Livre blanc

LE SYNDROME DE L'IMPOSTEUR EN CYBER

Pourquoi êtes-vous légitime ?

Un ouvrage co-écrit par :

CSB . School
CYBERSECURITY BUSINESS.SCHOOL

CEFCYS

Ce livre blanc est l'occasion pour le CEFCYS de rendre hommage à un confrère et ami de la cybersécurité, Nuno FILIPE qui a été emporté par le cancer le 04 mars 2022, à l'âge de 45 ans.

Nuno est passé par l'école des sous-officiers de l'armée de l'air et était réserviste. Nuno était un homme engagé et dévoué aux autres.

Dévoué à la nation, à sa famille, aux nombreuses personnes et entreprises qu'il a protégées dans ses différentes fonctions de Responsable de la Sécurité des Systèmes d'Information (RSSI) et aussi Manager en cyber et adhérent du CEFCYS.

Il était également bénévole au sein d'une équipe sportive de handball et œuvrait pour le développement des valeurs de ce sport auprès des plus jeunes.

Son engagement, sa bienveillance et son humilité sont une source d'inspiration.

Son départ est une grande perte pour tout le monde et j'adresse toutes mes condoléances à sa femme et ses enfants. Puisse-t-il reposer en paix

Nacira Salvan

Ce livre blanc est dédié à

NUNO FILIPE

SOMMAIRE

ÉDITO

Le domaine de la cybersécurité est un secteur professionnel passionnant dans lequel les opportunités de carrière sont nombreuses.

Toutefois, c'est un domaine dont les offres sont supérieures à la demande et ce, pour plusieurs raisons. Les stéréotypes de genre, la méconnaissance des métiers de la cyber, les représentations sociales, le manque d'information sur les modèles féminins ou encore le manque de communication contribuent aux difficultés de recrutement et de formation.

La question de la diversité est importante dans le domaine de la cybersécurité. En effet, le regard et la perception sont de réels atouts dans la gestion des crises, la façon de répondre aux attaques, le management et la gouvernance ou la communication. Bien que la cyber ait besoin de plus de femmes, le domaine souffre également du syndrome de l'imposteur.

Si celui-ci touche, statistiquement parlant, plus d'une femme sur deux, le fait est qu'il touche tout le monde, et ceci indépendamment de l'âge.

Ce secteur professionnel a besoin de talents divers.

Que ces talents soient des hommes ou des femmes, en situation de handicap ou pas, des jeunes au collège et au lycée, en questionnements sur leur avenir, ou encore des personnes en reconversion après une première expérience ou plusieurs, certains de ces talents peuvent souffrir de ce syndrome de l'imposteur et ignorer toute l'étendue de leurs capacités bien supérieures à ce qu'ils peuvent penser.

C'est dans ce but que ce livre blanc a été rédigé en collaboration entre le CErcle des Femmes de la CYberSécurité (CEFCYS) et la Cybersecurity Business School (CSB.School).

Et quand il m'a été demandé de rédiger son édito, j'ai tout de suite dit oui. Depuis 20 ans dans le domaine et étant responsable de la sécurité des systèmes d'information depuis de nombreuses années, je rencontre régulièrement des personnes curieuses, investies, appliquées, qu'elles travaillent dans le domaine de la cyber, avec ou sans syndrome ou qui justement sont des profanes mais qui s'intéressent à ces métiers ; là aussi avec ou sans syndrome.

Vous l'aurez compris, ce livre blanc s'adresse donc aux plus jeunes comme au moins jeunes. S'il parle de la cybersécurité, il peut néanmoins parler à toutes les personnes curieuses qui se questionnent sur la suite de leur carrière.

Des personnes qui veulent la commencer, après le lycée, ou lui donner une nouvelle direction suite à une première orientation qui ne convenait pas ou une expérience professionnelle dont le vent a fait tourner les voiles.

La cyber a besoin de vous et je suis persuadée que vous pouvez lui apporter vos compétences humaines et techniques !

Et quand je parle de compétences techniques, je pense à toutes les compétences ; peu importe le parcours scolaire, professionnel, associatif ou personnel. Je parle bien sûr des compétences transversales. Celles que l'on apprend ailleurs mais qui peuvent être exploitées dans les métiers de la cyber. Celles que l'on acquiert de façon formelle ou informelle, ici ou ailleurs et que l'on peut utiliser autrement et au service des métiers de la sécurité informatique.

Le but de ce livre blanc a aussi pour objectif de démystifier l'univers de la cybersécurité. Oui, il est accessible ! Et pas uniquement aux profils scientifiques ou aux hommes. On peut faire de la cyber peu importe qu'on soit une femme ou un homme, peu importe son profil et peu importe ses appétences.

Qu'on ait un profil littéraire, juridique, artistique, scientifique ou autre, la cyber a besoin de compétences et de vision en management pour encadrer et fédérer, en gouvernance pour structurer et organiser, en leadership pour inspirer, en communication, en formation et en pédagogie pour prévenir, sensibiliser et expliquer, en renseignement pour collecter des informations et données utiles, en créativité pour inventer et innover, en psychologie pour mieux comprendre et anticiper les comportements, ou encore en éthique pour garantir des usages et comportements respectueux des autres ! Et j'en oublie sûrement d'autres.

Quant aux domaines où on peut avoir besoin de l'ensemble des compétences requises en cybersécurité, eux aussi sont nombreux et concernent toutes tailles d'entreprises, car aujourd'hui tout le monde est concerné par les cybermenaces, voire par les effets de la cyberguerre. Que vous ayez envie de travailler dans le public, le privé ou l'associatif, dans une entreprise internationale, une PME ou une TPE, les besoins en cyber sont bien présents !

La France est un pays reconnu dans le domaine de la cybersécurité. Nous avons tout : des talents, des compétences, des écoles, des écosystèmes, des institutions et des dispositifs de financements pour promouvoir la formation et la reconversion. Et pourtant ! L'Europe a besoin de 300 000 personnes dans la cyber, 180 000 rien qu'en France. Sur 6000 postes nécessaires dans notre pays, seules 1000 personnes sont aujourd'hui formées. C'est dire à quel point il y a des opportunités !

Nous avons souhaité que ce livre blanc soit synthétique et pragmatique. Une première partie sur le syndrome de l'imposteur. Peut-être vous reconnaîtrez-vous. Ce n'est pas pour autant une fatalité ! On peut le dépasser ; j'en ai été témoin de nombreuses fois. Alors pourquoi pas vous ?

En deuxième partie, vous trouverez quelques interviews de personnes qui œuvrent aujourd'hui, chacune et chacun à leur façon, dans le domaine de la cybersécurité. Nous espérons que ces témoignages pourront vous inspirer et, qui sait, vous donner envie de rejoindre une communauté très active et engagée.

