cette phase d'expansion, personne n'a

envisagé d'organiser l'entreprise. De nombreux rôles et tâches ont été partagés, et les défis ont été traités de manière ad hoc. Heureusement, aucun incident de cybersécurité grave ne s'est produit au cours de cette phase de transition.

Finalement, la société a acquis une certaine visibilité médiatique qui est devenue virale, ce qui a entraîné un intérêt accru des nouveaux investisseurs et clients pour la petite start-up. Cependant, les grands clients et investisseurs ont exigé l'assurance et la preuve de mesures de sécurité adéquates et d'une structure organisationnelle avant de s'impliquer dans l'entreprise. Les fondateurs ont réalisé qu'ils devraient vraiment façonner les choses au sein de leur organisation. Ils étaient conscients que la clé **du succès de l'organisation** était les employés et que, pour permettre à l'organisation de prospérer et d'offrir des services résilients, **il était essentiel de définir leurs rôles et responsabilités en matière de cybersécurité**. Cependant, la question à laquelle il fallait répondre était de savoir quelle organisation était nécessaire et quels rôles et quels types de compétences l'organisation avait-elle besoin ?

Les bailleurs de fonds ont **utilisé l'ECSF et ont identifié que leur organisation avait besoin de cinq rôles clés** pour soutenir leur base de référence en matière de cybersécurité :

- un responsable stratégique de la cybersécurité (CISO)
- un juriste en cybersécurité
- un architecte en cybersécurité
- quelques chargés de mise en œuvre en cybersécurité
- un intervenant en cas de cyber attaque

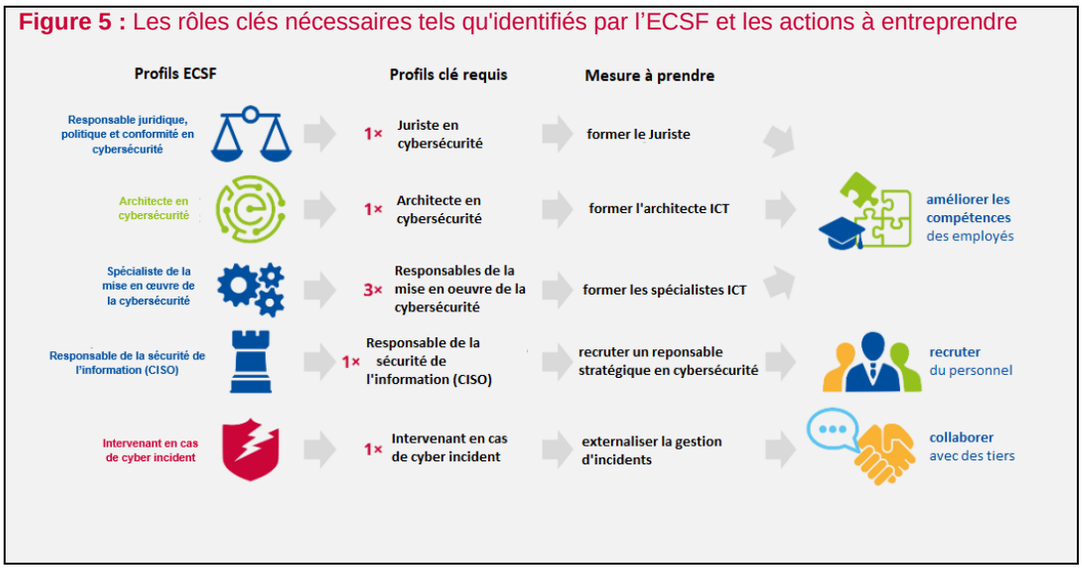
En cherchant en interne à **déterminer** si leurs **employés** étaient **en mesure de remplir ces rôles**, ils ont constaté que leur conseiller juridique gérait déjà le respect des cadres juridiques et réglementaires et qu'elle avait intérêt à **enrichir** ses **compétences** en matière de protection de **la vie privée et de cybersécurité**. Les ressources humaines seraient en mesure **de soutenir le perfectionnement professionnel en utilisant** une liste de **connaissances** et de **compétences** clés acquises dans **le cadre de l'ECSF**.

L'architecte TIC de l'organisation avait une expérience préalable dans la conception de réseaux sécurisés et, par conséquent, avec une formation supplémentaire pour **mettre à jour et enrichir** ses **compétences**, il pouvait également **couvrir les exigences de cybersécurité architecturale de l'organisation**.

Les administrateurs système suivaient de nombreuses bonnes pratiques en matière de cybersécurité, mais travaillaient principalement de manière ad hoc sans stratégie ni structure. Par conséquent, les fondateurs **ont identifié la nécessité de recruter un responsable stratégique de la cybersécurité**. Le responsable du recrutement a été chargé de **rédiger une description de poste sur la base du profil du CISO de l'ECSF** et de répertorier le poste vacant sur son site web.

Enfin, il a été établi que les fonctions de réaction aux incidents de l'entreprise devaient fonctionner 24 heures sur 24 et 7 jours sur 7 pour assurer le fonctionnement continu des services.

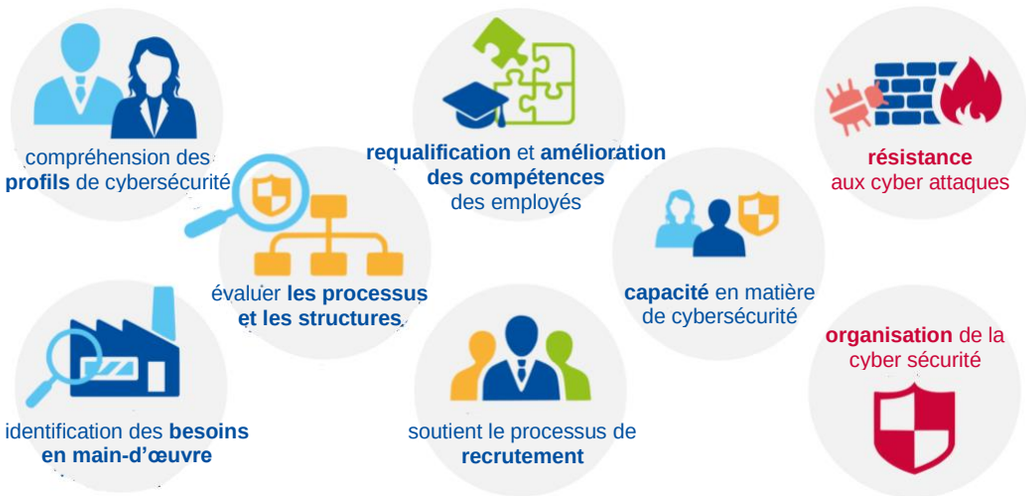
Figure 5 : Les rôles clés nécessaires tels qu'identifiés par l'ECSF et les actions à entreprendre



L'exemple I montre à quel point l'ECSF peut être utile pour les avantages suivants :

- comprendre les rôles en matière de cybersécurité
- identifier les besoins en main-d'œuvre
- évaluer les processus et la structure
- la reconversion et/ou le perfectionnement professionnels des salariés;
- soutenir le processus de recrutement
- renforcer les capacités en matière de cybersécurité
- construire une organisation cyber sécurisée et de confiance
- renforcer la résistance face aux cyberattaques.

Figure 6 : Avantages de l'utilisation de l'ECSF, comme le montre l'exemple



Exemple II : *L'élaboration d'une description de poste* démontre l'application de l'ECSF lors de la création d'une description de poste. Il montre comment l'ECSF peut être bénéfique du point de vue des ressources humaines sans avoir besoin d'avoir une compréhension approfondie de la profession de cybersécurité. Cet exemple montre comment un poste vacant peut être créé et comment éviter la création d'attentes trompeuses ou déroutantes et comment attirer du personnel dûment qualifié. Il montre également comment combiner les composantes d'un profil de rôle de l'ECSF et comment les adapter en fonction des besoins professionnels d'une organisation.
Cet exemple montre comment une organisation peut utiliser l'ECSF pour créer une description d'un

rôle. Même sans formation RH, il est possible de définir les tâches, les compétences et les connaissances requises d'un candidat pour le recrutement en connaissant la mission du rôle. En plus de soutenir le processus de recrutement, l'ECSF peut également aider l'entreprise à définir des plans de formation pour le personnel nouvellement recruté. Il convient de noter que l'ECSF fournit non seulement un langage commun pour les marchés publics en matière de cybersécurité, mais également à des fins d'audit, en particulier lorsque le principe de responsabilité est mis en œuvre et qu'une séparation des tâches essentielle et claire est requise.

Exemple II : Élaboration d'une description de poste

Une grande compagnie d'assurance étend son portefeuille à l'assurance de cybersécurité, car de nombreux clients recherchent ce service. Après une légère restructuration interne et la mise à jour de l'inventaire du personnel, l'entreprise décide d'ajouter la cybersécurité au département de conformité. Par conséquent, la direction du département de conformité conclut qu'**elle doit recruter un responsable de la conformité cyber** pour soutenir la nouvelle mission.

Le service des ressources humaines de l'entreprise est chargé **de trouver et de recruter le candidat le plus approprié**. Étant donné que la cybersécurité est un nouveau domaine pour l'organisation, les RH doivent également créer une **description des rôles**. Pour définir ce nouveau rôle, les **RH interrogent** les **managers et le personnel compétents** afin de **déterminer** les **besoins** et les **tâches clés** pour ce poste. Ces besoins sont identifiés et les principales tâches retenues sont les suivantes :

- garantir le respect des normes, lois et réglementations en matière de confidentialité et de protection des données et fournir des conseils et des orientations juridiques en la matière;
- identifier et documenter les lacunes en matière de conformité;
- élaborer un plan d'audit décrivant les cadres, les normes, les procédures et les tests d'audit;
- exécuter le plan d'audit et recueillir des éléments probants et des mesures;
- élaborer et communiquer les résultats des audits (rapports).

Le responsable des ressources humaines reconnaît qu'il s'agit d'un rôle complexe et qu'aucun modèle de recrutement correspondant à ce rôle n'est disponible. Par conséquent, **une nouvelle description de rôle et un nouveau modèle doivent être créés** et approuvés par la direction.

Le responsable des ressources humaines, qui **utilise désormais l'ECSF**, **analyse différents rôles dans le cadre**. Les tâches spécifiées sont incluses dans **les tâches clés identifiées dans les rôles** de **Responsable juridique, politique et conformité en cybersécurité et Auditeur en cybersécurité**.

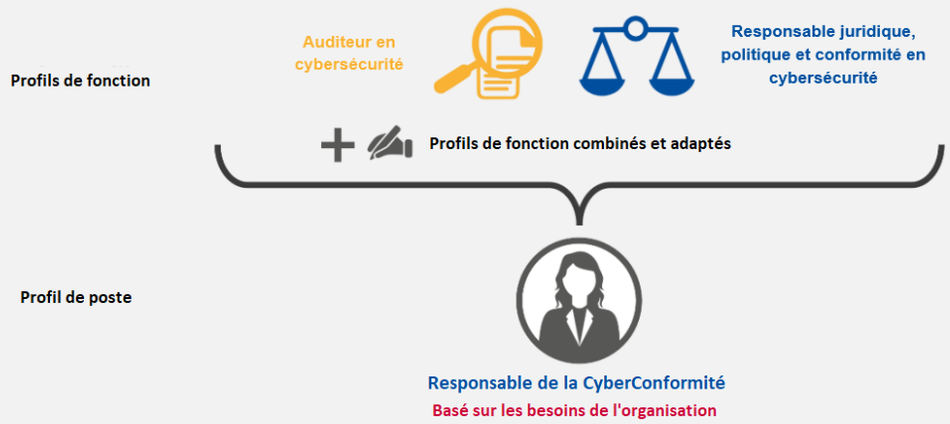
Pour exécuter ces tâches, les **compétences identifiées et les connaissances requises** sont les suivantes :

- Compétences
  - comprendre les implications des modifications du cadre juridique sur la stratégie et les politiques de l'organisation en matière de cybersécurité et de protection des données;
  - suivre et mettre en pratique les cadres, normes et méthodologies d'audit;
  - appliquer des outils et des techniques d'audit;
  - travailler en équipe et collaborer avec des collègues.
- Connaissances
  - une connaissance approfondie de la cybersécurité nationale, européenne et internationale et des normes, législations, politiques et réglementations connexes en matière de protection de la vie privée;
  - connaissance de la conformité en matière de sécurité de l'information et des exigences réglementaires aux niveaux international, national et de l'UE;
  - compréhension de base du stockage, du traitement et de la protection des données

dans les systèmes, les services et les infrastructures.

Une nouvelle description de rôle adaptée aux besoins des entreprises peut maintenant être créée **en cartographiant et en combinant** des parties du profil pour le rôle de **Responsable juridique, politique et conformité en cybersécurité** et des parties du profil pour le rôle d'**Auditeur en cybersécurité**. Il est important de noter qu'en s'adaptant au cadre, ce nouveau rôle unique repose sur **le contenu essentiel du ECSF**. Cela fournit un rôle uniforme et structuré qui peut être retracé jusqu'à son origine.

Figure 7 : Profil d'emploi en cybersécurité créé sur la base des profils de rôle du ECSF



Après cette mise en correspondance avec le ECSF, la description de rôle requise est disponible et peut être utilisée pour rédiger le rôle et la description de poste correspondante que les RH doivent faire approuver en interne et publier sur le site web de recrutement de l'entreprise. D'autres éléments, tels que la mission du profil, peuvent être utilisés comme texte d'introduction pour la publication de cette offre d'emploi.

L'exemple II a démontré l'utilité du ECSF pour les avantages suivants :

- comprendre les rôles en matière de cybersécurité
- identifier les besoins en main-d'œuvre
- identifier les exigences en matière de rôle
- soutenir le processus de recrutement
- soutenir la mise en place d'un modèle d'offre d'emploi personnalisé
- utiliser une langue commune pour les postes vacants.

