LES DOSSIERS TECHNIQUES

INCLUSION ET DIVERSITE DANS LA CYBERSECURITE

Décembre 2023

CLUSIF

Table des matières

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Anne	**DORE**	ADHEL

Les contributeurs :

Alpha	**CAMARA**	ARKHINEO
Elisabeth	**LY**	ALLIANZ IARD
Benoît	**JOUANNETAUD**	EALIS
Vidyarshini	**JUNGLEEA**	ILEX INTERNATIONAL
Audrey	**MAGRO**	EDUGROUPE
Valentin	**JANGWA**	JUMIO
Frédéric	**MIRAULT**	SUEZ
Lazaro	**PEJSACHOWICZ**	CLUSIF
Laura	**PEYTAVIN**	PROOFPOINT
Eric	**TETELIN**	MINISTERE DE LA TRANSITION ECOLOGIQUE ET DE LA COHESION DES TERRITOIRES

Le Clusif remercie également les adhérents ayant participé à la relecture.

1 Synthèse opérationnelle

Il est avéré que la filière cybersécurité en France et dans le reste du monde est en manque de compétences et de talents. Les entreprises offreurs et utilisateurs peinent à recruter et les formations à attirer des profils souhaitant se former en cyber.

Face à ce constat, il est vital pour les organisations – publiques ou privées – de mettre en place des méthodes et moyens disruptifs afin de trouver des solutions adaptées à court et moyen termes. C'est là tout le propos de ce document : émettre des recommandations, proposer des approches concrètes et pragmatiques pour aider les DRH, RSSI et l'ensemble des acteurs impliqués dans la filière de recrutement à sourcer et embaucher les talents requis. Les entreprises et les organisations pourront y trouver des éléments propices à élargir le nombre de candidats éligibles à la cybersécurité. L'approche cible les organisations qui souhaitent mettre en œuvre des solutions innovantes et changer le prisme de la gestion de compétence et des talents au sein de leur organisation.

Dans un premier temps, elle incite les décideurs à se poser des questions : « Quelles sont les compétences dont j'ai vraiment besoin ? Ai-je besoin de recruter des personnes diplômées d'études supérieures pour ce poste ? Puis-je former un de mes collaborateurs pour faire ce métier ? »

Dans un second temps, elle propose des recommandations structurées et des bonnes pratiques afin de recruter des talents en cybersécurité requis pour le bon fonctionnement de son organisation.

Ces propositions s'appuient sur la volonté des organisations de mettre en place une approche de diversité et d'inclusion. Ces termes renvoient à la diversité des origines culturelles, sociales, territoriales et des parcours personnels et professionnels.

Dans les faits, le manque de ressources est généré par le manque de personnes formées, et intensifié par le fait que les organisations recherchent les mêmes profils – des profils d'ingénieurs – et que les métiers de la cybersécurité sont mal connus ou paraissent inaccessibles.

Pour inverser cette logique, les organisations doivent mettre en œuvre de nouvelles approches et changer les critères en termes de recrutement et de profils attendus. L'enjeu est d'être concentré sur les compétences requises et d'ouvrir de nouvelles perspectives de « sourcing » des profils pouvant être recrutés. Ces évolutions doivent intervenir au sein de l'organisation et plus largement dans tout l'écosystème de la cybersécurité.

Ces recommandations peuvent être implémentées progressivement en fonction de la maturité et de la volonté de chaque organisation. La mise en place d'un plan de gestion des ressources alliant inclusion et diversité est un investissement qui permet de répondre au besoin prégnant de ressources en cybersécurité et l'obligation permanente de renforcer la responsabilité sociétale des entreprises (RSE) de chaque organisation.

2 Introduction

Avec la croissance exponentielle des menaces, la gestion des compétences et des ressources en cybersécurité constitue un véritable enjeu et prend une place centrale et cruciale au sein de la filière cybersécurité et des organisations. Par ailleurs, la guerre des talents n'a plus de frontières. Le télétravail, qui s'est généralisé durant la crise Covid, a encore accentué ce phénomène, celui-ci étant même un des critères de choix pour les candidats.

Au-delà du bien-fondé de développer ou de renforcer nos filières de formation classiques afin de former plus d'ingénieurs et de chercheurs en cyber, l'ensemble des acteurs du secteur est unanime pour affirmer que cela ne répondra pas suffisamment aux besoins des organisations.

Par ailleurs, au-delà du nombre de personnes formées, se pose la question de l'adéquation de l'offre et des demandes, et la capacité à retenir les bons profils.

Toutes les structures – publiques ou privées – sont concernées par ce sujet. Le manque de ressources génère une inflation sur les salaires, que certaines entreprises privées ou organismes publics ne sont pas à même de suivre.

Le risque encouru par ce manque de ressources ne peut être mentionné sans prendre en considération l'éventualité d'une pandémie cyber ou d'une crise systémique générée par une attaque cyber massive sur un secteur d'activité. Le manque de ressources constitue un risque économique et fragilise la souveraineté de l'État.

Que ce soit au sein des organisations publiques ou privées, le manque de ressources pénalise et impacte à l'échelle nationale, voire internationale, la capacité des organismes à se protéger et les États à préserver leur souveraineté numérique. Pour y répondre rapidement, chaque organisation doit adopter une démarche adaptée à son environnement, permettant de coordonner réactivité et efficacité.

Force est de constater que les formations actuelles ne fournissent pas assez de candidats, que la demande de ressources en cybersécurité ne cesse de croître et que l'éventail de compétences requises ne cesse d'évoluer et de s'étoffer. La cybersécurité est une nouvelle filière économique en très forte croissance et toujours en cours de structuration. Les propositions soumises ici constituent une première série d'actions pouvant aider les structures à trouver des solutions concrètes ou à enrichir les initiatives lancées par les grandes entités.

Ce document regroupe des recommandations. Il peut être considéré comme une boîte à outils permettant à chaque organisation de choisir la ou les solutions qui lui conviendront et qu'elle pourra déployer. Il s'appuie sur la conviction que la diversité et l'inclusion offrent la possibilité d'élargir le nombre potentiel de talents, devenant à la fois un enjeu de performance économique et sociétale.

2.1 Diversité et inclusion

Selon la définition du dictionnaire Larousse©, la diversité s'entend comme étant « l'ensemble des personnes qui diffèrent les unes des autres par leur origine géographique, socioculturelle ou religieuse, leur âge, leur sexe, leur orientation sexuelle, etc., et qui constituent la communauté nationale à laquelle elles appartiennent… Cette notion, qui intègre des différences comme le handicap, est développée pour lutter contre la discrimination ».

Or il est souvent constaté que le processus de recrutement est généralement fondé sur la possession d'un diplôme – idéalement école d'ingénieurs pour la cybersécurité – et une solide

expérience dans un secteur d'activité.

Cette approche laisse peu de place aux parcours atypiques, aux profils différents ou à des personnes souhaitant changer de métier et/ou secteurs d'activités. Ces profils ne rentrent souvent pas dans les « cases » RH des grands groupes et les plus petites structures doutent souvent de leur capacité ou possibilité de former ces personnes.

Le cadre est souvent rigide, identique d'un groupe à l'autre, et toutes les organisations se retrouvent ainsi à chercher les mêmes profils et à proposer des postes parfois sous-qualifiés ou peu évolutifs, rendant la rétention des personnes difficiles.

Penser « diversité et inclusion », c'est penser différemment. C'est aller vers des personnes différentes par leur cursus, leurs formations, leur culture, leurs origines sociales ou territoriales ou leur handicap.