Nacira Salvan
Fondatrice et présidente du CErcle des Femmes de la CYberSécurité (CEFCYS)

INTRODUCTION

Pour parler du syndrome de l'imposteur, il faut commencer par parler de Pauline Rose Clance et Suzanne Imes, les deux professeures de psychologie américaines qui l'ont identifié dans les années 70. Avant qu'un abus de langage n'en fasse un "syndrome", elles l'avaient en fait nommé "phénomène de l'imposteur".

Le syndrome de l'imposteur ou syndrome de l'autodidacte se caractérise par un doute permanent et constant. La victime va rejeter le mérite de ses actions, vouloir attribuer sa réussite à une tierce personne, ne pas se sentir légitime sur son poste et se remettre en cause. Il est convenu qu'au cours de sa carrière, chacune et chacun développera ce syndrome.

Pour la grande majorité, ce syndrome sera temporaire car lié à une promotion ou à un changement de carrière. Toutefois, pour d'autres, ce syndrome persistera malgré la nouvelle prise de fonction.
Cela est davantage le cas dans les métiers associés à un stéréotype. Exemple typique : la cybersécurité, domaine généralement associé à un homme ayant réalisé des études d'ingénieur, parfois cadre, souvent geek.

Comment pouvons-nous nous sortir de cette spirale ? Comment aider nos proches qui en souffrent ? Ce syndrome est-il toujours négatif ? Pourquoi est-il plus marqué dans certains domaines ? Voici quelques questions auxquelles nous allons répondre.

Nous souhaitons remercier l'ensemble des personnes ayant contribué à cet ouvrage en livrant leur témoignage, et pour les plus curieux nous vous donnons rendez-vous en page 20.
Grâce à l'Échelle de Clance*, il est possible de découvrir si l'on souffre ou si l'on a souffert de ce syndrome dans son parcours académique ou professionnel.

*Du nom de l'une des psychologues - Pauline Rose Clance - qui a théorisé ce syndrome

UN SYNDROME BIEN CONNU MAIS MAL DÉTECTÉ

Selon vous, quel pourcentage de la population a déjà subi le syndrome de l'imposteur ? 38% - 62% - 70% ?

La bonne réponse est 62%. Plus d'une personne sur 2 s'est déjà dit "si j'ai réussi, c'est surtout parce que j'ai eu de la chance " et autres phrases de ce type.

Mais savez-vous que dans le domaine des sciences, comme la cybersécurité, ce chiffre atteint les 70% ? Plus de 2 personnes sur 3, ont, un jour, eu ce sentiment.

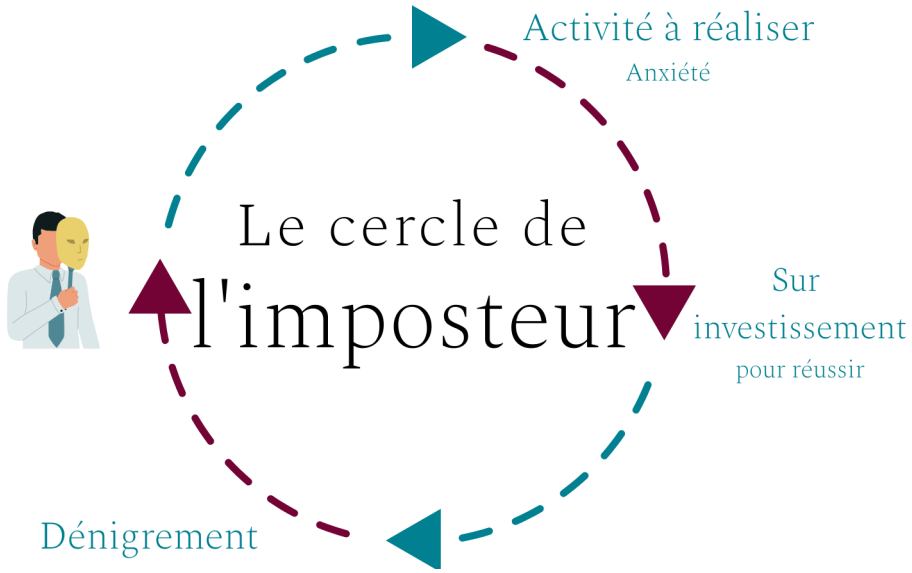
Le syndrome est ainsi bien présent dans la sphère professionnelle, mais étonnamment les personnes concernées, ne se qualifient pas comme étant des "imposteurs" lorsque nous leur posons la question.

Il y a presque autant de formes du syndrome que d'individus, toutefois il est possible d'identifier 3 piliers communs à ce sentiment. Piliers définis par le docteur en psychologie Kevin Chassangre :

- l'impression de tromper son entourage
- la tendance à la mauvaise attribution
- la peur d'être un jour démasqué

La plupart de ceux ou de celles qui souffrent d'un syndrome de l'imposteur ne se qualifient pas volontiers d'imposteurs . Or, lorsqu'ils entendent parler de ce syndrome, ils s'écrient : "C'est exactement ce que je ressens, comment le savez-vous ? " (Clance, 1985).

UN SYNDROME À DÉDRAMATISER ?



> “Si c’était à refaire, je l’appellerais l’expérience de l’imposteur parce que (...) c’est quelque chose dont presque tout le monde fait l’expérience”

La réponse est Oui !

Car avant tout, ce syndrome ne concerne que les personnes qui réussissent ou qui bousculent leur zone de confort.

C’est là un élément essentiel à retenir car, rappelons-le, il ne s’agit pas d’une condition qui se diagnostique et se soigne comme une maladie psychiatrique, mais d’une expérience psychologique.

Pouvoir se remettre en question

Remettre en doute ses capacités à petite dose ou de façon temporaire permet d’évoluer.

Si vous êtes capable de remettre en question vos compétences, vous êtes probablement capable de remettre en question votre remise en question, non ?

