GOUVERNEMENT
Liberté
Égalité
Fraternité

« FORMATION, EMPLOIS ET COMPÉTENCES DE LA FILIÈRE CYBERSÉCURITÉ DU GRAND NANCY »

DIAGNOSTIC PROSPECTIF & PARTICIPATIF

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 en 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
31 mai 2023

Sommaire

Préambule

Le diagnostic sur l'écosystème cybersécurité de la Métropole du Grand Nancy a été réalisé par un consortium d'acteurs composé de :

- La **Maison de l'Emploi du Grand Nancy**,
- **Numeum**, organisation professionnelle nationale de l'écosystème numérique,
- **CESI** Ecole d'ingénieurs,
- Le cluster **Nancy Numérique**.

L'animation de la démarche a été portée par la Maison de l'Emploi du Grand Nancy, chef de file du projet, en réponse à l'appel à manifestation d'intérêt « Compétences et métiers d'avenir » du programme France 2030. La mise en œuvre opérationnelle de FORE-CY a été confiée à **Randea,** bureau d'étude et cabinet de conseil spécialisé en accompagnement des transitions de filière et prospective territoriale.

Fidèle aux méthodes participatives d'implication des parties prenantes au diagnostic et à la préparation de l'avenir, la mission a mobilisé **un comité de pilotage étendu aux parties prenantes**, lors de trois séminaires de travail en décembre 2022, avril et mai 2023 :

Note : sont présentés ici les partenaires impliqués dans la conduite de la mission ; il ne s'agit pas d'une cartographie de la filière Cybersécurité du Grand Nancy

Les auteurs tiennent à **remercier l'ensemble des membres impliqués** dans le Comité Technique du consortium, les parties prenantes locales et régionales mobilisées (entretiens, séminaires), **les interlocuteurs nationaux de l'AMI** « Compétences et Métiers d'Avenir » et de Numeum ainsi que les **organismes de formation et entreprises** ayant répondu aux deux enquêtes menées sur le territoire en appui du présent diagnostic.

Introduction et démarche méthodologique

La seconde levée de l'appel à manifestation « Compétences et métiers d'avenir » de France 2030

La Maison de l'Emploi du Grand Nancy, organisme associatif créé sous l'impulsion de la Métropole du Grand Nancy, a été désignée lauréate de la levée 2 de l'Appel à Manifestation d'Intérêt « Compétences et Métiers d'Avenir » (AMI CMA). Lancé en décembre 2021, l'AMI CMA est opéré conjointement par l'ANR (Agence nationale de la recherche) et la Banque des Territoires pour le compte de l'État, dans le cadre de France 2030.

L'appel à manifestation d'intérêt « Compétences et métiers d'avenir » vise à répondre aux besoins des entreprises en matière **de formations et de compétences nouvelles pour les métiers d'avenir.** L'adaptation et le développement capacitaire de l'appareil de formation sur des métiers en tension pourra également renforcer la capacité du pays à atteindre les objectifs de France 2030.

Il ambitionne d'**anticiper** autant que possible et de contribuer à satisfaire **les besoins en emplois ou en compétences**. Il s'agit aussi d'**accélérer la mise en œuvre des formations** y préparant, que celles-ci soient sanctionnées par des titres, des certifications ou des diplômes, ainsi que leur accès (information, attractivité et inscription) tant en cursus de formation initiale qu'en formation continue, quel que soit le statut de l'actif (apprenti, lycéen, étudiant, salarié, demandeur d'emploi, indépendant, libéral ou entrepreneur). La demande des entreprises porte fréquemment sur le manque de personnel formé et adapté à un marché du travail qui change sans cesse. Au-delà des attentes propres à chacune des entreprises, **les besoins d'un territoire ou de la filière concernés par la stratégie,** s'ils ne sont pas satisfaits, peuvent être sources de faiblesse dans la mise en œuvre de chaque priorité de France 2030.

Construit en consortium avec Numeum, Nancy Numérique, CESI École d'ingénieurs et la Maison de l'Emploi du Grand Nancy en chef de file, le projet porte l'acronyme FORE-CY, pour Formation, Emplois et Compétences de la filière Cybersécurité du Grand Nancy. L'ambition de FORE-CY est de **réaliser le premier diagnostic des besoins en compétences et en formations de l'écosystème cybersécurité sur le territoire** afin de disposer d'un état des lieux et d'un macro-plan d'action pour adapter l'offre de formation locale aux besoins des employeurs. Parmi les 59 projets de la catégorie « Diagnostics » retenus pour les vagues 1 et 2, FORE-CY est le seul dossier porté par une maison de l'emploi, et le deuxième projet localisé en région Grand Est[1].

FORE-CY : les forces du Grand Nancy s'unissent pour anticiper les besoins en cybersécurité et former les professionnels de demain

Porteuse sur le plan économique et génératrice de valeur sociale, la filière numérique du Grand Nancy, avec plus

[1] https://travail-emploi.gouv.fr/IMG/pdf/dp_-_france_2030_-_70_nouveaux_laureats_pour_la_deuxieme_vague_de_l_appel_a_manifestation_d_interet_competences_et_metiers_d_avenir_cma_.pdf

de 7 000 emplois et 1 000 entreprises, constitue le **deuxième pôle digital de la région Grand Est**, après Strasbourg. Le tissu entrepreneurial, caractérisé par une forte densité de TPE et PME, est fort d'expertises reconnues à l'échelle nationale et européenne dans des **domaines de pointe** comme l'intelligence artificielle, le cloud et les data centers, les technologies immersives...

À l'échelle locale, les synergies développées par les pôles d'enseignement (200 cursus à dominante numérique dispensés par près de 40 établissements), les structures de recherche (Loria, Inria) et les entreprises (PME, ETI, startups) illustrent les **capacités du territoire à soutenir l'innovation** et à irriguer en compétences le marché du travail.

La cybersécurité, domaine stratégique touchant aux conditions mêmes de notre souveraineté et de notre intégrité tant économique que démocratique, est un levier de résilience territoriale pour ceux qui en relèvent les défis, une vulnérabilité sinon. La cybersécurité constitue l'une des **spécialisations fortes du territoire grand-nancéien** avec trois secteurs économiques exprimant d'importants besoins de compétences en ce domaine :

- **La finance,** Nancy accueillant plusieurs DSI d'établissements bancaires avancés dans la dématérialisation des services (Crédit Mutuel, Caisse d'Epargne, Boursorama Banque…) ;
- **Le secteur public et les services administrés** sont également très présents (collectivités, Éducation, Ministère de la Justice, Ministère des Armées avec en sus de la Base de Défense de Nancy, le Centre expert des ressources humaines et de la solde) ;
- **La filière santé et biotechnologies** (CHRU, Banook Group, Pulsy…) fait aussi la renommée internationale de Nancy avec une problématique forte de digitalisation des parcours de soin, de multiplication des objets connectés et de protection des données personnelles.

Dès 2010, Nancy ouvre l'**un des premiers laboratoires civils de haute sécurité informatique** en France, Loria (Université de Lorraine, CNRS, Inria). En 2018, **un pôle régional de formation et d'intervention en cybersécurité** y est créé : centre civilo-militaire, il prépare une force de réserve opérationnelle susceptible d'intervenir en cas de cyberattaque majeure, avant de se spécialiser sur deux thématiques clés du territoire : la santé et la finance.

Le Grand Nancy compte également parmi les premiers pôles universitaires français. Avec **plus de 50 000 étudiants,** soit près de 18% de sa population, le territoire dispose d'**une offre en études supérieures complète** et constitue un terrain d'expérimentation pertinent pour l'intégration de modules dédiés à la cybersécurité dans les formations non spécialisées.

Malgré ces atouts indéniables, **la filière cybersécurité connaît une pénurie de candidats disponibles sur le marché du travail.** Plusieurs hypothèses peuvent expliquer cette tension sur le marché du travail : la forte attractivité des territoires voisins (Luxembourg, Strasbourg, Ile-de-France), une relative faiblesse des formations courtes ou modulaires à destination des métiers connexes indispensables (commercial, juridique, management), ou encore les pratiques de recrutement des entreprises polarisées sur les profils à haute technicité et diplômés de Master ou d'école d'ingénieur. L'ouverture à des profils plus diversifiés (féminisation, âge, parcours professionnels atypiques) constitue un levier à explorer par les employeurs ; l'identification des leviers de facilitation de ces trajectoires doit encourager ce type de dynamique.

Sur le marché du travail, le Grand Nancy comptait fin 2021, plus de 1 400 personnes inscrites à Pôle emploi dans un métier numérique. Les professions de l'informatique - ingénieurs (R&D, chefs de projet, télécom) et techniciens (développement, maintenance, support) - regroupent, à elles seules 400 projets de recherche d'emploi, un nombre en augmentation de 10 % en 5 ans. **Le vivier de demandeurs d'emploi ayant un profil de spécialiste numérique** (toutes activités confondues) représente une réserve de compétences à accompagner et former aux compétences liées à la cybersécurité en réponse à la demande croissante des employeurs.

Cependant, dominé par les accélérations, voire les ruptures technologiques, **le marché du travail des métiers numériques demeure hautement sélectif et concurrentiel, au risque d'exclure durablement certains demandeurs d'emploi** : un technicien ou ingénieur en informatique sur deux inscrit à Pôle emploi l'est depuis plus d'un an, un sur cinq depuis plus de 3 ans. A ces chômeurs identifiés s'ajoutent toutes les personnes qui ont une appétence pour la technique et ce secteur, sans disposer de qualifications identifiables. Accompagner les

reconversions professionnelles en répondant aux besoins en compétences en cybersécurité s'impose.

La Maison de l'Emploi du Grand Nancy, en partenariat avec Numeum, Nancy Numérique et CESI Ecole d'ingénieurs, en association avec les employeurs, les services de Pôle emploi et la Région Grand Est **a souhaité mener un diagnostic prospectif « Formation, Emploi et Compétences de la filière Cybersécurité du Grand Nancy » (FORE-CY)**.

Au travers d'une **méthodologie compréhensive et associant l'ensemble des parties prenantes de l'écosystème** Cyber du territoire, FORE-CY interroge quatre enjeux-clés pour le Grand Nancy :

STRUCTURATION

Qui sont les employeurs de l'écosystème cybersécurité du Grand Nancy ? Comment sont-ils organisés localement ? Quelles sont les interactions entre employeurs de l'écosystème cybersécurité et organismes de formation ?

FORMATION

Quelle offre locale de formation à la fois pour les spécialistes informatiques et les autres profils de la cybersécurité ? Comment pourrait-elle mieux répondre aux besoins territoriaux directs et indirects en cybersécurité, à l'échelle de la Région Grand Est ?

DIVERSITE ET INCLUSION

Comment rendre plus inclusifs les parcours d'accès à l'emploi et à la formation dans la filière (mixité professionnelle, intégration de profils jugés « atypiques ») ? Comment mieux accompagner les projets de reconversion professionnelle dans la filière cybersécurité ?

ANTICIPATION

Quelles perspectives de développement de la filière (marchés à consolider et à conquérir, métiers et technologies en émergence…) ? Quels seront les besoins des employeurs en termes de recrutement (métiers, compétences, spécialités) à l'horizon 2030 ?

Démarche méthodologique générale

Le diagnostic prospectif et participatif repose sur quatre « briques » méthodologiques complémentaires permettant de disposer d'un état des lieux robuste afin d'étayer la réflexion sur les perspectives d'avenir et d'ancrer au cœur de l'écosystème des acteurs, l'approche créative pour répondre aux problématiques et défis à relever. La méthodologie propre à chaque « brique » méthodologique est détaillée en Annexe méthodologique.

1| L'étude des besoins actuels en compétences de l'écosystème cybersécurité

Le volet d'étude des besoins actuels et à 12-36 mois en compétences de l'écosystème cybersécurité comprend :

- La réalisation d'un portrait statistique des entreprises de l'écosystème et de leurs ressources humaines *via* l'exploitation des données DSN ;
- Une enquête auprès des employeurs de profils Cyber du territoire, notamment des prestataires de service en cybersécurité. L'enquête s'est attachée à apprécier le degré de spécialisation Cyber, les enjeux RH et les leviers mis en œuvre pour répondre aux besoins en emplois, les besoins en compétences et formation à 12-36 mois et les perspectives d'activité et défis à relever d'ici 2030 ;
- Une analyse du marché du travail local en cybersécurité à partir des données Pôle Emploi.

2| Cartographie et diagnostic de l'offre de formation en cybersécurité

Pour apprécier l'offre de formation en cybersécurité, l'approche mise en œuvre conjugue :

- Un travail de cartographie des formations initiales et continues à la cybersécurité à l'échelle du Grand Est avec une double focale : (a) les formations spécialistes du « cœur de métier » cybersécurité aux savoir-faire technologiques d'une part, (b) les formations aux métiers connexes de la cybersécurité ou comportant une composante Cyber dans un parcours non dédié d'autre part ; le recueil a porté sur les formations initiales du Bac professionnel au Doctorat, en incluant les formations professionnelles et de reconversion, du local au régional ;
- Une enquête auprès des établissements identifiés afin de valider le recensement réalisé et l'enrichir du retour d'expérience des organismes sur l'attractivité de leur formation, leurs interactions avec les entreprises du territoire et leur vision des défis à relever pour préparer 2030.

3| Monographie des parcours de reconversion vers les métiers de la cybersécurité

Les monographies de parcours de reconversion professionnelle à la cybersécurité réalisées dans le cadre de la mission éclairent quant à elles, les défis et difficultés à lever pour élargir le vivier de recrutement de l'écosystème. Elles mettent en valeur des parcours inspirants de transition professionnelle et permettent notamment d'identifier les compétences d'appui facilitant une évolution vers les métiers de la cybersécurité.

4| Diagnostic prospectif territorial

Le diagnostic prospectif territorial constitue le quatrième volet de l'étude. Il croise les trois premières « briques » pour permettre un cadrage des perspectives en emplois et recrutements potentiels à l'horizon 2030. Les politiques territoriales régionale et métropolitaine en matière de cybersécurité y sont prises en compte afin d'anticiper au mieux les facteurs de dynamisation à l'œuvre.

Le diagnostic est enfin le socle d'un travail d'intelligence collective d'esquisse d'un projet original de formation pour répondre aux manques pointés. Cette approche s'est appuyée sur trois séances de travail avec l'ensemble des parties prenantes et sur une veille comparative nationale et internationale des formations à la cybersécurité.

Une démarche de préparation de l'avenir résolument participative

Initié en décembre 2022, le diagnostic FORE-CY s'appuie sur la mobilisation de l'ensemble de l'écosystème cybersécurité et sur l'implication de nombreux partenaires institutionnels et économiques :

- Les employeurs et leurs représentants (Inherent group et Adista, Capgemini, Cyber-Detect…) ;
- Les organismes de formation (Afpa, Cnam en Grand Est, Pôle Formation de l'UIMM Lorraine, Epitech, Simplon Grand Est, l'Université de Lorraine avec ses composantes spécialisées et les écoles d'ingénieur de Lorraine INP dont TELECOM Nancy et l'École Nationale Supérieure des Mines) ;
- Le monde de la recherche (Inria, Loria) ;
- Les acteurs publics et les prescripteurs (Pôle emploi, Région Grand Est, APEC Grand Est, Lorr'Up, OPCO Atlas…).

Le diagnostic débouche sur des préconisations coconstruites avec les acteurs, rassemblées en un macro-plan d'actions. La démarche mise en place est résolument inductive et participative afin de renforcer l'alignement des acteurs de l'écosystème et de favoriser leur mobilisation collective ultérieure.

Calendrier général de la mission

Source : https://fore-cy.fr/

Partie I. Étude des besoins en compétences de la filière cybersécurité du Grand Nancy

La transition numérique de l'économie et de la société s'accompagne d'opportunités importantes, mais aussi d'un renouvèlement des menaces et des atteintes, avec un nombre en forte augmentation des cyberattaques. Dans un contexte d'évolutions technologiques extrêmement rapides, **les vulnérabilités inhérentes à la transition numérique sont devenues un enjeu structurant pour tous les acteurs qui peinent à s'organiser pour y faire face ; elles le resteront assurément à moyen et long terme.** Les attaques en « rançongiciel » se multiplient, les criminels s'attaquent désormais aux plus faibles – citoyens, hôpitaux, collectivités territoriales…

Le législateur doit affronter les questions épineuses posées par ces problématiques montantes, autour de la cyber-assurance par exemple. Le projet de Loi pour « Sécuriser et réguler l'espace numérique » propose quant à lui le déploiement d'un « filtre national de cybersécurité » pour sécuriser les usages numériques du grand public, et la Loi de programmation et d'orientation du ministère de l'Intérieur du 23 janvier 2023 comme la Loi de programmation militaire (LPM) 2024-2030 du 4 avril 2023 actent d'efforts majeurs du pays en matière de capacités Cyber.

La Stratégie nationale d'accélération pour la cybersécurité initiée en 2021 vise ainsi à renforcer la protection des citoyens, des administrations et des entreprises. Elle se traduit par **une structuration nouvelle à l'échelle nationale, régionale et locale afin de faire face collectivement à ces défis d'ampleur** avec :

- une dotation importante en moyens via le **Programme d'investissement d'avenir (PIA4)** en vue de faire émerger des champions français pour garantir à la France la maîtrise des technologies essentielles à sa souveraineté ;
- **des programmes structurants** avec la mise en place du **Campus Cyber** en février 2022 pour accueillir et favoriser la collaboration entre les entreprises (grands groupes, PME et start-ups), les services de l'État (ANSSI, ministères de l'Intérieur et des Armées, etc.), les acteurs de la recherche, les organismes de formation et les associations ainsi que les **centres d'alerte et de réaction aux attaques informatiques (CSIRT)** destinés aux entreprises ou aux administrations de plusieurs régions.

La Métropole du Grand Nancy : carrefour de mise en œuvre régionale de la Stratégie d'accélération pour la cybersécurité

Le volet économique de la STRATÉGIE NATIONALE D'ACCÉLÉRATION POUR LA CYBERSÉCURITÉ vise à :

- Développer des solutions souveraines et innovantes de cybersécurité ;
- Renforcer les liens et synergies entre les acteurs de la filière ;
- Soutenir l'adoption de solutions Cyber (individus, entreprises, collectivités et État *via* la sensibilisation et la promotion des offres nationales) ;
- Former plus de jeunes et de professionnels aux métiers de la cybersécurité, la Stratégie nationale d'accélération ayant fixé l'objectif de **multiplier par 2 le nombre d'emplois dans la filière pour passer de 37 000 à 75 000 à l'horizon 2025**. Environ **9 250 personnes seront formées afin de devenir des spécialistes du domaine** à tous les niveaux de bac+2 à bac+8 et **10 000 salariés devront pouvoir bénéficier d'une formation professionnelle** courte en ce domaine.

La stratégie nationale se décline dans les territoires avec le déploiement progressif d'un réseau de campus Cyber en région en parallèle de la création des CSIRT.

C'est à Nancy, que le CSIRT de la région Grand Est a ouvert ses portes le 14 février 2023, à proximité de l'Université de Lorraine pour favoriser les synergies avec ses formations et pôles de recherche sur la cybersécurité. Bénéficiant du soutien de l'ANSSI et de l'agence régionale d'innovation Grand E-Nov+ en phase d'amorçage, il a vocation à offrir une assistance aux PME, ETI, collectivités et associations victimes de cyberattaques en offrant :

- un centre d'appel d'urgence pour répondre aux incidents de 1er niveau (non technique) via une plateforme téléphonique ;
- une mise en relation des victimes avec des prestataires régionaux pour mettre en sécurité les systèmes d'information suite au référencement des offreurs de solutions de la région (cartographie en cours) ;
- un accompagnement à la judiciarisation en partenariat avec la Gendarmerie et la Police nationale ;
- la consolidation des statistiques d'incidentologie à l'échelle régionale.

Le centre d'appel porte d'ores et déjà ses fruits : une cinquantaine d'appels d'urgence ont été pris en charge en trois mois confirmant les besoins locaux en ce domaine. Les attaques concernent toute la typologie d'acteurs bénéficiaires : PME, ETI, collectivités, associations et particuliers[2].

La Métropole du Grand Nancy est également pressentie pour être le « lieu totem » du Cyber Campus du Grand Est que la Région ambitionne de lancer au second semestre 2023 suite à l'accord intervenu avec le Campus Cyber national. Fidèle au concept inspiré du campus de Beer Sheva en Israël, de Skolkovo en Russie et de la Silicon Valley, ce lieu sera ouvert à tous les acteurs de la cybersécurité du territoire, travaillant en réseau pour apporter la cybersécurité au plus près des utilisateurs. Il « coordonnera et mutualisera les efforts et ressources de la communauté régionale en matière de sensibilisation, de **développement des compétences,** de partage de données, d'innovations et de coopérations transfrontalières »[3].

Le projet FORE-CY s'inscrit résolument dans cette Stratégie d'accélération nationale et régionale avec la volonté de renforcer l'ensemble des acteurs du territoire nancéen.

Enjeux et défis de la cybersécurité : cadrage stratégique du diagnostic local des besoins en compétences

[2] Mme Irène Weiss, Conseillère régionale déléguée à la cybersécurité

[3] https://www.grandest.fr/actualites/un-plan-regional-pour-la-cybersecurite/

Les entretiens menés auprès de l'écosystème et les échanges avec les parties prenantes intervenus lors des COTECH et des séminaires du Comité de pilotage élargi permettent de tracer quelques lignes de forces cadrant la réflexion sur les besoins en compétences Cyber. Ce cadrage ne prétend pas à l'exhaustivité mais a nourri la réflexion sur le périmètre des métiers et compétences à retenir dans le cadre de la mission.

1| **Après la RGPD, la crise de la COVID** avec le développement du télétravail et la prise de conscience des risques systémiques a généré **une forte hausse des besoins des entreprises et administrations en cybersécurité** qui semblent avoir brutalement pris conscience de la nécessité de protéger les données dont elles disposent. Certaines maîtrisent mal les enjeux de récolte, enrichissement, stockage et même destruction des données dont elles disposent utiles ou non, parfois sensibles. Les besoins sont croissants avec le **développement technologique très rapide** caractéristique du domaine numérique.

L'arrivée du quantique constitue à cet égard, à plus long terme, un changement de paradigme pour la cybersécurité. Si sa généralisation devrait intervenir au-delà de 2030, les recherches sont nécessaires en ce domaine. Le territoire grand nancéien dispose de pépites technologiques en ces domaines, en particulier le Loria pour n'en citer qu'une à titre de cadrage des enjeux territoriaux. Le Loria[4] a pour mission depuis sa création en 1997, la recherche fondamentale et appliquée en sciences informatiques et se positionne sur plusieurs problématiques majeures d'intérêt pour la présente mission avec notamment :

- L'équipe MOCQUA s'intéressant au calcul quantique, au calcul à l'ordre supérieur ou en précision infinie, ainsi que des thèses en co-direction au sein du laboratoire comme celle ciblée de 2022 sur « la programmation quantique avec types (co)inductifs » ;
- La start-up Cybi qui utilise l'apprentissage automatique au service de la cybersécurité en détectant automatiquement les chemins d'attaques possibles au travers des vulnérabilités d'un réseau. Elle établit alors les failles les plus à risques et les plus importantes pour les besoins du client. Fruit de recherches menées par l'équipe RESIST du Loria – CNRS/Inria/Université de Lorraine, en seulement six mois d'existence, Cybi s'est classée finaliste du prix de la start-up du Forum international de la cybersécurité (FIC) 2023.

↹ Points clés & conséquences métiers/compétences : la cybersécurité a bien évidemment partie liée avec les technologies numériques et informatiques dont elle exige la maîtrise, en relevant le défi de la **rapidité des évolutions technologiques**. Le risque numérique est aussi passé du champ purement technique vers un risque structurel pour l'activité des organisations. Ce changement de paradigme oblige dorénavant les entreprises, les collectivités et les institutions à intégrer le numérique au même niveau que les préoccupations stratégiques, économiques et juridiques au sein de leur modèle de gestion des risques. Cette nouvelle donne impacte notamment les compétences liées au **management des risques et à l'accompagnement des dirigeants** et directions d'organisation.

2| Si la cybersécurité est l'affaire de tous, elle reste encore assez largement méconnue, opaque ou sujette à des idées reçues tant de la part des étudiants que des acteurs économiques ou administrations. **L'un des défis amont pour l'écosystème est ainsi d'expliquer et faire comprendre la cybersécurité à tous les niveaux.** L'écosystème se doit ainsi d'**être plus lisible** sur les différentes prestations et leurs objectifs pour les acteurs économiques comme les acteurs publics. La certification ou la labellisation[5] des acteurs prestataires pourraient faciliter l'identification des savoir-faire et des niveaux de qualité, d'expertise et de protection obtenus.

La Région Grand Est a pour ce faire conduit avec Grand E-Nov+ une cartographie et un référencement des offreurs de solutions du territoire, en finalisation. Cybermalveillance.gouv.fr a quant à lui animé un groupe de travail impliquant le Centre de Formation de l'ANSSI (CFSSI), l'AFNOR et le Campus régional de Cybersécurité et de Confiance numérique de Nouvelle-Aquitaine (C3NA) pour concevoir un *Référentiel de compétences* explicitant les champs d'intervention et savoir-faire d'accompagnement des prestataires. Le RCPP a été publié le 15 mars 2023 ; s'il est à l'attention des organismes de formation, il pourrait constituer un outil de sensibilisation et d'aide à l'identification de leurs besoins pour les entreprises et organisations. Il est organisé autour de 5 grands besoins

[4] Le Laboratoire lorrain de Recherche en Informatique et ses Applications (Loria) est une Unité Mixte de Recherche (UMR 7503) commune au CNRS, à l'Université de Lorraine et à l'Inria.

[5] Cf. Le label ExpertCyber créé début 2021 par Cyber malveillance.gouv.fr en collaboration avec Cinov Numérique, la fédération EBEN, NUMEUM, France Assureurs et l'AFNOR. Son objectif est de reconnaître l'expertise en sécurité numérique d'un prestataire informatique dans trois domaines : la sécurisation, la maintenance et l'assistance.

des bénéficiaires – identifier, protéger, détecter, répondre, rétablir – et conforte le diagnostic amont des enjeux réalisé dans le cadre de la mission auprès des acteurs de la métropole nancéienne et de la Région Grand Est.

Point clé & conséquences métiers/compétences : sensibiliser et expliquer l'enjeu de la cybersécurité, prévenir en informant sur le coût d'une absence de protection restent indispensables aujourd'hui. Pour chaque métier de la Cyber, **les compétences pédagogiques** (adapter son discours, être capable de transmettre des contenus techniques à des non spécialistes, conduire une action de sensibilisation…) sont capitales.