La diversité et l'inclusion, c'est recruter la personne qui possède – ou a la volonté d'acquérir – les compétences requises pour réaliser le travail attendu, indépendamment de son diplôme ou de son parcours personnel. C'est la capacité à croire en l'humain, ses compétences, sa volonté et sa capacité à évoluer et apprendre quand il le faut et le veut.

La diversité et l'inclusion ce sont la capacité et la volonté d'intégrer des personnes différentes au sein de son organisation sans déroger à ses attentes de performance, de résultats et de rentabilité.

2.2 À qui s'adressent ces recommandations ?

Lorsqu'il s'agit de cybersécurité et de recrutement, ces recommandations s'adressent à l'ensemble des acteurs opérationnels de la cybersécurité, mais aussi aux DRH, aux cabinets de recrutement et plus largement à l'ensemble de l'écosystème.

Quel que soit le secteur d'activités – ou le fait que l'entreprise soit offreur ou utilisateur –, la mise en œuvre des propositions s'inscrit dans une politique RH sponsorisée par la direction générale.

Si les grandes organisations peuvent avoir initié certaines de ces démarches, leurs mises en œuvre demeurent souvent marginales. Quant aux structures de plus petites tailles, l'objectif est d'obtenir des informations pratiques et concrètes pour faciliter la mise en œuvre de ces recommandations.

Ce document fournit des modes opératoires, propose un ensemble de solutions et identifie des acteurs, des OPCO (opérateurs de compétences) ou des associations à même de soutenir de telles initiatives.

Ce document aura aussi atteint son objectif s'il peut contribuer au débat public et à enrichir la réflexion autour de la définition de politiques publiques.

2.3 Pourquoi changer de prisme ?

Toutes les organisations peinent à attirer et recruter des profils et compétences en cyber. La pénurie est mondiale. Rechercher une solution à l'international a peu de sens et conduit à se concentrer sur les ressources en local. En effet, la croissance exponentielle du risque cybersécurité et le fait que toutes les structures recherchent des profils similaires font que les ressources sont à la fois rares, chères et difficiles à retenir au sein des organisations.

Les chiffres sont éloquents. En 2021, 2,72 millions de postes en cybersécurité ont été non

pourvus dans le monde[1]. À l'échelle de la France, ce serait plutôt 15 000 postes selon une étude de l'ANSSI[2].

Une approche différente et proactive est donc indispensable : il faut aller chercher de nouveaux candidats dans de nouveaux viviers de ressources et de nouveaux profils sans pour autant remettre en cause le besoin de former davantage de profils issus de la filière technique, chercheurs inclus. Mais pour reprendre un vieil adage, « toutes les bonnes volontés sont requises » pour permettre aux organisations de renforcer leur cyber résilience, de répondre à la croissance du marché et plus largement de contribuer à la souveraineté numérique de la France. Il faut ainsi construire de nouvelles approches, de nouveaux modes de pensée, et adapter la gestion des RH et des carrières en conséquence.

Dans un monde toujours plus dépendant, certaines de ces approches requièrent une collaboration avec d'autres acteurs de l'écosystème, des entreprises, des associations ou organismes de formation. Mais elle exige un changement fondamental dans les codes et la culture de l'entreprise et ne pourra se faire qu'avec le soutien des dirigeants et l'adhésion des collaborateurs.

Dans un contexte où les pirates informatiques redoublent d'imagination pour tromper les utilisateurs, les organisations doivent rivaliser d'imagination et d'initiatives pour répondre à leur besoin de ressources en cyber.

L'heure n'est donc plus au constat, mais à la mise en œuvre d'actions concrètes pouvant avoir un impact à court et moyen termes. Cette démarche proactive de l'entreprise nécessite une adaptation et une approche basée sur la compétence et les aptitudes requises pour chaque poste. Elle propose aussi de combiner expertise, cybersécurité et RSE.

[1] Étude 2021 de l'ISC2 – International Systems Security Consortium

[2] https://www.ssi.gouv.fr/uploads/2021/10/anssi-profils_de_la_cybersecurite-marche_ouvert-france.pdf

3 La cybersécurité : métiers et compétences

3.1 Introduction

La cybersécurité est une discipline assez récente qui va bien au-delà du simple antivirus et de la gestion des flux à travers des pare-feux des années 90 pour protéger les SI (Systèmes d'Information) couvrant l'IT (Information Technology, correspondant à l'informatique de l'Entreprise) et l'OT (Operational Technology, correspondant à l'informatique industrielle gérant les chaînes de production).

L'explosion des concepts autour d'internet, la transformation digitale d'une très grande partie des métiers et des services privés ou publics, mais aussi l'interconnexion des équipements (IoT : Internet of Things ou Internet des Objets) ou des usines 4.0 font croître le risque cybersécurité qui doit être pris en compte dès la phase projet / conception jusqu'à la phase de réception (BUILD) et maintenu durant la phase d'exploitation / d'utilisation (RUN). Cette généralisation du risque cybersécurité crée de manière continue de nouveaux métiers et la nécessité d'acquérir de nouvelles compétences dans son domaine ou dans des métiers connexes.

Le Clusif a créé un groupe de travail pour répondre à ces constats. Fort des premiers travaux menés, le Clusif a choisi de rejoindre le groupe de travail dédié à la formation créé en 2021 au sein du Campus Cyber et coanimé par Cap Gemini. Ainsi, le Clusif a pu partager son approche et sa méthodologie basées sur le Panorama des métiers de la cybersécurité de l'ANSSI. La vingtaine d'experts de la formation et de la cybersécurité qui s'y réunissent tous les quinze jours ont souhaité poursuivre sur la voie déjà ouverte.

La finalité de ce groupe de travail Formation a été la réalisation d'un Référentiel de compétences des métiers de la cybersécurité. Ce référentiel permettra de démystifier et faire connaître les métiers de la cybersécurité et les compétences requises pour occuper les différents postes. À terme, il pourra également orienter les différents publics vers les formations adéquates.

L'objet de ce chapitre est donc de présenter ce référentiel en introduisant les métiers retenus, puis de mettre en exergue les compétences nécessaires pour exercer un métier cible. Ces compétences sont triées par type (compétences propres au métier ou compétences transverses propres à la personne) et par domaine d'activité.

3.2 Profils les plus recherchés

Le panorama de l'ANSSI recense 26 principaux métiers liés à la cybersécurité, 6 exemples de « métiers pouvant contribuer à la démarche de cybersécurité » et enfin 3 exemples de « métiers pouvant se spécialiser dans la cyber ». Ces 9 derniers métiers sont classifiés comme métiers connexes à la cybersécurité. Ce panorama est disponible via le lien ci-après : https://www.ssi.gouv.fr/guide/panorama-des-metiers-de-la-cybersecurite/

L'objectif de ces recommandations est de se focaliser sur les métiers de la cybersécurité. Les métiers propres à la cybersécurité sont classifiés en quatre catégories dans le document de l'ANSSI :

1. Gestion sécurité et pilotage projets sécurité – les métiers de RSSI pour grands groupes et PME/TPE ont été rassemblés en un seul métier.
2. Conception et maintien d'un système d'information sécurisé, à l'exclusion de chef sécurité de projet, spécialiste en développement sécurisé et cryptologue.
3. Gestion des incidents et des crises de sécurité.
4. Conseil, services et recherche.

Forts de ces hypothèses de départ, une matrice de compétences a donc été formalisée et disponible sur le site du Clusif : https://clusif.fr/emploi-et-formation-publication-dune-matrice-des-competences-cyber/

3.3 Quelles compétences cyber ?

Quatre domaines de compétences métier sont définis au sein de la matrice :

- La sécurité opérationnelle du système d'information
- Le pilotage de la sécurité du système d'information
- La supervision du système d'information
- L'investigation numérique du système d'information

Pour chacune de ces compétences, des remarques et des exemples sont proposés.