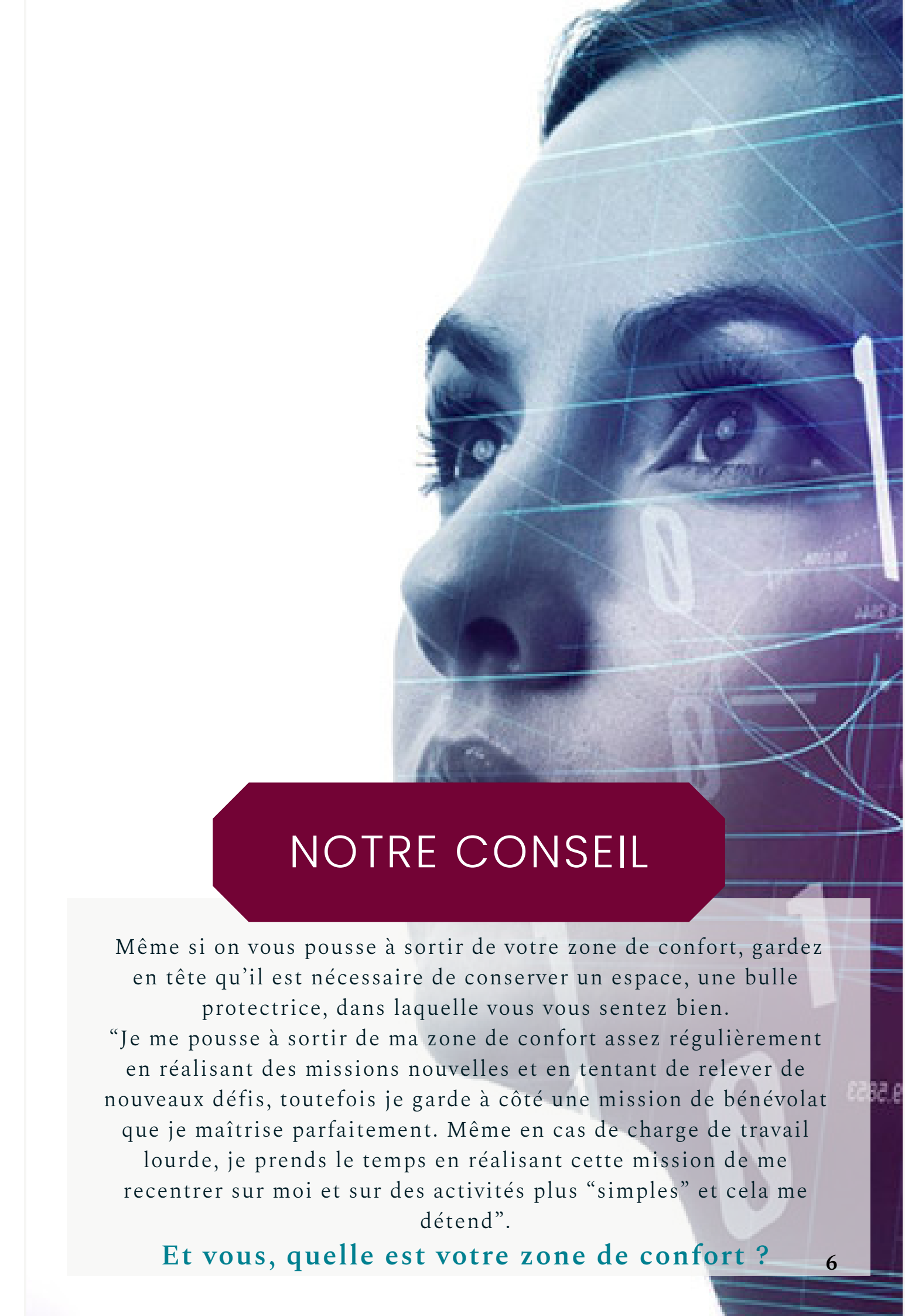
Développer sa confiance en soi et envers les autres

Le syndrome nous fait nous questionner sur nos capacités, au point où nous avons parfois du mal à entendre le bien que les autres pensent de nous.

Lutter contre ce biais, c’est avant tout apprendre à écouter et à entendre les messages positifs. De cette façon naît notre propre reconnaissance. Oui, ma réussite vient de mes actions !

Faire bouger les lignes

Ce syndrome n’est pas une fatalité et prendre conscience de son état, c’est aussi permettre aux autres de se retrouver au travers de notre histoire. C’est ouvrir la voie au dialogue !



NOTRE CONSEIL

Même si on vous pousse à sortir de votre zone de confort, gardez en tête qu'il est nécessaire de conserver un espace, une bulle protectrice, dans laquelle vous vous sentez bien.
"Je me pousse à sortir de ma zone de confort assez régulièrement en réalisant des missions nouvelles et en tentant de relever de nouveaux défis, toutefois je garde à côté une mission de bénévolat que je maîtrise parfaitement. Même en cas de charge de travail lourde, je prends le temps en réalisant cette mission de me recentrer sur moi et sur des activités plus "simples" et cela me détend".

Et vous, quelle est votre zone de confort ?

UN SYNDROME INÉVITABLE EN CYBER ?

Ce syndrome s'observe dans tous les secteurs d'activité, mais il est plus fréquent dans les secteurs scientifiques. Pourquoi ? Car des stéréotypes nous poussent à douter de notre capacité à agir.

Ainsi, il est courant que dans les secteurs tels que la cyber, les femmes ou les personnes n'ayant pas un bagage scolaire classique s'interrogent sur leur légitimité.

Pourquoi se sent-on moins légitime en cyber qu'ailleurs ?

N° 01 - Les stéréotypes

La cybersécurité reste perçue comme un domaine réservé à ceux sortis du moule "fort en maths - bac S - école d'ingénieur" ; ce qui en miroir peut agir comme un repoussoir pour tous les autres profils tels que les femmes, les reconversions professionnelles ou les diplômes non scientifiques. Une des pistes pour rapprocher ces mondes et rendre ce secteur attrayant au-delà des stéréotypes, pourrait consister pour la cybersécurité à adopter une approche plus décontractée et plus pratique.

N° 02 - Adaptation du secteur

Le monde du travail évolue afin de répondre aux attentes multiples et variées de ressources aux profils de plus en plus divers. Aujourd'hui, de nombreuses entreprises du secteur des technologies de l'information et de la communication s'adaptent pour attirer des ressources rares. Mais, cette adaptation est souvent plus complexe à mettre en œuvre dans les entreprises dont le cœur de métier est centré sur la technique, la conduite du changement pouvant y être plus longue à engager.

NOTRE VISION

Dans un domaine faisant face à une pénurie de ressources, il est nécessaire d'ouvrir le champ des possibles en matière de cybersécurité à des profils différents.

Cela passe inévitablement par la formation, qui doit prendre en charge ces profils au sein de son cursus. Le monde de la cyber doit créer des passerelles et rappeler qu'il n'est pas nécessaire d'appartenir au sérail pour devenir un expert.

De nombreux métiers connexes au domaine existent et sont propices à des réorientations ou reconversions professionnelles réussies.

> N'oubliez pas, entreprendre un nouveau défi est déjà un acte légitime.

LE SYNDROME DE L'IMPOSTEUR, POURQUOI ÊTES-VOUS LÉGITIME ?

Les profils en cybersécurité sont complémentaires. Notre domaine tient sa richesse de cette complémentarité. Pour vous démontrer que tous les profils sont légitimes, nous vous proposons 4 témoignages.

4 témoignages pour comprendre ce que vous pouvez apporter à la cybersécurité en ayant un parcours loin du schéma classique.

LAETITIA SOYER

Responsable de projet en cybersécurité et continuité d'activité dans le secteur de la banque et assurance

Peux-tu m'en dire plus sur ton parcours et ton métier ?

