GOUVERNEMENT
Liberté
Égalité
Fraternité

« Synthèse :

Diagnostic CS&IA-92 »

Premier levier des transitions numériques et écologiques, la formation des jeunes et des salariés permet de renforcer le capital humain indispensable au fonctionnement de nos entreprises et au-delà de toute la société. C'est aussi le meilleur moyen pour proposer des emplois durables et de tous niveaux de qualification sur l'ensemble du territoire.

C'est également une des conditions majeures pour la réussite du plan France 2030 : soutenir l'émergence de talents et accélérer l'adaptation des formations aux besoins de compétences des nouvelles filières et des métiers d'avenir. 2,5 milliards d'euros de France 2030 seront mobilisés sur le capital humain pour atteindre cette ambition.

L'appel à manifestation d'intérêt « Compétences et métiers d'avenir » s'inscrit dans ce cadre et vise à répondre aux besoins des entreprises en matière de formations et de compétences nouvelles pour les métiers d'avenir.

Dans le cadre de ce dispositif, **la réalisation de diagnostics des besoins en compétences et en formations sont financés et diffusés.**

DIAGNOSTIC DE FORMATION
10 février 2023

Enjeux du diagnostic

Le diagnostic a pour objectif :

- Définir et structurer les besoins en compétences des entreprises des Hauts-de-Seine, sans distinction de taille et de secteur, en matière de cybersécurité et d'IA, en vue de la mise en place d'une offre adaptée, notamment de formations et de parcours (apprentissage) de proximité ainsi qu'à l'accueil de candidats aux profils divers (jeunes formés ou peu formés, personnes en reconversion professionnelle, sous réserve de prérequis).

Au-delà de ce diagnostic, le Consortium souhaite initier une dynamique territoriale, dans le temps, autour de 2 axes :

- Mieux accompagner les TPE-PME dans leur développement par le recours à l'IA et à la cybersécurité, dans leur process de production au travers de recrutements adaptés. Si les grands groupes sont structurés afin de répondre à ces enjeux, la plupart des entreprises (TPE-PME) n'ont pas mis en place ou ne sont pas en mesure d'assurer leur transition numérique dans toutes ses dimensions.
- Former les jeunes et les demandeurs d'emploi aux compétences demandées.

Méthodologie

L'étude concerne les entreprises implantées dans les Hauts-de-Seine de plus de 5 salariés, et de tout secteur (à l'exception des commerces de détail).

Technique de recueil des données :

Plusieurs techniques de recueil de données ont été mobilisé dans le cadre de ce diagnostic :

- Recherches documentaires
- Relevés d'offres d'emplois
- Entretien avec l'OPCO Atlas : l'opérateur de compétences de la branche professionnelle du secteur des services financiers et du conseil dont numérique.

La population d'entreprises cible de l'étude a été divisée en catégories suivant leurs tailles, en raison de la diversité des pratiques selon le type de l'entreprise. Le secteur du numérique a fait l'objet d'un traitement particulier. Le mode d'administration des questionnaires et leurs types ont été différents pour chaque catégorie :

- Enquêtes quantitatives auprès des :
  - Entreprises de plus de 20 salariés, par téléphone ;
  - Entreprises de 5 à 19 salariés, questionnaire en ligne.
- Enquête qualitative par entretiens semi-directifs en face à face avec :
  - De grandes entreprises (notamment du CAC40) et les collectivités
  - Quelques TPE/PME.
- 2 Focus group dédiés respectivement à l'IA et à la cybersécurité.

Analyse des besoins en compétences des entreprises des Hauts-de-Seine exprimés lors des enquêtes