3| Dans un monde où la compétitivité des entreprises repose de plus en plus sur leur maitrise des outils numériques, la capacité à se protéger face aux attaques informatiques représente un enjeu vital tant pour garantir leur croissance, que pour conserver la confiance de leurs clients. Cette **prise de conscience est cependant paradoxale dans la mesure où un grand nombre d'acteurs restent essentiellement attentistes** malgré le constat d'importance et sous-estiment presque systématiquement l'engagement budgétaire à consentir.

La Région Grand Est constate, elle aussi, à l'appui de la présente analyse, que **les entreprises du territoire recourent peu à l'aide régionale mise en place pour le financement de diagnostics d'évaluation de leur niveau de maturité en cybersécurité**[6]. Ce dispositif mis en place depuis novembre 2022 et qui permet de déboucher sur la définition d'un plan d'actions sera prochainement élargi aux acteurs publics et associatifs, ainsi qu'aux établissements de santé du territoire.

Au-delà de l'enjeu de sensibilisation, **il est impératif pour les prestataires de service Cyber d'accompagner les entreprises dans le diagnostic de leurs besoins** qu'elles sont rarement en mesure de réaliser seules. L'exercice de prospective réalisé par le Campus Cyber, conforte cet enjeu-clé, en l'adressant de façon plus systématique encore. Il cible ainsi les outils d'évaluation comme étant l'une des cinq priorités pour l'avenir de la Cyber : « construire des méthodes et des outils d'évaluation faciles, fiables et automatisables du niveau de sécurité des solutions, des produits, des composants et des organisations (tiers, fournisseurs, clients...) pour permettre le passage à l'échelle des évaluations de cybersécurité ».

Source : Horizon Cyber 2030. Perspectives et défis | Campus Cyber

Point clé & conséquences métiers/compétences : face à la complexité de la problématique, les entreprises et les organisations ont besoin d'être accompagnées dans l'évaluation de leurs besoins, ce qui ne va pas sans ressources et compétences dédiées.

4| Face aux besoins potentiels, le vivier de ressources humaines et candidats aux métiers de la cybersécurité apparaît insuffisant. Ce constat est largement partagé à l'échelle nationale comme internationale ; « Assurer la disponibilité des compétences cyber sur le marché et augmenter l'attractivité de la filière » constitue l'une des 5 priorités et l'un des défis majeurs à relever, comme le pointe l'exercice prospectif du Campus Cyber national.

Les raisons en sont multiples. (i) La cybersécurité apparaît encore trop souvent comme un **milieu sacralisé réservé aux « techs » particulièrement doués en informatique**, attirant peu les talents féminins (ii). Or dans le domaine de la cybersécurité, les besoins de compétences dans le domaine juridique, commercial ou en

[6] https://www.grandest.fr/vos-aides-regionales/diagnostic-cybersecurite/

accompagnement des organisations, résilience opérationnelle, fraude, gouvernance, etc. sont tout aussi dimensionnants. Cette méconnaissance des métiers et compétences de la cybersécurité est préjudiciable.

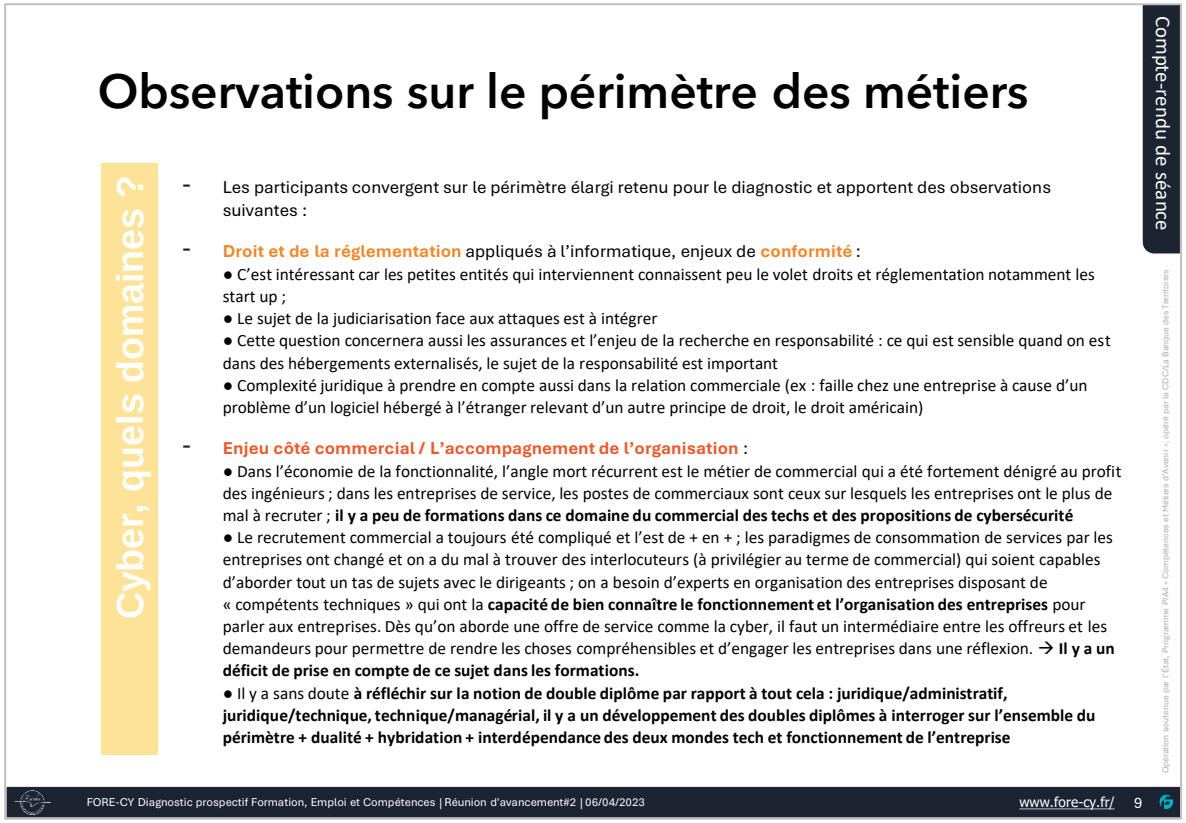
Face à ce constat, la Faculté de Droit de Nancy (Université de Lorraine) et le Loria (CNRS, Inria, Université de Lorraine) ont organisé le 4 juillet 2022 **à Nancy, les premières assises universitaires interdisciplinaires « Droit & cybersécurité » de la Région Grand Est** à l'attention des acteurs académiques et des professionnels du droit et de la cybersécurité, à la croisée du droit et de l'informatique.

(iii) La filière jouit également d'une **ambivalence d'image en matière éthique** entre hackers aux pratiques illicites et pratiques légales. Une sensibilisation est à mettre en œuvre pour mieux expliquer les métiers de la Cyber et les savoir-faire à maîtriser par l'*ethical hacker* tout à la fois procéduraux et créatifs pour être capable de trouver les failles.

↹ **Point clé & conséquences métiers/compétences :** initialement issue des pratiques informatiques et numériques dont elle a été une spécialisation de pointe, la cybersécurité est aujourd'hui **en phase de structuration en tant que filière pluridisciplinaire pleine et entière**. Les besoins en compétences souvent **expertes** sont attendus non seulement dans les domaines **technologiques**, mais aussi dans les champs **juridiques, éthiques et de l'accompagnement de l'entreprise** (cf. *infra* diapositive des échanges du séminaire élargi du 5 avril 2023). Le Campus Cyber territorial a notamment pour objectif d'être une vitrine pour montrer aux jeunes et aux publics en reconversion, l'ensemble des métiers de la filière.

5| Enfin, **la cybersécurité n'échappe pas au défi environnemental :** certains systèmes numériques s'avèrent particulièrement énergivores, leur protection peut l'être tout autant. « *En 2022, la réalité climatique impose à tous les secteurs d'intégrer dans leurs évolutions les paramètres du développement durable. Le numérique et la cyber sont particulièrement consommateurs en énergie, à la fois lors de la conception des systèmes, de leur utilisation au quotidien et de leur décommissionnement. Les principes de sobriété doivent s'inscrire dans leur modèle de développement* »[7]. Aussi les enjeux de **sobriété numérique** et de maîtrise d'approches y concourant se posent-ils au sein de la filière.

[7] *Source : Horizon Cyber 2030. Perspectives et défis* | Campus Cyber



Source : Exercice FORE-CY, séminaire élargi du 6 avril 2023

Périmètre des métiers et compétences de la cybersécurité : une vision « chaîne de valeur » résolument pluridisciplinaire

Le projet FORE-CY a retenu la définition de la cybersécurité de l'Agence Nationale de la Sécurité des Systèmes d'Information comme point de départ de la réflexion sur la typologie des domaines de compétences à considérer dans l'étude. Pour rappel, la cybersécurité est définie comme :

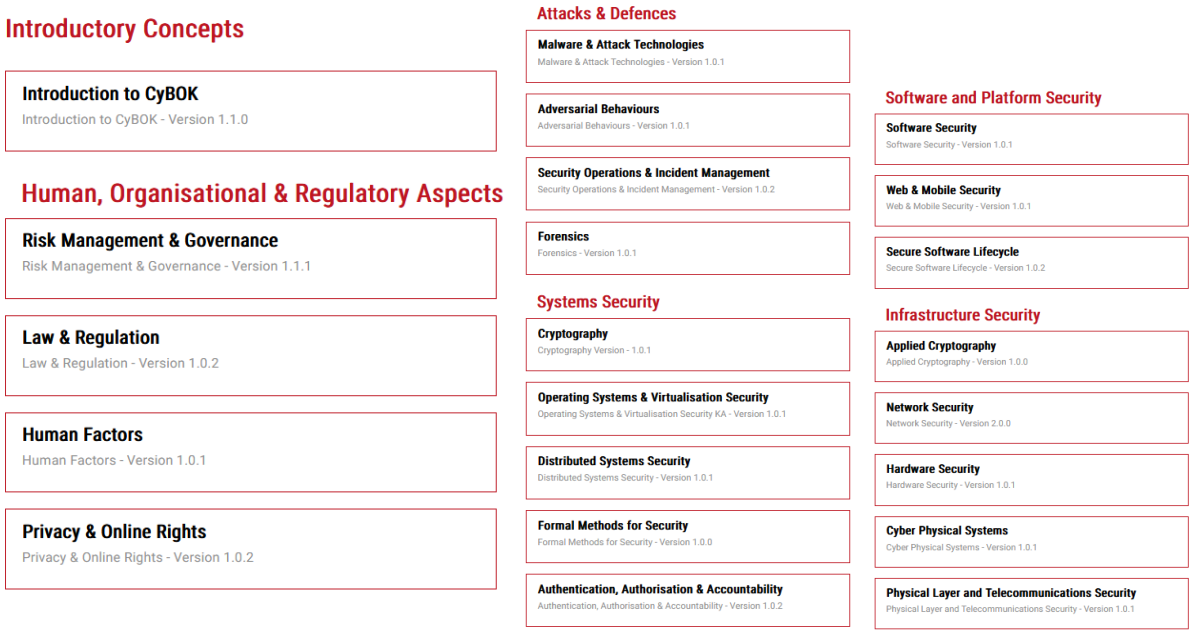
« L'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense. » (ANSSI)

Pour obtenir cet état chez les bénéficiaires, dans le contexte des 5 enjeux et défis décrits précédemment, le projet FORE-CY a estimé nécessaire de retenir **une acception large des métiers dans une logique de « chaîne de valeur complète »** en faisant toute leur place :

- aux métiers **technologiques** bien sûr sur la base du *Panorama des métiers de la cybersécurité* de l'ANSSI (édition 2020) ;
- aux métiers « **pouvant se spécialiser en cybersécurité** » **juridique** notamment et aux **métiers dits « connexes »** à la cybersécurité désignés dans l'édition 2020 du *Panorama des métiers de la cybersécurité* de l'ANSSI comme « contribuant à la démarche de cybersécurité » (management des risques, sûreté, contrôle interne, continuité d'activité, protection des données ; métiers du conseil également identifiés par le groupe

de travail régional sur les métiers du numérique et l'industrie 5.0 au titre de la famille « Sécurité des SI ») ;

- ces métiers sont davantage traités **« à équivalent »** des métiers technologiques au sein de l'*European Cybersecurity Skills Framework* de l'Agence de l'Union Européenne pour la cybersécurité (ENISA), ce qui a également retenu l'attention de l'équipe FORE-CY ; en particulier, le métier de formateur en cybersécurité y est l'un des 12 profils clés de la cybersécurité. Ces métiers sont également mis en avant au sein du référentiel *Cyber Security Body of Knowledge* (Cybok[8]) de l'Université de Bristol en les positionnant en amont des compétences technologiques avec un accent plus net mis sur le comportemental et le cognitif (cf. *Human factors*), tout comme sur la diversité des indispensables expertises juridiques (cf. *Law and Regulation Knowledge Tree*), dimensions sur lesquelles le projet FORE-CY a souhaité capitaliser.



Source : https://www.cybok.org/knowledgebase1_1/

Fort de cette approche comparative des référentiels et de l'analyse faite des 5 enjeux et défis de la cybersécurité (cf. section précédence), **le projet FORE-CY a retenu une typologie des domaines de compétences liés à la cybersécurité en 5 champs :**

- Champ 1 : la maîtrise des **technologies de sécurisation/protection** des systèmes d'information, réseaux, logiciels, applications ou systèmes embarqués ;
- Champ 2 : la maîtrise des **technologies et approches de détection et de gestion des incidents de cybercriminalité et la cyberdéfense** active ;
- Champ 3 : la connaissance des **normes et standards** ; la capacité à évaluer **risques et besoins** ; les enjeux de **conformité** en matière de vie privée et droits en ligne (PRA/PCA, RGPD, etc.) ; la connaissance du **droit appliqué à l'informatique** et à la **réglementation en matière numérique et Cyber** (y compris dans les aspects droit des contrats, recherche en responsabilité juridique, gestion des événements judiciaires) ;
- Champ 4 : **l'accompagnement de l'organisation** (gouvernance, procédure de gestion des risques et de crise…) et des **facteurs humains** (confiance numérique utilisateurs, usages de la Cyber, transformation, changement etc.) ;
- Champ 5 : **la sensibilisation et la formation** (socle ou spécialisée) à la cybersécurité.

Point clé & conséquences métiers/compétences (#6) : Les deux premiers domaines sont à dominante technologique mais ne peuvent être mis en œuvre sans une connaissance et une prise en compte des normes et standards comme de la règlementation. Les deux derniers domaines sont à dominante conseil organisationnel ou humain et ne peuvent, eux non plus, être mis en œuvre sans une maîtrise des normes et standards et de la

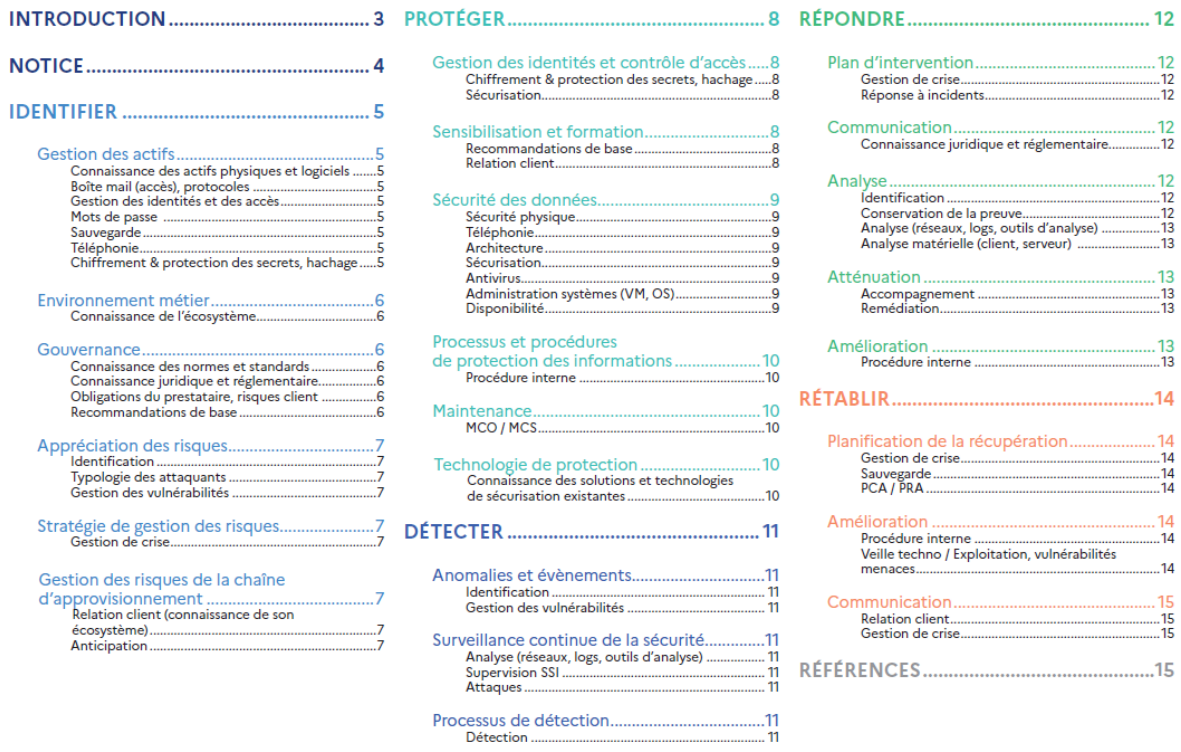
[8] Le projet CyBOK est financé par le *National Cyber Security Programme*, dirigé par un collectif de Professeurs des universités emmené par l'Université de Bristol.

règlementation. Ce champ de compétences « intermédiaire » d'essence juridique apparaît ainsi être une composante particulièrement partagée par les métiers technologiques comme d'accompagnement organisationnel et humain, mais aussi **un champ de spécialité Cyber en propre dont il est apparu progressivement qu'il ne se limitait pas aux connaissances juridiques en lien avec la mise en œuvre** de la sécurité des SI, logiciels ou autres, de la protection des données ou de la bonne gouvernance de ces enjeux. La demande en expertise juridique s'intensifie fortement en matière de **droit des contrats, de recherche en responsabilité juridique et de gestion des événements judiciaires**, point déjà souligné dans le rapport *Les formations et les compétences en France sur la cybersécurité* réalisé par EY pour le compte de l'OPIIEC 2017[9].

Ce point est clé ; il gagnerait à être partagé notamment à l'attention des Commissions des Titres au regard du récent *Référentiel de Compétences Cyber pour les Prestataires* (RCCP) dont la publication est intervenue en cours de mission. Le RCCP vise à « inventorier les compétences de sécurité sur un large spectre d'activité en embrassant tout le cycle de la cybersécurité, de la chaîne de la sécurisation, au maintien en conditions opérationnelles et de sécurité jusqu'à la remédiation ».

Les métiers à dominante technologique comme de conseil y figurent bien décrits, en revanche, il faut noter que les métiers d'expertise juridique en lien avec la cybersécurité (droit des contrats, recherche en responsabilité juridique, gestion des événements judiciaires, au-delà des connaissances juridiques en lien avec la sécurité des SI et à la protection des données) y sont peu présents. En matière d'accompagnement de la filière Cyber, « il est déterminant de s'extraire d'une vision d'ingénierie technique pour embrasser l'ensemble de l'ingénierie humaine et les défis juridiques qui se trouvent posés » commente l'une des parties prenantes du consortium FORE-CY.

Référentiel de Compétences Cyber pour les Prestataires (RCCP) | Cybermalveillance.gouv.fr

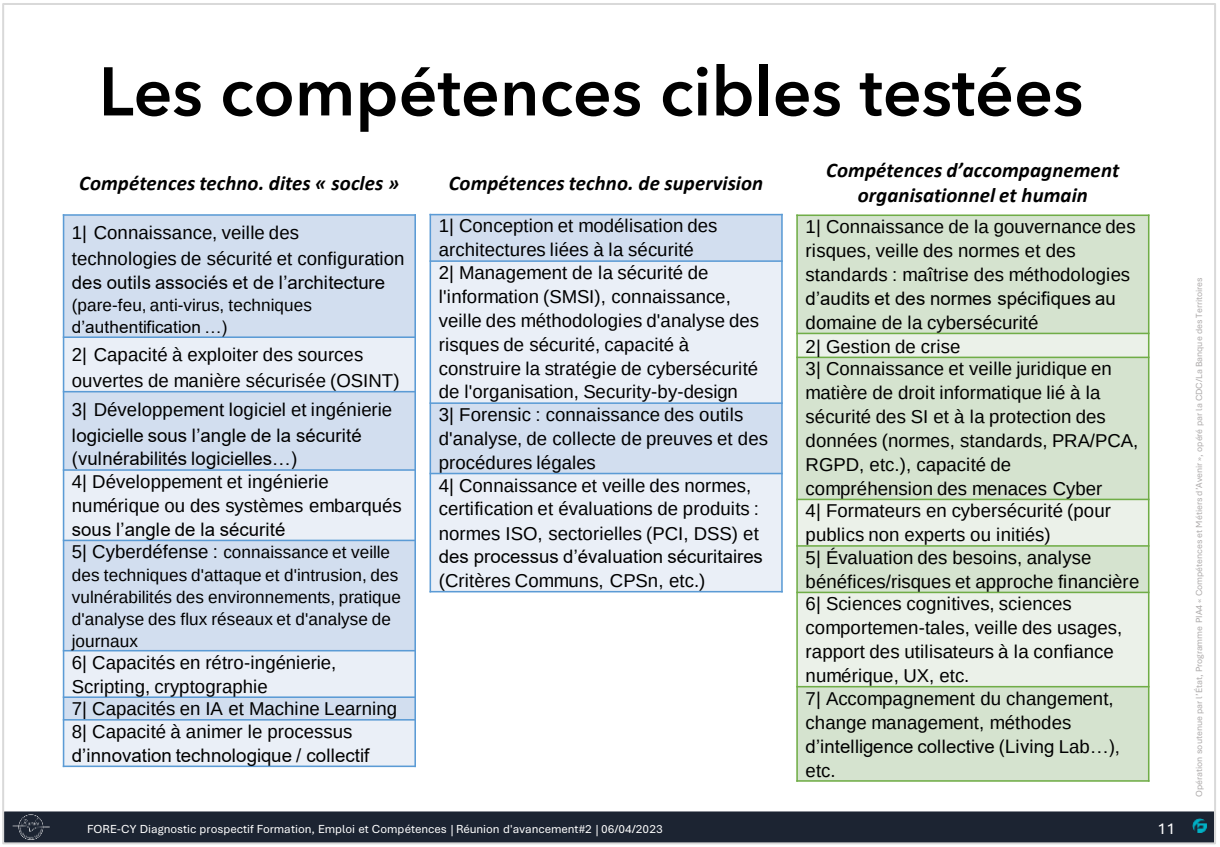


Résultat-clé : Au terme du diagnostic, l'équipe FORE-CY conclut ainsi **sur une triple polarisation des métiers de la filière Cybersécurité :** (i) technologique, (ii) juridique et (iii) d'accompagnement organisationnel et humain.

[9] https://www.opiiec.fr/sites/default/files/inline-files/21-05-2017_Etude_cybersecurite_rapport.pdf

Au-delà de l'indispensable réflexion sur le périmètre des métiers à considérer, le projet FORE-CY a souhaité approfondir de manière fine les besoins en compétences des entreprises prestataires de service Cyber ou disposant d'un service Cyber interne. **19 compétences recomposées** du référentiel ANSSI (cf. Annexe méthodologique) ont été retenues comme des compétences cibles. Elles ont été testées auprès des entreprises en trois sous-blocs afin d'éviter une liste trop longue :

- 8 **compétences technologiques socles** (cf. première colonne ci-dessous) ;
- 4 compétences dites de **supervision** (cf. deuxième colonne ci-dessous) ;
- 7 compétences davantage liées à l'**accompagnement** organisationnel ou humain (cf. troisième colonne ci-dessous).



Les compétences cibles testées

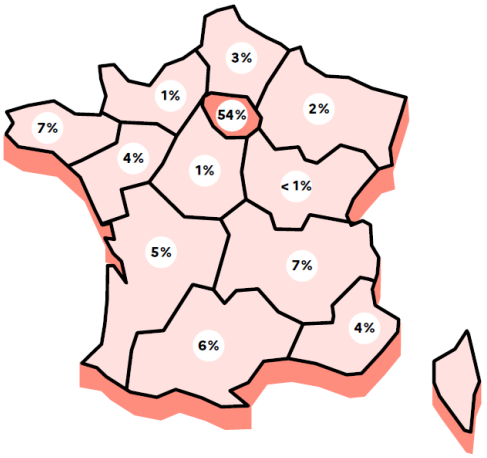
Compétences techno. dites « socles »	*Compétences techno. de supervision*	*Compétences d'accompagnement organisationnel et humain*
1| Connaissance, veille des technologies de sécurité et configuration des outils associés et de l'architecture (pare-feu, anti-virus, techniques d'authentification …)	1| Conception et modélisation des architectures liées à la sécurité	1| Connaissance de la gouvernance des risques, veille des normes et des standards : maîtrise des méthodologies d'audits et des normes spécifiques au domaine de la cybersécurité
2| Capacité à exploiter des sources ouvertes de manière sécurisée (OSINT)	2| Management de la sécurité de l'information (SMSI), connaissance, veille des méthodologies d'analyse des risques de sécurité, capacité à construire la stratégie de cybersécurité de l'organisation, Security-by-design	2| Gestion de crise
3| Développement logiciel et ingénierie logicielle sous l'angle de la sécurité (vulnérabilités logicielles…)	3| Forensic : connaissance des outils d'analyse, de collecte de preuves et des procédures légales	3| Connaissance et veille juridique en matière de droit informatique lié à la sécurité des SI et à la protection des données (normes, standards, PRA/PCA, RGPD, etc.), capacité de compréhension des menaces Cyber
4| Développement et ingénierie numérique ou des systèmes embarqués sous l'angle de la sécurité	4| Connaissance et veille des normes, certification et évaluations de produits : normes ISO, sectorielles (PCI, DSS) et des processus d'évaluation sécuritaires (Critères Communs, CPSn, etc.)	4| Formateurs en cybersécurité (pour publics non experts ou initiés)
5| Cyberdéfense : connaissance et veille des techniques d'attaque et d'intrusion, des vulnérabilités des environnements, pratique d'analyse des flux réseaux et d'analyse de journaux		5| Évaluation des besoins, analyse bénéfices/risques et approche financière
6| Capacités en rétro-ingénierie, Scripting, cryptographie		6| Sciences cognitives, sciences comportemen-tales, veille des usages, rapport des utilisateurs à la confiance numérique, UX, etc.
7| Capacités en IA et Machine Learning		7| Accompagnement du changement, change management, méthodes d'intelligence collective (Living Lab…), etc.
8| Capacité à animer le processus d'innovation technologique / collectif		

Portrait statistique des employeurs de compétences informatiques pourvoyeuses de profils Cyber

L'écosystème cybersécurité s'avère particulièrement difficile à appréhender à travers la statistique publique. Pour disposer d'éléments de cadrage, seuls les employeurs de techniciens et cadres informatiques de droit privé susceptibles d'être employés en cybersécurité (pour tout ou partie de leur temps de travail) peuvent être identifiés (cf. Annexe méthodologique). Ils constituent le sous-jacent des profils Cyber qui selon l'« Enquête auprès des professionnels des métiers de la cybersécurité 2021 » de l'Observatoire des métiers de la cybersécurité, proviennent à près de 50% de l'informatique (hors cybersécurité) et à 33% de la cybersécurité proprement dite.