J'ai un parcours dit « atypique », un terme que l'on pourrait trouver négatif au premier abord mais qui, finalement, a fait de moi une professionnelle « bien dans ses baskets ». Durant ma scolarité, mes activités étaient tournées vers l'informatique, le secourisme et l'art plastique. Je me suis tout d'abord orientée vers le secteur de la biologie (bac +3), puis j'ai décidé d'entamer une reconversion et de choisir une formation de bac+2 en informatique tout en démarrant en parallèle, mon premier emploi en service client informatique (helpdesk).

C'est en découvrant la diversité des sujets, la nécessité de veille permanente et d'apprentissage continu face aux nouvelles technologies que le domaine de la sécurité a pris tout son sens.

Depuis 5 ans, j'ai pu insérer de la créativité dans mon travail, l'une de mes premières natures, afin de rendre plus innovante ma façon de travailler et d'accompagner la transformation du métier. Lorsqu'il y a des incidents, on se sent utile de part nos compétences et connaissances. Les pics d'adrénaline sont récurrents et demandent une certaine flexibilité, mais c'est ce qui fait la force de ce métier qui est plus qu'intéressant. C'est un métier dans lequel la communication écrite, orale ainsi que la sociabilité est vitale, notamment lors de la gestion de crise.

> En cybersécurité j'ai tendance à dire que l'on ne doit jamais dire « non » , dire toujours « oui mais » car on peut toujours mieux sécuriser sans bloquer pour autant le business. Au final, le lien avec la biologie n'est pas si éloigné, on y retrouve aussi des virus et la part humaine est très importante.

Est-ce que tu as déjà entendu des personnes te dire que ce domaine n'était pas fait pour une femme ?

Je n'avais jamais entendu que ce domaine n'était pas fait pour une femme par contre on me dit parfois que je ne suis pas assez technique, ce qui est difficile à entendre, car après 15 ans dans ce métier, on est forcément technique et on connaît beaucoup de solutions et de systèmes. À défaut, on invente de nouvelles solutions avec les experts dédiés à un sujet comme les comptes d'accès ou les gestionnaires des règles de firewall ou les responsables de la sécurité des données etc… Par contre dans ce domaine, nous sommes souvent entourées d'hommes. Ce qui n'est pas désagréable car on est plutôt chouchoutée.

Petite remarque : ma directrice de sécurité est une femme et ma première manager l'était également. Les mentalités progressent car les équipes deviennent de plus en plus mixtes. D'ailleurs, il est essentiel que les métiers de la sécurité aient cette diversité de genre. Il ne faut pas oublier que la sécurité des informations et des usages s'adresse à un public d'hommes et de femmes.
Les solutions proposées doivent donc être adaptées à tout public.

Est-ce que tu as déjà entendu des personnes te dire que ce domaine n'était pas fait pour une personne n'ayant pas un profil technique ?

Le domaine de la cybersécurité ne contient pas que des métiers techniques, il y a plein de compétences attendues, le management transversal est assez recherché, on a aussi des métiers de gouvernance, de contrôle, de communication, de juridique, de développement applicatif etc.

Pour changer le monde (de la cyber), par quoi tu commencerais ?

J'accompagnerais tout un chacun et j'amènerais les individus à avoir leur propre détecteur de signaux faibles et à développer leur sens critique. Cela passe par la culture, la connaissance et l'inclusion.

Est-il obligatoire de maîtriser les mathématiques pour travailler dans la cyber ?

J'avais des résultats corrects en mathématiques, d'où mon orientation vers des métiers scientifiques. Les sciences sont importantes pour acquérir une certaine connaissance, une logique de pensée et une capacité d'analyse. Dans tous les cas, gardez à l'esprit que tout s'apprend, tout est une question de pratique et de volonté ! Apprendre est ce qui est de plus enrichissant et valorisant dans un métier, c'est d'ailleurs une des raisons pour lesquelles on ne s'ennuie jamais !

Quelles sont les qualités qu'il faut posséder pour travailler dans ce domaine ?

Dans les métiers de la sécurité des systèmes d'information, je pense qu'il faut avoir du sang-froid, ne pas agir trop vite sans réfléchir. Une rigueur est également essentielle et elle s'apprend tout comme l'organisation, la méthodologie. L'envie continue d'apprendre est donc un atout majeur, tout comme la curiosité.

Quels conseils aurais-tu souhaité entendre quand tu as commencé ta formation, et quels conseils donnerais-tu à une personne souhaitant s'orienter ou se reconvertir ?

"Ose être qui tu es ! ». Si tu ne sais pas encore qui tu es, alors ose expérimenter et ose dire que tu ne sais pas, pour aller plus loin, plus vite. Sachant qu'à plusieurs on est plus fort et que l'on va plus vite : demande des feedbacks réguliers à des gens de confiance et augmente tes chances de réussite.
N'aie pas peur du jugement car tout le monde est passé par là ! Si je devais donner des conseils à travers mon expérience je dirais :

Regarder et être fier de nos compétences acquises et ne pas se focaliser sur celles que l'on n'a pas (encore).
Ne pas gaspiller notre énergie à travailler trop longtemps sur des sujets qui ne nous intéressent pas.
Penser « carrière » dès notre premier travail et ne pas le faire au bout de 10 ou 15 ans.
Entretenir son réseau le plus tôt possible : car ce n'est pas lorsque l'on cherche un travail qu'il faut se préoccuper de son réseau, de plus, il faut bien un à deux ans pour construire un premier réseau actif.

Est-ce que tu peux partager avec nous une réussite dont tu es fière ?

- Avoir mené à la réussite un projet d'innovation en matière de lutte contre la fraude avec une diminution importante des pertes liées.
- Avoir réalisé une structuration complexe des règles de gestion des habilitations des utilisateurs.
- Avoir déployé un programme de pentest (test d'intrusion) et de test de vulnérabilités.
- Avoir participé à la fusion d'un centre des opérations de sécurité.

Être à l'origine de la création d'un programme de sensibilisation à la sécurité du numérique pour les jeunes avec l'association du CEFCYS (Cercle des femmes de la cybersécurité).

Une intuition concernant le monde du travail de demain dans la cyber ?

La sécurité informatique nous impacte aussi bien dans notre quotidien que dans notre travail, ainsi, tous les corps de métiers sont concernés, tous les secteurs, qu'ils soient publics ou privés. Dans le monde du travail, chaque métier devra avoir une connaissance toujours plus pointue de la sécurité informatique et humaine dans son domaine. C'est pour cette raison que des sociétés de conseil se développent de plus en plus, et que les profils dans la cybersécurité sont et seront de plus en plus recherchés.

CLARA FOUCHER

Consultante en protection des données personnelles se spécialisant en cybersécurité

Peux-tu m'en dire plus sur ton parcours et ton métier ?