L'ensemble de ces compétences correspond à la compétence générique « savoir ».

3.4 Quelles compétences transversales ?

Deux domaines de compétences transversales sont définis au sein de la matrice :

1. Posture personnelle
2. Travail en équipe

Ces deux domaines couvrent à la fois le « savoir être » et le « savoir-faire » ou « savoir faire-faire ».

3.5 Comment utiliser la matrice de compétences ?

Chaque métier lié à la cybersécurité nécessite tout ou partie de compétences métier et transverses. Ce niveau de compétence requis est évalué à travers la notation ci-après :

- Niveau 0 : aucune connaissance sur le sujet
- Niveau 1 : comprend les principaux enjeux et problèmes liés à la compétence
- Niveau 2 : réalise des actes simples liés à la compétence
- Niveau 3 : compétence confirmée
- Niveau 4 : expert

À noter qu'il est à la discrétion de l'utilisateur de la matrice d'adapter les compétences requises en fonction du contexte et du poste à pourvoir.

Une fois que cette matrice est adaptée aux besoins de l'entreprise, le candidat potentiel souhaitant évoluer vers l'un des métiers de la cybersécurité s'autoévalue en aveugle en complétant son niveau (0 à 4) pour chaque compétence.

Ensuite, la comparaison des compétences du candidat avec les niveaux requis par l'entreprise permettra de combler les écarts par une ou plusieurs formations adéquates.

Cependant, cet exercice a des limites :

- Si l'écart entre le niveau du candidat et le niveau de compétences recherché est trop important, s'assurer qu'il se limite à quelques domaines qui pourront être comblés par des formations dans un temps raisonnable.
- Si le candidat est surqualifié, il sera difficile de le fidéliser.
- Si certaines aptitudes propres à la personne sont insuffisantes, elles seront probablement difficiles à combler grâce à une formation. Ces aptitudes sont principalement :
    - La rigueur
    - Le travail sous pression
    - L'esprit d'innovation
    - La collaboration en équipe
    - La fédération d'une équipe / d'un projet, le leadership
    - La priorisation de ses actions selon les contraintes (urgent / important)

Cette approche peut être utilisée pour inclure ou faire évoluer de nouveaux talents dans le cadre de l'inclusion et la diversité.

Cette méthode n'est pas figée. L'utilisateur doit se l'approprier en l'adaptant au contexte de l'entreprise et des métiers recherchés.

4 Changer de paradigme au sein des entreprises et organisations

4.1 Objectifs

- Permettre aux organisations de répondre à leurs besoins de talents et de compétences cybersécurité dans un contexte de pénurie d'offres.
- Optimiser la gestion des Ressources humaines en les faisant évoluer vers la cybersécurité.
- Élaborer des parcours de formations et organiser des tutorats internes pouvant appuyer la démarche.
- Initier un système de parrainage qui aura des effets à court, moyen et long terme.

4.2 Préconisations

- Attribuer à la Formation interne de la DRH des tâches liées à l'inclusion dans le domaine de la cybersécurité.
- Donner aux équipes Cybersécurité des objectifs en matière de diversité et d'inclusion pour favoriser le recrutement de personnes venant d'autres entités de l'organisation ou de l'extérieur.

4.3 Porteurs du projet

- Les RH et les équipes cybersécurité.

4.4 Description

Les métiers de la cybersécurité et les compétences associées sont en constante évolution du fait de l'évolution de la nature du risque et des technologies. Il en résulte un besoin de former les collaborateurs de manière continue et permanente.

Si la gestion des Ressources humaines consiste à mettre à disposition des profils les plus adaptés à ces évolutions rapides, le responsable de la formation interne doit accompagner les équipes dédiées à la cybersécurité dans le développement et l'acquisition de ces connaissances.

Pour ce faire, le responsable de la formation pourra notamment s'appuyer sur la matrice de compétences présentée dans le chapitre précédent pour développer des programmes de formations internes ou externes, participer à des conférences ou adhérer à des organisations professionnelles dédiées.

La montée en compétence de collaborateurs ayant par exemple une bonne connaissance des processus métier, des systèmes industriels, des applications ou des systèmes d'information peut permettre de résoudre, au moins partiellement, les difficultés de recrutement des professionnels de la cybersécurité.

La collaboration entre les RH et les équipes cybersécurité doit donc amener à attirer et intégrer progressivement ces profils au sein des équipes cybersécurité.

Face à la surcharge de travail des équipes cybersécurité sous-dimensionnées et la gestion des incidents, la RH et le responsable de la formation jouent un rôle déterminant pour initier et faire aboutir cette initiative. En parallèle, l'intégration de ces nouveaux profils doit être incluse dans les objectifs du responsable cybersécurité et de ses équipes.

La meilleure façon de conduire cette démarche d'inclusion est de travailler en mode projet avec un budget dédié et des objectifs quantifiables préalablement déterminés.

Par ailleurs, au-delà du partage des compétences, la mise en place de parrainage ou mentorat constitue un facteur clé de succès pour accompagner les candidats intéressés à travailler en cybersécurité. La mise en œuvre d'une telle approche peut aider les profils motivés à prendre confiance en eux et répondre à leurs interrogations.

5 Intégrer des personnes en situation de handicap[3] en développant leurs compétences

5.1 Objectifs

- Rassurer les services recruteurs / dissiper les craintes et a priori.
- Accompagner les services d'accueil de personnes en situation de handicap à prendre en compte les préconisations d'aménagement de poste.
- Mettre en lumière des expériences réussies d'intégration en valorisant les compétences exprimées pour créer un phénomène de contagion dans les services et valoriser l'image de l'organisation.

5.2 Préconisations

- Intégrer des personnes en situation de handicap au sein des équipes.
- Accompagner les services qui accueillent les personnes en situation de handicap.

5.3 Porteurs du projet

- Départements : Cybersécurité, Système d'Information, Ressources humaines, Formation…

5.4 Description

L'inérêt d'intégrer des personnes en situation de handicap au sein des équipes devrait être une évidence, mais leur faible représentativité démontre le besoin de rappeler une nouvelle fois la formidable opportunité d'intégrer ces personnes au sein des équipes cybersécurité.

Si les personnes en situation de handicap sont peu nombreuses dans le secteur du numérique, une étude réalisée par l'Agefiph[4] explique qu'il s'agit souvent « d'une méconnaissance des opportunités du secteur, une représentation stéréotypée du handicap par les recruteurs et des parcours vers l'emploi qui n'invitent pas suffisamment à s'orienter et à se former à ces métiers ».

C'est pourquoi il est apparu évident et important de faire de l'emploi des personnes en situation de handicap une des recommandations fortes.

---

[3] « Constitue un handicap, au sens de la présente loi, toute limitation d'activité ou restriction de participation à la vie en société subie dans son environnement par une personne en raison d'une altération substantielle, durable ou définitive d'une ou plusieurs fonctions physiques, sensorielles, mentales, cognitives ou psychiques, d'un polyhandicap ou d'un trouble de santé invalidant. » (https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006796446/)

[4] « Numérique : emploi et handicap » (agefiph.fr)

Le vivier des personnes en situation de handicap recèle de nombreuses personnes ayant des aptitudes et/ou des compétences à même de répondre aux besoins de ressources en termes de cybersécurité. Par ailleurs, la cybersécurité et la résolution des incidents exigeant des angles d'analyse différents et complémentaires, il semble dommage de se priver de ces profils à la fois disponibles sur le marché et pouvant être formés rapidement.