Une analyse comparative territoriale a ainsi été réalisée pour cerner les typicités du territoire nancéien. La comparaison a été réalisée avec principalement avec trois territoires :

- La Bretagne qui a engagé une stratégie de développement des activités numériques de pointe, notamment à Rennes ;
- Les Hauts-de-France ;
- le Gand Est, moins pourvoyeurs d'emplois Cyber.



Source : *Enquête auprès des professionnels des métiers de la cybersécurité. Enquête 2021* | Observatoire des métiers de la cybersécurité

L'analyse comparative régionale de l'évolution des effectifs des techniciens et cadres informatiques de droit privé met en lumière quelques points saillants. Si les effectifs informatiques s'avéraient proches en 2015 entre les régions constituant aujourd'hui la région Grand Est et celles de la région Bretagne (~16 500 salariés), le dynamisme de la stratégie régionale bretonne en ce domaine s'est traduit par une hausse de +41% des effectifs en 5 ans, soit 9 points de plus que la moyenne nationale, là où **les effectifs en informatique du Grand Est n'ont progressé que de 22%, soit 9 points de moins que la moyenne nationale entre 2015 et 2020.** C'est après le Centre-Val de Loire, la croissance la moins dynamique d'effectifs informatiques au sein du territoire métropolitain.

La situation au sein de la Métropole du Grand Nancy tranche par rapport à cette toile de fond régionale. Ainsi, **les effectifs de techniciens et cadres informatiques de droit privé du Grand Nancy ont progressé de +36% entre 2015 et 2020,** soit une évolution légèrement plus dynamique que la moyenne nationale (+4 points).

Territoire	Effectifs des techniciens et cadres informatiques (de droit privé)		Indicateurs clés	
	2015	2020	Poids des effectifs régionaux en 2020	Variation des effectifs 2020/2015
Métropole du Grand Nancy	*1 643*	*2 227*	*11% des effectifs régionaux*	***+36%***
Grand Est	16 776	20 388	3%	+22%
Bretagne	16 152	22 812	3%	+41%
Hauts de France	25 548	33 360	5%	+31%
Occitanie	40 272	53 196	8%	+32%
Auvergne-Rhône-Alpes	54 984	70 476	10%	+28%
France entière	**520 032**	**683 436**	**100%**	**+31%**

Source : INSEE/BTS 2015 et 2020, Traitements Randea

La Métropole du Grand Nancy se démarque également par une **part assez significative de salariés de droit privé[10] aux compétences informatiques au sein des administrations publiques, organisations de santé humaine** ou d'enseignement (+4 points par rapport à la moyenne nationale), et ce, dès 2015. Le secteur public, la santé et la finance constituent en effet des spécialisations économiques du territoire.

	Métropole du Grand Nancy		Grand Est		Bretagne		Hauts de France		France	
	2015	2020	2015	2020	2015	2020	2015	2020	**2015**	**2020**
Industrie	7%	6%	16%	13%	9%	12%	9%	8%	**8%**	**8%**
Construction	1%	1%	2%	2%	0%	1%	0%	0%	**0%**	**1%**
Commerce, transports, Héb. & Rest.	4%	5%	7%	8%	4%	3%	9%	6%	**6%**	**5%**
Services divers	81%	81%	72%	73%	83%	81%	78%	83%	**84%**	**84%**
Administration publique, santé humaine, enseign.	**8%**	**6%**	4%	4%	3%	2%	3%	2%	**2%**	**2%**

Source : INSEE/BTS 2015 et 2020, Traitements Randea

Comme partout en France, si certains acteurs du Grand Nancy étaient en 2015 des entreprises de très petite taille avec 2% d'entreprises individuelles, ce profil a quasiment disparu en 2020. Le tissu d'employeurs de profils informatiques s'est concentré sur **les sociétés privées** partout en France.

Les effectifs de techniciens et cadres informatiques de droit privé ont diminué à l'échelle nationale au sein de la sphère publique, avec une nette baisse des cadres informatiques au sein de la Fonction publique territoriale et des organismes publics administratifs, là où la Fonction publique d'État s'est renforcée de compétences recrutées sur des contrats de droit privé. Cette évolution ne s'est pas produite de façon homogène sur l'ensemble du territoire ; ainsi, la Bretagne et plus encore **le Grand Est, dont la métropole nancéienne, ont connu au contraire une croissance de leurs effectifs informatiques de droit privé au sein des trois fonctions publiques.** Les techniciens et cadres informatiques (de droit privé) de la sphère publique du Grand Nancy sont ainsi passés d'une 20^{aine} à 70 ; ils constituent 3% des effectifs locaux de salariés de droit privé dont l'activité principale du poste est l'informatique, soit +2 points par rapport à la moyenne nationale.

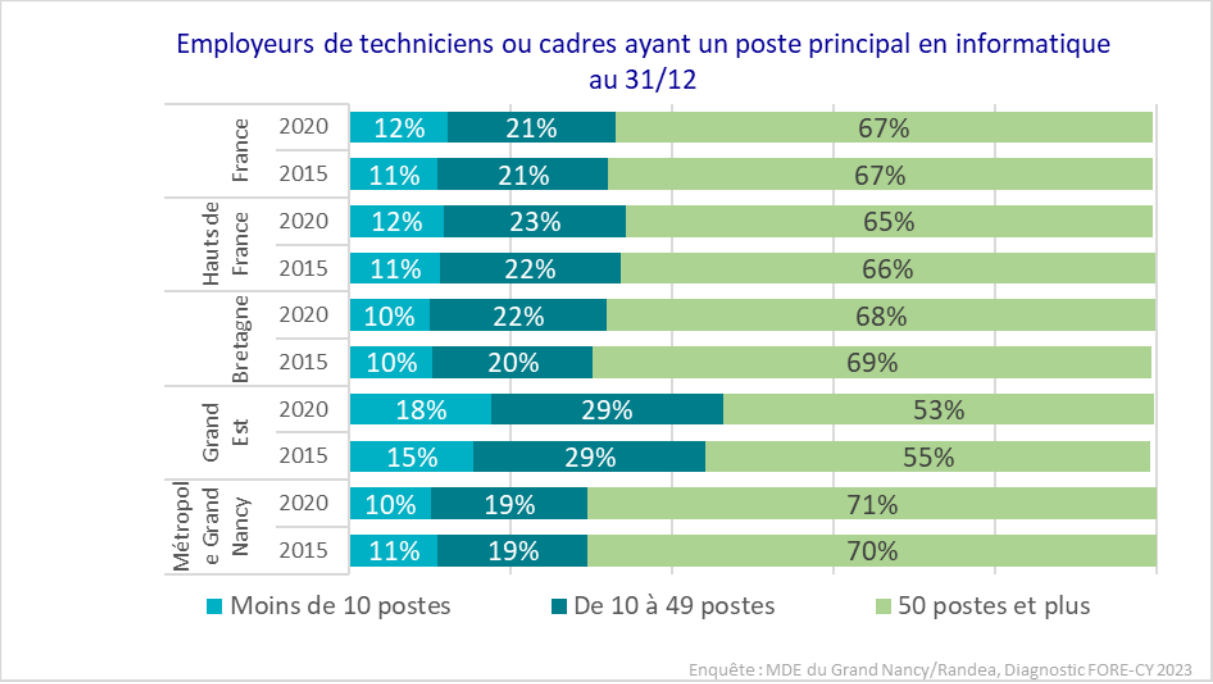
	Métropole du Grand Nancy		Grand Est		Bretagne		Hauts de France		France	
	2015	2020	2015	2020	2015	2020	2015	2020	**2015**	**2020**

[10] N.B. La statistique publique ne permet pas de repérer les techniciens et ingénieurs informatiques parmi les agents des différentes fonctions publiques recensés dans d'autres codes de nomenclature.

Fonction publique d'état ou territoriale	1%	**3%**	1%	2%	1%	1%	1%	0%	**1%**	**1%**
Entreprises individuelles	2%	0%	3%	0%	3%	0%	3%	0%	**2%**	**0%**
Sociétés privées	86%	92%	90%	93%	91%	94%	91%	96%	**94%**	**96%**
Autre	12%	5%	6%	5%	5%	5%	5%	4%	**3%**	**3%**
Part du territoire dans l'emploi public en informatique	0,2%	1,3%	1%	9%	5%	6%	7%	6%	**100%**	**100%**
Variation de l'emploi public en informatique	**+215%**		**+290%**		**+100%**		-6,5%		**-23%**	

Source : INSEE/BTS 2015 et 2020, Traitements Randea

Cette spécificité locale joue sur la répartition des effectifs par taille des employeurs : **les salariés de l'informatique sont à 70% rattachés à des entités de plus de 50 postes au sein du Grand Nancy,** ce qui s'avère légèrement supérieur à la moyenne française et nettement supérieur à celle du Grand Est (> +15 points).



Côté âge et féminisation, les profils informatiques du Grand Nancy restent assez peu féminisés (17%, soit -8 points par rapport à la moyenne française) et ont connu un net rajeunissement entre 2015 et 2020 ; leur structure par âge rejoint celle de la moyenne nationale :

	Métropole du Grand Nancy		Grand Est		Bretagne		Hauts de France		France	
	2015	2020	2015	2020	2015	2020	2015	2020	**2015**	**2020**
Moins de 30 ans	18%	27%	25%	26%	24%	25%	27%	28%	**24%**	**26%**
De 30 à 49 ans	58%	52%	54%	53%	61%	57%	58%	57%	**59%**	**56%**
50 ans et plus	24%	21%	22%	22%	15%	18%	15%	16%	**17%**	**18%**
Part de femmes	16%	17%	20%	20%	20%	19%	17%	18%	**21%**	**25%**
Part de contrats d'apprentissage	<1%	3,4%	1,2%	2,3%	0,6%	2,2%	0,9%	2,2%	**0,8%**	**1,8%**

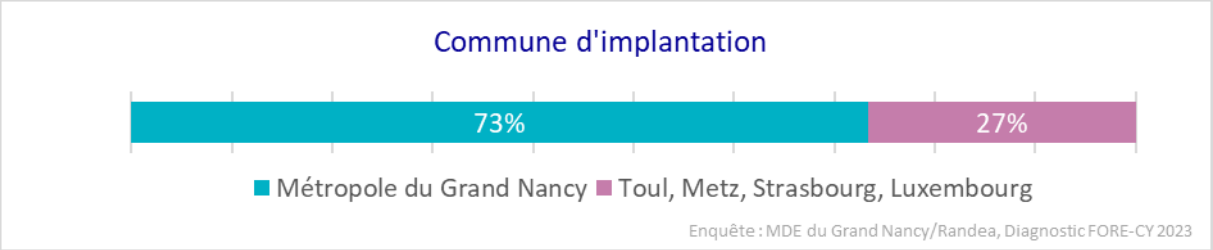
Source : INSEE/BTS 2015 et 2020, Traitements Randea

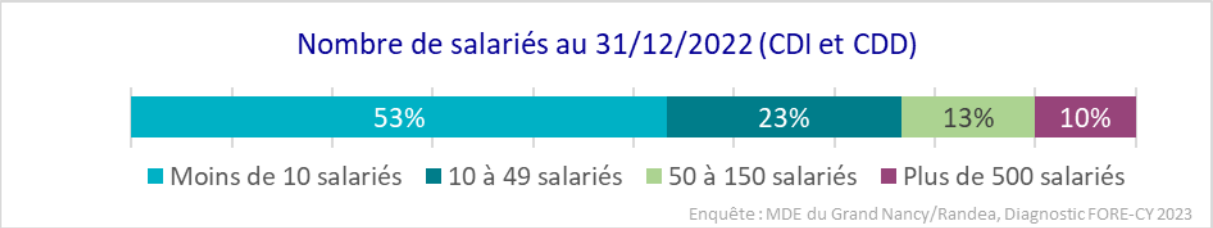
Point positif partagé sur l'ensemble du territoire, mais plus encore en région Grand Est et sur le territoire du Grand Nancy**, le taux de recours à l'apprentissage progresse** pour atteindre 2,3% des emplois de profils informatiques en Grand Est et même **3,4% au sein de la métropole**, soit 1,6 points de plus que la moyenne nationale.

En complément des données issues de la statistique publique, l'enquête FORE-CY menée auprès des employeurs de profils Cyber du territoire permet d'affiner le portrait de ces derniers et de présenter l'échantillon des répondants en en précisant la commune d'implantation et la typologie d'acteurs au regard de leur taille et de leurs activités principales et secondaires (cf. graphiques et tableau de la page suivante).

Portrait des 30 employeurs de profils Cyber de l'enquête FORE-CY

(soit 25% de l'écosystème identifié)
N.B. À des fins de facilitation de la lecture, les résultats sont présentés en % malgré la taille restreinte de l'échantillon





N.B. En tenant compte du nombre de collaborateurs Cyber au sein des différentes entités, il ressort de l'enquête que les profils Cyber des employeurs strictement nancéiens ayant répondu à l'enquête, relèvent à 35% d'entités de moins de 10 salariés, à 35% d'entités de 10 à 49 salariés et à 30% d'entités d'au moins 50 salariés, l'écosystème Cyber concernant des structures de plus petite taille que les employeurs de profils informatiques (cf. portrait statistique précédent).

Activités principales et secondaires des entreprises répondantes

	Activité principale	Activités secondaires
Ingénierie, édition et intégration de solutions logicielles	**7**	2
Ingénierie et intégration de solutions numériques ou systèmes embarqués ou solutions immersives	2	3
Activité numérique	3	
Informatique (infrastructure, support etc.), Télécommunications, hébergement de données	3	**6**
Cybersécurité, sécurité des SI	2	**6**
Gestion et valorisation de la donnée		**5**
Activité d'audit ou de conseil (organisation, transformation, gestion des risques…)	**5**	3

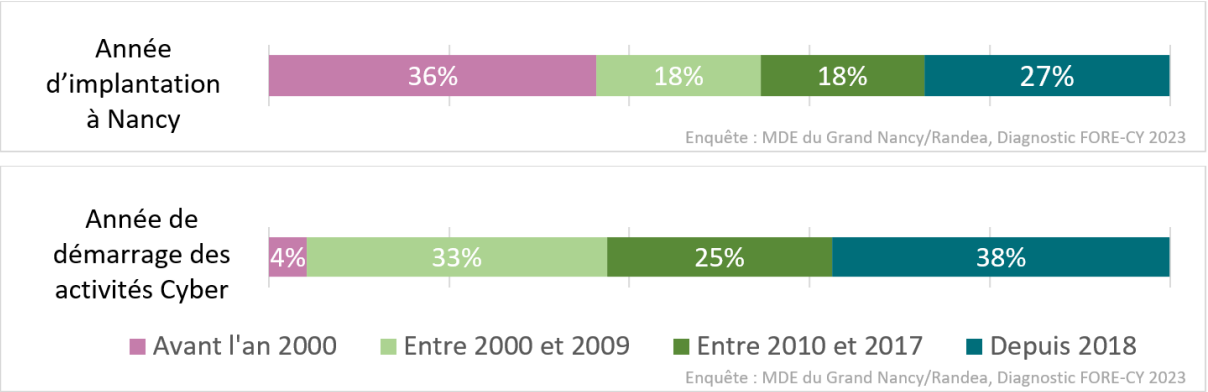
Services administratifs, Santé, Banque-assurance	**4**	
Services aux entreprises (marketing digital…)	3	
Services aux particuliers	1	
Activité de recherche		1
Commercialisation de produits software ou de supports informatiques, accessoires ou composants		3
Aucune activité secondaire		6

Enquête : MDE du Grand Nancy/Randea, Diagnostic FORE-CY 2023

Une enquête fine d'exploration des besoins en compétences Cyber des employeurs

1| L'écosystème des employeurs de profils Cyber de la Métropole du Grand Nancy

Les employeurs de profils Cyber impliqués dans l'enquête FORE-CY sont constitués d'acteurs implantés sur le territoire nancéien avant l'an 2000 pour le tiers d'entre eux et pour un quart depuis moins de 5 ans. Rares sont ceux à avoir débuté leurs activités en cybersécurité avant l'an 2000, un tiers d'entre eux l'ont fait entre 2000 et 2009 et pour 40% depuis moins de 5 ans, près d'un quart depuis moins de 3 ans. Notons par ailleurs, que dans 2/3 des cas, l'implantation locale a précédé ou a été simultanée de l'activité cybersécurité.



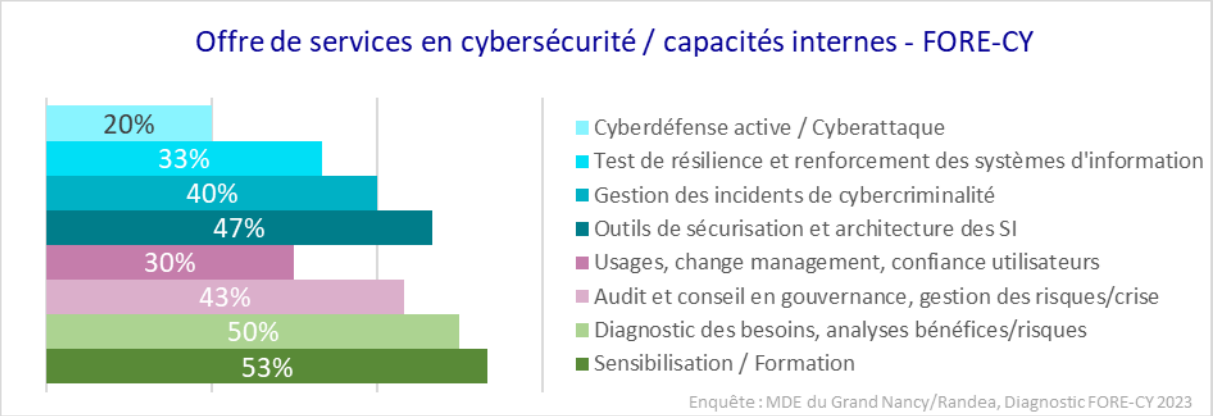
Rappel : Les résultats sont présentés en % malgré la taille restreinte de l'échantillon : 22+8 acteurs, soit 25% de l'écosystème

Qu'ils relèvent de la filière numérique ou des secteurs utilisateurs, les employeurs de profils Cyber disposent de savoir-faire en compétences Cyber non distinctifs et très variés d'un acteur à l'autre. Une partie des acteurs est spécialisée sur certains services Cyber, l'autre non. Ainsi, l'enquête dénombre parmi les réponses exprimées (cf. graphique en pyramide ci-dessous) :

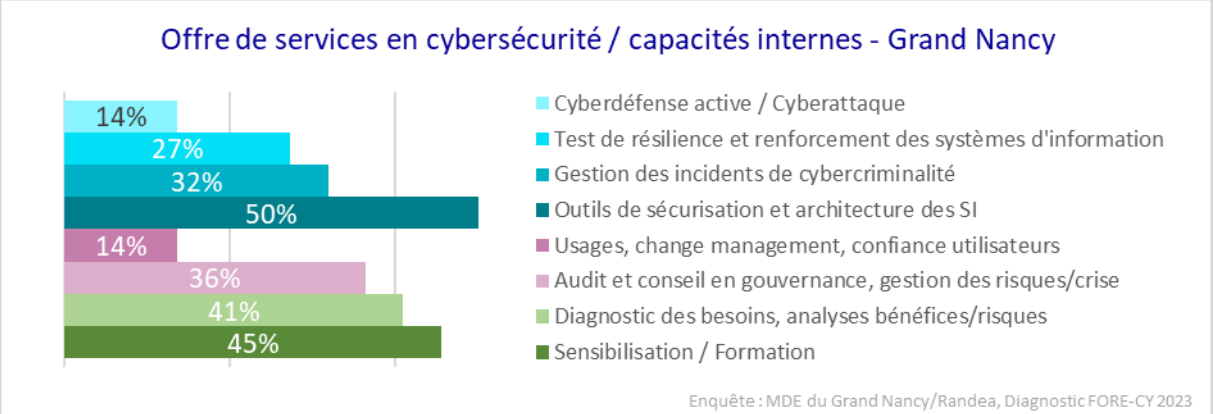
- 5 entreprises disposant de compétences **en audit et en conseil** en gouvernance, gestion des risques, gestion de crise ou encore en usages, confiance numérique et management du changement ;
- 11 positionnées sur les **approches technologiques de la cybersécurité** (sécurisation et architecture SI, tests de résilience et renforcement des SI, gestion des incidents de cybercriminalité, cyberdéfense active) ;
- 12 couvrant **l'ensemble du spectre des compétences,** des interventions technologiques à l'audit et au conseil.

Une entreprise sur deux propose également un **service de sensibilisation/formation** et de **diagnostic des besoins** clients en cybersécurité. Au sein de l'offre de service technologique, la cyberdéfense/cyberattaque (précisée par

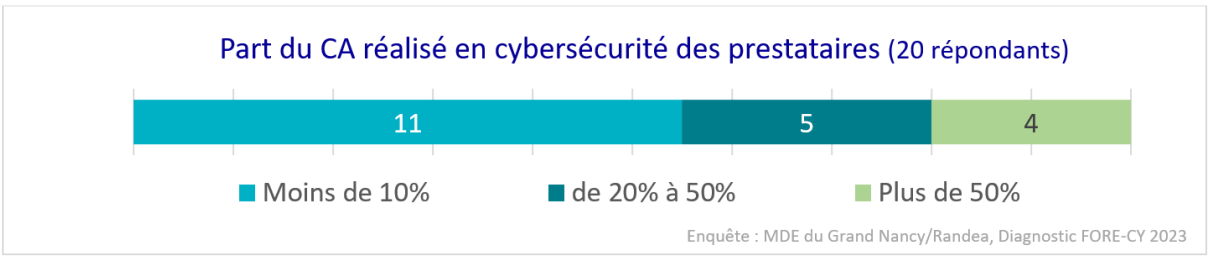
les mots-clés *honeypots, hack-back, activité militaire*) est naturellement moins développée ; le socle des outils de sécurisation et de l'architecture SI est le service le plus répandu (47% de l'ensemble de l'échantillon, soit 60% des acteurs concernés par une offre technologique).



L'écosystème métropolitain[11] semble légèrement plus polarisé sur les services technologiques de la cybersécurité :



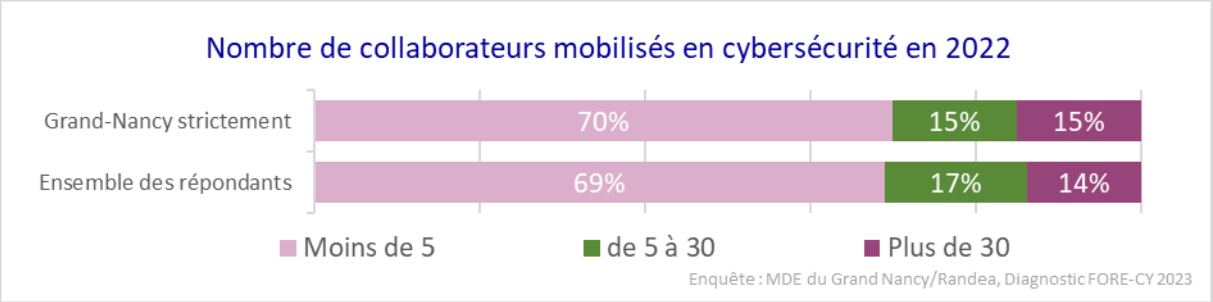
Les acteurs spécialisés dans la cybersécurité sont minoritaires ; seules 4 entreprises prestataires de l'échantillon réalisent plus de 50% de leur chiffre d'affaires en cybersécurité, les *pure players* étant assez peu nombreux en cybersécurité[12].



70% des acteurs du territoire ont mobilisé moins de 5 collaborateurs pour leurs activités Cyber ; 15% en ont mobilisé plus de 30 et constituent des acteurs majeurs de l'écosystème territorial.

[11] Il est rappelé que pour étoffer le retour d'expérience sur les compétences et la vision d'avenir, le diagnostic FORE-CY a été élargi à des entreprises prestataires des villes voisines du Grand Nancy ; ces acteurs constituent un quart des répondants.

[12] N.B. Au sein de l'« Enquête auprès des professionnels des métiers de la cybersécurité 2021 » de l'Observatoire des métiers de la cybersécurité, **23%** des répondants du Grand Est relèvent de structures spécialisées en cybersécurité, contre 39% dans les Hauts-de-France et même 53% en Bretagne, signe positif du dynamisme de la filière sur ce territoire.



L'écosystème cybersécurité du Grand Nancy apparaît ainsi diversifié à tous points de vue : l'ancienneté de positionnement sur la cybersécurité, la spécialisation Cyber (technologique, conseil ou mixte), la proportion du CA réalisé en cybersécurité comme la taille et le nombre de collaborateurs Cyber. L'enquête permet d'établir que **750 à 875 professionnels sont mobilisés sur le territoire nancéien en Cybersécurité[13] :**

- **23%** ont moins de 30 ans, soit une proportion proche des répondants à l'enquête 2021 ANSSI/DGEFP auprès des professionnels des métiers de la cybersécurité (3 points de moins stricto sensu) ;
- **17%** ont plus de 50 ans (2 points de plus que l'étude nationale 2021) ;
- **14%** sont des femmes, soit 3 points de plus que la proportion de l'enquête nationale 2021 ;
- **660 à 775** ont un profil de techniciens, ingénieurs ou experts en technologies Cyber, **90 à 100** ont un profil juridique ou conseil à expertise Cyber.

À ces 750 à 875 professionnels s'ajoutent 145 à 170 collaborateurs déclarés employables sur les sujets Cyber en cas de surcroît de charge[14], soit un écosystème local fort de 900 à un peu plus de 1 000 professionnels en donnée de cadrage.