J'ai effectué un bac littéraire parce que j'ai toujours eu une appétence pour les langues et la littérature. Depuis toute petite je détestais les mathématiques alors, je n'imaginais pas une seule seconde faire des études dans la cybersécurité. Notamment parce que c'était un domaine qui (à cause de mes préjugés) était selon moi inaccessible alors qu'il m'attirait énormément. Ainsi, quand le choix s'est imposé de déterminer les études que j'allais faire, j'ai décidé de m'orienter vers le droit car c'était un domaine qui correspondait à mes valeurs et se rapprochait le plus de mes aspirations professionnelles. En réalité, tout a débuté en 2018, à l'époque, on commençait tout juste à parler du RGPD qui était un sujet qui me passionnait. Puis, lorsque la DPO (déléguée à la protection des données personnelles) de l'Université Jean Moulin Lyon 3 m'a donné l'opportunité de faire un stage à ses côtés pour l'épauler dans la mise en conformité de l'établissement, j'ai eu un véritable déclic : la protection des données personnelles était la raison même pour laquelle j'avais choisi de faire des études de droit.

À la suite de cette expérience, la Présidence de l'Université m'a permis de continuer à travailler dans ce domaine à travers un CDD en qualité d'assistante DPO en parallèle de ma dernière année de droit. L'année suivante, j'ai décidé d'entreprendre un Diplôme Universitaire de transformation numérique au Disrupt'Campus de Lyon. J'ai eu à cette occasion l'opportunité d'effectuer un stage de 3 mois au sein d'une DSI dans un site industriel classé Seveso. Puis ce stage s'est transformé en contrat de travail, toujours dans le cadre de la mise en conformité RGPD mais avec une dimension plus centrée sur la cybersécurité.

C'est à cette occasion que j'ai eu une véritable révélation pour ce domaine et toute la diversité des métiers qui en font partie !

En collaborant principalement avec le Responsable de la sécurité des systèmes d'information (RSSI), j'ai réalisé que le domaine du juridique et de la cybersécurité étaient intimement liés. J'ai eu ensuite l'opportunité de rejoindre un cabinet d'avocats en tant qu'assistante juridique et conformité RGPD.

Est-ce que tu peux préciser les spécificités de ton métier ?

Après avoir acquis toutes mes compétences sur le terrain, j'ai décidé de me lancer en freelance comme juriste consultante en protection des données personnelles. La raison ? Au cours de mes expériences, j'ai découvert une chose qui m'a profondément interpellée : toutes les entités sont soumises à la même réglementation mais n'ont pas toutes les mêmes moyens. Mon objectif étant ainsi de rendre le droit accessible à tous et de rendre possible un accompagnement à taille humaine. Ainsi j'accompagne désormais des TPE, PME, start up dans la conformité RGPD de leur structure, et je n'ai jamais été aussi épanouie qu'en partageant ma passion pour ce domaine.

Pourquoi avoir entrepris une spécialisation en cybersécurité en plus de tes compétences de consultante en protection des données ?

Au fil de mes missions je me suis rendu compte que de plus en plus de mes clients me demandaient de répondre à des problématiques de cybersécurité et de gouvernance. La cybersécurité et le droit sont selon moi indissociables et c'est pour cette raison que j'ai décidé de reprendre des études en droit du numérique à travers un Master de Cybersécurité Cyberveille Cyberdéfense au sein de l'Université de Besançon.

Cette formation ayant obtenu le label SecNumedu de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) m'a semblé être l'enseignement parfait pour compléter mes connaissances pratiques. Par ailleurs, ce n'est pas pour autant que j'ai arrêté mon activité. Je continue à réaliser mes missions de consulting et conseils RGPD en parallèle de ma reprise d'études, et continue également à m'investir au sein du CEFCYS dans son pôle sensibilisation.

Pourquoi la cyber en plus du juridique ? Parce qu'on ne peut pas faire une bonne conformité RGPD si les recommandations cyber ne sont pas respectées. Or, difficile de vérifier si ce que l'on a préconisé est appliqué lorsque l'on ne connaît pas un minimum le monde de la cyber. Je vais m'efforcer de contrôler l'utilisation adaptée des données collectées mais si derrière, le système d'information n'est pas protégé, tout le travail effectué en amont peut être réduit à néant.

> **D'où mon souhait d'acquérir une double casquette juridique (conformité) et cyber (technique) pour permettre d'organiser une gouvernance optimale dans n'importe quelle structure collectant des données.**

Je pense avoir trouvé ma voie dans un domaine qui me passionne et qui va me passionner encore longtemps grâce à l'accompagnement et la dimension humaine (que l'on ne soupçonne pas) et qui se cache derrière ces métiers ! On est dans une veille permanente, et c'est ce que je trouve fabuleux. Quoi de plus beau que de se réveiller un beau matin et réaliser que notre monde technologique a encore évolué et que de nouvelles réglementations sont nécessaires pour les encadrer. Alors oui il faut être passionné, ne pas avoir peur de se remettre en question et d'accepter de ne pas « tout savoir ». Mais ce qui est beau dans notre métier c'est de grandir intellectuellement chaque jour.

Quels conseils aurais-tu souhaité entendre quand tu as commencé ta formation, et quels conseils donnerais-tu à une personne souhaitant s'orienter ou se reconvertir dans le domaine de la cybersécurité ?

Aujourd'hui je me dis que le prochain métier ou activité que j'exercerai dans 10 ans n'existe pas encore, la formation qui me permettra d'y accéder sûrement pas non plus.
Est-ce que ça me fait peur ? Non, plus maintenant, au contraire ! Il m'a fallu beaucoup de temps pour le réaliser, mais parfois on a tendance à ne pas s'écouter et à se dévaloriser, à ne se focaliser que sur les compétences qu'il nous manque au lieu de valoriser nos compétences acquises.

En réalité, rien n'est acquis pour toujours, tout évolue. Nous ne sommes pas dans les années 50, aujourd'hui je ne pense pas qu'une personne souhaite exercer le même métier toute sa vie. Ce qui est beau dans la cyber, c'est qu'il comprend une telle diversité de métiers qu'il est possible de bifurquer à travers ses différentes branches. Il existe de nombreuses formations professionnalisantes, plus ou moins techniques dans une branche qui est en perpétuelle expansion et qui recherche de nouveaux talents.

La « reconversion professionnelle » n'est pas un gros mot, pour moi c'est une preuve de courage et de dépassement de soi. C'est un moyen de prouver que l'on n'est pas formaté pour un métier type, mais que dans une vie on évolue nécessairement, que les goûts changent, ainsi que notre situation familiale et personnelle. Et que parfois, prendre le risque de sortir de sa zone de confort est la meilleure chose que l'on puisse faire dans sa vie.