Figure 8 : Avantages de l'utilisation de l'ECSF présentés par l'exemple II

Exemple III : *Une grande entreprise dont l'activité principale est en dehors des TIC doit mettre en place un départementde cybersécurité* démontre l'application de l'ECSF lors de la création d'un nouveau département de cybersécurité et de la préparation d'une stratégie de cybersécurité pour l'entreprise. Il propose également une catégorisation des 12 profils en quatre (4) macro-domaines pour une compréhension et une communication de haut niveau. Il montre comment une grande organisation pourrait utiliser l'ECSF pour soutenir l'élaboration d'une stratégie de cybersécurité, y compris la planification des ressources humaines et le développement des compétences dans le domaine de la cybersécurité.

Exemple III : Une grande entreprise ayant son activité principale en dehors des TIC doit mettre en place un département de cybersécurité

Une grande entreprise dont l'activité principale n'est pas liée aux TIC ou aux services de cybersécurité s'est rendu compte de la nécessité de protéger ses actifs précieux contre les menaces de cybersécurité. En fait, la stratégie commerciale adoptée comprenait un plan massif de numérisation des processus d'entreprise et la dépendance à l'égard des TIC devenait nettement plus élevée pour les opérations commerciales critiques.

Comme la société ne disposait d'aucune expertise interne pour gérer les risques de cybersécurité, le conseil d'administration a décidé d'embaucher un Responsable de la sécurité de l'Information (CISO) pour **définir la stratégie globale de cybersécurité** en alignement avec les objectifs commerciaux de l'entreprise. Cela nécessiterait également **la mise en place d'un service** chargé **de la gestion des risques en matière de cybersécurité.**

Le CISO, fraîchement nommé, **a utilisé l'ECSF comme ligne directrice** et **comme référence solide** pour les **rôles en matière de cybersécurité nécessaires** pour gérer ses risques en matière de cybersécurité. Elle s'en est servie comme d'un **outil flexible** pour aider à **structurer un service de cybersécurité.** Elle a également reconnu que, pour fournir un schéma clair, il serait utile de placer **les rôles de l'ECSF dans le contexte d'un cercle de gestion,** sous quatre (4) macro domaines : a) Planifier, b) Mettre en œuvre, c) Exploiter et d) Améliorer.

Figure 9 : Placer les profils de rôle de l'ECSF dans le contexte d'un cercle de gestion

Dans le macro-domaine du plan, des priorités et des objectifs ont été fixés, des stratégies, des politiques et des plans d'action ont été élaborés, des architectures ont été définies et des ressources ont été allouées. Dans ce macro-domaine, les profils CISO, Responsable de la politique et de la conformité, Gestionnaire des risques et Architecte ont été naturellement positionnés.

La mise en œuvre des mesures de cybersécurité (responsable de la mise en œuvre) et la formation et la sensibilisation (éducateur) ont été allouées au macro-domaine « Mise en œuvre ».

Les opérations au jour le jour constituent la zone la plus « tangible ». En réponse aux incidents (y compris les équipes SOC), les activités criminalistiques sont des activités quotidiennes des spécialistes de la cybersécurité. Le profil de renseignements sur les menaces a également été considéré comme un domaine opérationnel, car ces professionnels travaillent sur des données opérationnelles à l'aide de sources multiples.

Le testeur d'intrusions (test des menaces actuelles et émergentes), le chercheur (apport de nouvelles technologies et solutions) et l'auditeur (identification des lacunes) soutiennent la phase d'amélioration.

Toutefois, étant donné que l'ECSF est un outil flexible à utiliser sur mesure dans un contexte particulier, la CISO **a appliqué le guide en 5 étapes pour adapter les profils de rôle à ses besoins et objectifs spécifiques**. L'analyse des profils de l'ECSF l'a aidée à **définir les plans de ressources nécessaires** pour atteindre l'objectif de l'entreprise.

Dans le domaine macro du Plan, elle a décidé de :

- être en charge des tâches de politique et de conformité afin de rationaliser la structure organisationnelle;
- embaucher un architecte de la cybersécurité qui contribuerait à définir la stratégie globale en matière d'architecture pour faire face aux risques de cybersécurité et garantir des solutions sécurisées dès la conception pour soutenir la transformation

numérique ;
- embaucher un gestionnaire des risques en matière de cybersécurité qui aiderait à évaluer la position de l'entreprise en matière de risques de cybersécurité et à définir des plans d'action pour gérer les risques recensés.

Dans le macro-domaine de la mise en œuvre, elle a **tiré parti des compétences et des connaissances de l'ECSF** pour **comprendre en quoi le perfectionnement serait nécessaire** pour tirer parti des ressources internes disponibles ou décider d'embaucher à l'extérieur. La multinationale disposait déjà d'une équipe d'instructeurs dans un domaine différent. Cependant, il n'y avait pas d'équipe spécialisée pour concevoir et mener des cours de sensibilisation ou de formation à la cybersécurité. La CISO **a cherché à savoir si certains des formateurs possédaient les compétences et les connaissances énumérées dans l'ECSF** et s'ils souhaitaient **rejoindre sa nouvelle équipe**.

Dans le domaine des macro-opérations, la CISO a examiné comment gérer les opérations quotidiennes de cybersécurité et a décidé de **mettre en place des centres d'opérations de sécurité mondiaux avec des intervenants en cas d'incident** travaillant sur différents continents pour fournir une assistance 24 heures sur 24, 7 jours sur 7. En outre, **un spécialiste du renseignement sur les menaces a été employé** pour fournir des informations opérationnelles afin de guider la chasse aux menaces et l'atténuation des risques. La CISO a conclu **qu'il n'était pas nécessaire d'engager un enquêteur en criminalistique numérique**, mais plutôt de **faire appel à une société de conseil spécialisée** pour tous **les besoins en matière de criminalistique**.

Dans le domaine macro d'Amélioration, la CISO a décidé d'employer **un fournisseur de services externe pour les tests d'intrusion** dans le but de tester la résilience de l'infrastructure et des applications de l'entreprise. La CISO a également évalué la capacité de l'équipe d'audit interne et a décidé **d'engager un auditeur en cybersécurité** pour auditer les politiques liées à la sécurité. La CISO n'a pas ressenti le besoin d'embaucher un chercheur en cybersécurité, car la recherche en cybersécurité ne relevait pas du champ d'application de son organisation.

En résumé, l'exemple III a mis en évidence l'utilité du ECSF pour les avantages suivants :

- comprendre les rôles en matière de cybersécurité
- contribuer à la création d'une structure organisationnelle identifiant les exigences relatives aux rôles en matière de cybersécurité;
- aider à la planification des ressources humaines
- mise à niveau des compétences des salariés
- soutenir l'évaluation des candidats
- en utilisant une terminologie commune pour la collaboration.

Figure 10 : Avantages de l'utilisation de l'ECSF démontrés par l'exemple III

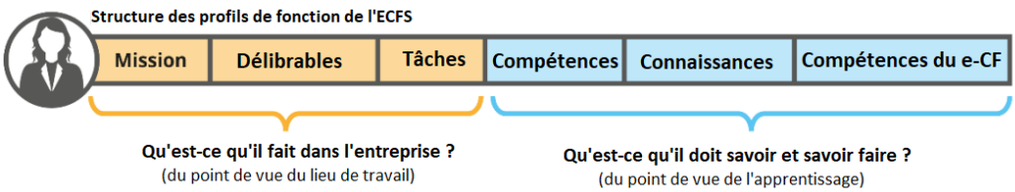
3.2 COMPÉTENCES DES PROFESSIONNELS DE LA CYBERSÉCURITÉ – APPLIQUER L'ECSF EN TANT QU'ORGANISME DE FORMATION

L'ECSF propose une langue et un vocabulaire communs pour le développement des compétences professionnelles en matière de cybersécurité aux prestataires de programmes d'apprentissage et aux établissements d'enseignement de tous types, tels que l'enseignement supérieur (ES), l'enseignement et la formation professionnels (EFP) ou tout autre programme éducatif ou formation en matière de cybersécurité. Les profils de rôle définis fournissent une approche axée sur le lieu de travail et intégrée à l'échelle européenne en matière de cybersécurité afin de lier les exigences actuelles en matière de pratique professionnelle aux programmes d'études et aux programmes d'apprentissage liés à la cybersécurité.

L'ECSF définit les exigences typiques d'un profil à partir de deux points de vue fondamentaux.

- Que fait ce rôle dans l'organisation ?
  Aborde la perspective du lieu de travail (sections du profil sur la mission, les éléments livrables et les tâches)
- Qu'est-ce que ce rôle doit savoir et pouvoir faire ?
  Aborder la perspective de l'apprentissage (sections du profil sur les aptitudes, les connaissances et les compétences e-CF)

Figure 11 : Les sections des profils de rôle de l'ECSF liées au lieu de travail et aux perspectives



L'ECSF place les acquis d'apprentissage dans un contexte de travail réel. En particulier, les descriptions des rôles dans les profils de l'ECSF permettent aux prestataires de programmes d'apprentissage de revoir leurs programmes d'études de manière structurée et systématique, y compris du point de vue des praticiens.

L'ECSF propose un langage et un vocabulaire communs pour le développement des compétences professionnelles en matière de cybersécurité aux prestataires de programmes d'apprentissage et aux établissements d'enseignement de tous types.

Comme l'illustre l'annexe B.2, l'ECSF pourrait contribuer à plusieurs activités menées dans des établissements universitaires.

- L'ECSF pourrait servir à développer ou à mettre à jour les acquis d'apprentissage des cours et à les aligner sur les besoins du marché du travail. Les aptitudes, les connaissances et les compétences au sein d'un profil de rôle peuvent être utilisées pour guider la phase de conception des programmes d'études et soutenir l'établissement des résultats d'apprentissage souhaités. Par exemple, lors de l'analyse des besoins éducatifs d'un emploi spécifique en cybersécurité, un profil ECSF aligné fournit un point de départ solide pour comprendre les exigences éducatives associées.
- L'ECSF pourrait servir d'outil de collaboration pour créer des programmes académiques communs et permettre la mobilité des étudiants.
- L'ECSF pourrait servir de base à la définition d'un cadre pour un programme de cybersécurité qui aiderait les universités à cartographier l'objectif principal de leur programme de cybersécurité et à le communiquer aux étudiants.

Comme l'illustre l'annexe B.1, l'ECSF répond à certains des défis recensés dans le paysage européen des qualifications professionnelles en matière de cybersécurité. En particulier :

- l'ECSF soutient une terminologie intersectorielle et interindustrielle commune en ce qui concerne les compétences en matière de cybersécurité;
- l'ECSF pourrait soutenir le développement d'une plateforme intégrée pour les compétences afin de fournir des informations actualisées sur le marché du travail, les compétences, les cours de formation, les systèmes de certification et une feuille de route de carrière.

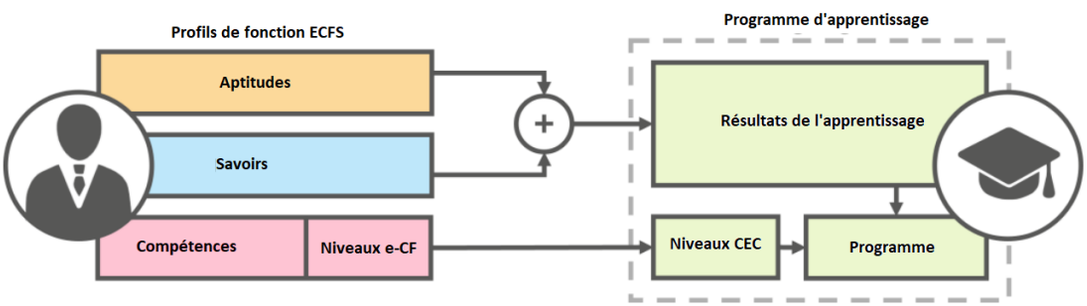
Figure 12 : Avantages de l'utilisation de l'ECSF en tant qu'organisme de formation

L'ECSF peut être utilisé comme un outil de communication entre les employeurs et les éducateurs.

Dans le contexte de l'élaboration des qualifications en matière de cybersécurité et de la conception des programmes d'études, les profils de rôle de l'ECSF servent d'outil de communication entre les employeurs et les éducateurs afin d'améliorer le processus de consultation et les résultats de la collaboration. L'employeur peut rapidement définir les activités ou les tâches requises et revenir en arrière pour identifier les compétences, les aptitudes et les connaissances que les éducateurs devraient inclure dans les programmes d'études. Cette approche accélère considérablement la conception des programmes convenus entre les employeurs, les gouvernements et les éducateurs.

La figure 13 illustre comment les sections des profils de rôles de l'ECSF consacrées aux compétences, aux connaissances et aux aptitudes peuvent être utilisées pour définir les acquis d'apprentissage, identifier les niveaux appropriés de programmes d'apprentissage et créer des programmes d'études pour les professions liées à la cybersécurité. Étant donné que les connaissances et les compétences, comme tout le contenu des descriptions de rôles, sont fournies comme exemples d'orientation pour une adaptation flexible au contexte, d'autres sources peuvent également être utilisées[9].

Figure 13 : Profils de l'ECSF guidant l'apprentissage professionnel



Connexion des niveaux d'apprentissage (CEC) et des niveaux de compétence en milieu de travail (e-CF)

Le cadre européen des certifications (CEC) est un cadre de référence européen commun pour les certifications. L'objectif du CEC est de comparer les certifications et les acquis d'apprentissage obtenus dans différents pays et systèmes éducatifs nationaux. Le CEC est fondé sur la

[9]Les sections relatives aux aptitudes, connaissances et compétences du CECS ne sont ni exhaustives ni restrictives, ce qui permet à l'utilisateur de les enrichir en incluant également des ressources externes, par exemple le Cyber Security Body Of Knowledge (CyBOK).https://www.cybok.org/; classification du CCR https://joint-research-centre.ec.europa.eu/publications/unified-conceptualframework-tasks-skills-and-competences_en

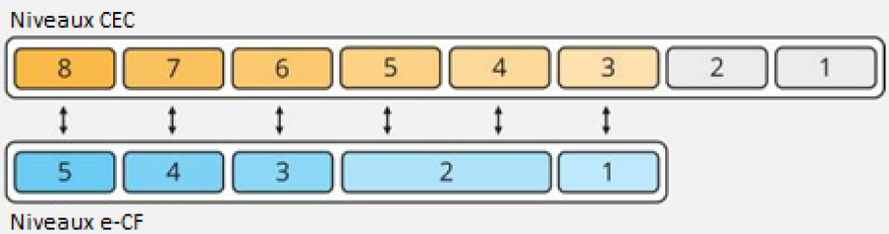
Recommandation relative au cadre européen des certifications pour l'éducation et la formation tout au long de la vie, adoptée par le Parlement européen et le Conseil le 23 avril 2008[10].