Afin de conforter cette estimation, en l'absence de données de référence, tant à l'échelle locale que nationale, un modèle de simulation RH a été élaboré dans le cadre de la mission FORE-CY. Il s'agit d'une reconstitution de l'écosystème sur les années 2000-2023 tenant compte du nombre et de l'ancienneté moyenne des entités, du taux annuel moyen de recrutement *versus* les départs de profils Cyber au sein de l'écosystème local[15]. Cette maquette de simulation permet de démontrer la cohérence d'un écosystème fort de 660 à 875 profils Cyber avec une moyenne de 8,4 collaborateurs par entité. Le consortium FORE-CY a donc validé cette estimation comme un résultat significatif de la mission, attendu dans la réponse à l'AMI Compétences et Métiers d'avenir Cybersécurité.

Résultat-clé : Sur la base de l'enquête menée auprès des employeurs de profils Cyber et d'un modèle de simulation reconstituant l'écosystème Cyber sur la période 2000-2023, l'équipe FORE-CY estime que **750 à 875 profils Cyber ont été impliqués sur des projets de cybersécurité au cours de l'année 2022, à temps plein ou partiel,** et que **l'écosystème nancéien est fort au total de 900 à un peu plus de 1000 professionnels Cyber.**

2| Besoins des entreprises et flux RH Cyber au sein du territoire

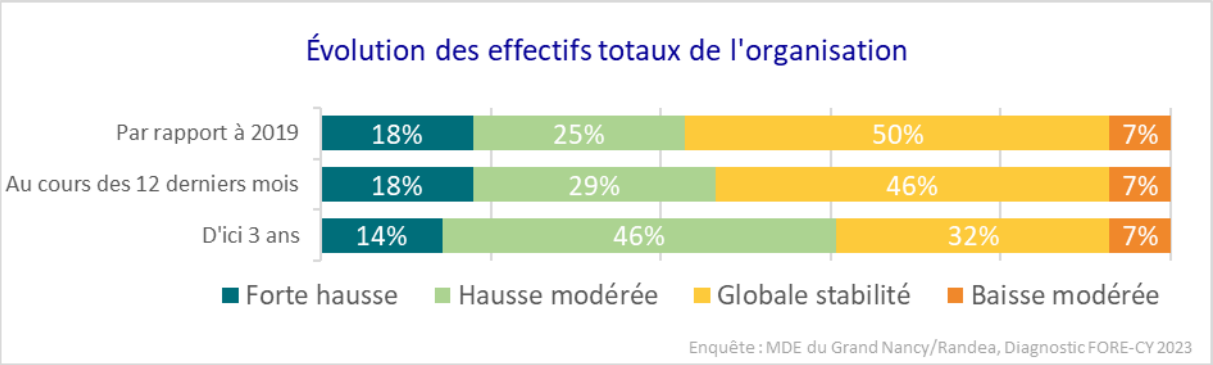
Très divers dans leur profil et positionnement Cyber, **les employeurs du diagnostic territorial FORE-CY le sont aussi en matière de dynamiques RH.** Ainsi, si ¼ des acteurs ont connu une hausse modérée de leurs effectifs par rapport à 2019 comme ces douze derniers mois et près de 20% font état d'une forte hausse de leurs effectifs tant depuis 2019 que depuis un an, la moitié des employeurs fait part d'une stabilité de ses effectifs. **Les**

[13] Estimation obtenue par retraitement des données de l'enquête en tenant compte des réponses relatives au « nombre de salariés mobilisés pour les activités de cybersécurité au cours de l'année 2022 », pas nécessairement à temps plein sur l'activité Cyber, pour les répondants situés strictement sur le territoire de la métropole du Grand Nancy, N.B. Les quelques réponses aberrantes en « 0 » ont été corrigées de manière normative en « 1 » donnant une moyenne de 8,5 collaborateurs par entité (avec un effet de correction de 0,2 point). La moyenne a ensuite été multipliée par le nombre d'entités identifiées sur le territoire, à savoir 104 permettant d'estimer le contingent à un volume de 884 minoré à titre conservatoire à 875 collaborateurs Cyber mobilisés au cours de l'année 2022. Par ailleurs, les acteurs ayant répondu à la sollicitation d'enquête du projet FORE-CY étant susceptibles d'être parmi les plus dynamiques de l'écosystème, un second facteur correctif a été appliqué pour disposer d'une évaluation basse du contingent de collaborateurs Cyber ; il s'agit d'un facteur normatif de -15%.

[14] Ils sont en moyenne de 1,6 collaborateurs pour les répondants situés strictement sur le territoire de la métropole du Grand Nancy.

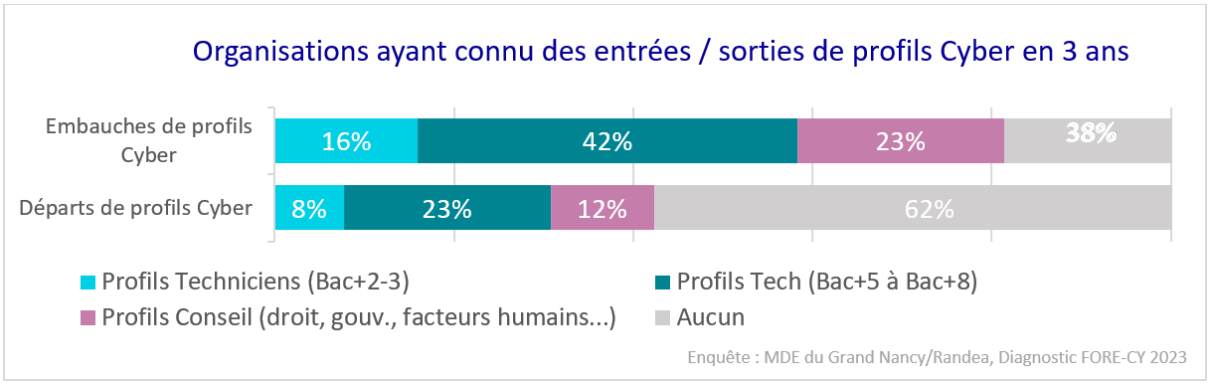
[15] La simulation s'avère plus cohérente en retenant les taux moyens de recrutement/départ des 30 répondants au diagnostic FORE-CY que les déclarations des 22 acteurs du territoire nancéen stricto sensu (effet d'aléas statistique ou de période plus prononcé concernant les trois dernières années marquées par la crise COVID).

anticipations à 3 ans sont davantage positives : 60% des acteurs envisagent une croissance modérée à forte de leurs effectifs d'ici 3 ans.



Qu'en a-t-il été des profils des spécialités Cyber ? Si comme le précise le graphique précédent, près de 60% des employeurs disent avoir connu une globale stabilité, voire baisse, de leurs effectifs totaux, **seuls 38% n'ont recruté aucun profil Cyber au cours des 3 dernières années : une majorité d'employeurs mise donc sur ces profils**, y compris lorsque leurs effectifs sont globalement constants**.**

Environ 40% des employeurs de profils Cyber du Grand Nancy ont recruté des ingénieurs ou docteurs de spécialité technologique et 16% des techniciens ; 23% ont recruté des profils de type conseil. **Comme partout en France, les employeurs privilégient assez fortement les Bac+5 et plus, près de 85% des employeurs n'ayant recruté aucun profil de techniciens au cours des 3 dernières années.**



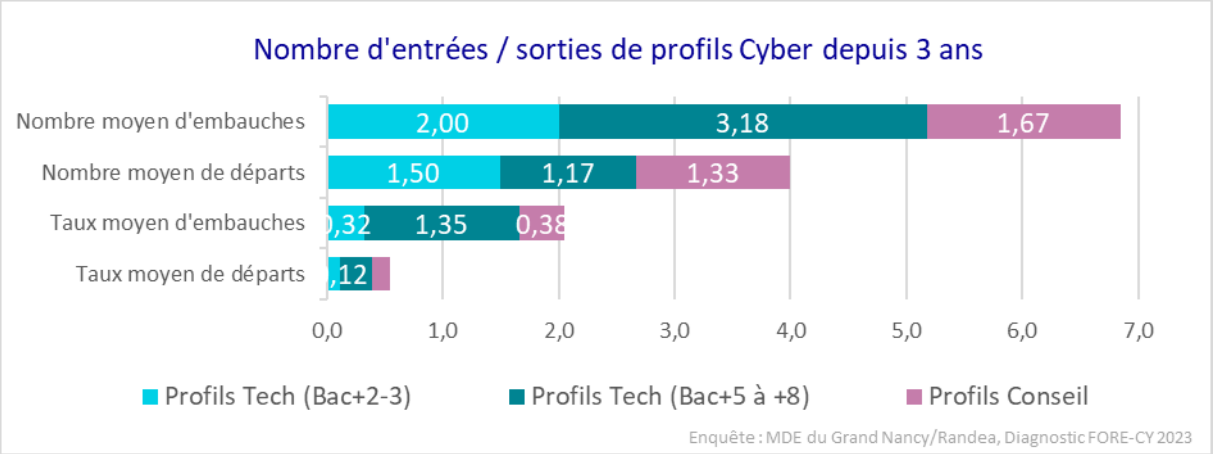
Note de lecture : Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

Les départs de profils Cyber concernent une proportion deux fois moindre d'employeurs que les entrées, et ce quel que soit le profil ciblé. 60% des employeurs n'ont connu aucun départ de collaborateurs en cybersécurité au cours des trois dernières années.

Ces tendances locales se traduisent dans les volumes d'entrées/sorties :

- le nombre moyen d'embauches est systématiquement supérieur aux nombre des départs (sur la base des seuls acteurs concernés par ces flux RH), ce qui traduit **une progression des effectifs Cyber sur le territoire** ;
- Les établissements ayant recruté l'un des profils au cours des 3 dernières années, ont ainsi accueilli en moyenne 3,2 ingénieurs ou docteurs, 2 techniciens et 1,7 consultant en organisation ou facteurs humains[16] ;
- Ramenés à l'ensemble des employeurs ayant ou non connu des entrées/sorties, la propension moyenne à avoir recruté s'établit à **1,3 ingénieur ou docteur par entité, 0,3 technicien et 0,4 consultant[17],** les écarts se creusant entre les profils ingénieur ou docteur de spécialité technologique d'une part, les techniciens et les profils conseil d'autre part, confirmant la **polarisation du recrutement sur les profils de niveau Bac+5 à Bac+8**.

[16] Concernant les acteurs du Grand Nancy stricto sensu qui ont recruté au cours des 3 dernières années, ils ont accueilli en moyenne 3,8 ingénieurs ou docteurs, 2 techniciens et 1,0 consultant, signe de la polarisation légèrement plus accentuée sur les profils techniques, avec potentiel effet COVID.
[17] Ces valeurs passent à 1,2 ingénieur, 0,2 technicien Tech et moins de 0,1 profil conseil pour les acteurs du Grand Nancy stricto sensu.



Ramenés à l'échelle métropolitaine :

- les acteurs auraient ainsi finalisé entre 150 et 210 recrutements au cours des trois dernières années[18], soit **entre 50 et 70 recrutements par an** : 8 à 10 techniciens et 40 à 45 Bac+5 sur des compétences technologiques, ainsi que 2 à 10 profils consultants ;
- **des départs** seraient intervenus pour 45 à 55 salariés en trois ans, soit 15 à 20 par an ;
- sur la base d'un taux normatif de 15% à 30% de perte pour la filière nancéienne (personnes quittant la région et/ou ne souhaitant pas poursuivre en cybersécurité), le besoin annuel de l'écosystème nancéen s'établit à 40 à 50 nouveaux profils Cyber par an. Il s'agit de la cible de sortants des écoles et organismes de formation à fidéliser sur le territoire. En faisant l'hypothèse d'un taux de rétention locale voisin de 15 %, il est nécessaire de former 250 à 330 spécialistes Cyber chaque année pour répondre aux besoins actuels de l'écosystème (les arrivées par mobilité géographique sur le territoire grand nancéien étant négligées dans ces valeurs de cadrage).

Résultat- clé : L'approche méthodologique mise en place conduit à estimer que **250 à 330 spécialistes Cyber, ou talents capables de rejoindre la Cyber, doivent être formés par l'écosystème de formation local pour répondre aux besoins actuels des employeurs de profils Cyber.**

3| Les besoins en compétences des employeurs : une approche novatrice pour la filière

L'étude des besoins locaux en compétences de l'écosystème Cyber a été menée en considérant plusieurs variables[19] :

- **Le besoin en compétences « en absolu »** (en rose pâle) : il est le négatif du pourcentage des entreprises n'ayant pas de besoins dans une compétence cible (en gris) ; il renseigne sur la volumétrie globale du besoin et permet de discriminer les compétences les plus attendues des entreprises en valeur absolue.
- **Le besoin déjà couvert** (en rose foncé) renseigne quant à lui sur les efforts déjà réalisés par les entreprises ; il est une fraction du besoin total (d'où la superposition) et décrit les compétences disponibles au sein de l'écosystème local ; afin de préserver une certaine confidentialité et pour ne pas alourdir l'enquête, les besoins sont exprimés en « acteurs exprimant/ayant déjà couvert au moins un besoin dans la compétence cible » et non en « nombre de collaborateurs ».
- Ces deux variables donnent par différence une bonne idée **des besoins restant à couvrir** (partie rose claire supérieure à la partie rose foncée), c'est-à-dire de la part d'entreprises exprimant un besoin non couvert dans une compétence cible ; stricto sensu, une entreprise peut avoir partiellement couvert son besoin et rester en

[18] Valeur basse obtenue en ne considérant que les acteurs du territoire métropolitain stricto sensu, borne supérieure en retenant l'ensemble des répondants au diagnostic FORE-CY.

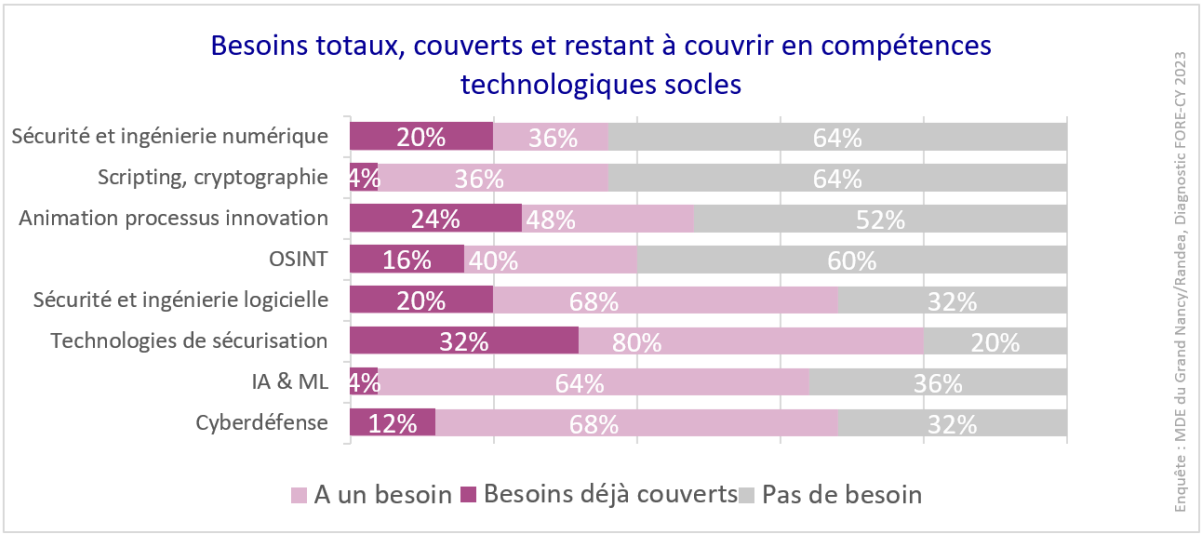
[19] L'approche est inspirée de celle développée par ML des Robert, en 2020-2021 en tant qu'associée senior du BIPE, pour l'Observatoire Régional des Compétences Industrielles (ORCI) Occitanie sur les compétences montantes de l'aéronautique, observatoire appuyé depuis 2022 par Randea. Retrouvez l'étude complète 2023 dont les compétences en cybersécurité à l'adresse suivante : https://www.orci-occitanie.fr/etudes/enquete-sur-levolution-du-besoin-en-competences-de-la-filiere-aeronautique-spatiale-en-occitanie

attente de compétences complémentaires ; dans les tableaux, le pourcentage d'entreprises exprimant un besoin restant à couvrir est donc obtenu en identifiant celles qui ont répondu envisager recruter, former ou sous-traiter d'ici 12-36 mois (au moins un de ces leviers retenu).

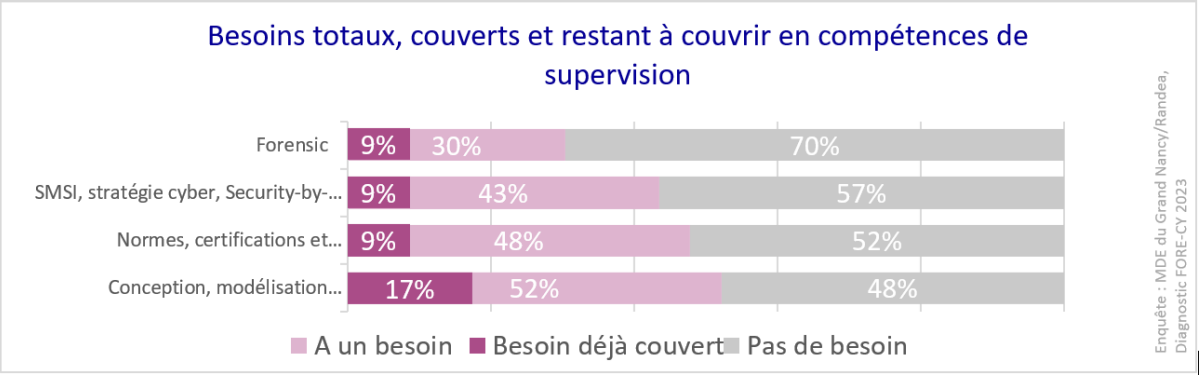
- Ces variables permettent d'identifier **les compétences dont le taux de couverture est le plus bas** ; ce sont les compétences montantes ou difficiles à pourvoir vis-à-vis desquelles **l'écosystème de formation devra être vigilant** à bien répondre aux besoins en vue de faciliter le recrutement des entreprises ou la formation de leurs collaborateurs en poste.
- Quant aux compétences restant à couvrir, le diagnostic a testé **trois principaux leviers** pour y répondre : **la formation** des collaborateurs déjà en poste, **le recrutement** ou **la sous-traitance** ; ces leviers renseignent sur les besoins de la filière adressés à l'écosystème de formation pour les deux premiers leviers, mais aussi à la filière elle-même concernant la sous-traitance.

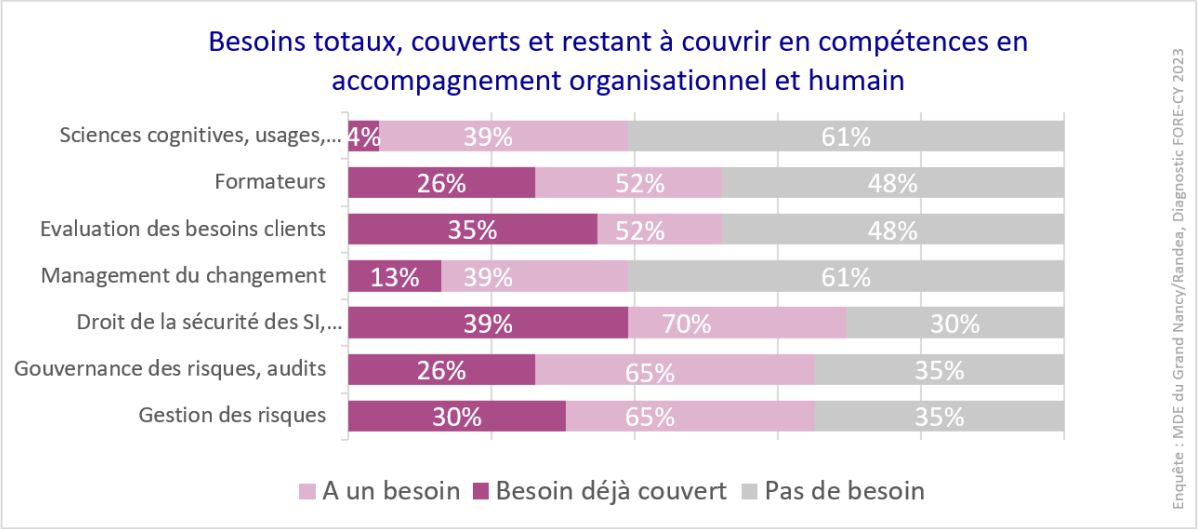
Les besoins exprimés dans l'enquête agrègent ceux des concepteurs de services et produits et ceux des utilisateurs qui intègrent des solutions tierces (comme prestataires ou en interne au sein d'une entité disposant d'un pôle cybersécurité). Les compétences attendues par plus de 60% des employeurs de profils relèvent de deux familles (cf. trois graphiques ci-dessous de couleur grise et rose) : les technologies dites « socles » de la cybersécurité et l'accompagnement de l'organisation, à savoir :

- La connaissance, la veille des **technologies de sécurité et la configuration des outils associés** ou de l'architecture (pare-feu, anti-virus, techniques d'authentification …) qui arrive en tête des besoins de **80%** des acteurs de l'écosystème ;
- Le développement et l'**ingénierie logicielle sous l'angle de la sécurité** (vulnérabilités logicielles…), la **cyberdéfense**[20] entendue comme la connaissance et la veille des techniques d'attaque et d'intrusion, des vulnérabilités des environnements, pratique d'analyse des flux réseaux et d'analyse de journaux, ainsi que les capacités en **intelligence artificielle** (IA) et **Machine Learning** avec un besoin partagé par 64% à 68% des employeurs ;
- Côté accompagnement de l'organisation, les compétences juridiques arrivent en tête s'agissant du **droit lié à la sécurité des SI, à la protection des données** (normes, standards, PRA/PCA, RGPD, etc.) **ou aux menaces** avec un besoin exprimé par 70% des acteurs de l'écosystème, juste devant **la gestion des risques** d'une part, la connaissance de **la gouvernance des risques, la veille des normes et des standards** (maîtrise des méthodologies d'audits et des normes spécifiques au domaine de la cybersécurité) d'autre part, besoins qui concernent 65% de l'écosystème Cyber.



[20] Cette notion recouvre des compétences en cyberprotection et des compétences en cyberattaque/cyberdéfense liées aux activités régaliennes, notamment militaires.





Les trois graphiques qui précèdent permettent également d'identifier **les compétences sur lesquelles les entreprises ont d'ores et déjà investi** (en rose foncé), pour lesquelles elles disposent de collaborateurs pour répondre à tout ou partie de leurs besoins en ce domaine :

- **Les compétences juridiques[21] :** près de 40% des entreprises de l'écosystème Cyber local en disposent, **signe de leur caractère structurant** ;
- Les capacités d'**évaluation des besoins clients** (analyse bénéfices/risques et évaluation financière) pour un tiers des employeurs, ainsi que les capacités de **gestion des risques** (30% des employeurs) ;
- Les **technologies de sécurité** pour 30% également de l'écosystème.

Ce « palmarès » des compétences les plus disponibles au sein de l'écosystème local traduit d'une part le **positionnement de l'écosystème au sein de la chaîne valeur**, centré pour un grand nombre d'acteurs sur le déploiement d'outils et de technologies de sécurisation développés par d'autres, et confirme d'autre part **l'importance de la problématique de l'accompagnement client** évoquée dans le diagnostic stratégique amont **et surtout l'importance de la maîtrise des enjeux juridiques liés à la cybersécurité.**

A l'inverse, trois compétences tranchent par leur criticité au sein de l'écosystème Cyber et appellent à être renforcées au vu des besoins exprimés. Il s'agit en premier lieu de :

- **l'IA et le Machine Learning :** seules 4% des entreprises du territoire disposent de compétences en ce domaine alors que 2/3 des entreprises estiment avoir besoin de ces profils, soit un taux de couverture de 6%, particulièrement faible ;

[21] Ces compétences visent les enjeux juridiques nationaux mais aussi l'incidence des régulations européennes et internationales (14 réglementations ou conventions internationales sont en préparation : IA Act européen, DORA I, Directive européenne NIS II, etc.).

- **le scripting et la cryptographie[22] :** avec là aussi 4% d'entreprises disposant de compétences en ce domaine pour 1/3 d'entreprises estimant partager ce besoin, soit un taux de couverture de 11% ; l'avènement de l'aire de l'IA pourrait apporter une réponse rapide aux besoins de scripting, déjà assez bien maîtrisés par certaines IA, ce qui renforce encore les besoins en compétences en IA/ML ;
- **les sciences cognitives et comportementales, les compétences en usages, confiance numérique utilisateurs, UX,** etc. : en ce domaine également, seules 4% d'entreprises Cyber locales estiment disposer de ces compétences alors qu'elles sont 40% à en exprimer le besoin, soit un taux de couverture de 11%.

Le diagnostic des compétences réalisé dans le cadre de l'étude FORE-CY permet enfin d'établir **le classement des compétences les plus en attente** voire critiques de l'écosystème**,** c'est-à-dire les compétences rassemblant le plus d'acteurs exprimant avoir un besoin encore non couvert (en tout ou partie) en ce domaine. Le tableau ci-dessous en présente la liste hiérarchisée en fonction de l'intensité du besoin résiduel (colonne 3) :

- plus le nombre d'acteurs exprimant un besoin est élevé (colonne 1) et moins le taux de couverture est fort (colonne 2), plus la compétence se positionne en haut de classement (avec un taux élevé de besoin résiduel, colonne 3 ou écart entre le rose clair et le rose foncé sur les trois graphiques précédents) ; cette situation est tout particulièrement le cas de l'IA et du ML ;
- à l'inverse moins elle est répandue et plus elle est déjà couverte, plus la compétence se positionne en bas de classement : c'est par exemple le cas du développement de la sécurité et de l'ingénierie numérique pour systèmes embarqués et autres objets connectés, segment de la chaîne de valeur sur lequel l'écosystème local est peu positionné.

En complément des compétences déjà citées dans les premières étapes d'analyse et qui apparaissent en gras dans la colonne 1 ou en rouge dans la colonne 2 :

- La connaissance et la veille des **normes, certifications et évaluations sécuritaires** de produits (ISO, PCI, DSS, Critères Communs, CPSn, etc.) apparaît en haut de tableau ;
- La **conception et modélisation des architectures** liées à la sécurité ainsi que le management de la sécurité de l'information (**SMSI**), les techniques d'analyse des risques de sécurité, la *Security-by-design* figurent en milieu de tableau.