Si j'étais restée dans ma zone de confort, jamais je ne me serais lancée en auto-entrepreneur, jamais je n'aurais repris mes études et jamais je ne serais arrivée à trouver une voie qui aujourd'hui me comble de bonheur.

Chaque matin, je sais pourquoi je me lève, je suis passionnée par ce que je fais et je m'efforce chaque jour de transmettre à chacun qu'il est possible de changer de voie et qu'il est possible d'être heureux dans son travail.

Si je pouvais remonter le temps et me donner un conseil ça serait :

« Ecoute ton cœur, n'aie pas peur du jugement des autres, n'aie pas peur de l'échec, car c'est grâce à tes échecs que tu progresseras et deviendras plus forte. Ne reste pas sur le chemin que l'on t'impose, passe par les petites routes, mets tes mains dans le cambouis. N'aie pas peur d'aller sur le terrain car c'est lui qui fera de toi une bonne professionnelle. Ton âge n'est pas important, il n'y a pas de mauvais moment pour décider de changer de voie. Aie confiance en toi, un jour tu seras fière du chemin parcouru ».

Une intuition concernant le monde du travail de demain dans la cyber ?

Le monde de la cybersécurité est vaste et vecteur d'opportunités pour des femmes et des hommes de tous âges. Halte aux préjugés !

Il n'y a pas que des métiers techniques réservés aux ingénieurs et aux informaticiens. J'en suis la preuve, la cybersécurité englobe de nombreux autres métiers : on a besoin de juristes dans la cyber-assurance, d'avocats pour gérer les conséquences pénales d'une cyberattaque, ou encore de communication dans la gestion de l'image de la société suite à un incident cyber etc.

Le CEFCYS vient par ailleurs, au-delà du fait de transmettre de bonnes pratiques et de sensibiliser les plus jeunes, communiquer sur les métiers qui existent et encourager les reconversions professionnelles.

J'ajouterais qu'il est toujours bon de garder à l'esprit que travailler dans la cyber, ce n'est pas porter un sweat à capuche et des métiers réservés aux hommes. Il manque aujourd'hui de présence féminine dans la cyber, et j'espère que dans le « monde du travail de demain » nous n'aurons plus à nous poser cette question.

CLOÉ VACHER

Consultante Gouvernance, Risques et Conformité

Peux-tu m'en dire plus sur ton métier et tes missions ?

Je suis aujourd'hui consultante, j'interviens chez tous types de clients pour les conseiller et les accompagner dans leurs projets en cybersécurité (sur la gouvernance, les risques et la conformité).

Spécialisée en GRC, quelles ont été les clés pour maîtriser ce domaine ?

Être à l'écoute de ses clients, se tenir au courant des évolutions dans le monde de la cyber (tout change très rapidement) et surtout de la volonté !

Pourquoi as-tu décidé de t'orienter vers le domaine de la cybersécurité ?

Je n'étais pas « destinée » au domaine de la cybersécurité à la base, j'ai fait des études de commerce, puis de droit (spécialisé en protection des données). J'ai commencé par faire des stages de mise en conformité RGPD, puis je me suis dirigée vers l'audit IT, pour enfin arriver dans le conseil en cybersécurité. J'ai été attirée par les nombreux enjeux en matière de cybersécurité, le conseil permet de voir différentes entreprises et secteurs, et de voir comment la cybersécurité se met en place chez eux et comment elle peut les impacter.

Est-ce que tu as déjà entendu dire que ce domaine n'était pas fait pour une femme ?

Me le dire directement non, mais de mes précédentes expériences j'ai pu voir ou ressentir la masculinité encore très présente dans ce domaine et l'étonnement des gens à voir des femmes dans ce domaine.

Est-ce qu'il est obligatoire de maîtriser les mathématiques pour travailler dans la cyber ?

À mon sens pas du tout, je n'ai pas fait de mathématiques depuis le lycée et pourtant je travaille dans la cyber !

Est-ce que tu as déjà entendu des personnes te dire que ce domaine n'était pas fait pour une personne n'ayant pas un profil technique ?

On ne me l'a jamais dit, mais je l'ai déjà ressenti lors d'entretiens que j'ai pu passer.

Quelles sont les qualités que tu as mises en œuvre pour réussir dans ce domaine ?

La persévérance, la curiosité et l'adaptation ! Ne venant pas de ce domaine initialement, je suis partie de zéro mais avec de la détermination, de la persévérance et de la curiosité j'ai pu apprendre.

Quels défauts / points perfectible as-tu surmonté/amélioré pour réussir ?

L'appréhension et la peur de ne pas être à la hauteur, je me suis longtemps demandée si ma place était légitime et si j'étais suffisamment compétente dans mon travail. Si j'en suis là aujourd'hui, c'est que des personnes ont cru en moi et m'ont fait confiance, même quand je n'avais pas confiance en moi-même !

Est-ce que tu peux partager avec nous une réussite dont tu es fière ?

Être arrivée au poste où je suis actuellement est une grande fierté pour moi, cela montre que si l'on veut on peut, même si le chemin ne semble pas tout tracé dès le début !

Quel conseil aurais-tu souhaité entendre quand tu as commencé tes études ?

J'aurais aimé que l'on me dise de ne pas me fermer des portes par « peur » de se faire rejeter. Je n'avais aucune connaissance ni compétences en système d'information et pourtant j'ai tout de même réussi mes entretiens !

JEAN-NOËL LORRIAUX

Dirigeant fondateur de Khelasys

Comment / pourquoi avez-vous choisi le domaine de la cybersécurité ?

Je tiens, en premier lieu, à préciser une chose. La cybersécurité n'est pas mon activité principale et la façon dont j'œuvre dans ce secteur aujourd'hui est singulière. Je dirais que deux choses m'y ont amené. L'un de mes films préférés, en 1983, de John Badham : Wargames. La deuxième, le parcours de Kevin Mitnick, hacker, appelé « le condor », au moins spécialiste si ce n'est pionnier, de l'ingénierie sociale, que j'ai suivi pendant les années 90 et qui et devenu, depuis, consultant en cybersécurité. J'ai toujours été geek et le monde du hacking et de la cybersécurité m'ont toujours fasciné. Issu du monde de la formation et du développement des compétences, pour le moment je me concentre sur ma société de conseil et formation dans le numérique. En tant que chef de projet digital, formateur numérique et intégrateur web, la sécurité numérique est fondamentale et je peux m'en faire l'ambassadeur auprès de mes clients.

Aujourd'hui, je fais partie d'une association, le CErcle des Femmes de la CYberSécurité (CEFCYS), au sein du collège sensibilisation qui intervient auprès des plus jeunes.