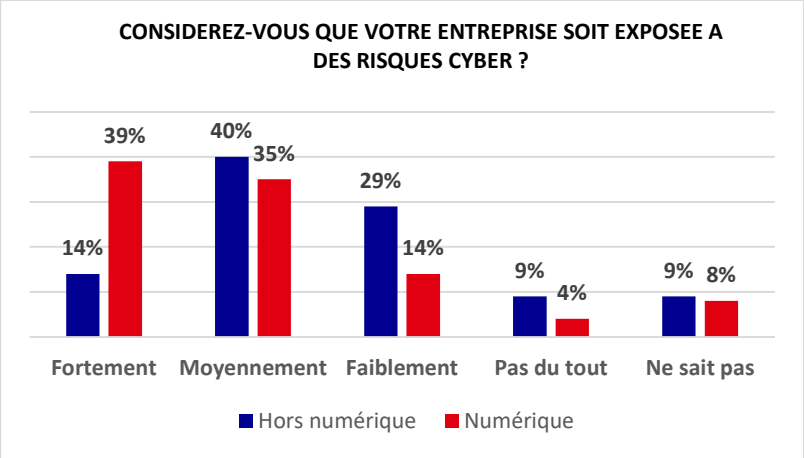
Un lien a été recherché entre d'une part la perception à l'exposition aux risques de cyberattaques et à l'introduction et au développement de l'IA dans les process de production et décision au sein de l'entreprise et d'autre part l'expression de besoins en compétences.

L'enquête quantitative et les entretiens semi-directifs confirment les écarts d'appréhension, et de prise en compte de la cybersécurité et de l'IA au sein de l'entreprise entre de très nombreuses petites et moyennes entreprises et les grandes entreprises.

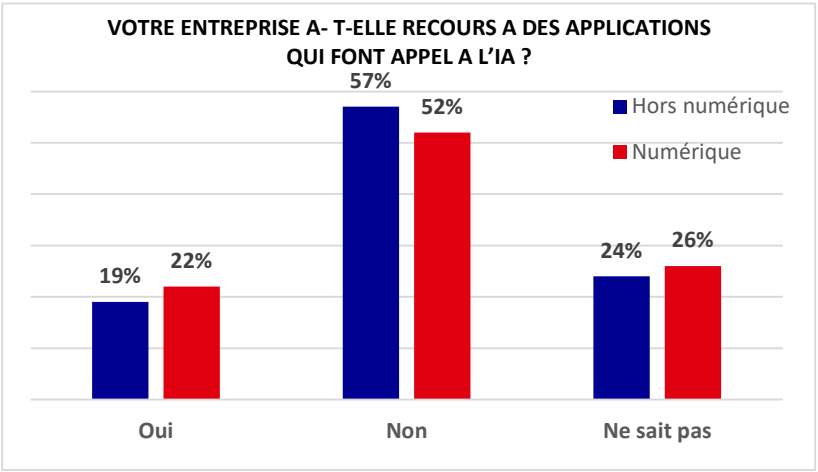
Une perception contrastée selon la taille et l'activité de l'entreprise

L'exposition aux risques est perçue différemment selon le secteur d'activité de l'entreprise. Les entreprises du numérique se considèrent plus exposées aux risques cyber, **75 %** estiment être y être fortement ou moyennement exposées, contre **54 %** pour les entreprises hors numérique.

90 % des personnes interrogées envisagent un renforcement prochain de la cybersécurité de leur entreprise.



Les grandes entreprises font ressortir une grande vigilance à l'égard des cyber-attaques, et sensibilisent la majorité de leurs collaborateurs pour faire en sorte de diminuer l'exposition de l'entreprise.



L'enquête quantitative fait apparaître peu de différences entre les PME numériques et celles des autres secteurs quant à leurs recours à des applications faisant appel à l'IA. En effet, plus de **50 %** des entreprises du secteur numérique et du secteur hors numérique interrogées déclarent ne pas avoir recours à ces applications. Le taux élevé de « Ne sait pas » traduit le fait qu'un certain nombre d'entreprises n'ont pas de vision sur ce qu'est l'IA et ses usages.

Les compétences internes à l'entreprise

Le niveau de satisfaction est globalement plus élevé en matière de cybersécurité qu'en IA peu importe le secteur ou la taille de l'entreprise. Les entreprises du numérique ont une satisfaction à l'égard de leurs collaborateurs plus importante que les entreprises extérieures à ce secteur.