L'approche est déjà très structurée. Il est facile pour les entreprises d'initier les démarches.

Pour déposer une offre d'emploi ou consulter des profils, l'Agefiph met à votre disposition Bienvenue sur l'espace emploi de l'Agefiph.

Sur ce site vous trouverez également le dispositif Cap Emploi. Il s'adresse à toute entreprise privée, quel que soit son effectif. Les conseillers apportent aide et conseils, que ce soit pour le recrutement, l'intégration dans l'entreprise ou le maintien dans l'emploi et l'évolution professionnelle.

Au-delà des modalités de recrutement qui sont fluides, les aides financières pour former des personnes en situation de handicap sont très attractives et intéressantes pour les entreprises.

Les services et aides financières proposées par l'AGEFIPH – Services et aides financières | Agefiph – regroupent notamment l'aide à l'adaptation des situations de formation, la participation financière à une embauche en contrat de professionnalisation ou en contrat d'apprentissage.

Ces aspects pragmatiques sont autant d'accélérateurs pour recruter des personnes en situation de handicap ou assurer leur reconversion vers des postes cyber. Les conditions financières mises à la disposition des entreprises permettent de former de nouveaux collaborateurs cybersécurité à moindre coût pour l'entreprise.

Par ailleurs, les personnes en situation de handicap sont considérées comme un public prioritaire par les opérateurs de compétences (OPCO). De fait, elles peuvent donc par exemple bénéficier de contrats de professionnalisation sans limite d'âge (ces contrats étant réservés habituellement aux moins de 25 ans ou aux demandeurs d'emploi de 26 ans et plus) : Formation et apprentissage : les critères de financement (opco-atlas.fr).

Enfin, au-delà des enjeux RSE (responsabilité sociétale des entreprises), des enjeux de diversité et d'inclusion au sein des équipes, ces aspects financiers peuvent contribuer à l'insertion de personnes en situation de handicap dans des équipes cyber.

Pour toutes ces raisons humaines, financières et pragmatiques, il appartient à chaque entreprise d'étudier ce sujet et ces opportunités avec attention pour des résultats concrets et opérationnels à court terme.

6 Approche de la neurodiversité[5] dans les compétences cyber

6.1 Objectifs

- Ouvrir de nouvelles perspectives dans la manière d'aborder la cybersécurité.
- S'appuyer sur un « vivier de ressources » non sollicité par les entreprises.

6.2 Préconisations

- Intégrer des talents issus de la neurodiversité au sein des équipes.

6.3 Porteurs du projet

- Départements : Cybersécurité, Système d'Information, Ressources humaines, Formation…

6.4 Description

Cette recommandation a pour objectif de promouvoir la cybersécurité comme une vraie opportunité pour les profils neuro-atypiques. Les stéréotypes sont à éviter. Ces profils ont un large éventail de compétences qui peuvent être utilisées de différentes façons.

Selon les tâches que l'on souhaite confier, il est intéressant de se pencher sur les caractéristiques spécifiques de certains modes de pensée différents.

Si certaines initiatives ont vu le jour en France, il reste néanmoins que ce vivier de talents et compétences n'est pas souvent pris en considération. Certains états comme les États-Unis ou Israël ont, depuis de nombreuses années, développé des programmes spécifiques pour profiter de ces qualités. Ils renforcent par exemple leur équipe de cyberdéfense au sein des

---

[5] « La **neurodiversité** se réfère aux différences neurologiques qui composent le genre humain.

Au moins **10 % à 15 %** de la population mondiale présentent une particularité cognitive ou un fonctionnement cognitif dit « atypique » par rapport à la norme, soit au moins **un milliard d'humains**, ce qui est très loin d'être négligeable !

Parmi les principales **neurodiversités**, se retrouvent :

- Le Trouble du Déficit de l'Attention avec ou sans Hyperactivité *(*TDA-H**)** qui concerne environ 5 % de la population mondiale ;
- Le **Haut-Potentiel Intellectuel** (HPi) ou **Douance** qui concerne autour de 2 % de la population ;
- L' **Autisme** et le **Syndrome d'Asperger** concernant environ 1 % de l'humanité ;
- Les **gauchers** qui sont entre 10 à 15 % de la population ;
- Le **Syndrome de Gilles de la Tourette** entre 0.5 % et 1 % des enfants d'âge scolaire ;
- Les **dys** (Dyslexie, Dyscalculie, Dysorthographie,….) qui concernent entre 5 et 15% des enfants. »

(https://academie-neurodiversite.com/la-neurodiversite/)

organisations civiles et militaires. Des entreprises comme SAP ou IBM ont même lancé des programmes au niveau mondial pour recruter des personnes neuro-atypiques.

Sans tomber dans la caricature ou la discrimination, une certaine sensibilité aux détails ou une capacité d'analyse différente peuvent être des atouts non-négligeables.

En créant les conditions d'une intelligence collective au sein d'une équipe composée de profils différents, de nouvelles perspectives s'ouvrent : elles offrent des opportunités d'innovation et d'efficacité. L'intégration passe par la mise en place d'un accompagnement qui, s'il est obligatoire pour la réussite de l'intégration, n'impacte en rien la rentabilité ou l'efficacité de l'équipe.

Par ailleurs, dans un contexte où les entreprises cherchent à acquérir et retenir les talents, la mise en qualité de valeurs humaines et de RSE contribue à développer un cadre de travail positif et bienveillant.

De plus en plus d'organismes de formation ou d'écoles ont pris conscience de la qualité et de la capacité de réussite de ces profils et mettent en œuvre des formations spécifiques pour eux.

Il est aujourd'hui possible de trouver des organismes compétents pour être accompagné dans cette démarche. Par ailleurs, le financement de certaines formations peut être pris en charge par des opérateurs de compétences (OPCO).

Pour autant, comprendre les opportunités et perspectives de recruter des profils issus de la neurodiversité, consiste aussi souvent à changer ses attentes vis-à-vis des diplômes. Il est en effet courant que ces personnes soient en situation d'échec scolaire ou aient suivi des études en relation avec un de leurs centres d'intérêt. Leurs compétences sont donc souvent acquises dans le cadre d'autoformation ou de formations spécifiques courtes.

Recruter des talents issus de la neurodiversité remet en cause certains principes établis au sein des organisations et certaines idées préconçues sur le niveau de qualification et les diplômes, mais donne accès à un vivier de ressources immédiatement disponible.

7 Promouvoir les métiers de la cybersécurité

7.1 Objectifs

- Promouvoir les métiers de la cybersécurité auprès des populations, en dehors de l'écosystème traditionnel.
- Donner envie et attirer des personnes vers la filière cyber.

7.2 Préconisations

- Mettre en place des relais internes et externes à l'organisation, pour gérer, animer, et assurer cette promotion.
- Assigner les différents rôles et responsabilités.
- Définir un plan d'action ciblé.

7.3 Porteurs du projet

- Une équipe dédiée : Direction générale, RH, SSI, DSI.
- Acteurs de l'écosystème cybersécurité.
- Acteurs en lien avec les associations travaillant pour la diversité et l'inclusion.

7.4 Description

La DRH avec le soutien de sa Direction générale doit promouvoir les métiers de la cybersécurité auprès de l'ensemble de la population.

La mission principale est de promouvoir les métiers de la cybersécurité et les compétences associées.

Pour ce faire, il faut développer un réseau en s'appuyant sur les associations travaillant sur la cybersécurité (cf. liste en annexe) et celles impliquées dans l'inclusion et la diversité.

La mission principale de cette équipe est d'attirer les candidats potentiels en proposant des formations permettant d'exercer un métier cybersécurité à court terme.