Je fais également de la sensibilisation au travers de mon blog de société. Enfin, j'ai créé une newsletter d'éducation numérique dédiée aux parents dans laquelle j'instille des informations liées à la sécurité des données, ainsi qu'une « Brève cyber » sur LinkedIn, et je partage de la veille sur Twitter. Mon rôle est donc modeste, à travers la création de contenus et la communication autour de la cybersécurité et de la protection des données personnelles : sensibiliser et informer sont « les bases » afin que tout un chacun puisse se protéger et protéger, a minima, son entourage personnel et professionnel.

Une intuition concernant le monde du travail de demain dans la cyber ?

Je pense que la prochaine décennie va évoluer encore plus rapidement que les vingt dernières années en matière d'évolution techno-sociétale. Le télétravail va, je pense, continuer même si nombre d'entreprises vont avoir du mal à ne pas revenir au « monde d'avant » et l'évolution du monde du travail va exiger une sécurisation toujours plus renforcée des outils numériques et des usages. Les questions d'éthique, de confiance, de liberté mais aussi de contrôle vont être fondamentales et structurer notre façon d'envisager nos relations de demain dans lesquelles la frontière entre vie privée et vie publique va de plus en plus s'effacer.

Comment faire pour vivre humainement et de façon humanisée dans un monde de plus en plus technologique ?

Paradoxalement, le numérique peut aussi nous permettre d'entretenir les liens sociaux ; nous l'avons vu pendant la pandémie. L'objectif va être de vivre avec les outils numériques tout en nous préservant des dangers de leurs usages. Cela nécessite la diffusion d'une culture et d'une sécurité numériques. L'actualité nous a également montré que la souveraineté numérique n'a jamais été aussi importante et il me semble essentiel de privilégier les solutions françaises et open source afin de (re)devenir plus indépendants sur le plan numérique. La cybersécurité est aussi géopolitique.

Pour changer le monde (de la cyber), par quoi commenceriez-vous ?

Si c'est pour une candidature à la présidence de l'État, je risque de vous décevoir, ça ne m'intéresse pas ! Plus sérieusement, Je pense tout d'abord que la cyber souffre d'une méconnaissance et d'un manque de communication. Ce qui peut se comprendre compte tenu des spécificités inhérentes, en matière de secret, au domaine de la cybersécurité.

Toutefois, je pense qu'on peut vulgariser et communiquer sur le secteur sans pour autant remettre en question certains principes de ce domaine professionnel. Faire découvrir les métiers de la cyber me semble être l'action première à mener. Encourager les talents en poste à intervenir davantage en milieu scolaire, que ce soit en primaire ou dans le secondaire, pour parler de leurs métiers autour de rencontres ludopédagogiques afin de susciter des vocations chez les plus jeunes. Même chose auprès des personnes qui ont déjà goûté à la vie professionnelle et, en plus, leur faire connaître davantage les systèmes de financement et de transition professionnelle.

La reconversion professionnelle devient, heureusement, de plus en plus banale. Dans les deux cas, cela nécessite un véritable accompagnement structuré et méthodique en orientation et gestion de carrière (orientation, bilan de compétences, coaching, mentorat etc.), par des spécialistes de l'accompagnement aux côtés d'experts métiers, afin de mettre en place des dispositifs d'immersion professionnelle pour construire des stratégies d'orientation et de reconversion professionnelle et garantir une plus grande réussite des projets professionnels.

La cybersécurité d'aujourd'hui et de demain a besoin de tous types de compétences : techniques, littéraires, artistiques, sociales, en communication etc.

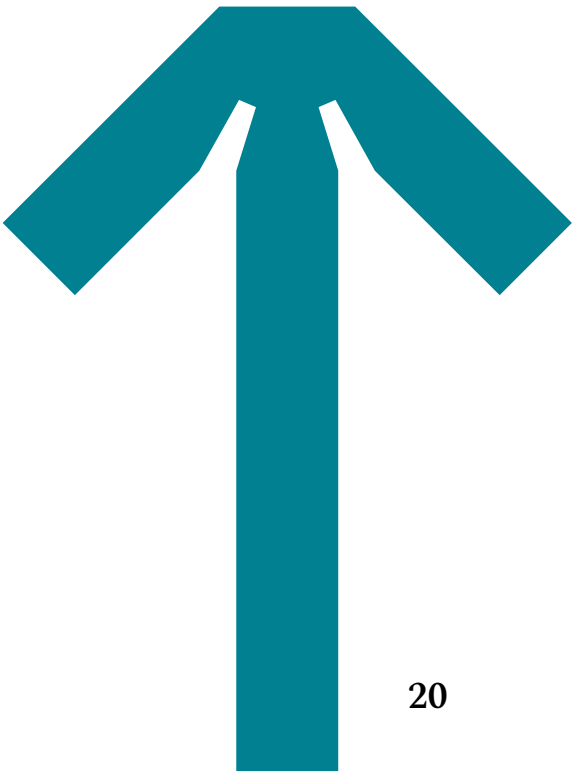
Une innovation / technologie que vous suivez particulièrement et pourquoi ?

Une seule ? Impossible, à mes yeux de n'en choisir qu'une, si ce n'est l'intelligence artificielle. Je suis surtout certaines applications de cette dernière telles que, dans le désordre, les drones, les véhicules autonomes (taxis, voitures, camions, avions) et le domaine des réalités étendues (virtuelle, mixte, augmentée).

Trois technologies qui vont prendre de plus en plus de place dans notre société de demain et qui vont interroger notre rapport à la liberté, aux autres et à la « confiance » accordée à des systèmes informatiques « indépendants ». La cybersécurité est, dans ces trois technologies, certes comme avec n'importe quelle autre, centrale. Cela va nécessiter des ressources humaines et techniques. Non seulement il faut former des gens à la cyber, mais ces spécialistes devront, en plus de leurs compétences en sécurité des informations, être de plus en plus pointus sur un domaine technologique en particulier. Aujourd'hui, nous sommes déjà en manque de talents, alors que les besoins ne cessent de croître.

Prochain rêve professionnel à réaliser ?

Rêve professionnel uniquement ou rêve professionnel cyber ? Je répondrai au deuxième : me former plus spécifiquement à certaines spécialités de la cyber : administration des réseaux, ingénierie sociale, OSINT - Renseignement de source ouverte. Ce sont, pour le moment, trois domaines qui m'intéressent particulièrement. Je me laisse du temps et je continue d'œuvrer dans l'immédiat dans la sensibilisation et la communication, ce qui me permet déjà d'acquérir des connaissances et des compétences que je considère transversales. Pour la suite, je verrai selon les opportunités qui se présenteront.



4 témoignages

4 PROFILS

CONCLUSION

Dans le cadre de notre campagne d'admission en cours à la CSB.SCHOOL, à la question "pourquoi voulez-vous faire de la cybersécurité ?", un candidat m'a, en substance, répondu ceci : "pour protéger le monde". Parmi d'autres réponses toutes aussi valables, telles que "je suis un passionné de technologie" ou "c'est la garantie de trouver un emploi", c'est le fait de faire oeuvre utile pour la société que le candidat a choisi de mettre en avant.