	Importance du besoin (% employeurs concernées)	**Taux de couverture du besoin**	**Intensité du besoin résiduel** (en % d'employeurs)
IA et **Machine Learning**...	**64%**	**6%**	60%
Cyberdéfense : techniques d'attaque et intrusion, vulnérabilités des environnements, analyse des flux réseaux et de journaux	**68%**	18%	56%
Connaissance, veille, mise en œuvre des **technologies de sécurité** (pare-feu, anti-virus, techniques d'authentification ...)	**80%**	40%	48%
Développement et **ingénierie logicielle** (vulnérabilités logicielles...)	**68%**	29%	48%
Connaissance et veille des **normes, certifications et évaluations sécuritaires** de produits (ISO, PCI, DSS, Critères Communs, CPSn, etc.)	48%	18%	39%
Connaissance de la **gouvernance des risques**, veille des normes et standards Cyber, méthodes d'audits	**65%**	40%	39%
Gestion des risques	**65%**	**47%**	35%
Conception et modélisation des architectures liées à la sécurité	52%	33%	35%
Management de la sécurité de l'information (**SMSI**), techniques d'analyse des risques de sécurité, Security-by-design	43%	20%	35%

[22] L'enquête menée ne permet pas d'expliciter davantage les compétences recouvertes par la notion de « cryptographie » ; un focus qualitatif pourrait permettre d'affiner les besoins entre conception de nouvelles solutions avec l'arrivée du quantique et de l'IA notamment (côté concepteurs de solutions, le domaine étant en pleine révolution) ou de l'assistance à la configuration, au déploiement de mécanismes cryptographiques, de distribution de clé (côté utilisateurs), notamment appliqués à la cyberprotection des communications et des échanges.

Sciences cognitives et comportementales, usages, confiance numérique utilisateurs, UX, etc.	39%	**11%**	35%
Droit lié à la sécurité des SI, à la protection des données (normes, standards, PRA/PCA, RGPD, etc.) ou aux menaces	**70%**	**56%**	30%
Rétro-ingénierie, **Scripting, cryptographie**...	36%	**11%**	32%
(suite)	**Importance du besoin** (% employeurs concernées)	**Taux de couverture du besoin**	**Intensité du besoin résiduel** (en % d'employeurs)
Formateurs en cybersécurité (pour publics non experts ou initiés)	52%	50%	26%
Management du changement, transformation, méthodes d'intelligence collective (Living Lab...), etc.	39%	33%	26%
Exploitation des sources ouvertes de manière sécurisée (**OSINT**)	40%	40%	24%
Animation du processus d'**innovation technologique**	48%	**50%**	24%
Forensic : connaissance des outils d'analyse, de collecte de preuves et des procédures légales	30%	29%	22%
Évaluation des **besoins clients**, analyse bénéfices/risques et approche financière	52%	**67%**	17%
Développement de la sécurité et **ingénierie numérique** (systèmes embarqués...)	36%	**56%**	16%

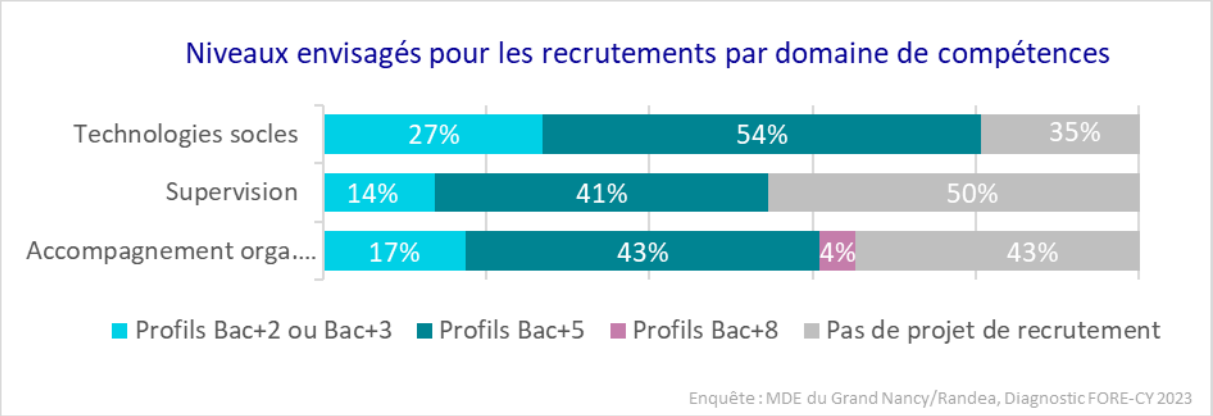
Résultats-clés : Le diagnostic des compétences met en avant **la centralité des compétences juridiques** comme l'une des trois composante des besoins en compétence Cyber avec les expertises technologiques et les expertises en gestion des risques. Il pointe **la criticité** des besoins locaux en **IA/ML**, scripting/**cryptographie**, **approches cognitives et comportementales** appliqués à la cybersécurité vis-à-vis desquels un effort doit être réalisé par les organismes de formation et les employeurs afin de s'assurer de disposer des compétences-clés de court et aussi moyen terme.

Après s'être focalisés pour un grand nombre d'entre eux sur le déploiement d'outils et solutions technologiques, les employeurs de l'écosystème local expriment leur intention ou a minima leur compréhension qu'ils gagneraient à **se renforcer également dans les compétences d'avenir** que sont l'IA et le *Machine Learning*, la **cyberdéfense** (techniques d'attaque et intrusion, vulnérabilités des environnements, analyse des flux réseaux et de journaux), la maîtrise des **normes et certifications**, la **gouvernance et la gestion des risques**. Les compétences en conception et modélisation des **architectures** liées à la sécurité et en **systèmes de management** de la sécurité des informations sont également clés.

4| Les intentions de recrutement et de formation des employeurs Cyber

Les employeurs disposent de trois principaux leviers pour répondre à leurs besoins en compétences non couvertes : **la formation** des collaborateurs déjà en poste (en bleu), **le recrutement** (en vert) ou **la sous-traitance** (en jaune) ; ces leviers renseignent sur les besoins de la filière adressés à l'écosystème de formation pour les deux premiers leviers, mais aussi à la filière elle-même concernant la sous-traitance. Avant de présenter les résultats pour chacune des 19 compétences cibles, des éléments complémentaires ont été sollicités par domaine de compétences (technologies socles, supervision, accompagnement organisationnel et humain).

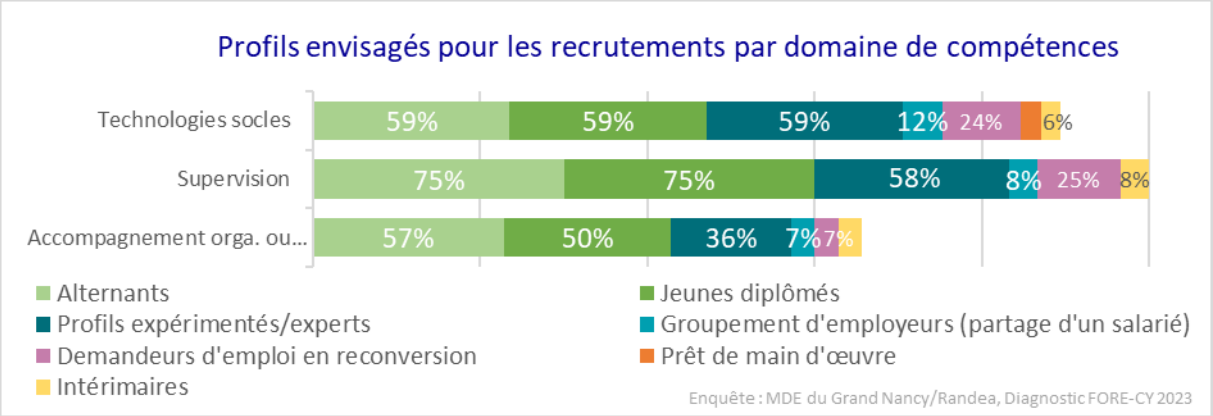
À l'échelle des domaines de compétences, **les technologies socles rassemblent le plus d'intentions de recrutement :** 65% des employeurs de l'écosystème envisagent au moins un recrutement dans ce domaine d'ici 12 à 36 mois : plus de la moitié des acteurs ciblent pour ce faire des collaborateurs de niveaux Bac+5, un quart visent des profils de niveau Bac+2 ou Bac+3. Viennent ensuite des intentions de recrutement en **accompagnement organisationnel et humain** pour plus de 55% des acteurs, ainsi que dans les compétences de **supervision** pour un acteur sur deux. Dans ces deux domaines les personnes de niveau Bac+5 sont nettement privilégiées.



N.B. Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur et tronqué à 100%

En matière de supervision, les profils juniors sont nettement privilégiés (cf. Graphique ci-dessous) : ¾ des employeurs envisageant un recrutement souhaiteraient accueillir des alternants ou recruter des jeunes diplômés. Les profils expérimentés intéresseraient également une majorité d'employeurs, dans les trois domaines et plus encore dans les deux champs technologiques.

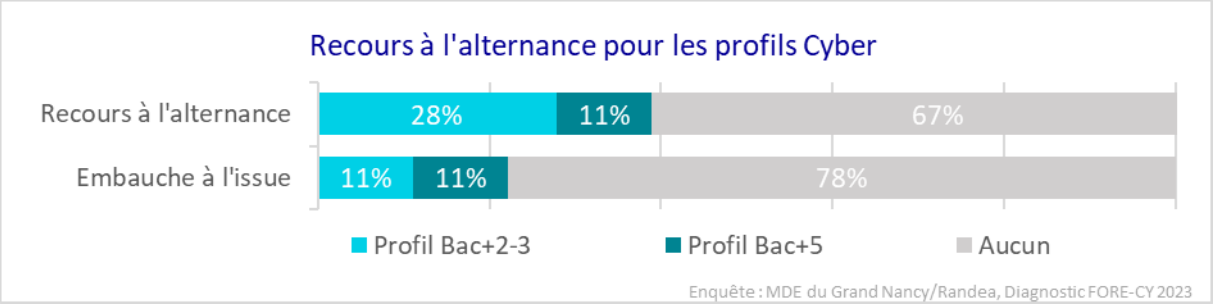
Point-clé : un quart des employeurs exprimant un besoin de recrutement en compétences technologiques se dit ouvert aux demandeurs d'emploi ayant réalisé un parcours de reconversion, c'est paradoxalement plus marginal pour les postes d'accompagnement organisationnel ou humain.



N.B. Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

Le recours à l'alternance est répandu : **un tiers des établissements du diagnostic déclare accueillir des alternants** : 30% des acteurs ont recruté des alternants de niveau 5 ou 6, techniciens Cyber ; 11% des acteurs des alternants de niveau 7 de type ingénieur. Cet écart tient à la typologie des employeurs, les très petites structures n'ayant pas le volume d'activité ou la notoriété suffisante pour accueillir des Bac+5 en alternance.

Le taux de conversion de l'alternance en emploi pérenne est en revanche plus favorable aux profils de niveau 7 : si la totalité des entreprises ayant accueilli des alternants de niveau Bac+5 en ont recruté au moins 1 de façon pérenne, ce taux chute à 40% pour les profils techniciens. Seuls 11% des acteurs ont pérennisé la relation d'alternance par une embauche réussie. Cette forte « déperdition » tient à la volonté d'une partie des alternants de poursuivre leurs études au-delà du Bac+2-3 d'une part, à la préférence de certains employeurs de privilégier une rotation d'alternants sur les postes de niveau technicien afin d'optimiser leur masse salariale d'autre part.



N.B. Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur et tronqué à 100%

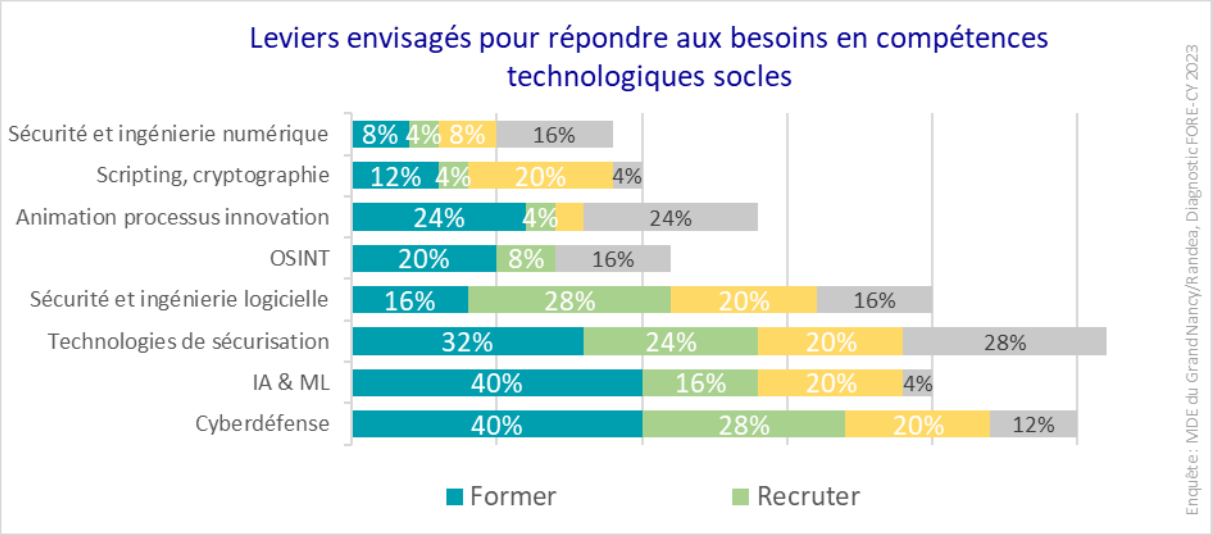
Résultat-clé : Enfin, en zoomant au plus fin, les compétences dans lesquelles un nombre élevé d'employeurs envisagent de **recruter** (en vert au sein des trois histogrammes ci-dessous) sont, selon l'enquête employeurs FORE-CY, par ordre décroissant :

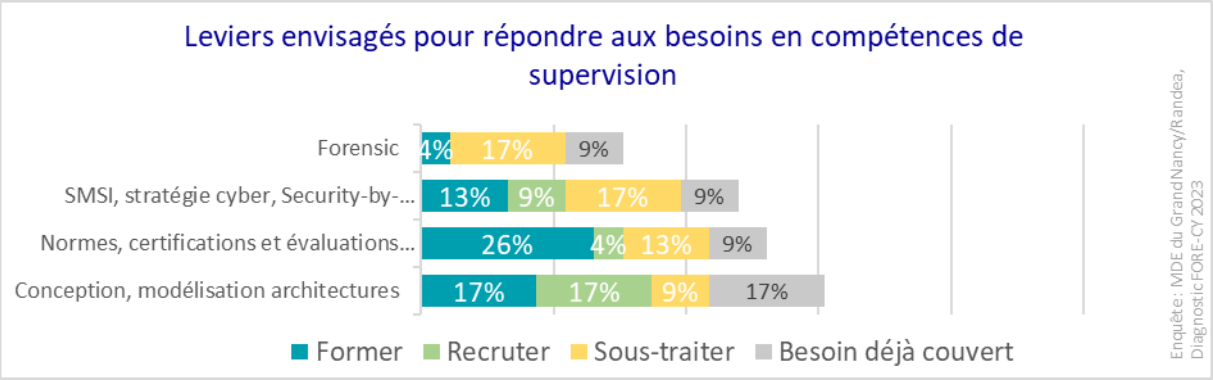
- Top 1. **La cyberdéfense & la sécurité et ingénierie logicielle** (28% d'employeurs ayant une intention de recrutement) ;
- Top 2. **Les technologies de sécurisation socles** (pare-feu, anti-virus, techniques d'authentification ... 24% d'intentions de recrutement)
- Top 3. **La conception et la modélisation des architectures liées à la sécurité, l'IA/ML et les formateurs** (16% à 17% d'intentions de recrutement)

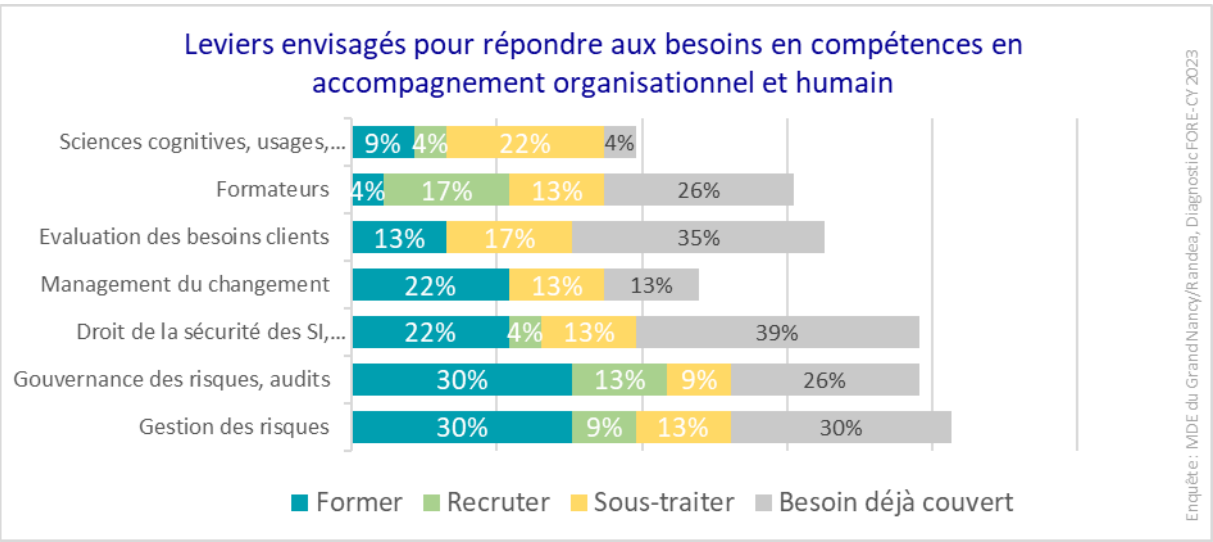
Résultat-clé : Les compétences dans lesquelles un nombre élevé d'employeurs envisagent de **former leurs collaborateurs** (en bleu canard dans les trois histogrammes ci-dessus) sont par ordre décroissant :

- Top 1. **La cyberdéfense & l'IA/ML** (40% d'employeurs ayant une intention de formation) ;
- Top 2. **Les technologies de sécurisation socles** (pare-feu, anti-virus, techniques d'authentification... soit 32% d'intentions de formation)
- Top 3. **La gouvernance et la gestion des risques (audit)** (30% d'intentions de formation).

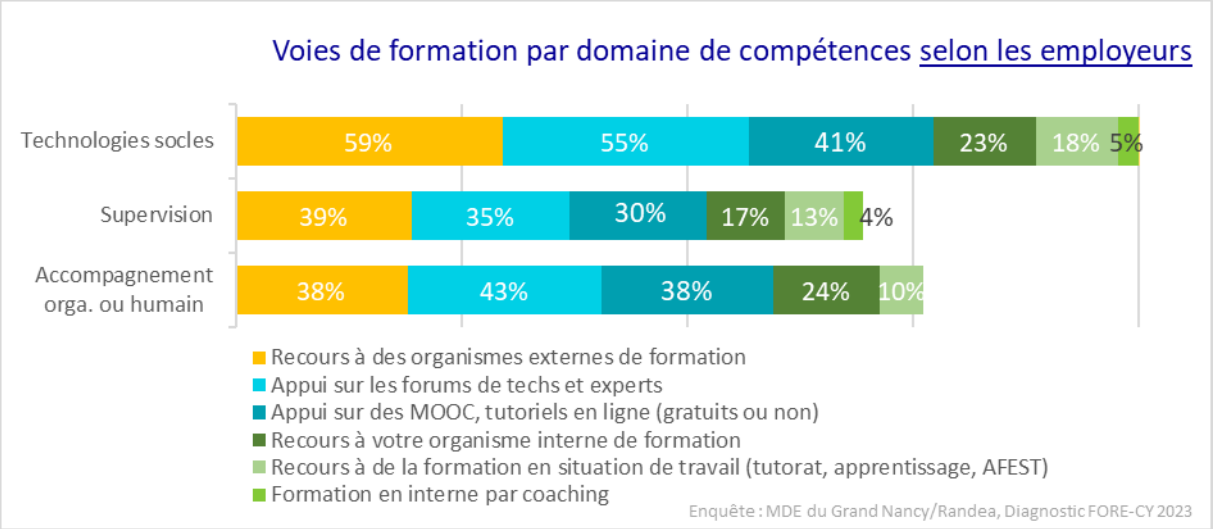
Il faut noter la **fréquence du recours à la sous-traitance** (en jaune) qui traduit le degré de technicité à maîtriser dans chaque domaine et la difficulté à y procéder en interne pour des petites structures. L'écosystème local gagnera donc à **opérer en réseau** de complémentarités. Pour les acteurs qui accepteront une évolution de leur taille critique, des consolidations entre acteurs pourraient intervenir.







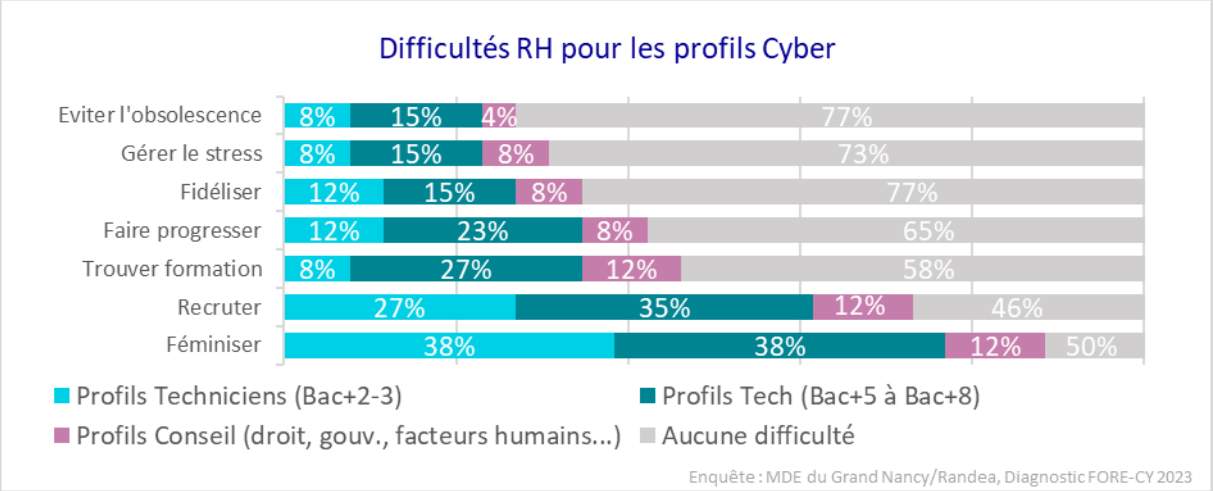
Les employeurs exprimant un besoin de formation de leurs collaborateurs à 12-36 mois envisagent pour 60% d'entre eux, de **recourir à des organismes de formation externes** pour leurs besoins en technologies socles, mais aussi d'avoir **une organisation structurée de formation interne** (organisme de formation interne, tutorat-mentorat, AFEST, coaching). Dans ces domaines où les technologies et le cadre normatif évoluent très rapidement, la formation passe aussi massivement par **l'autoformation** via des forums de techs ou d'experts ou les MOOC et autres tutoriels en ligne ; c'est particulièrement le cas pour les technologies socles, mais aussi l'accompagnement organisationnel et humain des entreprises.



N.B. Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

Pour conclure cette analyse, soulignons que deux difficultés RH tranchent par leur intensité : **la féminisation et les difficultés de recrutement invoquées par un employeur sur deux.** Le déficit de candidates touche de façon exacerbée les profils de techniciens ; il s'est accentué depuis la réforme du baccalauréat qui a eu pour incidence indirecte de réduire la proportion de filles poursuivant une spécialité « mathématiques » et s'orientant vers les profils scientifiques techniques.

Les difficultés de formation concernent également 40% des employeurs de profils Cyber, principalement pour leurs salariés de niveau Bac+5 à Bac+8.



N.B. Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur et tronqué à 100%

Ces réalités locales sont en ligne avec un marché du travail fortement sous tension à l'échelle de toute la France, notamment dans le secteur informatique et tout particulièrement pour le segment de la sécurité informatique.

L'analyse du marché du travail local en cybersécurité

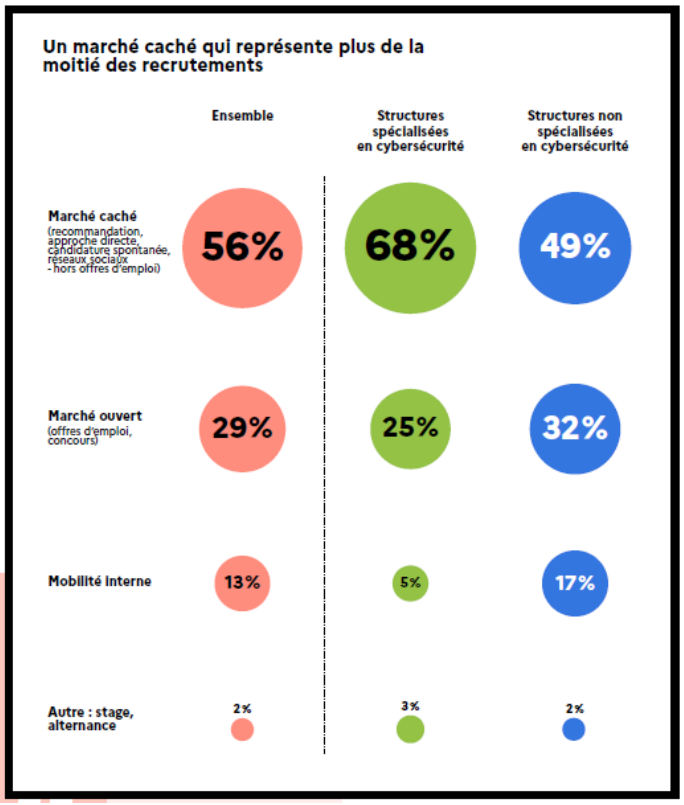
Les observatoires de l'emploi des fonctions IT font montre d'un déficit de candidats pour répondre aux 25 500 postes vacants pour 2023[23]. Les problématiques de sécurité informatique étant d'une sensibilité particulière, les postes qui en relèvent explicitement ou indirectement connaissent une forte demande. La cybersécurité est probablement le secteur de l'IT qui connaît la plus **forte pénurie de talents**.

Il manquerait environ 15 000 experts en sécurité informatique[24] sur des profils très variés, notamment des cryptologues, des architectes réseaux et des hackers éthiques. Ainsi, pour ne prendre qu'un exemple, « en plein boom, le nombre d'offres d'emplois d'experts en cybersécurité a augmenté de 30 % entre 2021 et 2022 »[25].

Par ailleurs, **le marché du travail en compétences Cyber se caractérise par l'importance du marché caché** qui représente près de 70% des pratiques de recrutement des structures spécialisées en cybersécurité, près de 50% pour les autres structures selon l'enquête 2021 de l'observatoire des métiers de la cybersécurité. En effet, il est fréquent en ce domaine, de procéder à des recrutements au sein des cohortes des écoles de formation ou via les réseaux sociaux sans publication d'offres d'emploi.