La promotion des métiers de la cybersécurité peut se faire par le biais :

- des salons (étudiants, tournés vers les jeunes, de l'orientation, de la neurodiversité ou spécialisés sur la gestion du handicap) ;
- des partenariats avec par exemple des MDPH (Maisons départementales pour les personnes handicapées) ;
- des évènements visant à promouvoir l'égalité des chances ;
- des clubs de loisirs informatiques ;
- des projets de réinsertion professionnelle ;
- du Service civil ;
- des écoles et universités privées et publiques.

On pourra aussi proposer des stages en entreprise à des collégiens et lycéens, afin de faire

naître des vocations avant même de quitter les cursus proposés par l'Éducation nationale.

Par ailleurs, il est possible d'initier des actions dédiées, comme par exemple la création ou la diffusion de vidéos postées sur l'extranet et les réseaux sociaux de l'entreprise, vidéos dans lesquelles des collaborateurs partagent leur expérience, leur parcours et leur motivation pour travailler dans la cybersécurité. La diversité des témoins est évidemment souhaitée pour faciliter l'identification.

Quelques exemples concrets :

Exemple 1 :

Le département Informatique d'un établissement financier français a récemment créé une entité dédiée à l'informatique au sein de la Direction des Ressources humaines. Son objectif est de féminiser ces métiers et développer des leaders féminins au sein des équipes SI.

Cette entité organise des formations (coaching / mentorat) pour encourager les montées en compétence. Des processus de reconversion sont, entre autres, mis en place. Par ailleurs, les fournisseurs de service et d'ingénierie informatique extérieurs sont encouragés à proposer des profils féminins pour les missions à accomplir. Pour susciter des vocations, les femmes de la tech sont plus souvent sollicitées pour les évènements internes et externes.

Cette initiative pourra être démultipliée en orientant plus spécifiquement les actions vers la cybersécurité et élargir sur des profils autres que féminins pour attirer des jeunes, des seniors, des personnes atteintes de handicap...

Exemple 2 :

Un réseau commercialement « neutre » qui met en ligne les CV de personnes en situation d'exclusion.

Ce genre d'initiative a pour objectif d'atteindre ces personnes et de leur donner l'envie et l'opportunité d'envisager de travailler dans la cybersécurité. Au travers de différentes actions de sensibilisation, on peut les accompagner et leur proposer des formations, du coaching, du mentorat, etc.

8 DÉVELOPPER LE MÉCÉNAT DE COMPÉTENCES[6]

8.1 Objectifs

- Développer le mécénat d'entreprise au sein des grandes entreprises et des ETI.
- Augmenter le nombre de professionnels à même de pouvoir accorder du temps et de la disponibilité pour incarner et témoigner des savoir-faire et des savoir-être en matière de cybersécurité.

8.2 Préconisations

- Mettre au bon niveau de visibilité, en Comité exécutif de l'entreprise, le programme de mécénat ayant comme objectif de contribuer à la diversité socioculturelle et de genre.
- Abonder les budgets de soutien à des partenaires de programmes institutionnels dont la spécialité est d'organiser les interventions en milieu scolaire, ainsi que la mise en relation mentors-mentorés (voir chapitres 5 et 9).
- Dégager un budget RH ou de fonctionnement interne permettant de sécuriser du temps non opérationnel pour les salariés motivés pour s'investir dans leurs actions de promotion du métier.

8.3 Porteurs du projet

- Entreprises, dont RH, institutions, associations.
- Les CCI, en tant que sponsors orientant les dirigeants d'entreprises vers les circuits de mécénat de compétences.
- Les écoles du numérique (grandes écoles et instituts universitaires) et leurs réseaux alumni.
- Les associations mobilisées du domaine de la cybersécurité comme le CEFCYS, Women4cyber.

8.4 Description

L'analyse du manque de diversité socioculturelle et de la faible représentation des femmes dans les métiers de la cybersécurité souligne irrémédiablement que tout se joue à l'école lorsque la motivation profonde et personnelle se crée. Le choix des matières d'enseignement est le fruit de la représentation mentale que les jeunes se font des métiers et de leur vie professionnelle future.

Résoudre le problème, notamment de la sous-représentation des femmes, passe par des actions auprès des plus jeunes.

---

[6] Le mécénat de compétences est un don en nature : il s'agit pour une entreprise de mettre des collaborateurs à disposition d'un organisme d'intérêt général, qui vont mobiliser pendant un temps leurs compétences ou leur force de travail. Le mécénat d'entreprise est un don auprès d'organismes à but non lucratif.

Le système de formation est en cours d'adaptation pour répondre aux besoins du marché. Le nombre n'y est pas, la diversité des profils, et en particulier, de genre, non plus. Des talents sont délaissés en amont de nos filières, alors même que de nombreuses études démontrent que la diversité dans les équipes et les organisations favorise la performance, l'innovation et la création des communautés de pratiques.

Or, il y a deux volets évidents sur lesquels les entreprises peuvent agir dans le domaine :

1. Le **mécénat de compétence** et la promotion de nos métiers dans les classes, dès le collège, pour témoigner et faire témoigner des rôles modèles.

2. Des contributions plus actives :

   - Sur l'écosystème amont de formation par le **mentorat** (voir chapitres 5 et 9) de ses professionnels auprès de jeunes et des élèves.
   - Dans l'écosystème interne aux entreprises, avec des **programmes mobilisant les personnels sur l'inclusion**, afin de continuer à rendre vivantes et effectives les actions de promotion et de témoignages vers les filières de recrutement en amont.

En ce qui concerne particulièrement l'attractivité du métier chez les jeunes filles, les chiffres clés de l'enquête Ipsos de 2021 réalisée pour l'Epitech le confirment : la première des priorités citées pour encourager les filles à s'engager dans des études d'informatique est d'inviter des professionnelles du secteur dans les classes, de l'avis des lycéens comme de leurs parents, juste devant le fait de faire connaître toute la variété des métiers du numérique.

9 Déployer une approche systématique de mentorat

9.1 Objectifs

- Augmenter significativement le nombre de mentors sur l'ensemble du territoire afin de démultiplier la transmission des représentations des métiers du numérique et de la cybersécurité auprès des jeunes.

9.2 Préconisations

Pour chaque entreprise du secteur de la cybersécurité :

- Dégager un budget RH ou de fonctionnement interne permettant de sécuriser du temps non opérationnel pour les salariés motivés pour s'investir dans leurs actions de mentorat.
- Mobiliser des personnes volontaires au programme de mentorat alumni des écoles du numérique par l'intermédiaire d'associations locales ou à partir de dispositifs de mise en relation mentors-mentorés coordonnés par l'action publique (programme « les Cordées de la réussite », par exemple).

9.3 Porteurs du projet

- Entreprises, dont RH.
- Action publique : ministère de l'enseignement supérieur, Éducation nationale (collèges et lycées).
- Acteurs de terrain, monde associatif, réseaux alumni.

9.4 Description

Les acteurs inscrits dans des programmes de partenariats pilotés par l'action publique[7], ont commencé à travailler les mises en relations de mentorat entre élèves ou étudiants et des professionnels en activité, comme :

MoovJee (Mouvement pour les jeunes et les étudiants).

L'objectif du MoovJee est d'amener les jeunes à considérer la création et la reprise d'entreprise pendant ou dès la fin des études (du CAP au Bac +5, toutes disciplines confondues).

Ses 3 axes d'action :

1. Promouvoir l'entrepreneuriat des jeunes par l'exemplarité.

2. Accompagner des entrepreneurs étudiants et jeunes diplômés dans la construction et le développement de leur entreprise.