Cette réponse illustre à quel point la cybersécurité est un élément essentiel dans la transformation numérique en cours, ce que l'actualité vient nous rappeler régulièrement au gré de cyberattaques qui gagnent en volume, en impact et en sophistication.

Si le monde change sous nos yeux, tel doit aussi être le cas de la cybersécurité. Jusque-là cantonnée à des aspects purement techniques, la cybersécurité doit s'ouvrir à des considérations plus larges et attirer des profils différents et plus représentatifs de la société qu'elle a pour mission de protéger.

Les témoignages collectés afin d'établir ce livre blanc démontrent avec force que le profil unique en cybersécurité n'a plus cours aujourd'hui. Si, en cybersécurité, un bagage technique minimum est nécessaire, ce dernier n'est désormais plus suffisant. À la CSB.SCHOOL, notre ambition est d'ouvrir le domaine de la cybersécurité aux femmes, aux étudiants au profil dit "non-scientifique", aux salariés en reconversion et à toutes celles et tous ceux qui aujourd'hui se sentent moins légitimes pour évoluer dans ce secteur ; et au-delà de l'acquisition du bagage technique nécessaire, de vous donner les clés pour inscrire la cybersécurité au coeur des enjeux stratégiques et métiers des organisations.

Seule une dynamique collective nous permettra d'atteindre cette ambition. La responsabilité de l'éducation et de la formation à la cybersécurité revient à l'ensemble des acteurs du secteur. Répondre aux problématiques de formation, de recrutement, faire bouger les lignes, combattre les préjugés, passe nécessairement par une réponse commune. Rendre la cybersécurité accessible, aider le plus grand nombre à en maîtriser les codes, tout cela permettra de parer au syndrome de l'imposteur que nous décrivons dans ce livre blanc.

Loin d'être un handicap, ce syndrome permet de se remettre en question, de rester en éveil et de ne jamais tenir ce qu'on a appris pour acquis. Il n'y a pas de destin professionnel tout tracé, celui-ci se forge à force de travail, d'apprentissage, de choix, d'opportunités et de rencontres. C'est également une des leçons des témoignages recueillis pour cet ouvrage.

Je remercie chaleureusement Nacira Salvan et le CEFCYS pour leur engagement aux côtés de CSB.SCHOOL à assurer la promotion de la diversité, de l'inclusion et de l'égalité des chances, nous permettant d'être fidèle à notre engagement à rendre la cybersécurité accessible à tous.

Je vous donne rendez-vous dès septembre au sein de notre établissement pour continuer à faire vivre ces témoignages et ces échanges autour des sujets d'éducation et de cybersécurité.

Patrice Chelim

REMERCIEMENTS

Liste des participants :
Clara Foucher,
Jean-Noël Lorriaux,
Nacira Salvan,
Laeticia Soyer,
Cloé Vacher,
Guillaume Delorme,
Thomas Guilloux,
Guillaume Collard,
Patrice Chelim,
Mélodie Collard.

C'est avec beaucoup de plaisir que les équipes du CEFCYS et de la CSB.School se sont associées pour vous proposer cet ouvrage.

CSB.School :


www.csb.school


contact@csb.school


csb.school


schoolcsb


csb_school

CEFCYS :


www.cefcys.fr


contact@cefcys.fr


cefcys


cefcys.officiel


cefcys_officiel

ÉCHELLE DE CLANCE

Après avoir passé le Test de l'Imposteur, additionnez les nombres correspondant aux réponses à chaque question. Plus le score est élevé, plus le Phénomène de l'imposteur interfère fréquemment et lourdement dans votre vie.

1. J'ai souvent réussi alors que j'avais peur de ne pas y arriver avant de commencer.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

2. Je peux donner l'impression d'être plus compétent(e) que je ne le suis vraiment.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

3. J'évite les évaluations quand c'est possible et je suis terrifié(e) que les autres m'évaluent.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

4. Quand des gens me félicitent, j'ai peur de ne pas être à la hauteur dans le futur.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

5. Je pense parfois que j'ai obtenu ma position actuelle parce que j'étais au bon endroit au bon moment ou parce que je connais les bonnes personnes.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

6. J'ai peur que les gens qui comptent pour moi découvrent que je ne suis pas aussi capable qu'ils le pensent.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

7. J'ai tendance à mieux me souvenir des fois où je n'ai pas fait de mon mieux.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

8. Je réussis rarement à réaliser un projet ou une tâche aussi bien que je le souhaiterais.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

9. Parfois j'ai l'impression que mes succès sont le résultat d'une sorte d'erreur.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

10. C'est difficile pour moi d'accepter les compliments.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

11. Parfois, je pense que mon succès est dû à une sorte de chance.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

12. Je suis parfois déçu(e) de mes accomplissements actuels.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

13. Parfois, j'ai peur que les autres découvrent à quel point certains savoirs ou compétences me font défaut.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

14. J'ai souvent peur d'échouer face à une nouvelle demande.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

15. Je doute d'être capable de répéter un succès.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

16. J'ai tendance à minimiser l'importance de ce que j'ai fait malgré les félicitations.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

17. Je compare souvent mes capacités à celles de mon entourage et je pense qu'ils pourraient être plus intelligents que moi.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

18. Je m'inquiète souvent de ne pas réussir un projet.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

19. Si je suis sur le point de recevoir une promotion ou une forme de reconnaissance, j'hésite à le dire aux autres avant que ce soit un fait accompli.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

20. Je me sens mal et découragé(e) si je ne suis pas « le/la meilleur(e) » ou au moins « très spécial(e) » dans les situations qui impliquent la réussite.
1-Pas du tout vrai 2-Rarement 3-Parfois 4-Souvent 5-Très vrai

Si le total est de 40 ou moins : Vous n'avez que peu de caractéristiques de l'Imposteur ;
Si le total est entre 41 et 60 : Vous avez une expérience modérée du phénomène ;
Si le total est entre 61 et 80 : Vous avez régulièrement l'impression d'être un imposteur ;
Si le total est supérieur à 80 : Vous présentez souvent d'intenses expériences du phénomène.

Tiré de The Impostor Phenomenon: When Success Makes You Feel Like A Fake, p20-22, P.R. Clance, 185 Toronto, Bantham Books. Coyright 1985 Pauline Rose Clance, PhD, ABPP. Traduction française par Ars Maëlle du document disponible en ligne sur le site de l'auteur paulineroseclance.com/pdf/IPTestandscoring.pdf

02.04.22

A LYON

SUITE À CE LIVRE BLANC UNE MATINÉE D'ÉCHANGE EST PRÉVUE, PLUS D'INFORMATIONS SUR NOS RÉSEAUX SOCIAUX

SAVE THE DATE