Le CEC définit huit (8) niveaux de niveau d'éducation avec des descripteurs qui différencient chaque niveau. Le critère pour chaque niveau est basé sur l'évaluation des connaissances, des compétences, de la responsabilité et de l'autonomie.

Le **cadre européen des compétences numériques (e-CF),** norme EN 16234-1, utilisé par l'ECSF, est un cadre européen commun pour les compétences, connaissances et aptitudes professionnelles[11] dans le domaine des TIC. Elle concerne les compétences nécessaires et appliquées sur le lieu de travail. La dimension 3 de l'e-CF définit les niveaux de compétence découlant des compétences sur le lieu de travail. Il existe cinq (5) niveaux de e-compétences définis, de e-1 à e-5, liés aux niveaux d'apprentissage 3 à 8 du CEC (les niveaux 1 et 2 du CEC ne sont pas pertinents dans ce contexte).

La relation entre les niveaux e-CF e-1 à e-5 et les niveaux CEC 3 à 8 est illustrée ci-dessous :

Figure 14 : Relation entre le CEC et les niveaux e-CF



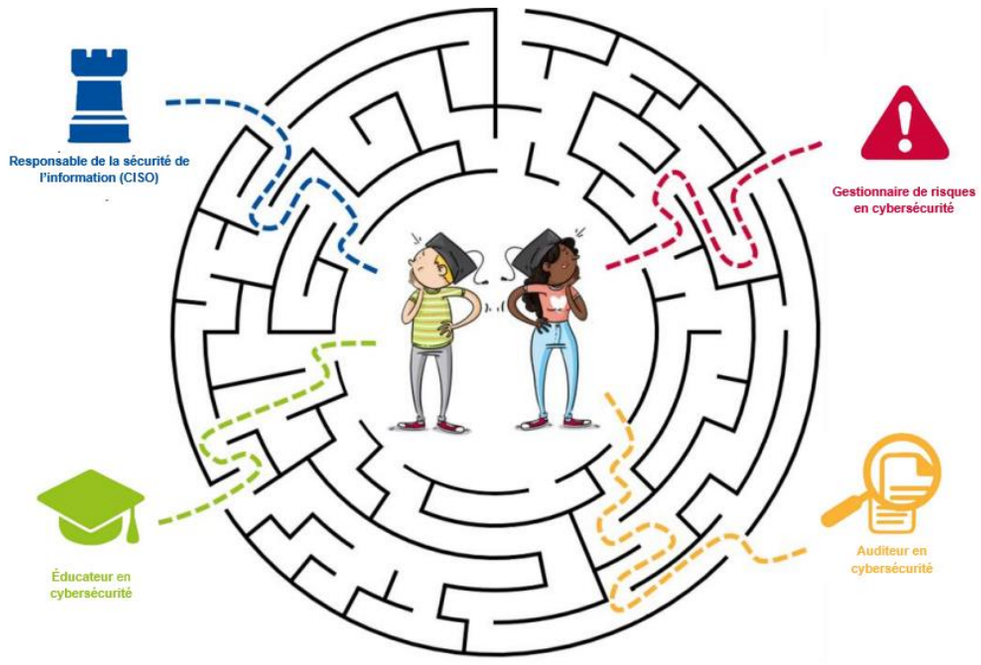
Grâce à cette relation systématiquement développée, il est possible d'établir un lien entre les niveaux de compétence e-CF et les niveaux d'apprentissage du CEC. La relation, en raison de la nature différente de chaque cadre, n'est pas de pleine équivalence. Toutefois, elle peut être appliquée pour accroître la transparence et **fournir un langage commun entre les exigences en matière de compétences professionnelles sur le lieu de travail et les qualifications connexes des établissements d'enseignement[12].** Ainsi, les niveaux de compétence e-CF intégrés dans les profils de rôles de l'ECSF peuvent être utilisés comme guide général pour les niveaux d'éducation requis.

[10] European Qualifications Framework for lifelong learning
[11] EN16234-1:2019: e-Competence Framework (e-CF) – a common European Framework for ICT professionals in all sectors
[12] For further practical guidance see: CEN/TS 17699:2022 Guidelines for developing ICT professional curricula as scoped by EN16234-1 (e-CF)

3.3 FAIRE SES PROPRES CHOIX DE CARRIÈRE – APPLIQUER L'ECSF EN TANT QUE PROFESSIONNEL INDIVIDUEL

Le langage commun défini par l'ECSF peut être utilisé pour dissiper toute confusion entre les rôles professionnels en matière de cybersécurité et les programmes éducatifs en matière de cybersécurité. En fournissant un langage commun et une description claire des rôles professionnels en matière de cybersécurité, des tâches qu'ils sont censés accomplir ainsi que des aptitudes, des compétences et des connaissances requises, l'ECSF peut construire une compréhension commune et apporter la clarté nécessaire pour attirer de nouvelles personnes dans le domaine de la cybersécurité ou les aider à planifier leur parcours professionnel.

Figure 15 : Utiliser l'ECSF pour définir les parcours professionnels des individus



L'ECSF peut construire une compréhension commune et fournir la clarté nécessaire pour attirer de nouvelles personnes dans le domaine de la cybersécurité ou les aider à planifier leur parcours professionnel.

Les professionnels travaillant déjà dans des postes liés à la cybersécurité peuvent utiliser l'ECSF comme guide pour progresser dans leur domaine. En adaptant leurs compétences et leurs connaissances aux profils de rôles d'intérêt de l'ECSF, les individus peuvent identifier les compétences ou les connaissances manquantes qu'ils doivent développer, maîtriser ou apprendre afin qu'ils soient prêts à couvrir les futures exigences professionnelles ou les transitions possibles entre les rôles de cybersécurité pendant qu'ils progressent dans leur carrière professionnelle. Cela facilite le dialogue entre les employés et les employeurs lors de la planification de la formation continue dans le domaine de la cybersécurité. Comme l'ECSF indique des parcours d'apprentissage formels et non formels, il aide également les nouveaux entrants qui ne savent pas par où commencer. L'ajout de connaissances et de compétences antérieures est souvent une voie plus facile que de recommencer complètement. L'annexe B.6 traite de ce sujet et fournit des informations et des exemples plus approfondis sur la « prise de décision individuelle en matière de carrière » à l'aide de l'ECSF.

En utilisant l'ECSF comme base de référence, une personne peut identifier les compétences et aptitudes requises pour passer d'un rôle à un autre ou pour identifier les besoins de formation actuels.

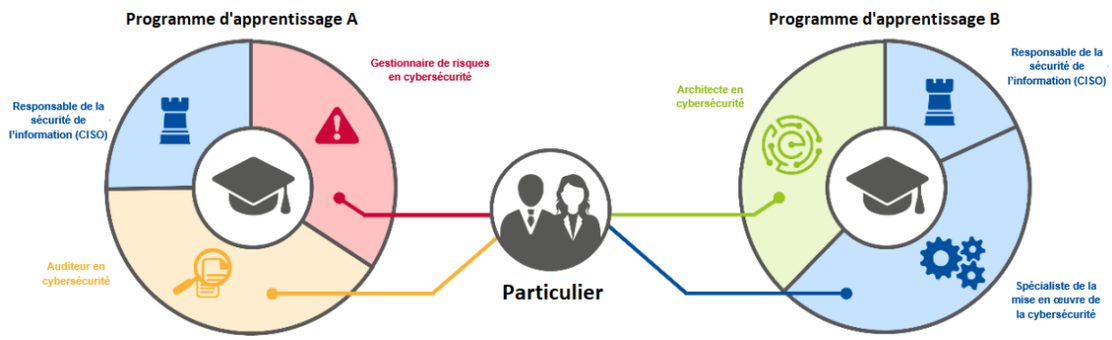
Le langage commun défini par l'ECSF peut être utile aux personnes à la recherche d'un emploi dans le domaine de la cybersécurité. L'ECSF peut aider à filtrer les offres d'emploi et à comprendre la description du poste, tout en facilitant la mobilité globale du poste dans le domaine de la cybersécurité en mettant en correspondance les aptitudes, les connaissances et les compétences de la personne avec l'ECSF.

La cybersécurité est une bonne opportunité de carrière, même pour les personnes actuellement spécialisées dans d'autres domaines, de sorte que la reconversion des personnes et leur transfert dans le domaine de la cybersécurité constituent un bon moyen de satisfaire les besoins en main-d'œuvre du marché et de réduire les écarts de main-d'œuvre dans ce domaine. Étant donné que la cybersécurité est un sujet multidisciplinaire, un tel changement de carrière pourrait être plus rapide pour les personnes ayant des antécédents proches de l'un des principaux aspects du domaine[13] :

- **technique** – lié à la technologie, aux approches technologiques concrètes et aux solutions pouvant être utilisées pour lutter contre la cybercriminalité et le cyberterrorisme;
- **humain** – lié aux facteurs humains, aux aspects comportementaux, aux questions de respect de la vie privée, ainsi qu'à la sensibilisation et à la connaissance de la société en ce qui concerne la cybercriminalité et les menaces terroristes;
- **organisationnel** – lié aux processus, procédures et politiques au sein des organisations, ainsi qu'à la coopération (public-privé, public-public) entre les organisations;
- **réglementaire** – lié aux dispositions de la loi, à la normalisation et à la criminalistique.

En ayant une compréhension claire des principaux profils des rôles en matière de cybersécurité sur le terrain et un langage commun en matière de cybersécurité dans un plus large éventail de secteurs, comme le prévoit l'ECSF, les personnes qui cherchent à changer de carrière vers la cybersécurité peuvent utiliser l'ECSF comme point de départ pour identifier les compétences et les connaissances spécifiques qu'elles doivent acquérir pour la transition.

Figure 16 : Utilisation de l'ECSF pour analyser et comparer les programmes d'apprentissage en cybersécurité



Que la personne travaille déjà dans le domaine de la cybersécurité (cherchant à élargir ses connaissances), qu'elle soit actuellement employée dans un autre domaine (cherchant à changer de carrière) ou qu'elle soit à la recherche d'une formation universitaire (cherchant à travailler dans le domaine de la cybersécurité à l'avenir), l'ECSF peut aider à comprendre les principaux profils de rôle en matière de cybersécurité (en fournissant une description et en les analysant en tâches, aptitudes, connaissances et compétences) ainsi qu'à analyser et comparer les programmes d'apprentissage disponibles (en cartographiant les acquis d'apprentissage aux compétences et connaissances requises des profils de préférence en matière de cybersécurité).

L'ECSF crée une terminologie commune et une compréhension partagée des profils de rôle des professionnels de la cybersécurité, ce qui permet d'éliminer la confusion terminologique et tout manque de compréhension.

3.4 CRÉER DES COMMUNAUTÉS DE CYBERSÉCURITÉ - APPLIQUER L'ECSF EN TANT QU'ASSOCIATION PROFESSIONNELLE

L'ECSF crée une terminologie commune et une compréhension partagée des profils de rôle des professionnels de la cybersécurité. Ainsi, il peut être utilisé par les associations professionnelles comme une norme pour garantir que leur travail peut être utilisé et appliqué dans toute l'UE, éliminant ainsi la confusion terminologique et tout manque de compréhension.

Les organisations professionnelles peuvent utiliser le cadre pour effectuer des analyses de marché à l'aide des profils de rôle de l'ECSF et présenter les résultats dans un langage commun. Par exemple, l'ECSF devrait être utile pour mettre en évidence les profils qui font défaut sur le marché,

[13] Analysis of the European R&D priorities in cybersecurity — ENISA (europa.eu)

les emplois en cybersécurité qui sont très demandés, ainsi que les aspects législatifs de certains profils professionnels. En outre, en utilisant l'ECSF comme terminologie commune, les associations professionnelles peuvent œuvrer à l'orientation professionnelle dans le secteur de la cybersécurité, comme indiqué à l'annexe B.5.

L'utilisation de l'ECSF permet également de consolider une communauté de parties prenantes afin de soutenir les nouveaux développements, les améliorations et la poursuite de la mise en œuvre dans les États membres de l'UE. Un tel cadre de collaboration permet une interaction humaine qui se traduit par des avantages tels que le partage des connaissances, l'identification des tendances à l'échelle de l'UE, les activités d'apprentissage par les pairs, l'application d'approches pluridisciplinaires et l'autonomisation pour adapter et modifier l'ECSF à des exigences spécifiques.

Dans l'ensemble, l'ECSF peut être utilisé par les associations professionnelles de cybersécurité comme un outil pour fonder leurs activités sur la garantie de leur applicabilité à l'échelle de l'UE, dans le but de parvenir à un meilleur durcissement contre les cyberattaques dans l'ensemble de l'UE en tant que société.

3.5 AMÉLIORER STRATÉGIQUEMENT LE SECTEUR – APPLIQUER L'ECSF EN TANT QUE MOTEUR DE POLITIQUES

Avec l'ECSF, une communauté professionnelle cruciale assure une visibilité claire car l'utilisation du cadre crée une compréhension commune de ce que font les spécialistes de la cybersécurité. Par conséquent, l'ECSF fournit un outil permettant d'analyser et de partager les collectes critiques de données et de statistiques relatives à la main-d'œuvre dans le domaine de la cybersécurité dans une terminologie commune et compréhensible à l'échelle de l'UE. Ces données sont importantes pour les décideurs politiques, car elles leur permettent d'obtenir de meilleures informations sur l'état de la main-d'œuvre dans le domaine de la cybersécurité dans l'ensemble de l'UE, ce qui leur permet de comprendre et d'estimer les besoins futurs en quantité et en qualité des spécialistes de la cybersécurité. Cette contribution stratégique contribue à la mise à jour et au maintien de l'ECSF lui-même, de sorte que sa pertinence à l'avenir reste valable. En outre, en définissant une terminologie commune, l'ECSF permet une collaboration transfrontière entre les décideurs politiques grâce au partage de données et d'informations.