L'étude statistique du marché du travail en est rendue délicate. Ce biais étant identifié, l'analyse des offres et demandes d'emploi auprès de Pôle Emploi apporte néanmoins un éclairage intéressant. Celle-ci a été réalisée sur trois périmètres :

Mode de recrutement



Source : *Enquête auprès des professionnels des métiers de la cybersécurité. Enquête 2021* | Observatoire des métiers de la cybersécurité

- les métiers de l'informatique à titre de cadrage,
- les métiers des systèmes d'information,
- et enfin les appellations métiers spécifiques incluant le terme « cybersécurité ».

[23] Source : Étude Adecco Analytics d'octobre 2022 citée par « Le recrutement dans l'IT en 2023 », 24/04/2023, https://www.free-work.com/fr/tech-it/blog/metiers-it/recrutement-tech-2023

[24] *Source :* Jean-Christophe Pitié, COO de Microsoft France cité par Clubic, 21/06/2022, https://www.clubic.com/pro/entreprises/microsoft/ actualite-427680 -il-manque-plus-de-15-000-experts-de-la-cybersecurite-en-france-microsoft.html

[25] Une tension sur le marché du travail créant même une vague de démissions des experts en cybersécurité selon l'étude réalisée par le cabinet Robert Half, cabinet de recrutement spécialisé, auprès des DSI en avril 2023, citée par « Le recrutement dans l'IT en 2023 », 24/04/2023, https://www.free-work.com/fr/tech-it/blog/metiers-it/recrutement-tech-2023

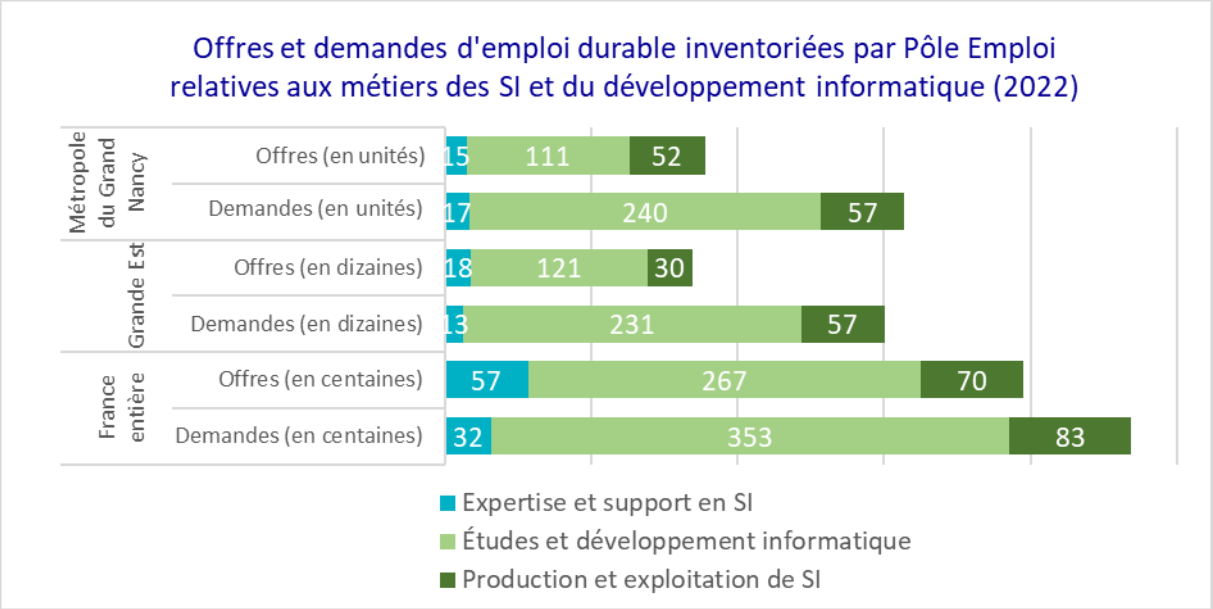
Concernant les offres de recrutement en informatique publiées via Pôle Emploi à l'échelle de la Métropole du Grand Nancy, si elles se sont réduites au global, elles ont néanmoins progressé de 9% en quatre ans, entre 2018 et 2022, pour ce qui concerne les offres durables d'emploi (d'une durée supérieure à 6 mois) et ce, par-delà même le développement des offres en marché caché. Les offres sont, du reste, devenues plus souvent **des offres d'emploi durable**, voire avec 93% et même 96%, des offres quasi exclusivement de plus de six mois pour les techniciens et ingénieurs ou cadres informatiques.

On constate également **un phénomène très net entre 2018 et 2022, de concentration des offres d'emploi publiées sur les profils d'ingénieurs ou cadres** d'étude, de recherche et développement en informatique ou chefs de projets informatiques passés de 19% des offres à 34%, avec un quasi doublement des offres d'emploi durables relatives à ce profil de qualification (de 53 à 104 offres). La part des offres d'emploi de niveau technicien informatique a en revanche fortement baissé en quatre ans, passant de 51% à 36%, là où celle des opérateurs progresse en structure, comme en volume (+4 points et +16 offres d'emploi durables, soit +27% en quatre ans).

	Nombre d'offres d'emploi		Nombre d'offres d'emploi durable		Taux d'OEE durables		Structure des OEE durables		Variation 2022/2018
Métropole du Grand Nancy	2018	2022	2018	2022	2018	2022	2018	2022	OEE durables
Employés et opérateurs en informatique	123	84 ↘	59	75 ↗	48%	**89%**	21%	25%	27%
Techniciens d'étude et de développement en informatique	55	46 ↘	47	43 ↘	85%	93%	17%	14%	-9%
Techniciens de production, d'exploit., d'installation, et de maintenance, support et services aux utilisateurs en informatique	157	71 ↘	95	66 ↘	61%	93%	34%	22%	-31%
Ingénieurs et cadres d'étude, R&D en informatique, chefs de projets informatiques	62	108 ↗	53	104 ↗	85%	96%	19%	**34%**	96%
Ingénieurs et cadres des télécommunications	30	19 ↘	23	15 ↘	77%	79%	8%	5%	-35%
Ensemble informatique	**427**	**328**	**277**	**303**	**65%**	**92%**	**100%**	**100%**	**9%**

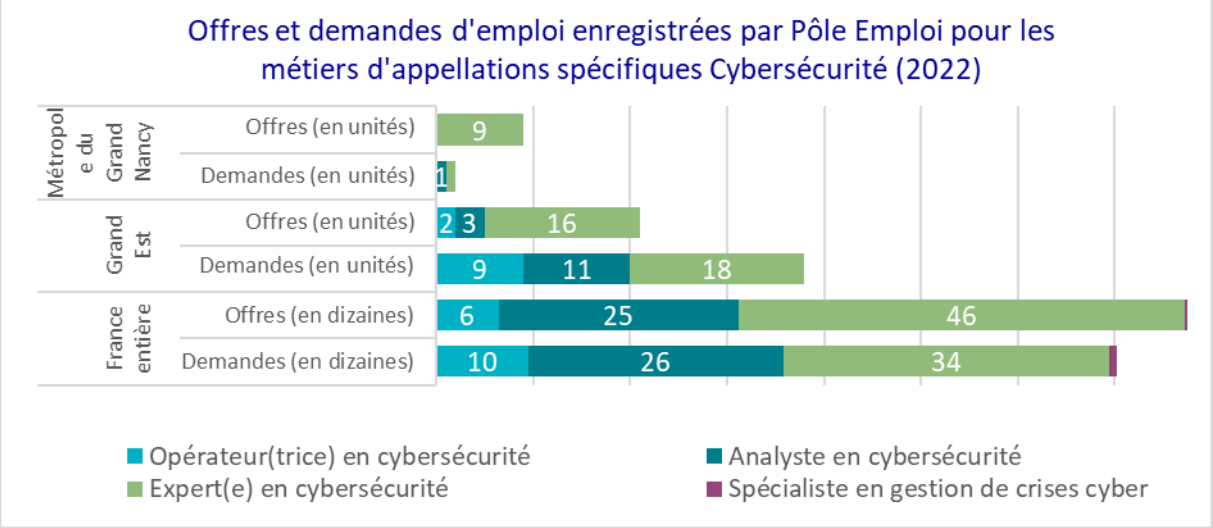
Source : Pôle emploi Grand Est, Service Études et Analyses | Champ : Offres d'emploi enregistrées par Pôle emploi, du 1er janvier au 31 décembre | Territoire : Métropole du Grand Nancy

En zoomant sur les trois métiers les plus en proximité avec les profils Cyber, à savoir l'expertise et le support en systèmes d'information, la production et l'exploitation de systèmes d'information ainsi que les études et le développement informatique, **les tensions relatives aux métiers des SI apparaissent au grand jour.** À l'échelle du Grand Nancy, comme du Grand Est et de la France entière, les offres d'emploi durables sont supérieures ou d'un ordre de grandeur proche du nombre de demandes d'emploi dans le domaine. Le vivier est ainsi insuffisant pour répondre aux besoins des employeurs.



Source : Pôle emploi Grand Est | Champ : Offres enregistrées par Pôle Emploi en 2022 / Demandes d'emplois inscrits à Pôle emploi au 31/12 en catégories A, B et C

En resserrant encore le zoom sur les quatre métiers d'appellations spécifiques Cyber, à savoir les opérateurs(trices), les analystes et les experts en cybersécurité, ainsi que les spécialistes en gestion de crises cyber, **les tensions sur le marché du travail apparaissent tout autant,** sur un contingent d'offres et demandes très réduit dans le Grand Est comme sur le territoire métropolitain. On notera plus particulièrement l'absence jusqu'alors de postes fléchés « Spécialiste en gestion de crises cyber » à toutes les échelles, y compris nationale avec seulement 2 offres publiées sur le marché ouvert sur ce profil en 2022 !



Source : Pôle emploi Grand Est | Champ : Offres enregistrées par Pôle Emploi en 2022 / Champ : Offres enregistrées par Pôle Emploi en 2022 / Demandes d'emplois inscrits à Pôle emploi au 31/12 en catégories A, B et C

La **polarisation du territoire métropolitain sur les profils technologiques de niveau ingénieur** identifiées dans l'enquête Employeurs FORE-CY est confortée par le profil des offres d'emploi enregistrées par Pôle Emploi sur le bassin : elles concernent exclusivement les expert(e)s Cyber.

Par ailleurs, sur la base d'un taux de marché ouvert moyen de 29% (source : Observatoire des métiers de la Cybersécurité cité *supra*), le nombre de postes Cyber ouverts au recrutement aurait été voisin de 30 en 2022 sur le bassin nancéien. Cette estimation est inférieure à la moyenne sur trois ans déclarée par les répondants de l'enquête FORE-CY : les répondants ont en effet pu retenir dans l'enquête FORE-CY des recrutements de profils davantage mixtes (par ex. réseau & compétence Cyber) ou à temps partiel qui peuvent ne pas être publiés comme des postes de spécialistes Cyber d'une part ; les répondants à l'enquête FORE-CY sont aussi vraisemblablement des acteurs plutôt plus dynamiques que le marché moyen (ce qui s'avère cohérent avec leur

mobilisation vis-à-vis de la démarche).

Pour conclure cette première partie consacrée à l'étude des besoins actuels en compétences de la filière cybersécurité de la Métropole du Grand Nancy, intéressons-nous aux critères de recrutement mis en avant par les employeurs de l'enquête FORE-CY.

Sur la première marche du podium des critères de recrutement, deux exigences usuelles figurent parmi les quatre critères de la moitié des employeurs : **la maîtrise d'une expertise de pointe d'une part, l'expérience utile d'autre part.** Ces deux qualités sont nettement différenciées du « diplôme adéquat » qui se positionne en fin de classement tout en étant l'un des quatre critères principaux d'un employeur sur six. Il y a donc place dans le secteur pour des profils aux parcours diversifiés pouvant faire montre de leur capacité d'apport.

Deux qualités comportementales arrivent sur la **deuxième marche du podium : la capacité à travailler en transverse / en équipe**, ainsi que **le savoir-être** général (ponctualité, savoir-vivre…) participent des principaux critères de recrutement de 35% des employeurs en cybersécurité.

Sur la troisième marche, se trouvent des capacités et savoir-faire fondamentaux **particulièrement précieux pour la performance et l'employabilité des profils Cyber : la curiosité, la pédagogie avec des non-experts** et la capacité à faire de **la veille**, trois capacités et appétences, corroborées par les remontées qualitatives tout au long du projet FORE-CY, clés pour l'orientation et le maintien durable dans le métier. La cybersécurité exige en effet d'aller au-delà de la simple mise en place et application de protocoles en ayant le souci de l'organisation qu'elle vient défendre et de son activité ; elle nécessite de s'intéresser et de veiller en continu à l'évolution des technologies, des menaces, des techniques, des offres à mettre en œuvre. La rencontre des univers – technologiques, menaces, l'organisation et son métier – exige de la pédagogie pour apprécier les besoins de sécurisation et de cyberdéfense de l'entreprise cliente, expliciter les alternatives possibles, la gouvernance et le protocole de confiance et résilience à mettre en place.

Ce tableau des critères prioritaires au recrutement en Cyber rend l'équation souvent complexe comme le souligne l'étude réalisée par le cabinet Robert Half, cabinet de recrutement spécialisé, auprès des DSI : « Les DSI se retrouvent face à une équation complexe. Leur principale difficulté réside dans le fait de trouver des talents dont les compétences sont en adéquation avec les profils qu'ils recherchent : entre technicité (cybersécurité, cloud, gestion de réseau…) et comportement (travail d'équipe, adaptabilité, motivation…). Des ressources rares sur le marché ! »[26]

Résultat-clé : Les cycles de formation doivent prendre en compte une troisième dimension en plus de la maîtrise d'une expertise technique (qu'elle soit technologique, juridique, en gouvernance et gestion des risques, en accompagnement des facteurs humains…) et des savoir-être fondamentaux clés (travail en équipe et en organisation formelle, adaptabilité face aux contraintes et besoins clients…) :

- **les aptitudes et appétences attitudinales** permettant d'établir et d'entretenir son expertise et son apport de valeur que sont dans la Cyber : la **curiosité**, la capacité à faire de la **veille** et la **pédagogie** avec des non experts.

[26] Étude citée par « Le recrutement dans l'IT en 2023 », 24/04/2023, https://www.free-work.com/fr/tech-it/blog/metiers-it/recrutement-tech-2023

Ces trois domaines complémentaires et distincts constituent autant de forces pour les collaborateurs et la filière cybersécurité dans son ensemble.

Cette vision rejoint le « top 5 des capacités transversales recherchées par les entreprises de la Branche pour les professionnels de la cybersécurité »[27] établi par EY pour le compte de l'OPIIEC 2017 (cf. illustration ci-dessous). En revanche, **elle tranche fortement avec les représentations des étudiants,** élèves d'écoles d'ingénieurs et professionnels en formation initiale du monde de la cybersécurité interrogés en 2022 par l'ANSSI. En effet, l'enquête 2022 sur l'attractivité et de la représentation des métiers de l'ANSSI montre que les personnes en formation certifiante ou diplômante en cybersécurité font de la « rigueur », de la « logique », « de la réactivité » et du « calme » les aptitudes les plus associées à la cybersécurité. Dans le même temps, ils font de « l'empathie », « la persuasion », « la diplomatie dans la communication » et de « la créativité », les aptitudes les moins associées à la cybersécurité alors même qu'il s'agit de celles s'approchant le plus de deux des critères clés de recrutement des employeurs en Cyber autour des notions de « curiosité » et de « pédagogie envers les non-experts ».

Un important travail sur les représentations des métiers et des compétences nécessaires en cybersécurité semble être encore à conduire au sein des parcours de formation initiale comme continue afin de réduire cette manifeste dissonance.

Point-clé : les représentations des aptitudes nécessaires aux métiers de la cybersécurité restent en dissonance avec les besoins exprimés par les entreprises quant aux *soft skills* : la curiosité, la créativité, l'appétence pour la veille et la pédagogie envers les non-experts sont des compétences clés et porteuses dans un parcours professionnel en cybersécurité insuffisamment perçues par les candidats au métier, en complément d'une indispensable maîtrise technique (technologique, juridique, en gouvernance et gestion des risques ou facteurs humains).

Top 5 des capacités transversales recherchées par les entreprises de la Branche pour les professionnels de la cybersécurité

Source : *Les formations et les compétences en France sur la cybersécurité,* étude *EY pour le compte de l'OPIIEC 2017*

Source : *Enquête 2022 L'attractivité et la représentation des métiers de la cybersécurité* | ANSSI

Ces soft skills constituent autant d'atouts à valoriser dans les parcours de transition professionnelle et seront mis en perspective avec les enseignements de l'approche monographique sur les parcours de reconversion de profils

[27] https://www.opiiec.fr/sites/default/files/inline-files/21-05-2017_Etude_cybersecurite_rapport.pdf

éloignés de la cybersécurité (cf. Partie III.).

Partie II. État des lieux de l'offre de formations

Corollaire de l'étude des besoins en emplois et compétences des employeurs de profils Cyber, l'état des lieux de l'offre de formation en cybersécurité est une composante structurante du diagnostic local : les organismes de formation initiale et continue sont en effet, des acteurs essentiels pour la constitution d'un vivier de talents adapté, en nombre et compétences, aux besoins des entreprises.

Le diagnostic FORE-CY s'est intéressé à deux champs complémentaires de formations, en procédant à un recensement cartographique des offres locales et régionales Grand Est, des formations suivantes :

- les **formations permettant d'accéder aux métiers spécialisés en cybersécurité à dominante technologique :** il s'agit de formations initiales du Bac Professionnel au Doctorat, mais aussi de formations professionnelles ou de reconversion ;
- les formations incluant des modules de compétences ou de connaissances de la cybersécurité **intégrés à des parcours ayant une autre dominante de spécialité** qu'il s'agisse de formations initiales ou de modules de formations professionnelles.

L'approche cartographique a été complétée par une enquête dédiée auprès des organismes de formations identifiés. L'objectif était de recueillir des éléments sur l'attractivité des formations et les difficultés rencontrées, les voies et moyens mis en œuvre pour répondre aux besoins des employeurs de profils Cyber, la vision partagée de l'évolution des métiers de la cybersécurité et les défis à relever pour les organismes de formation de ces domaines. La vision des organismes de formation a également été **mise en perspective avec les réponses des employeurs de profils** Cyber quant à leur capillarité avec l'écosystème de formation et leurs attentes (cf. Annexe méthodologique).

L'offre de formation en cybersécurité de la Région Grand Est : caractéristiques principales des 211 formations identifiées

La cartographie des formations réalisée recense **au sein de la Région Grand Est, un total de 211 formations** relevant du domaine de la cybersécurité. Certaines formations sont spécialisées, d'autres non : ces dernières correspondent à des modules de connaissance ou de compétences en cybersécurité et peuvent même être des modules dits d'« hygiène numérique ». Si les recherches ont été les plus extensives possibles (cf. Annexe méthodologique), elles ne prétendent cependant pas à l'exhaustivité, notamment vis-à-vis des formations continues dont le recensement a été plus délicat.

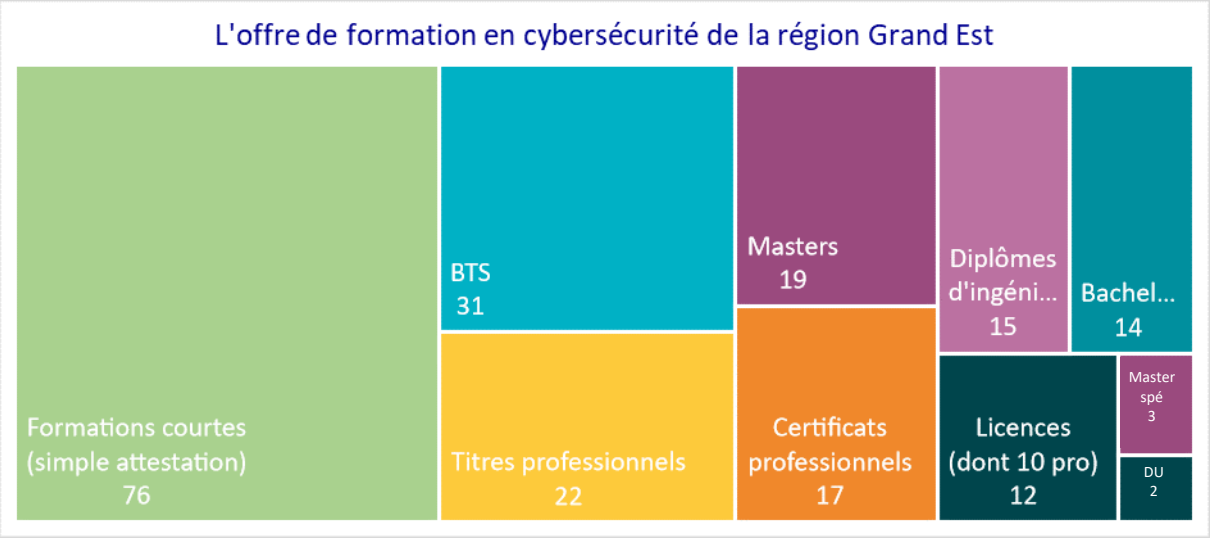
La cartographie recense **96 diplômes de l'Enseignement supérieur ayant un marquant Cyber** de niveaux Bac+2 à Bac+5 :

- 31 **BTS** ;
- 14 **Bachelor,** 10 **Licences** professionnelles, 2 Licences et 2 **DU**, soit 30 formations de niveau 6 ;
- 19 **Master** et 3 Mastères spécialisés ;
- 15 diplômes d'**Ingénieur**.

Parallèlement, **39 formations professionnelles certifiantes** donnent accès à des compétences en cybersécurité sous la forme de :

- 22 **titres professionnels** (8 de niveau 5, 9 de niveau 6 et 3 de niveau 7) ;
- 17 **certificats professionnels** (dont 4 formations longues et 13 formations courtes).

Enfin, **76** formations courtes délivrent une attestation de formation en lien avec la cybersécurité sans être ni diplômantes, ni certifiantes.

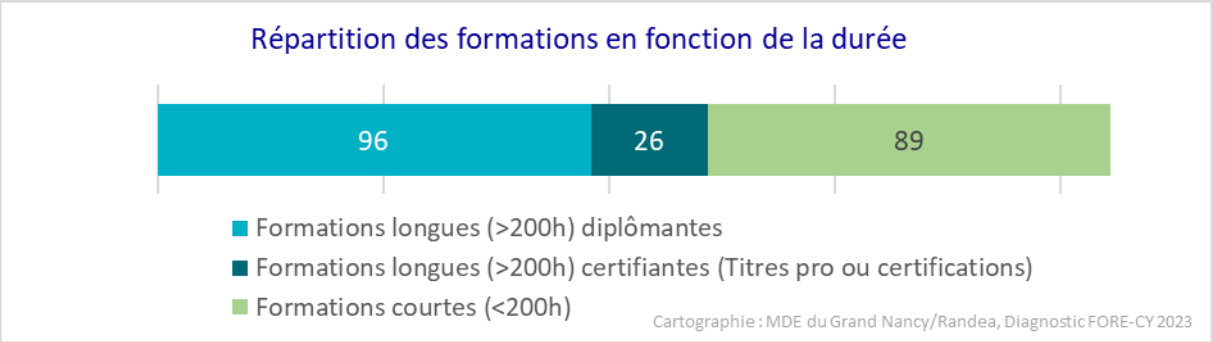


Cartographie : MDE du Grand Nancy/Randea, Diagnostic FORE-CY 2023

Résultat-clé : L'état des lieux réalisé met en évidence **l'importance de l'offre de formation dans le domaine Cyber en Région Grand Est**, notamment de **formations diplômantes de haut niveau** ainsi que la **richesse** et la **variété des formations professionnelles**.

Une grande variété de formations en cybersécurité : courtes et longues, à tous niveaux de qualification

Parmi les 211 formations identifiées, **40% sont des formations courtes** (de moins de 200h), près de **60% sont des formations longues de plus de 200h** : 20% sont des formations professionnelles (22 titres pro et 4 certifications professionnelles) et 80% des diplômes de l'Enseignement supérieur.



Sans surprise, les formations sont pour la plupart à dominante informatique. L'ensemble des organismes ou composantes proposent des formations en lien avec le domaine de l'informatique appliquée à l'administration, à la supervision et à la sécurisation des réseaux informatiques.

Les formations de plus de 200h couvrent plusieurs grands domaines. En très grande majorité, et quel que soit le niveau de qualification, les diplômes ou titres professionnels délivrés sont axés sur le développement de compétences en lien avec **les infrastructures informatiques (réseaux et télécommunications), leur administration, leur sécurisation et leur maintenance** (déclinées sous 99 formations différentes aux intitulés variés).

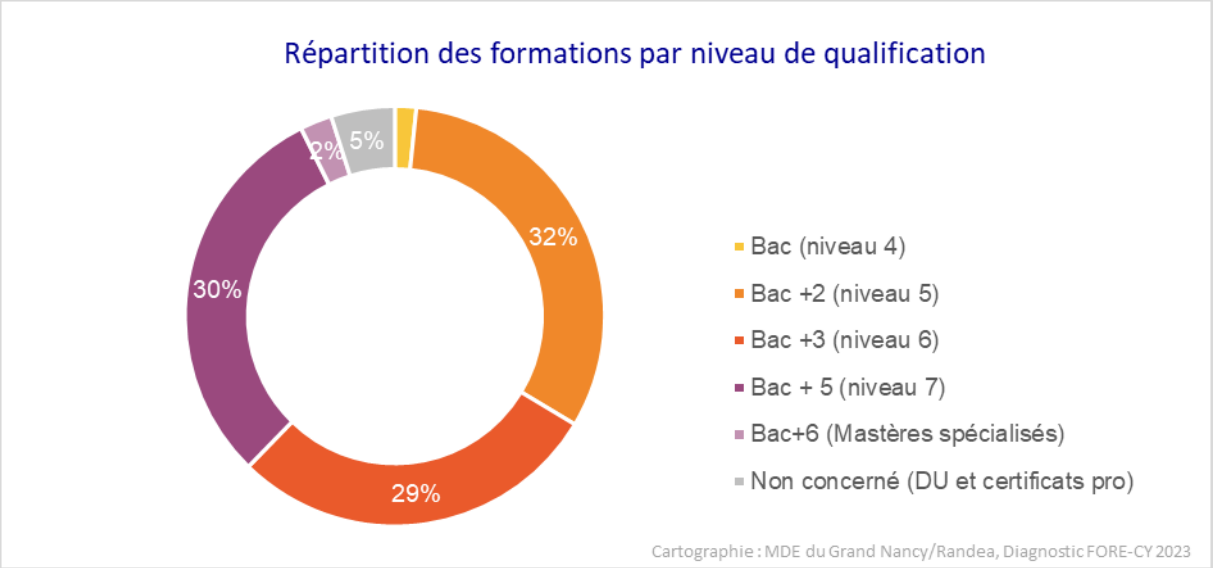
Parmi les formations longues et courtes spécialisées en cybersécurité, quelques-unes sont axées sur le **forensic, l'investigation informatique ou l'enquête numérique. De façon très minoritaire,** une dizaine de formations de

plus de 200h proposant des modules socles en cybersécurité est orientée sur les **compétences numériques en lien avec le développement d'applications mobiles ou web, de logiciels ou l'internet des objets**. En parallèle, 8 formations sont spécialisées dans **l'informatique et la robotique industrielle.**

La cartographie recense **6 formations positionnées sur des métiers non-technologiques.** Les Universités de Lorraine, de Strasbourg et de Troyes font en effet, montre de la volonté de **développer une forme de transversalité dans les enseignements « cybersécurité »** en déployant des diplômes dans des formations des Sciences humaines et sociales et du Droit. C'est le cas notamment du Diplôme universitaire Coordinateur de cellule de crise de l'Université Technologique de Troyes, du Master Veille stratégique et organisation des connaissances de l'Université de Lorraine et du Master de Droit Parcours Droit de l'économie du numérique de l'Université de Strasbourg. Deux autres parcours visent une spécialisation juridique en lien avec les problématiques de sûreté publique comme privée, avec le Master de Droit Parcours Cyberjustice de l'Université de Strasbourg et le Diplôme d'Université Sécurité intérieure, Option cybersécurité de l'Université de Lorraine.