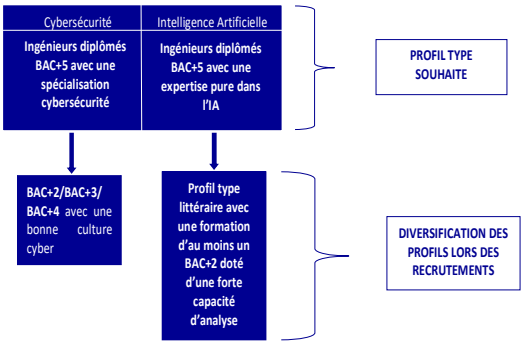
Une entreprise sur deux exprime un besoin de monter en compétences des équipes dans le domaine de la cybersécurité. A contrario, une entreprise sur deux déclare ne pas avoir de besoin en montée en compétences en IA. Ce fait démontre l'écart d'appréhension pour les entreprises en matière de cybersécurité et d'IA.

Les besoins en compétences nouvelles en matière d'IA émanent principalement des entreprises du numérique (**55 %**). Les grandes entreprises expriment des besoins de nouvelles compétences complémentaires à celle présentes dans l'entreprise, notamment en matière éthique et juridique.

40 % de ces entreprises déclarent acquérir ces nouvelles compétences par le biais de recrutement de nouveaux collaborateurs, et **22 %** par l'externalisation. Cependant, face aux difficultés de recrutement de collaborateurs, de fidélisation de ceux-ci, de surenchère de la part des entreprises pour attirer des compétences, les entreprises choisissent d'externaliser, faisant glisser les besoins en recrutement et compétences sur les entreprises du numérique.

Les besoins en recrutement

Les entreprises affichent une volonté de recruter principalement des profils Bac+5 pour **65 %** d'entre elles, ou pour **23 %** d'entre elles des profils Bac+3. Cependant, pour faire face aux tensions liées au recrutement des collaborateurs, les entreprises s'ouvrent sur d'autres profils, tels que des profils Bac+2 avec une forte capacité d'analyse pour des postes liés à la cybersécurité ou des Bac+2/3/4 avec une bonne culture cyber concernant des postes liés à la cybersécurité.



Afin de pallier ce manque, les grandes entreprises ont souligné l'importance de former les collaborateurs. Elles mettent en place des parcours de formation afin d'accompagner les collaborateurs dans l'évolution de leur métier. Les PME ont quant à elles des perceptions différenciées de ce besoin, moins de la moitié envisagent de former leurs collaborateurs. Les formations envisagées sont majoritairement des formations non diplômantes de courte durée dans le cadre du plan de l'entreprise. Les formations sous format de e-learning sont privilégiées.

Une évolution attendue des métiers de la cybersécurité et de l'IA selon les entreprises du numérique

Les entreprises du numérique questionnées perçoivent une future évolution de leur métier en matière d'IA et/ou de cybersécurité (**78 %**). L'interdépendance de l'IA et de la cybersécurité entraînera des évolutions de ces métiers. Des experts interrogés dans le cadre de ce diagnostic font état de l'impact croissant de l'IA sur la cybersécurité et inversement. Les modèles d'IA viennent en appui aux analystes de la sécurité afin de les aider dans la détection de dangers (identification des menaces, accélération du temps de réponse), ce qui implique une évolution du contenu du métier.

Cartographie des compétences

Les compétences nécessaires pour exercer des métiers dans les domaines de la cybersécurité et de l'IA diffèrent. Ils ont été cartographiés autour de trois catégories de profils : « En formation », « En développement », « En renforcement ».

Les compétences managériales et les softskills nécessaires dans les domaines de la cybersécurité et de l'IA sont relativement similaires : capacité à comprendre et à parler anglais, culture générale développée, ou aisance à l'oral. Les compétences managériales sont la pratique de certaines méthodes (AGILE, SCRUM), et la maitrise des outils de pilotages (GANTT, PERT).