Compte tenu d'une approche structurée d'un environnement de marché très diversifié, les profils de rôle de l'ECSF constituent un outil précieux pour le soutien des décideurs politiques, des enquêteurs de marché et d'autres parties prenantes ayant l'influence et le rôle de responsabiliser stratégiquement le secteur.

Compte tenu d'une approche structurée d'un environnement de marché très diversifié, les profils de rôle de l'ECSF constituent un outil précieux pour le soutien des décideurs politiques, des enquêteurs de marché et d'autres parties prenantes ayant l'influence et le rôle de responsabiliser stratégiquement le secteur. Les profils de l'ECSF peuvent être utiles pour les études de données sur l'offre et la demande réalisées aux niveaux national, européen et international. Les profils fournissent une définition commune et convenue pour faciliter la collecte de données fiables et comparables sur le marché du travail dans le domaine de la cybersécurité, y compris l'offre et la demande de différents types de professionnels de la cybersécurité et les exigences connexes en matière de compétences particulières.

Les processus d'élaboration des politiques en matière de cybersécurité peuvent bénéficier de la collecte de données au moment de prendre des décisions, par exemple les dispositions de financement, les priorités d'investissement et les périodes d'intervention. Outre les activités de base de chaque profil, les activités qu'ils mènent peuvent contribuer à la production et à la collecte d'ensembles de données pertinents susceptibles d'étayer les décisions politiques. L'annexe B.3 montre comment la fragmentation de l'information constitue un défi lors de la prise de décisions et les mesures prises par l'INCIBE pour relever ce défi avec le soutien de l'ECSF. En intégrant l'ECSF en tant que cadre homogène pour la définition des profils de cybersécurité, les États membres de l'UE bénéficient d'un soutien précieux pour atteindre leurs objectifs consistant à accroître les talents en matière de cybersécurité et à s'aligner sur le reste des pays au niveau européen.

4. CONDITIONS ET DÉFINITIONS

Durée	Définition	Source
cybersécurité	Toute activité nécessaire pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes touchées par les cybermenaces.	Mandat de l'ENISA [règlement (UE) 2019/881]
cybermenace	Toute circonstance, tout événement ou toute action susceptible d'endommager, de perturber ou d'avoir un impact négatif sur les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et d'autres personnes.	Mandat de l'ENISA [règlement (UE) 2019/881]
Technologies de l'information et de la communication	TIC est l'acronyme de Technologies de l'information et de la communication. Il est utilisé dans de nombreux contextes différents et, d'un point de vue technique, les TIC concernent les ordinateurs numériques et les systèmes Internet (de communication), y compris les logiciels, le matériel et les réseaux. D'un point de vue économique et politique, les TIC se rapportent à un secteur transversal d'entreprises, y compris les fabricants, les fournisseurs de produits ou les fournisseurs de services liés au domaine des TIC.	EN16234-1:2019 Cadre de compétences numériques (e-CF)
compétence	La capacité démontrée d'appliquer les connaissances, les compétences et les attitudes pour obtenir des résultats observables. Les exemples sont B.1. Développement d'applications et E.3. Gestion des risques.	EN16234-1:2019 Cadre de compétences numériques (e-CF)
habileté	La capacité d'effectuer des activités et des tâches de gestion ou techniques sur un plan cognitif ou pratique ; savoir comment le faire.	EN16234-1:2019 Cadre de compétences numériques (e-CF)
compétences non techniques	Compétences interactives utilisées pour s'engager avec succès dans des situations sur le lieu de travail ; peut faire référence à la qualité du travail, à l'interaction sociale ou à l'émotion. (également appelées compétences transversales, transférables ou comportementales)	EN16234-1:2019 Cadre de compétences numériques (e-CF)
connaissances	Ensemble de faits à appliquer dans un domaine de travail ou d'études ; savoir quoi faire.	EN16234-1:2019 Cadre de compétences numériques (e-CF)
attitude	Représentation de l'élément humain d'une e-compétence ; elle réfléchit à la manière dont une personne intègre les connaissances et les compétences et les applique de manière appropriée dans leur contexte.	EN16234-1:2019 Cadre de compétences numériques (e-CF)
résultats de l'apprentissage	Énoncé de ce qu'une personne sait, comprend et peut accomplir à la fin d'un processus d'apprentissage	Cadre européen des certifications (CEC)

profil de rôle	Un aperçu ou un document général qui démontre la relation entre des activités ou des tâches spécifiques dans un rôle et les aptitudes, compétences et connaissances individuelles requises pour les entreprendre. Contrairement à un emploi particulier, un rôle découle d'un besoin organisationnel de faire quelque chose. Les employés affectés peuvent répondre aux exigences organisationnelles en effectuant tout ou partie des tâches requises pour assurer leur rôle.	Leadership créatif – Gestion des talents Profils TIC CWA
profil d'emploi	Une description contextuelle et détaillée de ce qu'un employé fait pour s'assurer que le titulaire du poste n'a aucun doute sur ses tâches, ses fonctions, ses responsabilités et souvent sur ceux à qui il rend compte. Il contient généralement des informations précises sur les compétences, les aptitudes et les connaissances requises, ainsi que des informations pratiques sur la santé, la sécurité et la rémunération.	Profils TIC CWA
niveau de compétence	Une indication claire du degré de maîtrise qui permet à un professionnel de répondre aux exigences dans l'exercice d'une compétence. La norme EN 16234-1 (e-CF) intègre les niveaux de compétence e-1 à e-5. L'e-CF caractérise les niveaux de compétence en combinant les niveaux d'influence au sein d'une communauté, la complexité du contexte et l'autonomie.	EN16234-1:2019 Cadre de compétences numériques (e-CF)
niveau d'apprentissage	Indique un classement et peut être représenté par une qualification formelle. Les niveaux d'apprentissage découlent généralement d'un système éducatif ou indiquent une classification dans une taxonomie des comportements intellectuels ou d'apprentissage (tels que la mémorisation, l'application, l'interprétation) et ont une relation avec les niveaux de compétence, mais doivent être distingués de ceux-ci.	EN16234-1:2019 Cadre de compétences numériques (e-CF)

5. RÉFÉRENCES

Mandat de l'ENISA, règlement (UE) 2019/881, https://eur-lex.europa.eu/eli/reg/2019/881/oj

Profils de rôles professionnels européens dans le domaine des TIC, CWA 16458 https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0 :::FSP_PROJECT,FSP_ORG_ID:67523,412798&cs=1799176DA0D15C74D91B71423CAD4A9A3

EN 16234-1:2019 Cadre de compétences numériques (e-CF), Un cadre européen commun pour les professionnels des TIC dans tous les secteurs

CEN/TS 17699:2022 Lignes directrices pour l'élaboration de programmes professionnels dans le domaine des TIC conformément à la norme EN 16234-1 (e-CF)

CEN/TS 17834:2022 Cadre européen d'éthique professionnelle pour la profession des TIC (éthique des TIC dans l'UE)

Cadre européen des certifications (CEC)

ESCO La classification européenne multilingue des aptitudes, compétences et professions, http://www.ec.europa.eu/esco

Code de déontologie de l'IFIP

Cycle de vie de la réponse aux incidents du NIST

L'Initiative nationale pour l'éducation à la cybersécurité (NICE) de l'Institut national des normes et de la technologie États-Unis

Stratégies nationales de cybersécurité (SNCN), https://www.enisa.europa.eu/topics/national-cyber-security-stratégies/stratégies-orientations-outils nationaux-cybersécurité

The Cybersecurity Body of Knowledge (CyBOK) du programme national de cybersécurité du Royaume-Uni et de l'université de Bristol, https://www.cybok.org

JRC, Taxonomie et glossaire de la cybersécurité par la Commission européenne, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

La stratégie européenne en matière de compétences, https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_1196

Plan d'action en matière d'éducation numérique,https://education.ec.europa.eu/focus-topics/digital-education/about/digital-education- action-plan

Pact for Skills, https://ec.europa.eu/commission/presscorner/detail/fr/qanda_20_1197

Mener la décennie numérique, https://ec.europa.eu/commission/presscorner/detail/fr/qanda_20_1197

ENISA, Forensic Analysis, Webserver analysis, Handbook, Document for teachers (Analyse médico-légale, analyse du serveur Web, manuel, document à l'intention des enseignants), 2016, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe3_forensic_analysis_iii-handbook

Conseil de l'Europe, Preuves électroniques dans les procédures civiles et administratives, Directives et explications mémorandum, 2019, https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

ANNEXE A : RELIER L'ECSF AUX AUTRES NORMES ET CADRES DE L'UE

L'ECSF est un cadre destiné à soutenir le domaine professionnel de la cybersécurité dans l'UE. La connexion des structures européennes reconnues existantes présentant un intérêt pour le domaine professionnel de la cybersécurité de l'UE était un principe essentiel de la conception du ECSF (voir section 2.1).

Les paragraphes qui suivent donnent un bref aperçu des principales normes et des principaux cadres auxquels le FSC est lié.

A.1 EN16234-1 E-CF UN CADRE EUROPÉEN COMMUN DE RÉFÉRENCE POUR LES PROFESSIONNELS DES TIC DANS TOUS LES SECTEURS

La norme européenne (EN) 16234-1 Cadre européen des compétences numériques (e-CF) fournit une référence de 41 compétences appliquées sur le lieu de travail des technologies de l'information et de la communication (TIC) en utilisant une langue européenne standard pour les compétences, les aptitudes, les connaissances et les niveaux de compétence qui peuvent être compris dans toute l'Europe. L'objectif principal de cette norme est de fournir une langue européenne commune pour les compétences, les aptitudes, les connaissances et les niveaux de compétence liés aux TIC sur le lieu de travail, selon les besoins et les applications des organisations et des professionnels. De cette façon, toutes les parties prenantes du secteur, y compris les secteurs public et privé et les particuliers, ont accès à une référence commune.

La norme a été établie comme un outil pour soutenir la compréhension mutuelle et assurer la transparence du langage grâce à l'articulation des compétences requises et déployées par les professionnels des TIC. Cette norme est structurée en plusieurs dimensions. Les dimensions reflètent les domaines de la planification des activités et des ressources humaines et intègrent des lignes directrices sur les compétences professionnelles et professionnelles. En outre, cette norme ajoute une composante transversale qui fournit des descripteurs TIC génériques de base pour une application réussie des compétences e-CF dans le contexte d'un lieu de travail.

Tableau 4 : Vue d'ensemble de la norme EN16234-1 (e-CF). Source : CEN 2019

Dimension 1 5 domaine e-CF	**Dimension 2** 41 e-compétences identifiées	**Dimension 3** 5 niveaux de e-compétences				
		e-1	e-2	e-3	e-4	e-5
A. Planifier	A.1. Systèmes d'information et stratégie d'entreprise					
	A.2. Gestion des niveaux de service					
	A.3. Élaboration du plan d'entreprise					
	A.4. Planification des produits/services					
	A.5. Conception de l'architecture					
	A.6. Conception de l'application					
	A.7. Suivi des tendances technologiques					
	A.8. Gestion de la durabilité					
	A.9. Innover					
	A.10. Expérience de l'utilisateur					
B. Construire	B.1. Développement de l'application					
	B.2. Intégration de composants					

	B.3. Tests					
	B.4. Déploiement de la solution					
	B.5. Production de la documentation					
	B.6. Ingénierie des systèmes TIC					
C. Exécuter	C.1. Assistance aux utilisateurs					
	C.2. Assistance au changement					
	C.3. Fourniture de services					
	C.4. Gestion des problèmes					
	C.5. Gestion des systèmes					
D. Activer	D.1. Développement de la stratégie de sécurité de l'information					
	D.2. Développement d'une stratégie de qualité des TIC					
	D.3. Offre d'éducation et de formation					
	D.4. Achats					
	D.5. Développement des ventes					
	D.6. Marketing numérique					
	D.7. Science des données et analyse					
	D.8. Gestion des contrats					
	D.9. Développement du personnel					
	D.10. Gestion de l'information et des connaissances					
	D.11. Identification des besoins					
E. Gérer	E.1. Élaboration des prévisions					
	E.2. Gestion de projets et de portefeuilles					
	E.3. Gestion des risques					
	E.4. Gestion des relations					
	E.5. Amélioration des processus					
	E.6. Gestion de la qualité des TIC					
	E.7. Gestion du changement					
	E.8. Gestion de la sécurité de l'information					
	E.9. Gouvernance des systèmes d'information					

L'e-CF fournit des liens cohérents dans le contexte des certifications TIC et d'autres cadres pertinents pour le secteur (en particulier, le CEC, le DigComp, les profils professionnels européens des TIC, les compétences comportementales, l'ESCO, l'EQANIE, la SFIA, l'ensemble fondamental de connaissances pour la profession TIC, l'ISO et d'autres normes du secteur des TIC).

Pour chaque rôle en matière de cybersécurité, un ensemble de compétences e-CF applicables a été sélectionné au niveau de l'application en tant qu'élément intégré de la description de profil pour le rôle de professionnel de la cybersécurité.

A.2 PROFILS DE RÔLE PROFESSIONNEL EUROPÉEN DES TIC

Les profils de rôles des professionnels européens des TIC (CWA 16458) fournit un ensemble générique de rôles typiques joués par les professionnels des TIC dans n'importe quelle organisation, couvrant l'ensemble du processus métier des TIC. Trente profils au total constituent un bon point de départ et une source d'inspiration pour la création de profils plus flexibles et spécifiques au contexte, basés sur des rôles organisationnels, des descriptions de poste individuelles ou des spécialisations de sous-domaines de différents contextes. En appliquant les compétences e-CF à la construction de profils TIC, les profils professionnels européens des TIC fournissent également un outil et un point d'entrée pour l'application e-CF aux personnes et organisations qui souhaitent travailler avec l'e-CF.