[7] Exemple : le programme « les Cordées de la réussite », piloté par le ministère de l'enseignement supérieur avec de nombreux établissements « encordés » de l'Éducation nationale (collèges et lycées).

3. Les informer via un portail en ligne et les soutenir en proposant des services dédiés.

Les associations Article 1 et Institut Télémaque ont déjà commencé à travailler des partenariats directs avec les entreprises et affichent respectivement 175 et 190 entreprises partenaires pour mener à bien leurs actions.

Côté facilitateurs, les réseaux alumni s'investissent également dans des actions d'engagement de mentorat bénévole au service de la diversité sociale et de genre. Les actions de mentorat se distinguent auprès des élèves de leur propre école, mais aussi les actions de mentorat plus en amont (en collège, lycée, en accompagnement des premières années d'études supérieures), et cela avec les associations du programme « les Cordées de la réussite » citées plus haut.

Il ne s'agit pas d'appeler les acteurs du secteur de la cybersécurité à s'investir dans les sujets du mentorat en partant de la page blanche. De nombreux acteurs institutionnels et associatifs ont déjà tracé la voie dans le domaine plus large de la lutte pour la diversité sociale et l'insertion professionnelle. Il s'agit donc de les connaître et de travailler avec eux.

Côté écoles du numérique, sous l'impulsion de la Conférence des grandes écoles (CGE), l'attractivité des formations de haut niveau se concentre auprès des jeunes issus de la diversité et des étudiants. Le travail de mise en cohérence des actions s'est structuré au travers de chartes :

- En faveur d'un meilleur accès des étudiants en situation de handicap, en 2008.
- Sur l'égalité des chances, signée en 2010.
- Sur l'égalité femmes/hommes, lancée en 2013.

Plus récemment, des associations des grandes écoles se sont mises à organiser des actions de mentorat auprès des élèves mobilisant des alumni sur la base du volontariat pour suivre les élèves demandeurs.

10 Étendre la réserve opérationnelle aux institutions et au secteur privé

10.1 Objectifs

- Augmenter la résilience de notre économie au regard des attaques cybersécurité au niveau national.
- Contribuer à la pérennisation de l'activité économique des entreprises, voire de leur existence.

10.2 Préconisations

- De tout temps, les armées se sont dotées de réserves opérationnelles constituées de citoyens volontaires sous contrat capables d'être mobilisés pour faire face à n'importe quels imprévus. En temps de paix, ces réservistes viennent compléter le panel de compétences des armées et/ou renforcer les équipes militaires.
- Sur la base de ce modèle, il est proposé de construire un modèle d'entraide entre entreprises, permettant à certaines, sur la base du volontariat, de mettre à disposition des compétences cybersécurité au profit d'autres, plus démunies.
- Même si le modèle économique reste à construire, il est possible de s'inspirer de celui utilisé par le CyberPeace Institute[8], en le transposant aux chambres consulaires, éventuellement aux Régions qui détiennent la compétence de développement économique[9], et probablement à l'État au titre du maintien de sa souveraineté dans certains domaines d'activité jugés critiques.

10.3 Porteurs du projet

- Entreprises, dont RH.
- Ministère des armées.
- Chambres de commerce et d'industrie, chambres de métiers et de l'artisanat, chambres d'agriculture

10.4 Description

En se restreignant au secteur privé, dans le cadre d'une politique de responsabilité sociétale des entreprises (RSE), il est possible d'imaginer qu'en échange de l'octroi d'un label de type contribution à la résilience de l'économie nationale/régionale, une entreprise puisse verser des dons et/ou signer un partenariat avec une chambre consulaire mettant à disposition des employés disposant d'une compétence cybersécurité pour des missions de courte durée et en respectant l'image et l'éthique de l'entreprise signataire.

De son côté, une chambre consulaire pourrait, à la demande d'entreprises, mettre à disposition

[8] https://cyberpeaceinstitute.org/

[9] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000031104282/2015-11-04

ces ressources auprès de celles-ci, soit en anticipation, soit en gestion de crise ou reconstruction des SI. L'acceptation d'une demande de prise en charge pourra dépendre d'une politique ou de critères définis en amont par son assemblée et ses élus, de façon à ne pas être jugée en opportunité.

Trouver l'intérêt, pour une entreprise, à proposer des ressources et un coût de gestion de ce dispositif pour une chambre consulaire, nécessite de procéder par expérimentation. Aussi, la mise à disposition de réservistes par les armées pour le secteur lié à la défense pourrait être un moyen d'initier la démarche et d'illustrer son intérêt.

De façon à éviter de maintenir un intérêt réciproque entre entreprises offreuses de ressources et entreprises bénéficiaires, il serait intéressant de voir si ce soutien en matière de cybersécurité pourrait s'étendre à d'autres secteurs à risques, comme la possibilité d'offrir des capacités d'hébergement de certaines activités face à des risques naturels. Il est possible d'imaginer que la mutualisation de risques constituerait un gage de pérennisation du dispositif.

Pour mobiliser des spécialistes cybersécurité dans les entreprises contribuant à l'effort de défense nationale, le ministère des armées peut s'appuyer sur le dispositif de réserve opérationnelle, qui permet de détacher des réservistes provenant du secteur privé, du milieu associatif ou de la fonction publique. Cependant, pour étendre ce dispositif à d'autres secteurs d'activités, il faudra trouver un autre intermédiaire capable de gérer les disponibilités de spécialistes cybersécurité et la demande des entreprises. Les chambres consulaires – regroupant les chambres de commerce et d'industrie, les chambres de métiers et de l'artisanat et les chambres d'agriculture – pourraient être sollicitées, car elles représentent les acteurs des différents secteurs économiques et fournissent des activités d'appui comme le développement du territoire et la transition numérique. Toutefois, pour le milieu associatif, d'autres acteurs spécialistes cybersécurité devront être identifiés. Les collectivités territoriales pourraient jouer un rôle similaire dans le cadre de certaines associations locales.

11 Capitaliser sur les dispositifs liés à la formation et aux compétences

11.1 Objectifs

Permettre de recruter des demandeurs d'emploi ou favoriser la reconversion.

11.2 Préconisations

- Informer les entreprises à la recherche de nouveaux talents en cybersécurité des dispositifs d'accompagnement et de reconversion.
- Porteurs du projet.
- Les branches métiers par le biais des OPCO.
- Pôle emploi.
- Entreprises dont RH.
- Agefiph.
- Services RH et formation.

11.3 Description

Les branches métiers, via les OPCO, proposent à leurs adhérents plusieurs dispositifs pour répondre à la tension de personnes qualifiées sur des métiers définis comme stratégiques. C'est le cas pour la cybersécurité chez nombre d'entre eux (Atlas, Afdas, AKTO, Opco EP, OPCOMMERCE, OPCO 2i, Uniformation, etc.).

Tout d'abord, le dispositif le plus simple et le plus court : **les actions collectives ou clés en main**. Les OPCO proposent des formations qu'ils prennent souvent en charge en totalité sur des fonds mutualisés, dont la qualité est validée (choix des organismes dispensateurs sur appel d'offres), via une plateforme qui simplifie les démarches administratives.

Ces formations peuvent compléter les compétences d'un personnel déjà informaticien (pour les parcours métiers ou formations techniques), mais aussi pour convertir des personnes issues du juridique ou de la qualité (pour la sécurité organisationnelle).