Les compétences techniques requises diffèrent d'un domaine à l'autre :

IA	*Profil A : En formation*	*Profil B : En développement*	*Profil C : En renforcement*
Bloc 2 : Techniques	Matrices Fonctions à plusieurs variables Loi de probabilités Statistiques Modélisation Langage : Python Langage : R Base de données Sql, NoSql Règlement Général de la Protection des Données (RGPD)	Langage : Python Langage : R Machine Learning Deep Learning Gestion des bases de données (Github) RGPD	Algorithmie Computer Vision – Détection & reconnaissance Traitement automatique des langues (NLP) Apprentissage par renforcement RGPD
Cybersécurité	***PROFIL A : EN FORMATION***	***PROFIL B : EN DEVELOPPEMENT***	***PROFIL C : EN RENFORCEMENT***
Bloc 2 : Techniques	Bases de données Langage : C/C++ Systèmes d'exploitation Architectures & Administration des Systèmes d'informations (SI) Architectures & Administration des réseaux Cryptographie Sécurité des réseaux et terminaux ISO 27001	Gestion des antivirus Penetration testing Sécurité applicative Sécurité deceptive ISO 27001	Antivirus & EDR/XDR Framework AWS, CGP, Azure ISO 27001

L'offre de formation

Cartographie des formations et des dispositifs existants et financés dans les Hauts de Seine

La cartographie recense les formations situées dans les Hauts-de-Seine, ainsi que celles accessibles pour les personnes résidants ou travaillant dans les Hauts-de-Seine (liste non exhaustive).

La cartographie identifie 145 formations en Cyber sécurité et 60 formations en IA, tous publics, tous niveaux confondus.

Les établissements historiques de la recherche scientifique et de la formation en ingénierie implantées dans les Hauts de Seine sont l'Université Paris Nanterre (seule université dont le site principal se situe dans le département) et plusieurs écoles d'ingénieurs accrédités par la CTI (IFP School, ESILV, CESI et ISEP). Ces établissements mènent, au sein de leurs laboratoires, des travaux de recherche mono et pluridisciplinaires en Data Science, Informatique, Information et la communication et, plus récemment en IA et Cyber risques, proposent des formations, essentiellement de niveau bac+5 sur ces mêmes thématiques et aussi intègrent une initiation à l'IA et/ ou à la Cybersécurité, dans leurs formations plus classiques.

Aux côtés de ces établissements, se sont implantés plus récemment des organismes de formation de taille plus réduite, avec une offre de formation plus spécialisée, diplômante ou non, de durée variable, destinée principalement à des étudiants en alternance ou à des salariés comme l'IA School, l'ESGI ou bien de H2S ou Guardia Cybersecurity School.

Les enjeux environnementaux des formations et les axes d'amélioration de leur conception et de leur mise en œuvre

La croissance des industries du numériques associée à l'amélioration de leur qualité, la quête de modèles de plus en plus performants génèrent une augmentation des besoins énergétiques et de l'empreinte environnementale (Selon l'Union européenne, les industries numériques représentent 9% de la consommation mondiale d'électricité, avec une croissance de 9% par an).

A ces considérations environnementales et énergétiques s'ajoutent des exigences de bien-être sociétal, de respect de la vie privée, de gouvernance des données, ou encore de robustesse technique et de sécurité des systèmes.

Les enjeux environnementaux des formations portent tant sur la manière de former que sur leurs contenus (rapport Villani 2018), que la formation soit initiale, professionnelle, technique, de haut niveau.

Les contenus doivent couvrir un vaste champ de connaissances : au-delà du renforcement des enseignements mathématiques et informatiques, ils doivent porter sur des aspects géopolitiques, éthiques et sciences sociales. Seule la capacité à articuler sciences dures et sciences humaines est à même d'offrir les outils nécessaires à une appréhension correcte des enjeux environnementaux et sociaux.

Les axes d'amélioration

Accentuer les dimensions environnementales et éthiques dans les cursus d'ingénieurs ;

Créer de nouveaux cursus transverses traitant des aspects techniques et non-techniques dans lesquels les questions environnementales méritent une place particulière ;

Créer des formations plus généralistes au profit de personnes en formation ou en activité professionnelle ;

Créer de véritable formations hybrides dans lesquelles les sciences humaines ne seraient plus considérées comme des apports marginaux ou des modules d'ouverture. Les sciences humaines doivent trouver une place plus importante dans les formations des ingénieurs de manière à développer une capacité d'analyse des enjeux, dont ceux liés à l'environnement, plus précise et plus globale.