En matière de formations courtes (de moins de 200h), les domaines couverts sont très larges, allant de la sensibilisation à la protection contre les risques, la RGPD ou la cybersécurité (ex : « Parcours introductif à la cybersécurité ») jusqu'au développement de compétences techniques très avancées.

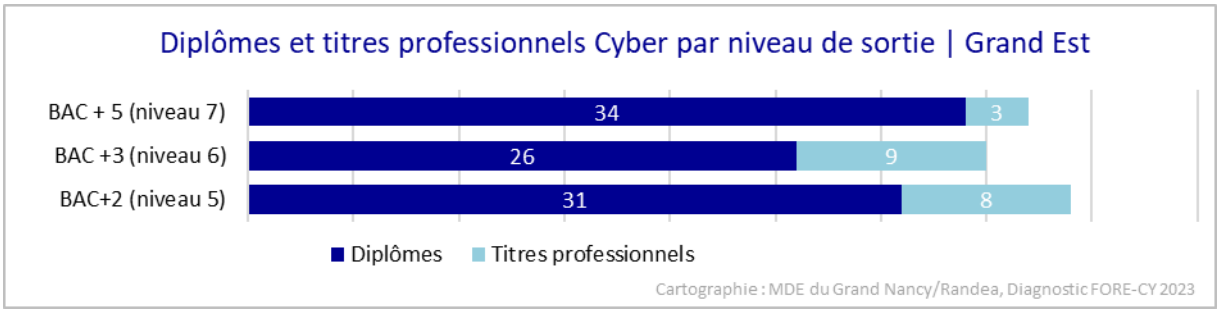
Les niveaux de qualification visés par les formations longues recensées concernent à part quasiment égale des niveaux Bac +3 (niveau 5), Bac +5 (niveau 6) ou Bac +6 (niveau 7). Seules deux formations s'adressent aux élèves de niveau Bac (niveau 4) à Metz et Strasbourg.

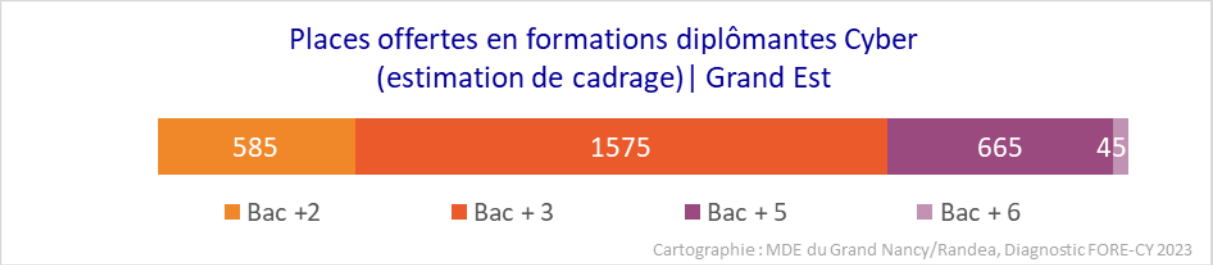


En ciblant les diplômes (hors titres professionnels), si le nombre de diplômes **de niveaux Bac +3 est moins important que la forte amplitude des possibilités de diplomation en cybersécurité de niveau Bac +5, ce constat s'inverse en tenant compte du nombre de sortants** (en estimation de cadrage[28])**.** Ainsi, sur les 96 formations délivrant des diplômes :

- 32 % sont des diplômes de niveaux Bac +2 et sont principalement composés de BTS ; ce niveau offre 20% des places diplômantes ;
- **29 %** sont des diplômes de niveaux Bac +3, principalement des Licences professionnelles et des Bachelors ; **ce niveau offre plus de 50% des places diplômantes ;**
- **32 % sont des diplômes de niveaux Bac +5 ou Bac +6,** Master, diplômes d'ingénieur ou Mastères spécialisés ; ce niveau offre 25% des places diplômantes.

[28] La veille réalisée et l'adressage des éléments identifiés à chaque composante n'a permis qu'un recensement partiel du nombre de places disponibles par formation. Néanmoins, il se dégage une moyenne : 15 places en BTS, 45 en licence pro ou Bachelor, 15 à 20 en Master ou diplôme d'ingénieur.



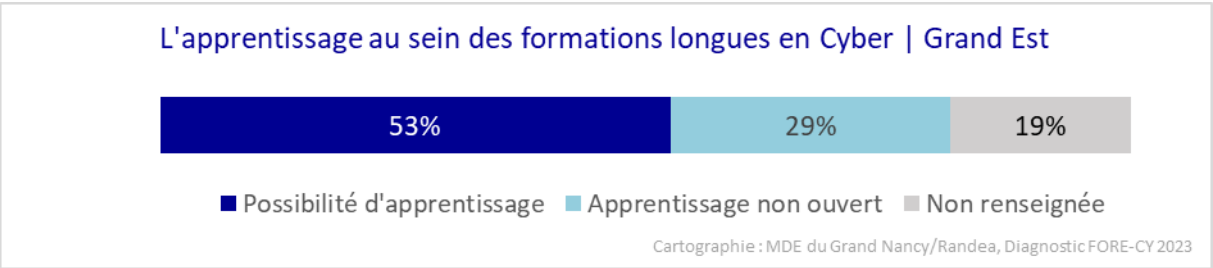


Cette situation reflète pour l'essentiel la progression de la spécialisation avec des Bac+3 encore assez généralistes en informatique notamment, *versus* des diplômes de niveau Bac +5 davantage spécialisés. **Cet état des lieux restitue les possibilités de parcours et de passerelles au sein du territoire du niveau Bac +2 vers un niveau Bac +5,** les étudiants diplômés d'un BTS ayant la possibilité soit d'intégrer le monde professionnel à l'issue de leur formation, soit de poursuivre plus avant leurs études.

Les publics ciblés par les formations en cybersécurité

Les formations en cybersécurité de la Région Grand Est **s'adressent à tous les publics en formation initiale ou continue** : étudiants, demandeurs d'emplois, salariés ou dirigeants. Les formations courtes ciblent principalement les salariés et dirigeants.

Près de 60% des formations Cyber de la région sont accessibles en alternance : apprentissage et/ou contrat de professionnalisation. La technicité des compétences opérationnelles dans le domaine fait de l'alternance, une modalité d'enseignement bien adaptée. Seules 25% des formations ne pratiquent pas cette modalité.



Degré de spécialisation en cybersécurité

En matière de spécialisation, **les termes « Cybersécurité » ou « Sécurité informatique » apparaissent dans l'intitulé de près de 40 % des formations longues, soit 47 diplômes, titres professionnels ou certifications professionnelles** ; 60% des formations sont non spécialisées tout en incluant des modules Cyber.

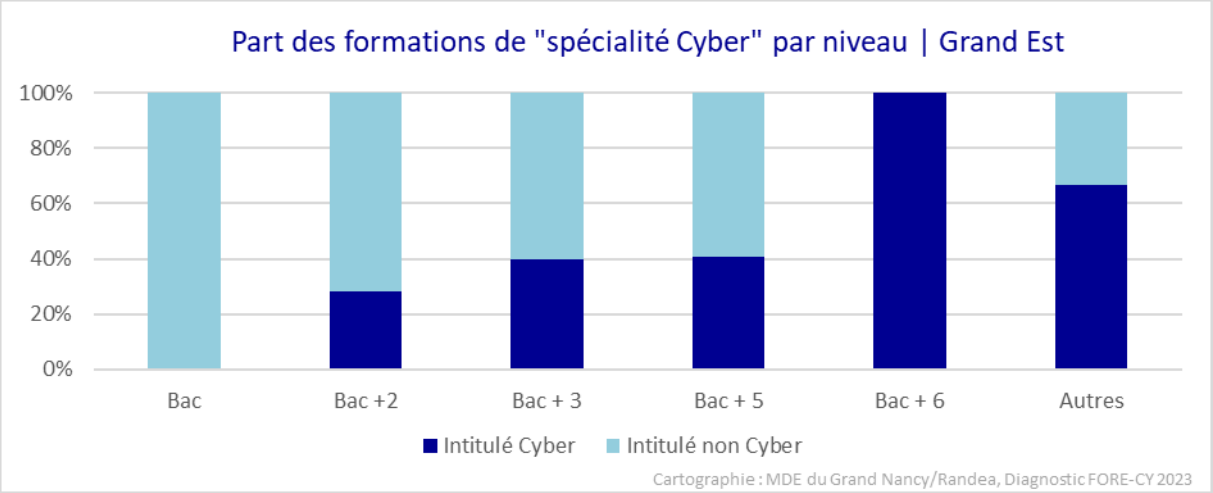
Parmi l'ensemble des formations diplômantes de spécialité « Cybersécurité » identifiées sur le territoire du Grand Est, **5 sont actuellement labellisées « SecNumEdu » par l'ANSSI** (2 Bac +3, 1 Bac +5 et 2 Bac +6) ou en cours de renouvellement par les organismes de formation sur un total national de 81, soit 6% des formations labellisées par l'ANSSI. **Deux formations SecNumEdu sont localisées sur le territoire de la Métropole du Grand Nancy.**

Établissement	Diplôme/Titre	Nom de la formation
Université de Technologie de Troyes	**Mastère Spécialisé ®**	Mastère Spécialisé « Expert Forensic et Cybersécurité »
IUT de Nancy Brabois - Université de Lorraine	**Licence pro**	Licence Professionnelle Métiers des Réseaux Informatiques et Télécommunications (MRIT) – parcours Cybersécurité et Cyberdéfense
Établissement	**Diplôme/Titre**	**Nom de la formation**
Mines de Nancy	**Mastère Spécialisé ®**	Mastère Spécialisé® « Cybersécurité : attaque et défense des Systèmes Informatiques »
Université de Reims Champagne-Ardenne	**Master**	Master Mention Réseaux et Télécommunication Parcours Administration et Sécurité des Réseaux (ASUR)
IUT de Colmar - Université de Haute-Alsace	**Licence pro**	Licence Professionnelle Métiers des Réseaux Informatiques et Télécommunications (MRIT) – parcours Administration et Sécurité des Réseaux (ASUR)

Résultat-clé : Le Grand Est, notamment à Nancy et Troyes, se distingue par une **haute spécialisation en mentions de cybersécurité**. L'état des lieux de la formation fait ressortir **la possibilité pour les étudiants, d'un continuum de parcours d'excellence Cyber au sein du territoire régional** :

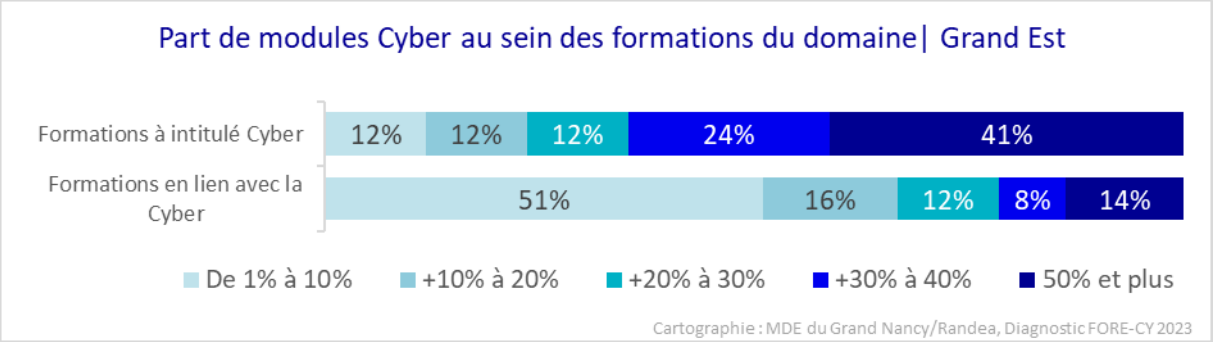
- **en Administration et Sécurité des Réseaux (ASUR)** avec une Licence professionnelle à Colmar et un Master à l'Université de Reims, tous deux labellisés SecNumEdu ;
- **en Cyberdéfense au sein du Grand Nancy** avec une Licence professionnelle MRIT parcours Cybersécurité et Cyberdéfense à l'IUT Nancy Brabois et un Mastère Spécialisé à l'École des Mines de Nancy en « Attaque et défense des Systèmes Informatiques », tous deux labellisés SecNumEdu.

La proportion de formations spécialisées augmente avec le niveau de qualification : **elle est de 35% et voisine pour les niveaux Bac+3 et Bac+5,** jusqu'à concerner 100% des Mastère spécialisés.



L'analyse du **détail du contenu des formations** (pour la cinquantaine de formations pour lesquelles il est disponible) met en évidence un **pourcentage très variable de la proportion des modules dédiés à la cybersécurité** en fonction des formations (nombre de modules Cyber / total des modules) : ce ratio oscille entre 1% et 100% ; **il est en moyenne de 20%**. La durée de chaque module (exprimée en heures) n'étant pas toujours disponible, l'analyse n'a pu être menée au grain le plus fin. L'analyse comporte donc des limites, ce d'autant plus que le nombre total de modules diffère fortement d'une formation à une autre, jouant à la hausse ou à la baisse sur la proportion de modules dédiés à la cybersécurité.

En considérant l'ensemble des formations, spécialisées ou non, la proportion de modules dédiés à la cybersécurité est inférieure à 10% des modules d'enseignement pour la moitié d'entre elles. Cette proportion s'inverse en ciblant **les formations spécialisées en cybersécurité qui ont en moyenne 50% d'intitulés Cyber** ; 65% des formations mobilisant les termes « cybersécurité » ou « sécurité informatique » dans leur intitulé ont plus de 30% de modules dédiés à la cybersécurité. Les pourcentages les plus élevés sont détenus, en toute logique, par les Masters, les Mastères spécialisés ainsi que par des certificats professionnels.



Il convient néanmoins de noter qu'un diplôme de niveau Bac +5 propose un parcours de spécialité en cybersécurité comptant moins de 5% de modules dédiés au domaine ; s'il ne s'agit pas d'une erreur de présentation de la maquette pédagogique, il conviendra de renforcer rapidement ces enseignements afin d'éviter un décalage entre le diplôme et les compétences acquises, préjudiciable à tous, jeunes diplômés, employeurs et organismes.

À l'inverse, quatre formations Bac +2, Bac +3 et Bac +5 non identifiées Cyber dans leur intitulé de diplôme proposent plus de 25% de modules dédiés à la cybersécurité ou à la sécurité informatique et contribuent ainsi nettement au vivier de talents en ce domaine.

Il aurait été intéressant d'aller plus loin dans l'analyse en procédant en nombre de sortants ; toutefois, ces données difficilement disponibles n'ont pas pu être consolidées pour l'ensemble des formations empêchant d'y procéder de façon fiable.

L'écosystème de formation en cybersécurité du Grand Est

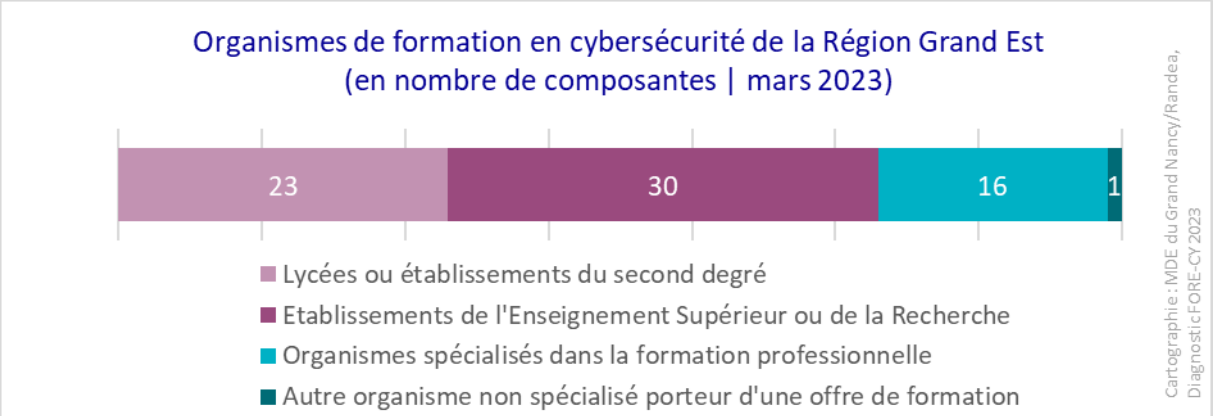
1| Carte d'identité des organismes du Grand Est dispensant des formations en cybersécurité

Ces formations Cyber sont dispensées par **48 organismes de formation publics ou privés, divers en termes de structure, mobilisant 70 composantes.** Le recensement a ainsi dénombré :

- 23 lycées ou établissements du second degré (LEGT ou LPO) ;
- 11 établissements de l'Enseignement supérieur et de la Recherche mobilisant 30 composantes ;
- 13 organismes spécialisés dans la formation professionnelle ;
- 1 organisme non spécialisé mais porteur d'une offre de formation.

Les lycées et établissements du second degré sont très représentés bien qu'ils ne proposent *in fine* que 11% des formations recensées. La lecture de l'écosystème s'avère donc davantage pertinente en composantes.

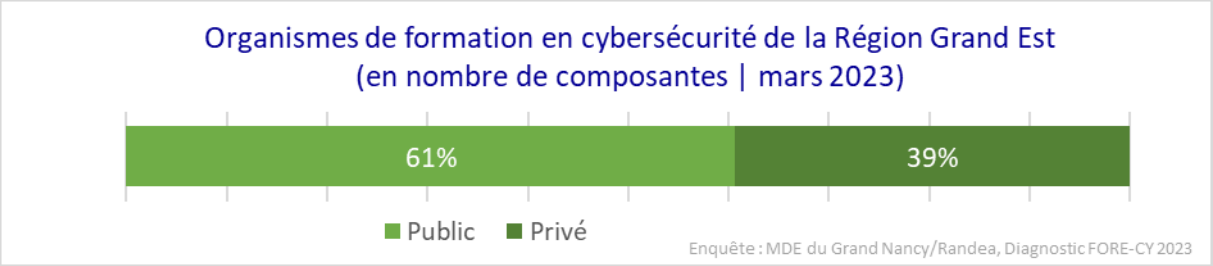
Les structures relevant de l'Enseignement supérieur et de la Recherche priment et sont même très prégnantes alors, tout en faisant la part belle aux établissements du second degré et aux organismes spécialisés dans la formation professionnelle. **L'écosystème de formation est ainsi riche et varié en types de structures.**



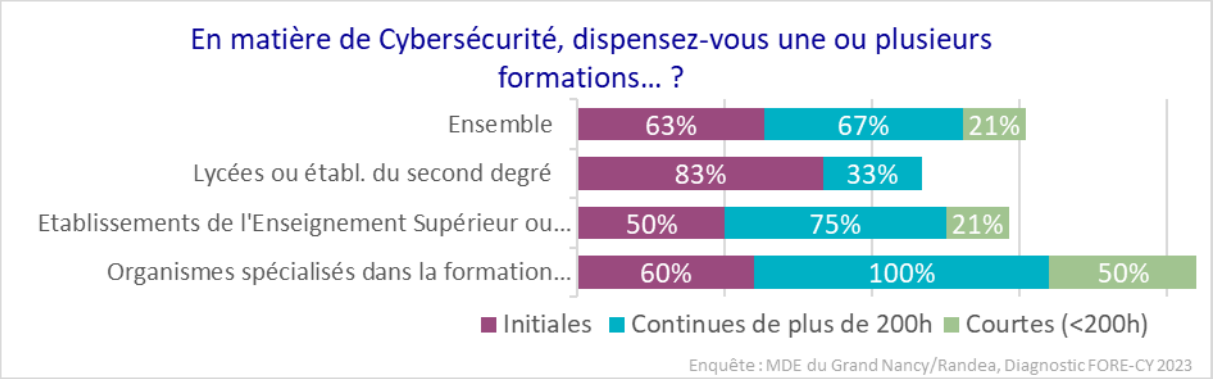
Les composantes de l'Enseignement supérieur et de la Recherche impliqués en cybersécurité sont :

- des écoles d'ingénieur ;
- des établissements privés ;
- des instituts universitaires de technologie (IUT) ;
- diverses composantes d'Université en Sciences, Mathématiques, Informatique, ainsi qu'en Sciences Humaines et Sociales et en Droit.

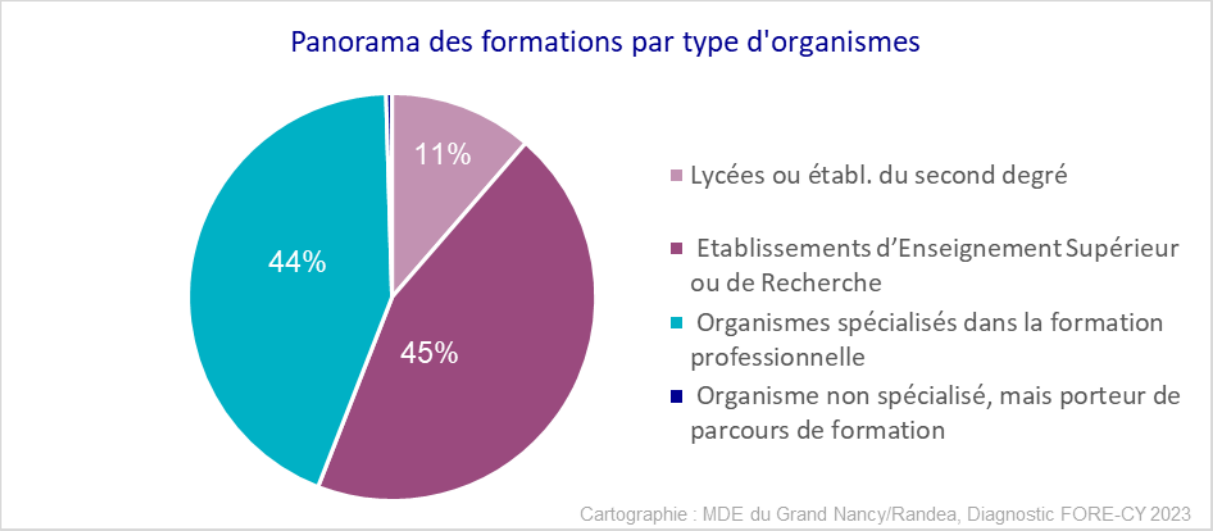
Les 70 composantes de formation impliquées en cybersécurité sont à 60% des structures publiques.



63% des structures formatrices interviennent en formation initiale, 67% en formation continues longues. 20% des structures du Supérieur ayant répondu à l'enquête FORE-CY proposent des formations courtes ainsi qu'un organisme spécialisé sur deux.



Pris sous l'angle des formations, **le panorama se rééquilibre en nombre de formations dispensées entre structures de l'Enseignement supérieur et organismes spécialisés dans la formation professionnelle** (près de 45% des formations Cyber du Grand Est pour chaque type d'acteurs). On notera aussi que les formations courtes en Cyber ne sont uniquement dispensées par les organismes spécialisés en formation professionnelle, mais aussi à **35% par des établissements de l'Enseignement supérieur.**



2| Géographie des formations en cybersécurité du Grand Est

Les formations recensées dont la localisation a pu être établie[29] se répartissent dans **23 villes au sein des 9 départements de la Région Grand Est**. **Les 122 formations longues sont inégalement réparties au sein du**

[29] Certaines formations courtes n'ont pu être localisées géographiquement en raison de la flexibilité des organismes de formation capables d'intervenir sur l'ensemble du territoire en fonction des besoins des entreprises.

territoire régional : **60% d'entre elles sont concentrées sur trois départements,** la Collectivité européenne d'Alsace avec Strasbourg, la Meurthe-et-Moselle autour du Grand Nancy et la Moselle avec Metz.