Les profils de rôles professionnels européens dans le domaine des TIC sont décrits selon un format cohérent intégrant les éléments suivants : un résumé, un énoncé de mission, des éléments livrables, des tâches principales, des compétences en ligne et des domaines d'indicateurs clés de

performance (ICP)[14].

En adoptant les éléments les plus appropriés du schéma européen de description des profils TIC convenu et axé sur la pratique, les profils ECSF deviennent comparables et fournissent une vue d'ensemble unique, facilement accessible et complète des exigences applicables aux professionnels européens de la cybersécurité.

Ces profils détaillés à contenu élevé ont des liens vagues avec les rôles génériques intégrés dans l'ensemble du profil professionnel européen des TIC. Du point de vue des utilisateurs de l'ECSF, la confiance peut être établie dans la durabilité de la structure grâce à son association avec les profils TIC européens, mais avec une application ciblée pour la communauté de la cybersécurité.

A.3 CADRE EUROPÉEN DES CERTIFICATIONS

L'UE a élaboré le **cadre européen des certifications (CEC)** en tant qu'outil de traduction pour rendre les certifications nationales plus faciles à comprendre et plus comparables. Le CEC vise à soutenir la mobilité transfrontière des apprenants et des travailleurs et à promouvoir l'apprentissage tout au long de la vie et le développement professionnel dans toute l'Europe.

Le CEC est un cadre fondé sur les acquis d'apprentissage à huit niveaux[15] pour tous les types de certifications. Il sert d'outil de traduction entre les différents cadres des certifications nationales. Ce cadre contribue à améliorer la transparence, la comparabilité et la portabilité des qualifications des personnes et permet de comparer les qualifications de différents pays et institutions.

Le CEC couvre tous les types et tous les niveaux de certification et l'utilisation des acquis d'apprentissage indique clairement ce qu'une personne sait, comprend et est capable de faire. Le niveau augmente en fonction du niveau d'apprentissage, le niveau 1 étant le plus bas et le niveau 8 le plus élevé. Plus important encore, le CEC est étroitement lié aux cadres nationaux des certifications[16], de sorte qu'il fournit une carte complète de tous les types et niveaux de certification en Europe, qui sont de plus en plus accessibles au moyen de bases de données sur les certifications. Le CEC a été mis en place en 2008, puis révisé en 2017[17].

Les profils ECSF contiennent des compétences e-CF et des attributions de niveau e-CF, qui fournissent un lien cohérent avec les niveaux du CEC (voir section 3.2). Cette relation d'orientation fournit un pont dans la compréhension entre la fourniture de programmes d'apprentissage et les exigences du lieu de travail.

A.4 ESCO - CLASSIFICATION EUROPÉENNE DES APTITUDES, DES COMPÉTENCES ET DES PROFESSIONS

L'ESCO est la classification multilingue des aptitudes, compétences, qualifications et professions européennes. L'objectif principal de l'ESCO est de fournir un dictionnaire décrivant, identifiant et classant les professions et les compétences professionnelles pertinentes pour le marché du travail, l'éducation et la formation de l'UE et montrant systématiquement les relations entre ces professions et compétences. L'ESCO est gérée par la Commission européenne, qui est responsable de la mise à jour de la classification. La ressource ESCO soutient deux des stratégies clés de l'UE dans ce domaine, à savoir la stratégie Europe 2020 et la stratégie en matière de compétences pour l'Europe[18].

L'ESCO a pour objectif de décrire toutes les professions sur le marché du travail européen, y compris la cybersécurité. Il est donc utile d'établir une cartographie d'orientation entre les profils de rôle de l'ECSF et certains des profils ESCO.

[14] CWA 16458 Profils des rôles des professionnels européens des TIC
[15] https://europa.eu/europass/fr/description-eight-eqf-levels
[16] https://europa.eu/europass/fr/national-qualifications-frameworks-nqfs
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&from=EN
[18] https://ec.europa.eu/social/main.jsp?catId=1326&langId=fr

Le tableau 5 énumère plusieurs professions de l'ESCO liées à la cybersécurité, ainsi qu'une cartographie indicative des profils de rôles de l'ECSF. Comme la relation entre eux n'est pas toujours un-à-un, les relations suivantes ont été définies pour expliquer les connexions correspondantes :

- **est** - Cette profession de l'ESCO peut être mise en correspondance avec le profil de rôle correspondant du ECSF, car tous deux décrivent le même rôle en matière de cybersécurité.
- **pourrait inclure** – Cette profession de l'ESCO peut inclure, en fonction du contexte, le profil de rôle de l'ECSF énuméré. (Il s'agit d'une cartographie indicative)
- **pourrait être inclus** – Certains aspects de cette profession de l'ESCO peuvent décrire des parties du profil de rôle de l'ECSF énumérées. (Il s'agit d'une cartographie indicative)

Tableau 5 : Relations entre les profils ESCO et les profils ECSF

Code ESCO	Profession d'ESCO	Relation	Profil du rôle de l'ECSF
2149.2.8	Ingénieur de recherche	pourrait inclure	Chercheur en cybersécurité
2310.1	Maître de conférences dans l'enseignement supérieur	pourrait inclure	Éducateur en cybersécurité
2356	Formateur en technologies de l'information	pourrait inclure	Éducateur en cybersécurité
2511.18	Auditeur informatique	pourrait inclure	Auditeur en cybersécurité
2519.2	Responsable de l'audit des TIC	pourrait inclure	Auditeur en cybersécurité
2529.1	Responsable de la sécurité informatique	est	Responsable de la sécurité de l'information (CISO)
2529.2	Expert en criminalistique numérique	est	Enquêteur en criminalistique numérique
2529.3	Ingénieur en sécurité des systèmes embarqués	pourrait être inclus	Spécialiste de la mise en œuvre de la cybersécurité
2529.4	Hackeur éthique	est	Testeur d'intrusion
2529.6	Administrateur de la sécurité des TIC	pourrait être inclus	Mise en œuvre de la cybersécurité
2529.7	Ingénieur en sécurité informatique	pourrait être inclus	Architecte en cybersécurité
2529.7	Ingénieur en sécurité informatique	pourrait être inclus	Spécialiste de la mise en œuvre de la cybersécurité
2619.4	Délégué à la protection des données	est	Responsable juridique, politique et conformité en cybersécurité

Remarque importante : La relation entre la profession d'ESCO et le profil de rôle de l'ECSF ne constitue pas une équivalence ; il offre une meilleure approximation que les lecteurs voudront peut-être étudier

ANNEXE B : CAS D'UTILISATION

Un cas d'utilisation montre pourquoi et comment une organisation utilise l'ECSF, en mettant l'accent sur la variété des approches et des avantages. La présente annexe est un recueil d'affaires qui étaient accessibles au public le 20 juillet 2022.

Les cas d'utilisation suivants ne sont que des exemples illustratifs. Les informations et le contenu inclus dans ces cas ne doivent pas être considérés comme une approbation ou une déclaration de validation de la part de l'ENISA. L'utilisation de ces exemples doit être considérée comme des cas d'inspiration plutôt que comme des références de conditionnement ou d'étalonnage.

B.1 CAS D'UTILISATION DU PROJET CONCORDIA H2020

Cette section comprend des parties du cas d'utilisation rédigé par le projet CONCORDIA H2020[19]

Vers une plateforme intégrée pour les compétences en matière de cybersécurité fondée sur le cadre européen des compétences en matière de cybersécurité

Difficile de comprendre la vue d'ensemble des formations

La nécessité de se protéger contre les menaces à l'information et aux opérations, de maintenir la posture de cybersécurité d'une organisation et d'accroître la résilience contre de telles menaces, est encore ressentie de toute urgence par toutes les parties intéressées. Un élément essentiel pour répondre à ces besoins est l'existence de professionnels compétents en matière de cybersécurité. Et la compétence en matière de cybersécurité n'est pas seulement nécessaire pour les professionnels dédiés (externes ou internes à une organisation), mais aussi pour tous les membres du personnel d'une organisation, même s'ils ne sont pas directement impliqués dans les processus et activités de cybersécurité.

En ce qui concerne les professionnels de la cybersécurité, diverses publications font toujours état d'un déficit de compétences en matière de cybersécurité, indiquant que les trois principales compétences manquantes ou insuffisamment couvertes par les professionnels existants varient d'une année à l'autre[20]. D'autre part, un nombre considérable de cours et de formations liés à la cybersécurité sont proposés par diverses organisations européennes et internationales. Une simple recherche sur Internet révélera de nombreux cours liés au domaine de la cybersécurité, sans donner une image claire des compétences offertes ou de la manière dont elles pourraient se rapporter à un rôle spécifique. Pour ajouter à cette confusion, il existe des cours de formation qui semblent aborder un rôle spécifique (par exemple, le CISO), ont des titres similaires mais ont un programme d'études différent.

Par conséquent, dans plusieurs cas, les informations fournies confondent le stagiaire sur ce qu'il doit percevoir et comment il doit percevoir les concepts de cybersécurité, ainsi que sur la manière de les utiliser pour couvrir ses besoins professionnels. En outre, les cours destinés aux professionnels sont promus sur diverses plateformes et il est difficile de les comparer en ce qui concerne les compétences couvertes et le profil de rôle abordé. Cela rend difficile pour une personne de construire un cheminement de carrière clair et d'identifier les opportunités de développement.

[19] https://www.concordia-h2020.eu/blog-post/towards-an-integrated-platform-for-skills-in-cyberbuilt-on-the-european-cyber-skills-framework/ (en anglais uniquement)
[20] https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/state-of-the-cybersecurity-workforce-new-isaca-research-shows-retention-difficulties-in-years

La carte CONCORDIA des formations pour les professionnels de la cybersécurité

Pour tenter de relever ces défis, nous avons élaboré la carte CONCORDIA des cours et formations destinés aux professionnels de la cybersécurité[21]. La carte affiche des informations structurées sur l'offre européenne existante de cours/formations de courte durée et fournit différents filtres pour faciliter la correspondance entre le besoin spécifique de développement des compétences et l'offre. [...]

On peut choisir de trier les cours en fonction du niveau de cybersécurité abordé (Appareil-, Réseau-, Logiciel/Système, Données/Application-, User-Centric), ou sur la pertinence pour un secteur industriel (par exemple Télécom, Financier, Transport e-mobilité, e-Santé ou Défense), mais aussi sur le format (face-à-face, en ligne, mixte), et le calendrier du cours/formation.

Manque d'un ingrédient clé – Solution rendue possible par l'ECSF

Bien que nous proposions sur la carte CONCORDIA une grande pléthore de filtres pour aider les utilisateurs à identifier plus facilement le ou les cours d'intérêt, la base de données manque d'un ingrédient clé : les liens vers les profils de rôle que chacun des cours aborde grâce aux connaissances et aux compétences couvertes. Le cadre européen des compétences e-CF pour les professionnels des TIC disponible au moment de la création de la carte définit 30 profils de rôle et 40 compétences associées, mais il est difficile de les associer aux spécificités du domaine de la cybersécurité.

Il s'agissait d'un défi de l'écosystème d'éducation à la cybersécurité que nous avons signalé il y a déjà deux ans et qui figure dans la feuille de route CONCORDIA pour l'éducation[22] sous la rubrique C5 : L'hétérogénéité de la terminologie liée aux compétences. Cette absence de terminologie inter sectorielle et inter industrielle concernant les compétences en cybersécurité nécessaires pour un rôle spécifique rend difficile pour les entreprises de pourvoir des postes vacants. Ils éprouvent des difficultés à faire correspondre les critères de recrutement avec les études et les qualifications énumérées dans les CV des candidats en raison de l'utilisation d'une terminologie non standard. Les individus, à leur tour, ne peuvent pas facilement identifier les compétences qu'ils doivent posséder ou développer pour répondre à la demande du marché. Et, enfin, les organismes de formation ont des difficultés à concevoir des programmes qui répondent aux besoins du marché.

Dans le cadre de la feuille de route CONCORDIA, nous nous sommes engagés pour une plate-forme unique hébergeant tous les programmes existants liés à la cybersécurité (programmes de niveau universitaire et de doctorat, cours de courte durée et formations pour les professionnels). [...]

La plateforme devrait envisager de collecter le contenu en utilisant des catégories basées sur une terminologie standard (cadre de compétences spécifiques inclus). Les catégories seraient ensuite utilisées comme filtres pour différentes demandes de renseignements de la base de données des cours. Les 12 profils de rôles définis dans la version actuelle du cadre européen des compétences en matière de cybersécurité (ECSF) semblent être une solution naturelle.

L'avantage pour les parties prenantes

L'adoption d'un lexique standard tel que celui proposé par l'ECSF, y compris les profils de rôle en matière de cybersécurité, aidera les entreprises à identifier les bons talents pour les emplois ainsi que les prestataires d'enseignement à mieux façonner leur programme d'études pour répondre aux besoins de la cyber-main-d 'œuvre. L'application de la même terminologie et l'utilisation d'un cadre de compétences à l'échelle de l'UE aux descriptions d'emploi, à la description des cours et au profil des rôles aideraient les personnes à sélectionner les modules d'éducation appropriés pour soutenir leur cheminement de carrière et à mieux filtrer les offres d'emploi en fonction de leurs compétences et de leur niveau d'expertise. Enfin, les décideurs politiques seraient en mesure de collecter des données plus structurées au niveau national/régional à l'appui de l'élaboration future des politiques et disposeraient d'une base solide lors de la coordination avec les pays extérieurs en vue de relever

[21] https://www.concordia-h2020.eu/map-courses-cyber-professionals/
[22] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf

les défis de cybersécurité à l'échelle mondiale.

Vers une plateforme intégrée pour les compétences

S'appuyant sur la base de données CONCORDIA de cours et de formations destinés aux professionnels de la cybersécurité, le projet REWIRE[23] tente de prendre de nouvelles mesures en vue d'intégrer les contenus pertinents liés aux compétences en matière de cybersécurité. La plateforme REWIRE CyberABILITY, actuellement en phase de conception, fournira des informations actualisées sur le marché du travail, les compétences, les cours de formation, les systèmes de certification et une feuille de route de carrière.