Les meilleures pratiques européennes et internationales

Il existe plusieurs classements des meilleures pratiques internationales en matière de cybersécurité et d'IA.

Depuis deux décennies, de nombreuses initiatives ont été développées aux Etats-Unis, en Israël et en Europe dont la France pour d'une part sensibiliser le plus grand nombre aux enjeux de la cybersécurité et de l'IA d'autre part conforter, au plan international, l'excellence d'établissements de formation et de recherche de ces deux disciplines. Dans un contexte de compétitions scientifique et économique majeures, les pratiques et les initiatives les plus impactantes ont été reprises par les états, les institutions et adaptées ; de telle sorte que les pratiques impactantes et inspirantes existent dans de très nombreux pays, c'est leur environnement qui leur permet de se démarquer.

Ces pratiques sont variées. Elles portent à la fois sur la mise en place d'écosystèmes réunissant établissements de formation et de recherche, entreprises et agences d'état, sur des actions de sensibilisation du plus grand nombre, de formation en milieu scolaire.

La pluridisciplinarité des formations

Cette pluridisciplinarité permet d'aller au-delà du simple enseignement technologique. Cette approche est privilégiée par les établissements israéliens : Le National Cyber Bureau (NCB) israélien De nombreux experts des sciences humaines interviennent dans les formations d'enseignement technologique. Cette pluridisciplinarité est fortement en œuvre en France p.ex. Le diplôme Data et finance de HEC Pais et l'Ecole polytechnique.

Développer une approche R&D dans la formation

La recherche joue un rôle central dans les formations. Les laboratoires de recherches sont des lieux qui rassemblent le plus souvent des acteurs du privé et publics autour des mêmes problématiques. Il existe de très nombreux exemples, à travers le monde, de collaborations universités/ entreprises / agences publiques ou gouvernementales : Cyber NYC de New-York, Digital Hub Cybersecurity de Darmstadt, « Bavarian IT security and safety cluster », Cyber Spark de Beer Sheva. National Cybersecurity Center of Excellence (NCCoE), aux Etats-Unis.

Parmi les initiatives internationales : l'institut DATAIA Paris-Saclay

Sensibilisation du plus grand nombre dont en milieu scolaire

Au travers du mois européen de la cybersécurité,

La gamification La gamification apporte un caractère ludique aux formations et facilite l'apprentissage. De nombreux évènements (ex hackathon) sont adossées à des institutions de référence tels que National Cybersecurity Centre (NCSC), au Royaume-Uni, organise le CyberFirst Girls Competition pour inciter les jeunes filles à s'engager sur ces sujets. A noter le Challenge européen de Cybersécurité, compétition de hackers éthiques âgés de 14 à 25 ans et le France Cybersecurity Challenge pour sélectionner les joueurs français.

Les formations de courte durée : L'OEA (Organisation des états américains) et l'Institut National Espagnol de Cybersécurité (INCIBE) organisent des « bootcamps » d'été en cybersécurité : programme de deux semaines rassemblant des étudiants du monde entier (techniciens, responsables de l'application des lois cyber etc.)

En milieu scolaire : L'Institut national espagnol de la cybersécurité (INCIBE) organise des « Espaces sur la cybersécurité » où des cours techniques et pratiques sont proposés à des classes de lycéens afin d'encourager les jeunes à s'intéresser à la cybersécurité. En France, le MENJS organise, dans le cadre de Campus Cyber, des formations pour les enseignants sur les sujets de cybersécurité liés au contenu des BTS SIO et SN.

Hypothèses des évolutions des besoins en formation à partir des travaux de recherche

Les besoins en formation résultent de l'élargissement du spectre des disciplines dans lesquelles sont impliquées l'IA et la cybersécurité : santé, droit, économie, gestion, sciences humaines et sciences sociales, arts, lettres, ….

Les besoins en formation peuvent être formulés peuvent être rattachés à deux grands profils :

Les chercheurs. L'élargissement des champs de l'IA et de la cybersécurité plaide en faveur d'une part de l'intégration d'une initiation à l'IA dans les modules de formation doctorale au-delà des écoles doctorales des disciplines Scientifiques et techniques et d'autre part, de l'organisation de séminaires de recherche pluridisciplinaires visant à stimuler les collaborations scientifiques entre spécialistes de l'IA et chercheurs d'autres disciplines.