Quelques exemples :

Parcours métiers Cybersécurité (opco-atlas.fr)

Afdas Formations

Catalogue des actions clés en main de l'OPCO 2i (linscription.com)

Pour trouver à quel OPCO une structure est rattachée, il suffit de consulter la table de correspondance : Opérateurs de compétences - OPCO (travail-emploi.gouv.fr)

Les préparations opérationnelles à l'emploi peuvent être aussi un deuxième dispositif à utiliser. Certaines sont financées uniquement par Pôle emploi (POEI), d'autres par Pôle emploi et l'OPCO commanditaire (POEC).

L'inclusion est plus forte sur ces dispositifs, car ils ne s'adressent qu'à des demandeurs d'emploi. Le but est de les mettre en capacité d'exercer un métier à l'issue de la formation.

Les POEI (préparations opérationnelles à l'emploi individuelles) sont en général mises en œuvre à la demande d'une entreprise qui souhaite embaucher (le contenu de la POE est alors adaptable aux besoins du commanditaire), alors que ce sont les OPCO qui décident du contenu et de la pertinence de la création d'une POEC (préparation opérationnelle à l'emploi collective).

Pôle emploi, en plus d'assurer tout ou partie du financement, informe les demandeurs d'emploi dès qu'une POE est proposée. Cela permet donc d'adresser ce public de façon efficace.

Exemples de POEC liées à la cybersécurité :

Une nouvelle POEC « Analyste Cybersécurité » en Bretagne | Opco Atlas (opco-atlas.fr)

Analyste cybersécurité - POEC - SIMPLON CO (1jeune1solution.gouv.fr)

Enfin, une structure peut mobiliser un autre dispositif : le certificat de qualification professionnelle (CQP). Il sert principalement à la reconversion de personnel. Il vise l'obtention d'une qualification reconnue par la branche métier et parfois par l'ensemble des branches (CQP interprofessionnel). Il est constitué de plusieurs blocs de compétences. Cela permet aux personnels de ne suivre que les blocs dont ils ont besoin.

Il existe un CQP Manager de la sécurité et des risques de l'information ouvert à l'ensemble des branches professionnelles. Cependant, il est en refonte au moment de l'écriture de ce document.

https://www.francecompetences.fr/recherche/rncp/29571/

Ce dispositif est accessible via une VAE.

En complément de ces dispositifs, il est intéressant de consulter :

Les pages internet des OPCO qui décrivent les critères de prise en charge, car il existe des abondements pour certains publics (personnes en situation de handicap).

Le site de l'Agefiph (qui propose des aides complémentaires pour faciliter l'embauche des personnes en situation de handicap).

12 CONCLUSION

La pénurie de ressources en cybersécurité est mondiale et impacte la filière française et l'ensemble des organismes privés ou publics.

Si ce constat est indéniable, force est de constater que les critères de recrutement, les profils recherchés, demeurent souvent inchangés. Les profils ciblés sont donc rares sur le marché et difficiles à recruter, car peu disponibles, ou très recherchés, ou souvent très chers.

Sans remettre en cause le besoin de former davantage de diplômés et d'experts en cybersécurité, les entreprises françaises doivent faire évoluer leur paradigme et développer une approche de diversité et d'inclusion tout en poursuivant l'attraction des candidats issus des filières d'excellence françaises.

Le mythe automaintenu au sein des organisations selon lequel les postulants en cybersécurité doivent posséder une gamme de qualifications et de certifications s'ils espèrent entrer dans l'industrie ou faire progresser leur carrière, devra être rompu. Cette approche permettra sans aucun doute d'ouvrir le champ du possible en termes de recrutement et d'aller chercher de nouveaux candidats.

La diversité et l'inclusion contribuent à assurer un riche bassin de talents. Elles sont un élément essentiel de la boîte à outils collective des organisations pour promouvoir et garantir des idées robustes, plus innovantes, plus agiles, et pour résoudre les problèmes de cybersécurité.

Les cyberattaquants viennent de tous les horizons et travaillent dans un environnement sans frontières. Que proposer de mieux pour relever les défis de sécurité que d'agréger des connaissances et expériences différentes et complémentaires ?

La curiosité, la capacité de résolution de problèmes et la pensée critique doivent être prises en considération lors du recrutement de talents expérimentés. La cybersécurité est un domaine dynamique, en permanente évolution. Les professionnels ne peuvent pas être statiques dans leurs connaissances.

Pour répondre aux besoins de compétence et de talents sur l'ensemble du territoire, la cybersécurité doit impérativement ouvrir ses portes à la diversité.

C'est là tout l'objet de ces recommandations qui proposent des actions à mettre en place au sein des organisations. Si ces recommandations peuvent paraître disruptives, elles sont pour autant inspirées d'expériences déjà mises en œuvre dans certains pays tels que les États-Unis ou Israël. Certains grands groupes les ont déjà actées.

Pour autant, si le manque de ressources et le manque de diversité dans la cybersécurité sont des thématiques évoquées de plus en plus aujourd'hui, force est de constater qu'il y a beaucoup de chemin à parcourir, et plus encore pour faire converger les deux thématiques de manière concrète et réaliste. Pour autant l'enjeu est considérable !

Au-delà de la méthode et des recommandations, c'est un profond changement de culture d'entreprise qu'il convient de mener. Certes, il appartient à la RH et au RSSI d'être acteurs, cependant, ils ne peuvent valablement pas porter seuls cette responsabilité.

L'implication des dirigeants et leur appropriation des enjeux du recrutement des profils cybersécurité sont primordiales. De leurs engagements dépendent les moyens pour développer la cyber résilience de l'organisation.

Une approche volontariste de la part des dirigeants est indispensable pour casser les idées préconçues et démontrer par les faits le bien-fondé, la faisabilité et la valeur ajoutée de la diversité.

Au-delà des enjeux économiques, humains, il est impératif de prendre en considération l'impact social et sociétal. La cyber résilience, la croissance de la filière cybersécurité et la souveraineté de la France ne peuvent se faire qu'en s'appuyant sur une volonté forte d'intégrer des talents issus de la diversité sociale, culturelle et territoriale. Le défi est de taille, mais réalisable !

ANNEXES

A. Liste non exhaustive des associations impliquées dans les enjeux diversité et inclusion

- Les associations entrant dans le cadre du programme « Cordées de la réussite » :
- Association de la fondation étudiante pour la ville (Afev) https://afev.org/
- Entraide Scolaire Amicale (ESA) https://www.entraidescolaireamicale.org/
- Article 1 https://article-1.eu/
- Chemins d'avenir https://www.cheminsdavenirs.fr/
- Proxité https://www.proxite.com/
- Socrate https://www.associationsocrate.org/
- Télémaque https://www.telemaque.org/
- L'Envol https://www.frateli.org/lenvol/
- Les Entretiens de l'Excellence http://www.lesentretiens.org/
- Capital Filles https://www.capitalfilles.fr/
- Fondation Culture & Diversité https://www.fondationcultureetdiversite.org/fondation
- Fondation Égalité des chances https://www.fondation-egalitedeschances.fr/
- Ma caméra chez les pros https://www.macamerachezlespros.fr/
- Le Réseau National des Entreprises pour l'Égalité des chances dans l'Education nationale http://www.lereseau.asso.fr/
- JobIRL https://www.jobirl.com/
- ViensVoirMonTaf (VVMT) https://www.viensvoirmontaf.fr/
- Les entreprises pour la Cité https://www.reseau-lepc.fr/
- Le programme « 1 jeune, 1 mentor » https://www.1jeune1solution.gouv.fr/mentorat

B. Déployer une approche systématique du mentorat

Sur l'attractivité des filières technologiques et numériques auprès des jeunes femmes, qui est le sujet majeur impactant le secteur de la cybersécurité, on peut noter le travail d'enquête réalisé depuis 2018 par l'Association Française des Managers de la Diversité (AFMD) avec la Conférence des grandes écoles (CGE), et les pistes d'actions qui ont été mises sur la table après coup, comme :

1. Rendre les formations relatives à l'égalité femmes-hommes obligatoires à tous les étudiants et toutes les étudiantes (y compris les membres du bureau des associations d'étudiant·e·s), afin de sensibiliser à la fois les femmes et les hommes, et d'inciter au dialogue.
2. Faire de la déconstruction des stéréotypes de genre un fil rouge tout au long du parcours des étudiant·e·s sous différentes formes (enseignements, ateliers, quiz, travaux pratiques, etc.).
3. Sanctionner les formations et les enseignements sur ce sujet par une note impactant les résultats académiques des étudiant·e·s.
4. Former tous les membres du personnel de l'établissement, enseignant·e·s et membres de l'administration, à la prévention des discriminations et à la déconstruction des stéréotypes.
5. Veiller au respect de l'égalité femmes-hommes et à la déconstruction des stéréotypes

de genre dans toutes les actions de formation et d'accompagnement impliquant des étudiant·e·s en formation initiale et continue.