B.2 CAS D'UTILISATION DU PROJET SPARTA H2020

Cette section comprend des parties du cas d'utilisation rédigé par le projet SPARTA H2020[24].

Améliorer l'enseignement supérieur en utilisant l'ECSF et SPARTA Curricula Designer

Introduction

Ce cas d'utilisation fournit des recommandations sur la manière dont l'ECSF peut être utilisé pour façonner des programmes éducatifs liés à la cybersécurité. Comme l'ECSF manifeste la structure des profils de haut niveau du point de vue des praticiens, y compris les tâches principales, les connaissances et les compétences pertinentes, cela peut fournir une approche plus ciblée pour la création de programmes d'études spécialisés et complets, adaptés à des profils spécifiques, au lieu de couvrir la cybersécurité en général.

Défi

Les établissements d'enseignement élaborent leurs programmes d'études en tenant compte du parcours complet, en commençant par les cours fondamentaux requis pour que l'étudiant apprenne comme base pour la prochaine série de cours de suivi, qui sont souvent spécifiques à la cybersécurité. Cependant, la sélection des cours à inclure dans les programmes de cybersécurité appartient à l'institution.

Chaque établissement d'enseignement a son propre environnement (déterminé par, par exemple, l'infrastructure, l'équipement, l'expertise des enseignants, la composition des programmes existants, etc.) et il n'y a pas de façon universelle de construire le programme d'études.

Les organismes de formation diffèrent quant au sous-domaine concret de la cybersécurité sur lequel ils aimeraient se concentrer. Certains organismes sont très techniques, se concentrant, par exemple, sur l'informatique, d'autres plus sociaux, se concentrant sur les aspects juridiques et sociétaux. Par conséquent, l'interopérabilité entre les programmes d'études qui en résultent et un langage commun est actuellement un défi important.

Certains programmes académiques ne développent pas d'aptitudes et de compétences qui préparent les étudiants à des rôles de travail spécifiques disponibles sur le marché du travail. Cela pose un défi pour les étudiants qui ne comprennent pas quelles sont les possibilités professionnelles à la fin de leurs études.

Solution activée par l'ECSF

L'ECSF peut contribuer aux activités suivantes visant à relever les défis susmentionnés :

- Évaluation : La description des profils permet aux établissements de revoir leurs programmes d'études de manière structurée et systématique, en comprenant le point de vue des praticiens. Cela permet de comprendre pour quel profil l'institution destine principalement ses diplômés.

[23] https://rewireproject.eu/
[24] https://www.sparta.eu/assets/pdf/ECSF%20Training%20and%20education%20use%20case%20with%20SPARTA%20Curricula%20Designer.pdf

- Amélioration : Peut être fait sur la base de l'exercice d'évaluation. Ceci est particulièrement important compte tenu de l'ensemble des connaissances / compétences attribuées à un profil spécifique.
- Objectif : L'enseignement dispensé par les universités peut différer dans la façon dont elles abordent les compétences de base. Certains pourraient être plus axés sur des cours technologiques spécifiques, d'autres sur le droit, d'autres sur la criminalistique, etc. Disposant du ECSF avec lequel travailler, ils peuvent cartographier leurs compétences de base sur divers domaines de cours, importants pour des profils définis. Cela permet à l'institution de développer des programmes ciblés plus efficaces en interne autour des compétences principales.
- Collaboration : L'ECSF donne aux prestataires d'enseignement la langue et le vocabulaire communs pour décrire leurs cours, créer des programmes communs et permettre la mobilité des étudiants.

Lors de l'application de l'ECSF à l'éducation à la cybersécurité, l'approche suivante est recommandée :

- Les cours dans les programmes peuvent être classés comme appartenant à des catégories fondamentales ou de cybersécurité. Les cours de base sont ceux qui ne sont peut-être pas directement liés à l'ECSF, mais qui servent de prérequis pour des études ultérieures. Par exemple, la cryptologie fondamentale est la condition préalable à la cryptanalyse ou à la cryptologie avancée. La théorie des nombres est nécessaire pour la plupart des cours informatiques intermédiaires et avancés.
- Une fois les cours fondamentaux identifiés, les cours de cybersécurité peuvent être proposés pour répondre aux exigences des rôles professionnels visés par les étudiants. Le lien est réalisé en fonction du contenu des cours individuels, qui peuvent être liés aux profils et enfin aux rôles professionnels. Les mesures concrètes, [...], sont les suivantes :
  a. Pour un rôle de travail spécifique 1, les organismes de formation trouvent les profils pertinents (profil 1 et profil 12 dans notre exemple). Cette cartographie, marquée par des flèches brunes, doit être spécifiée par les annonceurs/employeurs.
  b. Les organismes de formation identifient les connaissances et les compétences nécessaires pour les profils sélectionnés. Ces exigences sont définies par l'ECSF, marquées par des flèches bleues.
  c. Les organismes de formation conçoivent de nouveaux cours ou réutilisent des cours existants (dans notre exemple, les cours 1, 2, 3, 4) qui traitent des connaissances et des compétences identifiées à l'étape ci-dessus. Cette correspondance entre les cours et leur contenu doit être effectuée par les organismes de formation.
  d. Ayant tous les cours nécessaires (et toutes les conditions préalables pour eux, des cours généraux non de cybersécurité, d'autres cours pour élargir le champ des étudiants, etc.), le noyau du programme est prêt
- Bien entendu, l'ECSF peut également être appliqué d'une manière tout à fait opposée : d'abord en composant le curriculum à partir de cours individuels, en analysant les connaissances et les compétences fournies, en utilisant l'ECSF pour identifier les profils et, enfin, en trouvant les rôles de travail qui sont soutenus par le curriculum. Cette cartographie révèle quelles connaissances et compétences exactes sont déjà présentes dans les programmes ou, d'autre part, ce qui manque et devrait être souligné ou ajouté aux cours. De cette manière, l'ECSF contribue à structurer les programmes d'études pour qu'ils correspondent mieux aux profils et aux rôles attendus.

Résultat / valeur ajoutée par SPARTA

Le projet SPARTA a utilisé un cadre de compétences en cybersécurité pour créer un outil gratuit appelé Cybersecurity Curricula Designer. Il s'agit d'une application Web simple qui aide les organismes de formation à créer de nouveaux programmes d'études sur la cybersécurité et / ou à analyser les programmes d'études existants en fonction de leur contenu et de leur reflet des

exigences des emplois en cybersécurité.

L'outil [...] permet aux administrateurs de programme d'études de composer leur programme d'études en faisant glisser et déposer des cours de la section de gauche à la section du milieu. Les cours, à partir desquels les administrateurs développent les programmes d'études, peuvent être prédéfinis ou personnalisés. Lors de la composition du programme d'étude, les données statistiques sur son contenu sont affichées dans la section de droite. Outre d'autres données, les informations sur les compétences et les rôles de travail soutenus par le programme sont fournies. En utilisant l'outil, il est facile de savoir quel contenu manque dans le programme d'études et quels rôles de travail spécifiques conviennent le mieux aux diplômés du programme. Dans ce cas, le cadre des compétences en cybersécurité est au cœur des applications, ce qui permet de lier les compétences et les connaissances aux rôles professionnels. [...]

B.3 CAS D'UTILISATION DE L'INCIBE

Cette section comprend des parties du cas d'utilisation rédigé par l'INCIBE[25].

Cas d'utilisation de l'INCIBE

Introduction

L'efficacité de la protection d'un pays dépend en grande partie des capacités de sa population, et les estimations à cet égard indiquent que d'ici 2022, l'Espagne pourrait atteindre une main-d'œuvre dans le domaine de la cybersécurité de près de 122 284 travailleurs, avec un déficit de talents estimé à 24 119. Par conséquent, l'une des principales priorités de l'administration aujourd'hui est de relever le défi d'identifier, d'attirer, de développer et de retenir les talents dans les différents domaines de la cybersécurité.

La preuve de cet engagement est le développement de la stratégie nationale de cybersécurité 2019 du gouvernement espagnol[26], qui souligne la nécessité non seulement d'avoir une position de défense et de protection pour les entreprises et les citoyens, mais aussi de soutenir le renforcement de la cyber-industrie, en reconnaissant le rôle clé que joue la cybersécurité dans l'environnement actuel de transformation et d'incertitude et l'opportunité qu'elle offre d'accroître la compétitivité de l'Espagne. Conformément à l'objectif 4 de la stratégie, la ligne d'action 5 souligne l'importance de stimuler le secteur espagnol de la cybersécurité, en plus de la génération et de la rétention de talents pour le renforcement de l'autonomie numérique.

D'autre part, le plan Espagne numérique 2025[27] vise à renforcer les leviers qui faciliteront un retour sur la voie de la croissance économique, et l'un de ses axes stratégiques est de renforcer la capacité de l'Espagne en matière de cybersécurité afin d'atténuer les risques et d'accroître la confiance dans la voie vers une économie numérique et durable.

Dans son axe stratégique 4, consacré monographiquement à la cybersécurité, il intègre les mesures qui composent les trois grands axes d'action de l'INCIBE pour les années à venir : renforcer les capacités des citoyens et des entreprises en matière de cybersécurité ; renforcer l'écosystème espagnol de la cybersécurité autour de son industrie, de la R&D&I et des talents en matière de cybersécurité ; et la consolidation de l'Espagne en tant que nœud international dans le secteur. Spain Digital 2025 reconnaît déjà le rôle clé des talents de la cybersécurité en tant que force motrice du secteur.

Ces initiatives nationales génèrent un scénario approprié qui favorise la recherche, l'innovation et implique les agents les plus pertinents de la chaîne de valeur, tels que les établissements d'enseignement et les organisations, afin qu'ils voient l'avantage de gérer les connaissances, les

[25] https://www.incibe.es/en/talento-hacker/publications/european-cybersecurity-skills
[26] https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019
[27] https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Paginas/00_Espana_Digital.aspx

capacités et les expériences technologiques qui répondent aux grands défis que le pays a en termes de cybersécurité.

Pour sa part, l'Institut national espagnol de cybersécurité (INCIBE), une entreprise relevant du ministère de l'économie et de la transformation numérique, par l'intermédiaire du secrétaire d'État à la numérisation et à l'intelligence artificielle; et l'entité de référence pour le développement de la cybersécurité et de la confiance numérique des citoyens et des entreprises, ainsi que du réseau universitaire et de recherche espagnol (RedIRIS), a pour mission d'améliorer la cybersécurité et la confiance numérique des citoyens, des mineurs et des entreprises privées en Espagne.

En outre, sa mission comprend la protection et la défense de ces groupes, la promotion de l'industrie espagnole et de la R&D&I en cybersécurité, ainsi que l'identification, la génération et l'attraction de talents dans le secteur de la cybersécurité.

Les talents en cybersécurité sont donc une pierre angulaire des actions de l'INCIBE. Sans talent, il est impossible de développer une industrie forte ou les solutions à haute valeur ajoutée nécessaires pour participer à un marché hautement concurrentiel tel que la cybersécurité.

Toutefois, les informations disponibles jusqu'à présent sur la situation des talents dans le secteur de la cybersécurité en Espagne étaient variées et fragmentées, provenant de différentes sources, ce qui a entravé la compréhension approfondie de l'environnement nécessaire pour canaliser les actions. [...]

C'est pourquoi, dans le but d'offrir une vision claire des talents de la cybersécurité en Espagne, l'INCIBE publie en mars 2022, les résultats d'une analyse et d'un diagnostic des talents de la cybersécurité au niveau national, dont le processus a été réalisé à travers des prémisses analytiques rigoureuses, une approche de travail globale et des processus participatifs et inclusifs qui ont pris en compte les principaux acteurs de l'écosystème de la cybersécurité. [...]

Défi

Les recommandations issues de ce projet d'analyse sont le point de départ pour assurer une industrie de la cybersécurité robuste et rentable qui se caractérise par la mise du talent humain au cœur des initiatives. En ce sens, l'ensemble de la chaîne de valeur de la cybersécurité peut voir cette étude comme une opportunité de se connecter davantage et de mieux comprendre les talents de la cybersécurité en Espagne.

Il est donc nécessaire de structurer et de mettre en place des pratiques efficaces qui impactent la gestion de ce type spécifique de talents dans les organisations. L'importance de la cybersécurité pour la survie des organisations nécessite de s'attaquer au problème de l'identification de ce type de talents spécifiques en cybersécurité, à l'évolution du processus de recrutement et d'embarquement, ainsi qu'à l'adoption d'actions contribuant à améliorer la gestion et à atténuer la fuite des talents.

Pour cette raison, la promotion de politiques nationales, coordonnées par l'administration et axées sur le renforcement et la promotion d'initiatives visant à faire de la cybersécurité une priorité stratégique dans les organisations, ainsi que la structuration d'un itinéraire de formation pour la performance de la cybersécurité en tant qu'activité professionnelle sont des priorités sur lesquelles les organisations et les entreprises de recrutement établiront dans leurs actions pour l'identification, l'attraction, le recrutement et la gestion des talents en cybersécurité.

De cette façon, un ensemble de recommandations sont établies que ce type d'agents (administration publique, sociétés de recrutement et autres organisations) pourrait mettre en œuvre pour augmenter les talents en matière de cybersécurité en Espagne et qui constituent le point de départ pour résoudre les défis qui nous attendent à cet égard. [...]

Solution proposée par l'ECSF

Plusieurs facteurs (politiques, économiques, sociaux, technologiques, juridiques, etc.) peuvent avoir une incidence sur le secteur de la cybersécurité et, par conséquent, sur la pénurie de talents, les

lacunes et, d'une manière générale, l'inadéquation entre l'offre et la demande.

L'un de ces facteurs pertinents dans l'Union européenne est l'absence de normalisation de la définition des rôles et des compétences en matière de cybersécurité associés à ces rôles.