Les autres publics, en particulier ceux de l'entreprise. L'objectif d'intégrer les avancées de l'IA et de la cybersécurité dans l'entreprise suppose une intégration de ces sujets dans la formation initiale aussi bien sous forme d'initiation dès la licence pour les formations de tous les domaines disciplinaires que sous la forme de doubles cursus de Licence ou de Master qui permettraient l'arrivée en entreprises de cadres susceptibles de participer très rapidement à l'intégration des techniques IA et des process de cybersécurité.

Concernant le domaine de l'IA, les évolutions et les besoins de formation qui en découlent ont bien été identifiés lors de l'élaboration de **La stratégie nationale pour l'IA :** besoin d'experts en IA avec une double compétence pour le développement d'applications IA adaptées aux différents secteurs de l'économie a aussi été bien identifié, les champs identifiés étant : IA et santé, IA et environnement, A et éducation...).

Les évolutions récentes aussi bien des travaux de recherche identifiés que du développement de l'IA dans les différents secteurs de l'économie soulignent le besoin de développement d'une double compétence IA – Droit, IA-Sciences du comportement et aussi IA- philosophie pour la prise en charge des dimensions éthiques, juridiques et comportementales.

Concernant la Cybersécurité**, la Stratégie nationale d'accélération pour la cybersécurité lancée en 2021** met aussi fortement l'accent sur la nécessité d'augmenter de façon significative le nombre de personnes formées à tous les niveaux de bac+2 à bac+8 en proposant une offre de formation en cohérence avec les avancées technologiques du secteur. Les évolutions des travaux de recherches semblent, comme pour l'IA, plaider aussi, dans ce domaine, en faveur de la nécessité de proposer des formations permettant l'acquisition d'une double compétence : Cyber – Droit, Cyber-Sciences du comportement, Cyber-Actuariat pour répondre aux futurs besoins de compétences des entreprises.

Accompagner les évolutions professionnelles et l'accès aux métiers de la cybersécurité et de l'intelligence artificielle d'un large public

Les résultats de l'étude révèlent que le nombre de formations en IA et en cybersécurité a augmenté ces dernières années, et s'est enrichi aussi bien en matière de contenus que de niveaux proposés. Les différents volets du présent diagnostic ont permis d'identifier des freins à l'augmentation du nombre de personnes formées, et des pistes d'améliorations de l'offre de formation afin de répondre aux besoins actuels.

Freins : Attractivité limitée pour les lycéens et les étudiants des formations et des métiers nécessitant des connaissances poussées en mathématiques ; Un niveau en mathématiques insuffisant pour s'engager dans un parcours en informatique ; Des formations avec un tarif élevé ; Des délais importants pour l'élaboration et l'accréditation des formations diplômantes.

Pistes d'amélioration : Inclure dans les formations en cybersécurité et en IA : un bloc softskills et un bloc compétences managériales ; Inclure dans l'ensemble des formations en cybersécurité et en IA une sensibilisation aux enjeux environnementaux et aux questions éthiques ; Proposer des doubles formations cursus IA + X afin de rendre les diplômés les plus opérationnels dans le déploiement de l'IA à des domaines spécifiques.

Macro plan d'actions pour accompagner les évolutions de l'emploi et des compétences

Un macro plan en 12 actions autour de 3 objectifs :

Objectif I Répondre à la pénurie de compétences en IA et cybersécurité sur le marché du travail à court, moyen et long terme

I.1. Formation initiale

Action 1. Diversifier les profils de recrutement en formation initiale, au-delà des ingénieurs et diplômés de Master spécialisés IA ou cybersécurité vers des profils plus généralistes.

- Des formations scientifiques du domaine STS, et même EG et SHS accueillant des bacheliers avec un bon niveau en mathématiques, et comportant un volume horaire important en mathématique, statistique, informatique et programmation durant les cursus peuvent avoir les compétences nécessaires pour les métiers de la Cyber et de l'IA.