6. Travailler la communication de l'école dans son ensemble, afin de donner à voir la volonté de l'établissement de lutter contre les stéréotypes de genre.

Pour la filière en aval, on peut espérer que ces actions qui jalonnent le parcours étudiant des futurs experts et managers formés en grandes écoles porteront leurs fruits. Une génération plus inclusive, plus sensible aux stéréotypes de genre, va pouvoir nourrir les effectifs des entreprises du domaine cyber.

Mais attention aux effets de halo. Une fois les années sur les bancs de l'école terminées, l'environnement de travail et les pratiques pèsent et peuvent remettre en cause l'ouverture d'esprit et les enthousiasmes des nouveaux entrants. C'est pourquoi des programmes internes aux entreprises sur l'inclusion sont d'autant plus nécessaires pour maintenir le flambeau, n'oubliant ni les managers recruteurs ni le personnel dans les équipes, qui devront tous s'habituer à accueillir plus de femmes et plus de personnes issues de la diversité en général.

C. Exemple de mise en situation de cyberattaque dans les écoles, établissements de formation

Préconisations

Conduire, à chaque étape de la scolarité, un continuum de formation à l'hygiène informatique et aux métiers de la cybersécurité.

Objectifs

L'objectif est de promouvoir la diversité des métiers de la cybersécurité auprès d'une population de jeunes étudiants et de les sensibiliser aux risques liés aux cyberattaques, en leur proposant une simulation immersive.

Porteurs du projet

- Éducation nationale.
- ESN.
- Organisme de formation.
- Conseiller d'orientation.
- Professionnel de la cybersécurité.

Description

Afin de capter l'attention de l'auditoire, il est préférable d'adopter un format ludique pour la présentation de l'exercice, tel qu'un jeu de rôle, de manière à favoriser l'interaction au sein de la classe.

Pour rendre la formation captivante et encourager la participation des élèves, il est important de fournir des exemples concrets liés à leur vie quotidienne, afin de partager des analogies pertinentes et stimulantes.

Étape 0 :

Organisation : Cette formation ne requiert aucun investissement financier.

La présence d'un professionnel de la cybersécurité pour accompagner l'enseignant lors de l'exercice est essentielle. L'école pourrait s'appuyer sur les organismes et associations du

domaine de la cybersécurité pour l'aide d'un bénévole qualifié concernant l'accompagnement pour la durée de l'exercice.

Durée : Environ 2 heures

Étape 1 : Le maître du jeu présente un scénario d'attaque cyber à l'ensemble de ses élèves

Les scénarios sont adaptables selon le contexte où ils seront mis en œuvre

Exemple de scénario :

Scénario 1 : Une attaque par intrusion

Une attaque cyber touche l'établissement et paralyse toute l'infrastructure de l'école, rendant impossible toute entrée ou sortie.

Scénario 2 : Une attaque d'hameçonnage (phishing)

Vous recevez un message sur les réseaux sociaux envoyés par un de vos amis contenant un lien suspicieux de type « Est-ce toi sur la vidéo ? : Lien suspicieux »

Vous recevez un message du responsable d'établissement qui annonce : « Suite à la crise, vous avez droit à une bourse de xxxx €, pour pouvoir en bénéficier merci de me communiquer votre numéro de carte bancaire ».

Scénario 3 : Une attaque par Rançongiciel (Ransomware)

Vous naviguez sur internet sur un des ordinateurs de l'établissement et recevez soudainement un écran noir demandant une rançon pour pouvoir réutiliser l'ordinateur en question.

Un professeur télécharge un virus qui se propage sur la plateforme de partage d'information entre professeurs et parents, toutes les données sur la plateforme sont chiffrées et inaccessibles, y compris les notes des examens passés, cela nécessite donc de devoir repasser tous les examens.

Scénario 4 : Une attaque par Social Engineering

Vous recevez un appel ou un mail provenant de votre responsable d'établissement qui vous demande des informations personnelles.

Vous recevez un appel de votre CPE qui vous demande votre identifiant et mot de passe afin de pouvoir mettre à jour les absences sur PRONOTE.

Étape 2 : Scinder en petits groupes de réflexion l'auditoire et les faire réfléchir sur les différentes actions à mener dans ce genre de situation.

Les guider avec les étapes principales d'une gestion d'incident cyber :

1. **Détection** : Comment avons-nous détecté l'incident ? Est-ce vraiment un incident ?
2. **Réponse :** Quel est l'impact ? Déconnexion des équipements du réseau ? Changement de mot de passe ? Récupération des preuves ?
3. **Atténuation (mitigation) :** Maintenant que nous avons assez d'éléments sur l'incident, est-ce qu'il faut mettre des mesures de contournement en place pour continuer l'activité en attendant la résolution de l'incident ?
4. **Rapport :** Qui faut-il prévenir ? Faut-il prévenir la police ?
5. **Reprise / reconstruction (recovery) :** Que faut-il reconstruire ?
6. **Remédiation :** C'est la phase qui marque le retour à la normale.

7. **Retour d'expérience :** Revue du processus de réflexion dans son intégralité pour voir s'il y a des améliorations à faire sur le processus.

Étape 3 : Après 20 minutes de discussion, demander à chaque responsable de groupe de présenter les propositions d'actions et schémas de réflexions.

Résumer la réflexion fournie par l'ensemble de la classe et faire comprendre que l'exercice réalisé à leur échelle peut se produire à l'échelle d'une entreprise ou organisation.

Étape 4 : Faire le parallèle avec les métiers de la cybersécurité qui ne sont pas forcément mis en avant dans un cursus ordinaire, même en cybersécurité, tels que :

– La gestion de crise

– La sensibilisation

– L'analyse de risque

– Investigateur

– ANSSI / DGSI

Il est important de démontrer que les métiers de la cybersécurité ne concernent pas uniquement des profils purement techniques, et que l'exercice qui vient d'être réalisé pourrait se transposer en entreprise.

Étape 5 : Session de Questions/Réponses

Glossaire :

Phishing : L'hameçonnage ou phishing est une forme d'escroquerie sur internet.

Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.) en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de « mettre à jour » ou de « confirmer vos informations suite à un incident technique », notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.).

Ransomware : Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

Social Engineering : Une pratique de manipulation psychologique à des fins d'escroquerie

Intrusion : Événement / incident de sécurité dans lequel un intrus obtient, ou tente d'obtenir, l'accès à un système ou à une ressource du système sans en avoir l'autorisation.

Tour Eria
5 rue Bellini

92821 Puteaux cedex

France

✆ +33 1 53 25 08 80

clusif@clusif.fr

clusif.fr