Fournir une base pour une communication continue entre les différentes parties prenantes (gouvernement, industrie, universités, décideurs politiques et citoyens).

Ce type d'outil sert de base à une main-d'œuvre plus compétente et plus complète qui comprend la même langue que les autres professionnels de l'Europe. [...]

Résultat / valeur ajoutée

Par conséquent, dans le contexte présenté, deux initiatives ont été lancées au niveau national, qui donneront de la valeur à l'ECSF développé par l'ENISA et qui seront très utiles. [...]

Les deux initiatives, coordonnées entre elles, intégreront l'ECSF en tant que cadre homogène pour la définition des profils de cybersécurité, ce qui permettra à l'Espagne d'atteindre ses objectifs en matière de talents et de s'aligner sur le reste des pays au niveau européen. [...]

B.4 CAS D'UTILISATION DE LA SÉCURITÉ CYBRE EUROPÉENNE ORGANISATION (ECSO)

Cette section comprend des parties du cas d'utilisation rédigé par l'Organisation européenne pour la cybersécurité (ECSO)[28].

Vers une approche éducative harmonisée avec le cadre européen des compétences en matière de cybersécurité (ECSF)

Ayant travaillé sur l'éducation, la formation et les compétences au sein de son GT5 depuis 2016, l'ECSO a pu constater de première main les défis posés par la fragmentation et les approches dispersées qui existent aujourd'hui dans le domaine de la cybersécurité. Dans cet article de blog, l'ECSO réfléchit aux approches européennes existantes en matière d'éducation et de perfectionnement et se concentre sur le cadre européen des compétences en matière de cybersécurité (ECSF) de l'ENISA.

L'éducation n'est pas seulement une prérogative nationale. Elle est également intrinsèquement liée à la collaboration entre les entités nationales, la communauté plus large de la cybersécurité et les organismes européens. Dans cette optique, la collaboration est essentielle pour élaborer des approches paneuropéennes visant à harmoniser les programmes d'enseignement de la cybersécurité et à remédier aux compétences ou, plus concrètement, au déficit de main-d'œuvre. Il existe de nombreuses possibilités de tirer parti de l'esprit de collaboration de la communauté européenne de la cybersécurité pour proposer des solutions et des initiatives pratiques susceptibles d'avoir une incidence « sur le terrain », et le cadre européen des compétences en matière de cybersécurité (ECSF) de l'ENISA peut jouer un rôle important à cet égard.

Éducation à la cybersécurité : le point de vue de l'ECSO

Du point de vue de l'Organisation européenne pour la cybersécurité (ECSO), en tant qu'organe représentatif de l'écosystème et de la communauté public-privé européens en matière de cybersécurité, le potentiel la valeur de l'ECSF n'est pas négligeable lorsqu'il s'agit de relier les efforts existants, de fournir des éléments fondamentaux pour une main-d'œuvre européenne dans le domaine de la cybersécurité et de fournir un cadre et une taxinomie communs pour l'application des profils et des compétences. Les professionnels de la cybersécurité, les prestataires de formation,

[28] https://www.ecs-org.eu/newsroom/consolidated-educational-and-recruiting-scheme-the-glue-to-fix-todays-scattered-approach

les décideurs politiques et les professionnels du recrutement ont tout à gagner de la mise en œuvre plus large de l'ECSF.

Défi

Il est évident qu'il existe un besoin croissant de main-d'œuvre qualifiée dans le domaine de la cybersécurité. Diverses études menées dans le monde entier par l'industrie et le monde universitaire confirment que la demande de main-d'œuvre en cybersécurité est très élevée et qu'il est difficile d'embaucher des professionnels compétents. L'édition 2021 de l'étude annuelle sur la main-d'œuvre dans le domaine de la cybersécurité publiée par les membres de l'ECSO (ISC)[2] [29] indique que la pénurie de professionnels de la cybersécurité est de 2,72 millions dans le monde, ce qui, bien qu'ayant diminué par rapport aux 3,12 millions de l'année précédente, reste un nombre important. Bien que ces études offrent une base pour évaluer la situation mondiale, la réalité est qu'il est très difficile de quantifier l'ampleur de la pénurie de talents en cybersécurité en Europe. Nous savons que la demande d'experts augmentera inévitablement en raison de la croissance du marché de la cybersécurité et du paysage réglementaire, ce qui laissera un vide urgent à combler avec plus d'experts (et différents types d'experts). [...]

Mais ce n'est pas seulement une question de chiffres. Grâce à une récente étude de l'ECSO sur les pratiques et les tendances en matière de recrutement des ressources humaines, l'ECSO a également observé une augmentation du temps nécessaire, en moyenne, aux organisations pour pourvoir leurs postes dans le domaine de la cybersécurité. De nombreuses organisations indiquent que le processus de recrutement peut prendre jusqu'à six mois, ce qui est plus lent que dans l'ordre des domaines de connaissances, tandis que d'autres déclarent avoir des difficultés à pourvoir complètement leurs postes dans le domaine de la cybersécurité. Cela indique clairement qu'il existe un décalage entre l'offre et la demande (c'est-à-dire l'écart entre les exigences du monde universitaire et celles de l'industrie) et les facteurs d'incitation/d'attraction (c'est-à-dire l'aptitude et l'évaluation des candidats, l'attrait pour les emplois et les avantages). Cependant, le principal problème pour les employeurs reste le manque général, dans le monde entier, de spécialistes de la cybersécurité, alors que la demande ne cesse de croître. Plusieurs organisations soulignent également la complexité de l'embauche d'experts pour un domaine qu'elles ne maîtrisent pas. L'enquête de l'ECSO a également indiqué que, comme tendance croissante, plusieurs candidats, bien qu'ils ne possèdent pas de compétences significatives en matière de cybersécurité, enrichissent toujours leur CV avec des concepts et des mots clés en matière de cybersécurité.

Ces défis mettent clairement en évidence la nécessité d'un langage commun pour soutenir les efforts de recrutement et l'importance de tenir compte de la nature multidisciplinaire de la cybersécurité qui est si unique sur le terrain par rapport aux professions plus traditionnelles de l'informatique et des TIC. Alors que les cadres existants tels que NICE, CyBoK et e-CF fournissent des lignes directrices utiles pour le développement des compétences, un cadre européen qui fournit une taxonomie de profil globale et des parcours de carrière inhérents à la cybersécurité fait défaut. La publication de l'ECSF est donc très opportune et essentielle pour aider la communauté européenne de la cybersécurité à attirer, à former et à requalifier des experts.

Il y a une solution

L'ECSO appliquera l'ECSF de plusieurs manières afin de stimuler son adoption et de tirer parti de son potentiel pour harmoniser l'éducation et les compétences en matière de cybersécurité dans toute l'Europe.

L'ECSO prévoit de :

- Cartographier son programme de référence minimum à l'ECSF, donnant aux concepteurs de cours et aux praticiens un aperçu de première main sur la meilleure façon de définir leurs programmes d'études vers des parcours de carrière dédiés. Cela contribuera à faire en sorte que les cours universitaires reflètent adéquatement les réalités des besoins du marché du travail en matière de cybersécurité tout en permettant une mise à jour continue

[29] https://www.isc2.org/Research/WorkForce-Study

du programme.

- Utiliser l'ECSF et le manuel d'utilisation associé pour soutenir les RH/le recrutement dans la rédaction des offres d'emploi et l'organisation des procédures d'évaluation des compétences pratiques. Nous mènerons également une enquête de suivi sur les ressources humaines à l'aide des profils d'emploi de l'ECSF afin de comprendre quels rôles sont les plus nécessaires aux organisations et de développer progressivement une compréhension quantitative du marché européen de l'emploi dans le domaine de la cybersécurité.
- Utiliser l'ECSF comme taxonomie de base pour deux plateformes dédiées envisagées par la Women4Cyber Foundation et l'ECSO [...]

Résultat et valeur ajoutée

La valeur ajoutée de l'ECSF pour la communauté européenne de la cybersécurité consiste d'abord à disposer d'un cadre et d'une taxinomie communs sur lesquels travailler. Cela permettra de mieux comprendre les besoins en compétences et les réalités pratiques des différents profils d'emploi, ce qui améliorera la main-d'œuvre dans le domaine de la cybersécurité, non seulement grâce à des mesures de recrutement et de rétention plus efficaces, mais aussi en facilitant l'entrée ou le retour d'un plus grand nombre de femmes et d'autres groupes sous-représentés (c'est-à-dire les neurodivers) sur le terrain. L'ECSF, en mettant en évidence les aspects techniques et non techniques des différents profils, contribuera à éliminer l'idée fausse selon laquelle la cybersécurité n'est qu'un sujet technique, alors qu'il s'agit autant de personnes et de processus. À cet égard, le fait de souligner l'importance des compétences non techniques (transférables) dans ce domaine contribuera de manière significative à attirer davantage de femmes dans la profession de cybersécurité. L'ECSF réduira également la fragmentation des approches en introduisant des lignes directrices descendantes sur la manière de catégoriser la nature multiforme de la profession de cybersécurité. Les profils proposés par l'ECSF sont suffisamment larges pour pouvoir étayer les nombreux rôles que la profession a à offrir tout en étant segmentée d'une manière qui la rend compréhensible et applicable pour les praticiens, les experts de l'industrie, les décideurs politiques, les spécialistes du recrutement et les demandeurs d'emploi.

À l'ECSO, nous sommes convaincus que l'ECSF apportera une valeur significative à notre travail et soutiendra la communauté au sens large avec un outil concret pour harmoniser les efforts et combler le fossé entre la demande et l'offre d'experts.

B.5 CAS D'UTILISATION DE L'ISC2

Cette section comprend des parties du cas d'utilisation rédigé par le (ISC)[2] [30].

Utiliser le CISSP CBK (ISC)2 pour soutenir le cadre européen des compétences en cybersécurité / les communautés professionnelles de la cybersécurité

Introduction

Le CISSP CBK (ISC)2 – parfois simplement appelé le « corps des connaissances » – fait référence à un recueil élaboré par des pairs de ce qu'un professionnel de la cybersécurité compétent doit identifier et posséder, y compris les connaissances, les compétences, les aptitudes, les techniques et les pratiques pour réussir. Le CBK (ISC)2 est une collection de sujets pertinents pour les professionnels de la cybersécurité du monde entier. Il établit un cadre commun de termes et de principes en matière de sécurité de l'information qui permet aux professionnels de la cybersécurité et des TIC du monde entier de discuter, de débattre et de résoudre les questions relatives à la profession avec une compréhension, une taxonomie et un lexique communs. (ISC)2 a été créé, en partie, pour agréger, normaliser et maintenir le CBK (ISC)2 pour les professionnels de la cybersécurité du monde entier. Le CBK (ISC)2 présente une ressource prête à l'emploi pour les

[30] https://www.isc2.org/-/media/9644E0ED44954F7CAF895D45620213EA.ashx

professionnels de la cybersécurité actuels et en herbe à adopter dans le cadre de l'ECSF

Défi

Comme l'ENISA le décrit dans son rapport récemment publié intitulé « Addressing The EU Cybersecurity Skills Shortage And Gap Through Higher Education », les pénuries mondiales de compétences en cybersécurité et le manque de main-d'œuvre suffisante et qualifiée sont des préoccupations qui ont une incidence significative sur la capacité des États membres de l'UE à protéger le public contre les menaces croissantes émanant de l'utilisation croissante de la technologie dans la société. Malgré le travail accompli, les cyberattaques et la menace de cyberattaques continuent d'être un risque important pour la sécurité publique. Les organisations européennes ont du mal à doter leurs équipes de cybersécurité d'un personnel adéquat. Les conséquences évitables (systèmes mal configurés, déploiements précipités, réponse incomplète aux incidents, correction tardive, gestion inadéquate des risques) font que de nombreuses organisations européennes attirent des cibles pour les acteurs de la menace dans le monde entier.

Solution rendue possible par l'ECSF (comment les défis ont été relevés)

Pour relever les défis posés par le déficit de compétences et la pénurie de main-d'œuvre, (ISC)2 propose une solution visant à aider les professionnels de la cybersécurité à identifier et à cartographier les connaissances, les compétences, les aptitudes, les techniques et les pratiques nécessaires en fonction des profils recensés dans le cadre européen des compétences en matière de cybersécurité (ECSF). Le CISSP CBK (ISC)2 cartographie plusieurs domaines de compétences et de connaissances dans les profils ECSF suivants :

- 2.1 Responsable de la sécurité de l'information (CISO)
- 2.2 Intervenant en cas de cyber-incidents
- 2.3 Responsable juridique, politique et conformité en cybersécurité
- 2.4 Spécialiste du renseignement sur les cybermenaces
- 2.5 Architecte en cybersécurité
- 2.6 Auditeur en cybersécurité

En utilisant les concepts couverts dans le CBK, les professionnels qui travaillent actuellement dans les profils énumérés ci-dessus ou ceux qui aspirent à travailler dans ces profils peuvent utiliser les compétences clés et les domaines de connaissances des profils ECSF combinés avec le CBK (ISC) 2 pour déterminer comment le CBK remplit les connaissances et les compétences requises pour le poste et où ils peuvent avoir besoin de compléter leur éducation / formation d'autres sources. Cela permettra aux candidats de construire un parcours éducatif / de formation pour atteindre leurs objectifs.

Le tableau suivant fournit un exemple de la façon dont le CBK CISSP (ISC)2 peut être utilisé par un CISO actuel ou en devenir pour identifier les compétences et les domaines de connaissances clés du profil de CISO ECSF qu'ils ont ou doivent construire. [...]

Résultat / Valeur ajoutée

L'avantage escompté de la cartographie CISSP CBK (ISC)2 pour l'ECSF est qu'elle créera des parcours d'orientation professionnelle et de formation professionnelle pour aider les professionnels de la cybersécurité actuels et futurs à identifier et à acquérir les connaissances, compétences et aptitudes professionnelles nécessaires afin d'obtenir et de combler plus rapidement les profils ouverts, tels qu'identifiés dans l'ECSF, atténuant ainsi les pénuries mondiales de compétences en cybersécurité et réduisant le déficit de main-d'œuvre qualifiée.