Action 2. Accroître l'attractivité des filières IA et cybersécurité par des actions auprès des lycéens et auprès des étudiants.

- Travailler avec les lycées, l'ONISEP et les établissements d'enseignement supérieur pour mettre en œuvre un plan d'information et de communication sur les métiers de l'IA et la Cybersécurité.

Action 3. Intensifier au niveau régional la réflexion et le partage de pratiques en matière de formation et de recrutement sur les thématiques IA et Cyber en impliquant la CCI, les organismes professionnels et les organismes de formations.

- Un groupe de travail réunissant des représentants de ces différents acteurs pourrait être constitué et se réunir une fois par an pour un bilan qualitatif et quantitatif sur le territoire d'une part de l'évolution des inscrits en formation et des offres d'emploi, et aussi pour un échange sur les perspectives d'évolutions.

I. 2. Accompagner la mobilité professionnelle et la montée en compétence des salariés

Action 1. Créer des parcours de formation bien identifiés pour les professionnels leur permettant d'évoluer vers des postes de responsabilité en cybersécurité ou en Data management.

- Proposer des parcours de formation continue pour des professionnels de l'informatique vers la cybersécurité, pour des professionnels du droit vers des postes de délégués à la protection des données, pour des professionnels avec une formation scientifique vers la data science et l'IA, pour des cadres en informatique leur permettant d'évoluer vers le métier de Data engineer.

Action 2. Travailler avec les organismes professionnels et les organismes de formation pour la mise en place et la communication sur ces différents parcours de formations.

Action 3. Travailler avec les RH pour la communication auprès des salariés sur ces possibilités de mobilité professionnelle.

Objectif II Sensibiliser les TPE/ PME au potentiel de création de valeur que représente le traitement avancé des données, son automatisation, et la mobilisation des algorithmes de l'IA dans l'entreprise

Action 1. Organiser des campagnes d'information sur la valorisation et la culture de la donnée en entreprise.

Action 2. Créer un office départemental de sensibilisation, de conseils et d'orientation sur la valorisation des données et outils de l'IA à destination des TPE/PME.

Objectif III Anticiper les évolutions des besoins de compétences

Action 1. Intégrer une initiation en IA et Cybersécurité dans les formations universitaires dès la Licence.

- Une sensibilisation aux Cyber risques et à la Cyber sécurité est déjà majoritairement proposée dans les modules de préparation à la certification PIX. Il est possible de l'enrichir, notamment par des contenus plus interactifs. Concernant l'IA, des modules d'initiation peuvent être proposés suivant le même format (modules d'enseignement à distance combinés avec du présentiel ou du distantial synchrone) pour toutes les formations

Action 2. Proposer de nouveaux cursus de Master en Intelligence artificielle et Cybersécurité sur le territoire du 92

- Les nouvelles formations proposées doivent comporter l'ensemble des 3 blocs identifiés par les entreprises. Une composante indispensable du bloc de compétences transversales à inclure dans les futures formations en IA est un module sur la protection des données et sur l'éthique des algorithmes.

Action 3. Créer des doubles cursus de Licence ou de Master.

- Des doubles licences Cybersécurité- Sciences du comportement, IA-Sciences des organisations ou IA-Droit pourraient répondre à certains besoins de compétences relatifs à la sensibilisation aux cyber risques, à la protection des données personnelles et aussi à l'usage de l'IA dans les organisations.
- Des masters habilités sur les deux domaines STS et DEG ou STS et SHS peuvent permettent aux diplômés d'acquérir les compétences nécessaires pour l'implémentation des algorithmes de l'IA dans différents domaines.

Action 4. Stimuler les recherches pluridisciplinaires appliquées en IA et cybersécurité.

- Pour stimuler les recherches pluridisciplinaires, et aussi sur des sujets qui accompagnent les dimensions techniques de l'IA et de la cyber, par exemple sur les dimensions éthiques, environnementales et comportementales, des financements de thèse dans les disciplines du domaine DEG et SHS pourraient être proposés, par exemple au niveau de la région.

Action 5. Créer une cellule régionale de veille scientifique et technologique associant chercheurs et entreprises.