B.6 CAS D'UTILISATION DE L'ISACA

Cette section comprend des parties du cas d'utilisation rédigé par ISACA[31].

Prise de décision de carrière individuelle : Certifications professionnelles Cadre européen des compétences en matière de cybersécurité

Introduction

Sabine travaillait comme analyste SOC quelques années après l'obtention de son diplôme universitaire et était intéressée par la meilleure façon de faire progresser sa carrière. Elle a parlé avec son mentor, qui l'a informée que l'ISACA avait été une excellente rampe de lancement pour sa carrière et l'a encouragée à se pencher sur l'adhésion et la certification éventuelle. Il faut se rendre compte qu'entrer dans la cybersécurité donne la possibilité de travailler avec tout, des gens et de la psychologie en passant par le juridique, la politique et la gouvernance, jusqu'au niveau technique le plus bas (ou le plus élevé). Le défi consiste à trouver un point de départ, puis à identifier les compétences spécifiques que l'on peut apprendre, puis à maîtriser pour élargir ou même faire la transition entre les rôles de cybersécurité. L'ECSF précise plusieurs rôles avec leurs compétences nécessaires pour travailler dans le cadre de ce rôle spécifique. Observez que ces compétences ne sont pas tout ce qui est nécessaire pour un rôle spécifique, mais le strict minimum. En l'utilisant, Sabine peut identifier le manque de compétences si l'on veut changer de rôle ou se déplacer dans un autre domaine de la cybersécurité.

Défi

En tant que nouvelle professionnelle dans un domaine à forte demande et en tant que femme en cybersécurité, Sabine cherchait de l'aide dans différents domaines :

- Orientation professionnelle et ressources — y compris les titres de compétences — pour l'aider à progresser dans sa carrière
- Un réseau de pairs et de leaders de l'industrie pour l'aider à relever les défis professionnels
- Aide au développement de compétences non techniques pour l'aider à devenir une future dirigeante bien équilibrée
- Aperçus sur la façon de surmonter les défis et de tirer parti des opportunités en tant que femme dans le domaine de la cybersécurité
- Des informations pour l'aider à bien faire son travail actuel et l'aider à se préparer aux défis futurs dans des rôles de niveau supérieur

Toute personne peut utiliser l'ECSF pour voir quels rôles sont nécessaires pour gérer presque n'importe quel type de défi ou de tâche dans le domaine de la cybersécurité. En outre, en utilisant l'ECSF comme base de référence, un individu peut ensuite identifier les compétences nécessaires pour passer d'un rôle à un autre. Cela profitera au dialogue entre les employés et les employeurs lors de la planification de la formation continue dans le domaine de la cybersécurité. Cela profitera également à une personne qui souhaite entrer dans la cybersécurité, mais qui ne sait pas par où commencer. Pour la plupart des individus, il est plus facile d'ajouter des connaissances et des compétences antérieures que d'apprendre quelque chose de complètement nouveau.

Dans le but de devenir un professionnel de la cybersécurité dans ce domaine difficile, Sabine a fait des recherches sur les responsabilités des CISO :

Profil 1 CISO Mission	Définit, maintient et communique la vision, la stratégie, les politiques et les procédures en matière de cybersécurité et gère la mise en œuvre dans l'ensemble de l'organisation. Gouverne les activités liées à la cybersécurité dans l'ensemble de l'organisation. Gère les liens/liaisons avec les autorités externes et les organismes professionnels.

L'ambition de Sabine est d'identifier les lacunes dans ses compétences afin de faire progresser sa

[31] https://www.isaca.org/training-and-events/careers-home/career-pathway/european-cybersecurity-skills-framework-and-isaca-credentials

carrière avec des références correctement alignées au niveau suivant.

Solution de l'ECSF

Sabine a fait des recherches sur le PROFIL 1 de l'ECSF et a identifié des lacunes dans ses connaissances :

Connaissances clés	✓ Connaissance des normes, des cadres, des politiques, des règlements, des lois, des certifications et des meilleures pratiques en matière de cybersécurité et de protection de la vie privée Compréhension des exigences éthiques en matière d'organisation de la cybersécurité ✓ Connaissance des contrôles de sécurité Connaissance des modèles de maturité de la cybersécurité ✓ Connaissance des tactiques, techniques et procédures de cybersécurité Connaissance de la gestion des ressources Connaissance des pratiques de gestion Connaissance des cadres de gestion des risques

Sabine a décidé de suivre le conseil de son mentor et d'assister à une réunion du comité local de l'ISACA pour voir si cela lui convenait. Elle a été immédiatement impressionnée par les possibilités offertes. Le comité l'a chaleureusement accueillie et lui a présenté plusieurs personnes clés du comité, des personnes qui occupaient exactement le type de poste que Sabine recherchait et qui seraient d'excellents mentors ou sponsors.

La présidente de la certification du comité a informé Sabine que la certification Certified Information Security Manager (CISM) lui conviendrait parfaitement, car elle démontre une connaissance approfondie de la sécurité de l'information ainsi que de solides compétences managériales. La certification est pour ceux qui ont cinq ans ou plus d'expérience, alors Sabine a décidé de faire un plan de 18 mois pour étudier et obtenir la certification.

Elle a rejoint l'ISACA en tant que membre ce soir-là et a pleinement profité des ressources offertes par l'association aux niveaux mondial et local. Elle a rejoint les communautés en ligne de l'association, a commencé à participer à des webinaires et à des réunions de sections locales proposés par SheLeadsTech, un programme proposé par la fondation One in Tech de l'ISACA. Et elle a assisté à presque toutes les réunions offertes par le comité local.

À peine six mois après le début de son adhésion, une collègue membre du comité l'a approchée au sujet d'un emploi en tant qu'analyste de la sécurité de l'information au sein de leur organisation.

Résultat

Sabine est membre de l'ISACA depuis sept ans. Elle a obtenu sa certification CISM et a rapidement été promue responsable de la sécurité de l'information. Elle est maintenant directrice de la sécurité de l'information, avec une voie claire vers un rôle de CISO.

En plus de trouver des qualifications et des emplois grâce à l'ISACA, Sabine a également trouvé plusieurs ressources qui l'ont aidée à ajouter de la valeur à son organisation. Avant que le RGPD n'entre en vigueur, Sabine a pu tirer parti du Centre de ressources sur le RGPD proposé par l'ISACA pour l'aider à comprendre la situation en profondeur et apprendre quelles étaient les mesures les plus importantes à prendre dans le cadre de ses fonctions actuelles.

L'intérêt et l'expérience qu'elle a acquis dans le domaine de la protection de la vie privée grâce à ce projet lui ont permis de se qualifier pour le titre de Certified Data Privacy Solutions Engineer (CDPSE) de l'ISACA dans le cadre de son programme d'adoption précoce.

Elle a fait des présentations lors de conférences de l'ISACA au niveau national et local, ce qui lui a permis d'améliorer ses compétences en matière de communication, et elle a accepté un poste au

sein du conseil d'administration de l'ISACA l'année dernière. En tant que directrice, elle a eu l'occasion de recruter pour quelques postes, et la plupart de ses embauches ont été faites par le comité de l'ISACA, tout comme elle a obtenu sa première promotion il y a six ans. Ayant constaté la valeur de la certification CISM dans sa propre carrière, elle a commencé à proposer à son équipe une préparation à la certification CISM par le biais des offres de formation en entreprise de l'ISACA.

Le nouveau domaine d'intérêt de Sabine, alors qu'elle se prépare à assumer son rôle de CISO, est la sécurisation des technologies émergentes. Compte tenu de l'accent réglementaire accru sur l'IA en Europe, elle a d'abord dirigé ses efforts dans ce domaine, obtenant récemment un certificat de principes fondamentaux de l'intelligence artificielle de l'ISACA.

Sept ans après avoir franchi les portes de sa première réunion du comité ISACA, Sabine a développé son réseau par des centaines de professionnels locaux et des milliers dans le monde. Elle est une leader et conférencière confiante, et elle est maintenant un mentor pour plusieurs autres qui étaient autrefois à son poste. Parmi ses conseils à ses mentorés est de toujours apprendre - et que l'ISACA, en tant que communauté d'apprentissage mondiale, est une excellente ressource.

Sabine a décrit les mesures à prendre pour obtenir le C-suite et prévoit d'occuper un rôle de CISO d'ici cinq ans. Elle est convaincue que son réseau ISACA et ses références seront un avantage significatif dans la poursuite de ses objectifs

Cheminement de carrière :

- Analyste SOC
- Sécurité de l'information – Analyste
- Sécurité de l'information – Gestionnaire
- Directeur de la sécurité de l'information

B.7 CAS D'UTILISATION DES SANS/GIAC

Cette section comprend des parties du cas d'utilisation rédigé par l'institut SANS et le GIAC (Global Information Assurance Certification)[32].

Pourquoi les cadres de travail et les certifications sont importants dans la cybersécurité

La directive sur les réseaux et l'information (NSI) II constitue une mise à jour du mandat actuel de l'Union européenne. Cela contribuera à encourager un langage commun en matière de cybersécurité dans un plus large éventail de secteurs de l'économie et nécessitera un partage d'informations entre les États membres et entre les secteurs. Des directives comme celle-ci ont une importance croissante dans la mise en place de garde-corps pour les cyberactivités. Pour protéger la valeur actionnariale, la Security and Exchange Commission (SEC) envisage un cyber-rapport pour les sociétés cotées en bourse exigeant des rapports sur la façon dont leurs équipes de sécurité géreront les risques, les incidents et l'expertise cybernétique du conseil d'administration. Le rapport d'atténuation des risques de sécurité sera lié aux ensembles de compétences des rôles professionnels.

Les cadres aident à articuler ces rôles professionnels. Jusqu'à récemment, la plupart des offres d'emploi étaient des listes génériques recherchant des professionnels de la cybersécurité sans tâches, compétences ou connaissances bien définies sur ce qui est nécessaire pour protéger les actifs de l'organisation. Les cadres de travail tels que le Cadre européen de compétences en cybersécurité (ECSF) commencent à normaliser les talents nécessaires pour les postes de réponse aux incidents cybernétiques, d'enquêteur en criminalistique numérique et de responsable de la sécurité de l'information. La normalisation permet aux organisations d'identifier les bons talents pour gérer les menaces futures. C'est en ligne avec d'autres professions. Par exemple, les médecins ont des domaines spécialisés tels que les radiologues, les pédiatres et les chirurgiens du cerveau qui

[32] https://www.giac.org/blog/why-workforce-frameworks-certifications-matter-cybersecurity/

ont l'expertise nécessaire dans leur domaine pour fournir un traitement approprié.

La certification joue un rôle important dans la préparation des personnes à des postes spécifiques. La certification valide l'individu en utilisant les meilleures pratiques et lignes directrices pour les tests éducatifs et psychologiques tels que les normes internationales ISO / IEC 17024. Un exemple de certification considérée comme la norme mondiale est un expert-comptable agréé (CPA). L'expérience de travail peut faire de quelqu'un un expert, mais le CPA est la référence bien respectée d'un professionnel certifié et peut même être une exigence de conformité sur des projets ou des audits spécifiques.

Voici quelques exemples où les cadres de travail ont contribué à faire progresser l'industrie de la cybersécurité :

- Les grandes entreprises technologiques et financières disposent souvent de plusieurs équipes de sécurité qui normalisent leurs rôles et leurs exigences grâce au cadre permettant de repositionner et de faire pivoter rapidement les travailleurs en fonction de la mission.
- Les organisations peuvent cartographier l'expérience et la certification de leur main-d'œuvre afin de faire correspondre rapidement les compétences du personnel aux exigences du projet. Ceci est particulièrement important pour les sociétés de conseil, les entreprises de technologie et les entrepreneurs.
- Les cadres fournissent un langage commun au sein de la main-d'œuvre dans des secteurs tels que la technologie, la finance, les soins de santé, la vente au détail et les services publics, permettant aux équipes de travailler ensemble pour protéger les cybermenaces et les menaces de sécurité physique.
- Les cadres fournissent un modèle aux établissements universitaires pour combler le fossé entre leurs offres éducatives et les compétences actuelles en cybersécurité nécessaires dans tous les secteurs, préparant leurs étudiants à des emplois.

SANS et GIAC comprennent l'importance des cadres et ont aligné les cours et les certifications sur ces cadres. Les cadres sont un modèle pour les organisations pour normaliser les exigences de travail, même si chaque organisation et mission aura besoin d'une certaine personnalisation liée à leur mission spécifique. Nous avons aidé à concevoir et à mettre en œuvre des programmes de développement de la main-d'œuvre en utilisant des cadres comme modèle pour les entreprises Fortune 500, les organismes gouvernementaux et les organisations de toutes tailles.

TP-09-22-509-EN-N

À PROPOS DE L'ENISA

L’Agence de l’Union européenne pour la cybersécurité (ENISA) est l’agence de l’Union chargée d’atteindre un niveau élevé commun de cybersécurité dans toute l’Europe. Créée en 2004 et renforcée par le règlement de l'UE sur la cybersécurité, l'Agence de l'Union européenne pour la cybersécurité contribue à la politique de l'UE en matière de cybersécurité, renforce la fiabilité des produits, services et processus TIC grâce à des schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'UE, et aide l'Europe à se préparer aux cyber défis de demain. Grâce au partage des connaissances, au renforcement des capacités et à la sensibilisation, l’Agence collabore avec ses principales parties prenantes pour renforcer la confiance dans l’économie connectée, renforcer la résilience des infrastructures de l’Union et, par conséquent, préserver la sécurité numérique de la société et des citoyens européens. De plus amples informations sur l’ENISA et ses travaux sont disponibles à l’adresse suivante : www.enisa.europa.eu.

ENISA
Agence de l'Union européenne pour la cybersécurité

Bureau d'Athènes
Agamemnonos 14, Chalandri 15231, Attiki, Grèce

Bureau d'Héraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton, Héraklion, Grèce

enisa.europa.eu

ISBN: 978-92-9204-583-8
DOI: 10.2824/95989