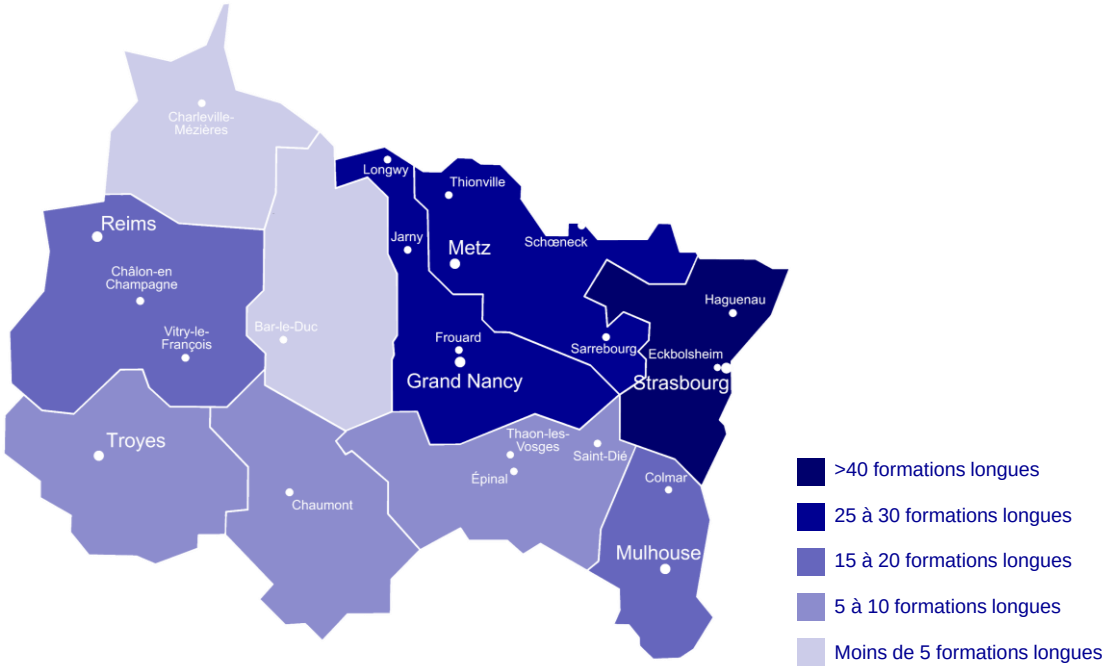
Les formations de plus de 200h de niveau Bac +5 et Bac +6 sont dispensées dans **6 moyennes et grandes villes de la Région proposant une offre de formation sur l'ensemble des niveaux du Bac +2 au Bac +5, voire Bac +6 :** Strasbourg (17 formations ; plus de 200 000 hab.), Grand Nancy (11 formations ; plus de 250 000 hab.), Mulhouse (8 formations ; plus de 100 000 hab.), Metz (4 formations ; plus de 100 000 hab.), Reims (3 formations ; plus de 150 000 hab.) et Troyes (3 formations ; plus de 50 000 hab.), réparties au sein de 6 départements sur les 9 que compte le Grand Est. **Les formations de qualifications les plus élevées en Cyber sont assez nettement polarisées sur Strasbourg, Nancy et Mulhouse.**

Parmi les 23 lieux de formation identifiés, **7 villes ne proposent que des BTS** (10 sur les 7 villes) : Bar-le-Duc (55), Jarny (54), Sarrebourg (57), Schœneck (57), Eckbolsheim (67), Vitry-le-François (51), Charleville-Mézières (08). Il s'agit pour la plupart de villes de 2 500 à 15 000 habitants, à l'exception de Charleville-Mézières en comptant plus de 45 000.

L'ensemble des autres formations est localisé au sein de 16 villes de la Région, avec **une nette moindre densité dans les Ardennes, la Meuse et la Haute-Marne ne disposant à eux trois que de 5 BTS en cybersécurité, laissant le sentiment d'une « verticale du vide ».**

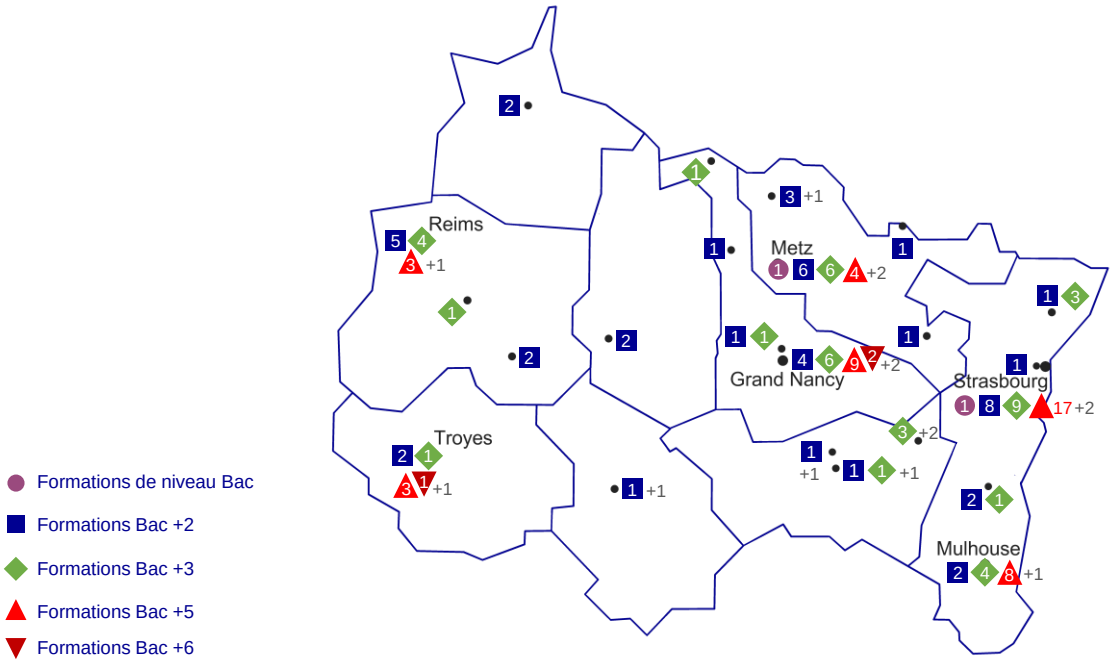
Résultats-clés : Six villes du territoire, moyennes et grandes, ont une forte spécialisation dans la formation en cybersécurité et proposent une offre de formation diplômante sur l'ensemble des niveaux de qualification du Bac +2 au Bac +5, voire du niveau Bac à Bac +6. **Les formations les plus diffusées sur le territoire sont les BTS, avec 23 lieux de formation (dont 7 dont ils constituent la seule offre de formation en cybersécurité) :** les BTS constituent ainsi le maillage de proximité des formations diplômantes du Supérieur en cybersécurité.

Localisation des 122 formations longues en cybersécurité de la Région Grand Est (>200h)



Cartographie : MDE du Grand Nancy/Randea, Diagnostic FORE-CY 2023

Localisation des différents types de formations longues en cybersécurité | Région Grand Est



Cartographie : MDE du Grand Nancy/Randea, Diagnostic FORE-CY 2023

Le département de Meurthe-et-Moselle accueille **par ailleurs une forte proportion de formations de moins de 200h identifiées** par le recensement (28 formations sur 45 géolocalisées sur le territoire). Cette sur-représentation s'explique par le poids des formations courtes dispensées par l'Université de Lorraine (contributrice pour près de la moitié des formations de cette durée) et impliquée dans le Comité de pilotage élargi de la mission.

Les formations Cyber de l'Enseignement supérieur

1| Les BTS Cybersécurité du Grand Est

La Région Grand Est compte **31 BTS** en cybersécurité, répartis **au sein de 23 villes dont 7 ne disposent que de ce niveau de formation dans le domaine**. Ils constituent le maillage territorial le plus fin de la formation en cybersécurité. Il s'agit systématiquement de **BTS centrés sur le domaine technologique** autour de quatre parcours principaux ; seul un parcours comporte le mot Cyber dans son intitulé :

- *BTS Services informatiques aux organisations (SIO) Option : Solutions d'Infrastructures, Systèmes et Réseaux (SISR) ;*
- *BTS Services informatiques aux organisations (SIO) Option : Solutions Logicielles et Applications Métier (SLAM) ;*
- *BTS Cybersécurité, informatique et réseaux, électronique (CIEL) ;*
- *BTS Services numériques.*

Quelques exemples des métiers et compétences cibles des BTS en lien avec la cybersécurité de la région Grand Est

Les titulaires du BTS SIO sont chargés d'installer des réseaux informatiques (parcours SISR) ou de fournir des services orientés solutions logicielles et applicatives (parcours SLAM).

Les titulaires du BTS CIEL option Informatique et Réseaux sont des techniciens polyvalents dans les domaines du développement logiciel, des réseaux et des systèmes d'exploitation, ainsi que la valorisation de la donnée et la cybersécurité.

Quelques compétences clés :

↻ Définir, valider et mettre en œuvre une architecture matérielle/logicielle | ↻ Adapter et/ou configurer un matériel | ↻ Superviser le fonctionnement d'un produit/logiciel et diagnostiquer les causes d'un dysfonctionnement

Cartographie : MDE du Grand Nancy/Randea, Diagnostic FORE-CY 2023

2| Les Licences, Licences pro et Bachelors Cybersécurité du Grand Est

La Région Grand Est compte **30 formations diplômantes de niveaux 5 ou 6** dans le domaine de la cybersécurité : **14 Bachelor, 10 Licences** professionnelles, **2 Licences** et **2 DU**. Ces formations sont localisées au sein de 13 villes, soit 7 villes de plus que les six pôles de formation spécialisés dans le domaine. Ces 7 villes sont : Châlons-en-Champagne, Longwy et Saint-Dié dont il s'agit de l'unique offre diplômante en cybersécurité ; Frouard, Épinal, Colmar et Haguenau offrant des BTS et des formations Bac +3 en cybersécurité.

Quelques exemples des métiers et compétences cibles des Licences professionnelles, Licences et Bachelors en lien avec la cybersécurité de la région Grand Est

« Les licences professionnelles préparent principalement aux familles de métiers suivantes : maintien en condition et conseil, audit et expertise en sécurité. » (OPIIEC, 2017)

Quelques compétences clés :

↻ Administrer des systèmes informatiques communicants

↻ Sécuriser les services et données d'un système

Cartographie : MDE du Grand Nancy/Randea, Diagnostic FORE-CY 2023

Il s'agit systématiquement de **Licences ou Bachelors centrés sur le domaine technologique** autour de 4 intitulés principaux (cf. Liste complète fournie en Annexe n°3) :

- *Licence professionnelle ou Bachelor Informatique / Métiers de l'informatique, Réseaux, systèmes et Télécommunication ;*
- *Licence ou Bachelor Génie électrique, systèmes automatisés, réseaux et informatique industrielle ;*
- *Licence ou Bachelor Métiers du numérique ;*
- *Licence professionnelle Enquêteur Technologies numériques.*

La licence professionnelle « Enquêteur technologies numériques » (N'TECH) délivrée par l'Université Technologique de Troyes est issue d'un partenariat entre l'UTT et le Centre National de formation de police judiciaire (CNFPJ) ; cette formation est dédiée exclusivement aux Officiers de Police Judiciaire de la Gendarmerie. Elle propose une approche globale de la cybercriminalité.

Les **deux Licences professionnelles Métiers des Réseaux Informatiques et Télécommunications** (MRIT) de l'IUT de Nancy Brabois et de l'IUT de Colmar sont labellisés SecNumEdu par l'ANSSI pour leurs parcours respectivement « Cybersécurité et Cyberdéfense » et « Administration et Sécurité des Réseaux » (ASUR).

3| Les diplômes d'ingénieur, Master et Mastères spécialisés en Cybersécurité du Grand Est

La Région Grand Est compte **37 formations diplômantes de niveau 7** dans le domaine de la cybersécurité : **19 Master**, **15 diplômes d'Ingénieur** et **3 Mastères spécialisés**. Ces formations sont toutes situées au sein des six pôles de formation spécialisés en Cyber de la Région Grand Est : soit d'Est en Ouest, Strasbourg, Mulhouse, Metz, Nancy, Reims et Troyes, villes qui offrent une formation en Cyber sur l'ensemble des niveaux de qualification du Bac +2 au Bac +5, a minima.

Ces formations sont plus diversifiées que les formations de niveaux 5 et 6, même si les parcours technologiques dominent ; elles couvrent principalement (cf. Liste complète fournie en Annexe n°3) :

- *Ingénieur ou Master informatique, réseaux et/ou télécommunications, sécurité des SI ;*
- *Mastère spécialisé Cybersécurité, attaque et défense des SI.*

Plus ponctuellement, mais avec un apport certain pour la filière :

- *Master de Droit ;*
- *Master Veille Stratégique et organisation des connaissances (VSOC) de l'Université de Lorraine ;*
- *Mastère spécialisé Expert Forensic et/ou cybersécurité.*

Quelques exemples des métiers et compétences cibles des diplômes d'ingénieur, Master et Mastères spécialisés en lien avec la cybersécurité de la région Grand Est

« Les formations de niveau master permettent aux étudiants de s'orienter vers des métiers de la famille du conseil, audit et expertise en sécurité, et la famille de pilotage, organisation de la sécurité et gestion des données.

Les formations de type ingénieur ont tendance à former des professionnels pour les familles de métiers suivantes : management de projets de sécurité et cycle de vie de la sécurité ; conseil, audit et expertise en sécurité ; et pilotage, organisation de la sécurité et gestion des risques.

les mastères spécialisés sont des cursus permettant une orientation vers l'ensemble des métiers de la cybersécurité. » (OPIIEC, 2017)

Le Master mention Réseaux et Télécommunications, parcours « Administration et Sécurité des réseaux » (ASUR) de l'Université de Reims et les deux Mastères spécialisés « Expert Forensic et Cybersécurité » de l'Université de Technologie de Troyes et celui de « Cybersécurité : attaque et défense des Systèmes Informatiques » de l'école des Mines de Nancy sont **tous trois labellisés SecNumEdu par l'ANSSI.**

Les formations Cyber relevant de la voie professionnelle

La Région Grand Est compte **39 formations délivrant des titres professionnels ou des certifications professionnelles** relevant du domaine de la cybersécurité dont **26 sont des formations de plus de 200h.**

22 formations délivrent des titres professionnels du niveau 4 au niveau 7. Elles sont **exclusivement ciblées sur des domaines technologiques** à tous les niveaux de formation, avec une spécialisation « cybersécurité » dans leur intitulé au niveau 7.

Dans le détail des titres professionnels accessibles dans le Grand Est :

- **2 formations** délivrent des titres professionnels de « Technicien d'**assistance informatique** » de **niveau 4 ;**
- **8 formations** délivrent des titres professionnels de **niveau 5** autour des 4 intitulés suivants :

- *Technicien supérieur systèmes et réseaux ;*
- *Gestionnaire en maintenance et support informatique ;*
- *Développeur web et web mobile ;*
- *Gestionnaire en maintenance et support informatique ;*

- **9 formations** délivrent des titres professionnels de **niveau 6** autour des intitulés suivants :
  - *Administrateur d'infrastructures sécurisées ;*
  - *Administrateur réseaux / NETOPS ;*
  - *Concepteur en architecture informatique ;*
  - *Analyste en génie informatique et réseaux ;*
- **3 formations** délivrent des titres professionnels de **niveau 7**, dont 2 plus ciblées en matière de thématique cybersécurité, autour des intitulés suivants :
  - *Manager en ingénierie informatique ;*
  - *Manager en infrastructures et cybersécurité des SI ;*
  - *Expert en cybersécurité et réseaux.*

Les certifications professionnelles sont réparties entre **4 formations de plus de 200h** et **17 modules courts**. Les intitulés sont beaucoup plus variés et proposent des degrés très différents de spécialisation Cyber, de la sensibilisation introductive (protection contre les risques, RGPD) au développement de compétences techniques très avancées en cybersécurité.

Synthèse des résultats-clés : En conclusion de l'approche cartographique, qu'il s'agisse de formations longues ou courtes, spécialisées ou non, la cartographie réalisée permet de mettre en évidence une **offre de formation importante sur le territoire.**

Pour les formations de plus de 200h, l'offre couvre l'ensemble du spectre des niveaux de qualification du Bac +2 au Bac +6, et même de niveau Bac, répartis entre parcours spécialisés ou non dès le Bac +2. Cinq formations sont labellisées SecNumEdu par l'ANSSI **avec la possibilité de composer des parcours d'excellence** en Administration et Sécurité des Réseaux (ASUR) au sein du territoire régional (entre Colmar et Reims) **et en Cyberdéfense au sein du Grand Nancy** (entre l'IUT Nancy Brabois et l'Ecole des Mines de Nancy).

La répartition géographique de l'offre est cohérente avec les pôles d'enseignement sur la Région. **Six villes du territoire, moyennes et grandes, ont une forte spécialisation dans la formation en cybersécurité** et proposent une offre de formation diplômante sur l'ensemble des niveaux de qualification du Bac +2 au Bac +5, voire du niveau Bac à Bac +6. **Les formations les plus diffusées sur le territoire sont les BTS, avec 23 sites dont 7 dont ils constituent la seule offre de formation en cybersécurité :** les BTS constituent ainsi le maillage de proximité des formations diplômantes du Supérieur en cybersécurité

Sans surprise, les formations sont pour la plupart à dominante informatique. La cartographie met également en évidence le souhait de la part de certaines universités de **développer une forme de transversalité dans les enseignements « cybersécurité »** en déployant des modules dans quelques formations des Sciences humaines et sociales et du Droit. **Cette dynamique encore émergente est à confirmer.**

Le retour d'expérience des organismes de formation du domaine

Les acteurs de la formation sont une pièce maîtresse du territoire : leur rôle est clé dans la constitution et le développement d'un vivier de talents adapté en nombre et compétences aux besoins des entreprises locales. En

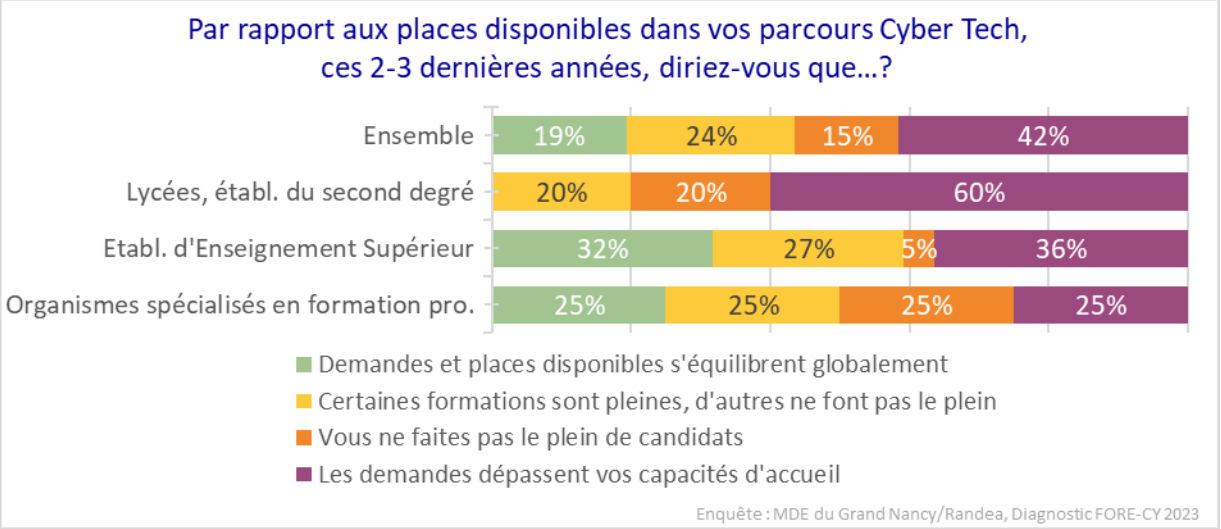
complément de l'approche cartographique, **le diagnostic FORE-CY a donc mis en place une enquête dédiée aux organismes de formation** pour enrichir les données descriptives avec leurs retours d'expériences et leur permettre d'exprimer leur vision de l'évolution des métiers de la cybersécurité et des défis à relever pour former au mieux les talents de demain de la filière[30].

1| Un bon niveau d'attractivité des formations Cyber

Plus de 80% des organismes de formation ayant répondu à l'enquête FORE-CY[31] offrent des parcours de formation Cyber à dominante technologique, ces parcours sont désignés dans les questions et la suite de l'analyse par l'expression « formation Cyber Tech ».

Le retour d'expérience en matière d'attractivité est contrasté, tant entre types d'organismes qu'au sein du portefeuille d'offres de formation. Ainsi, quel que soit le type d'acteurs, **il existe tout à la fois des formations qui peinent à « faire le plein » de candidats, là où d'autres parcours sont saturés et ne disposent pas de capacités d'accueil suffisantes** au regard de l'intérêt des élèves, étudiants ou salariés.

- Ce constat ambivalent est particulièrement marqué pour les organismes spécialisés de formation professionnelle où autant de structures déclarent avoir des formations à l'équilibre (25%), des formations en excès de candidats et d'autres en déficit (25%), des formations qui ne font par le plein de candidats (25%) et d'autres pour lesquelles les demandes dépassent leurs capacités d'accueil (25%).
- Les établissements de l'Enseignement supérieur semblent être moins en difficultés : un tiers des acteurs ayant des offres à l'équilibre et seulement 5% des formations manquant de candidats.
- Les lycées tranchent par l'absence de formations « à l'équilibre » et la prégnance des établissements ayant des capacités d'accueil insuffisantes par rapport aux demandes**. Au regard de l'appétence des jeunes, renforcer l'offre Cyber de niveau Bac +2 à l'échelle régionale pourrait peut-être constituer un levier porteur pour diversifier le recrutement du niveau 6.**



Résultats-clés : Passé ce constat d'ambivalence et de diversité de situations, **le bilan des organismes semble indiquer[32] que « la balance » penche en faveur d'une forte attractivité du domaine Cyber, avec comme situation la plus fréquente, des formations pour lesquelles les demandes dépassent les capacités d'accueil des structures formatrices tant dans les parcours Tech que juridiques ou d'accompagnement de l'organisation[33].**

[30] La méthodologie de l'enquête et la mobilisation des acteurs sont présentés en Annexe #2.

[31] L'enquête a été adressée aux 70 composantes identifiées au sein de la cartographie comme ayant une offre de formation ou a minima un module en rapport avec la Cyber ; 44 acteurs ont répondu à la sollicitation de FORE-CY, soit un taux de retour de 63%. Les réponses ont été redressées sur la base du type d'établissement, sans introduire de pondération relative au nombre de sortants des différents acteurs. Ainsi, une fois redressé en « 70 acteurs », chaque établissement vaut 1 indépendamment du nombre de sortants (cf. Annexe méthodologique pour les autres précisions).

[32] Des précautions s'imposent dans l'interprétation des données dans la mesure où les pourcentages expriment un nombre d'établissements concernés par la situation et ne sont pas directement une évaluation du nombre de formations.

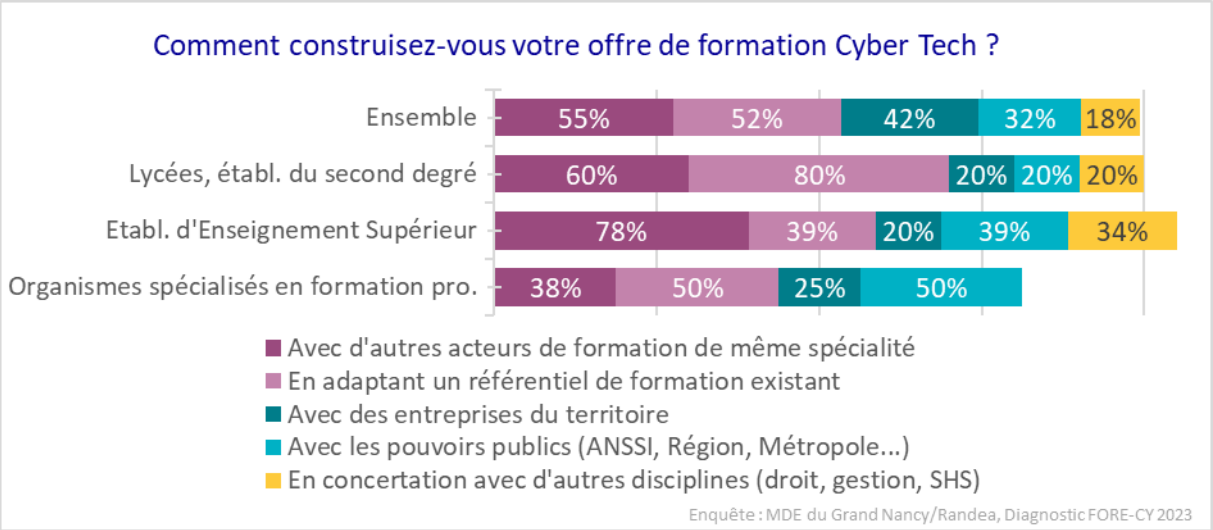
[33] Les résultats sur ce profil sont plus exploratoires compte tenu du petit nombre de répondants ; les valeurs citées dans cette partie ne sont que très indicatives.

Ainsi, 42% des établissements ne peuvent satisfaire l'ensemble des candidats sollicitant leur formation technologique en cybersécurité.

2| Interactions avec les employeurs de profils Cyber et élaboration des offres de formation

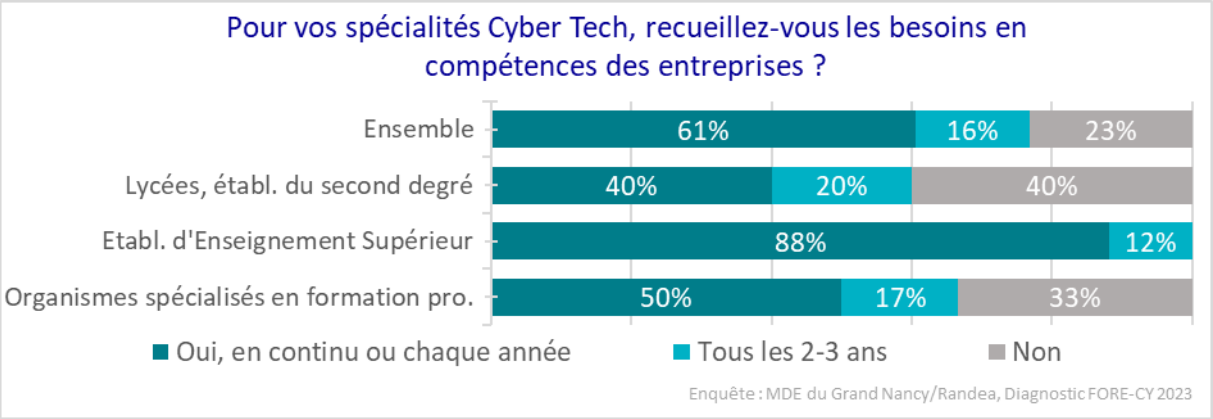
Concernant les voies et moyens d'élaboration et de mise à jour de leurs parcours de formation en Cyber Tech, les structures sont assez contrastées selon leur profil :

- Les lycées et établissements du second degré **font prioritairement référence aux programmes et référentiels de formation** dont ils dépendent (80% des établissements) ; **ils se concertent également entre pairs** pour 60% d'entre eux. Les autres approches sont minoritaires (rappelons que l'échantillon de répondants est de petite taille, il convient donc de ne pas surinterpréter un 20%) ;
- **Les organismes spécialisés en formation professionnelle** font également référence aux **référentiels de formation** existant qu'ils cherchent à décliner (50% des organismes) et dialoguent avec les **pouvoirs publics** compétents (ANSSI, Région… ; 50% des organismes) ;
- **Les structures de l'Enseignement supérieur** adaptent leur offre de formation prioritairement par la concertation entre pairs (80% des acteurs) ; 40% d'entre elles se réfèrent également aux référentiels de formation existant et dialogue avec les acteurs publics compétents du domaine (ANSSI, Région, administrations clientes, etc.) Un tiers des composantes de l'Enseignement supérieur élargissent leur approche par la concertation avec d'autres disciplines (droit, gestion, SHS) ;



Note de lecture : Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

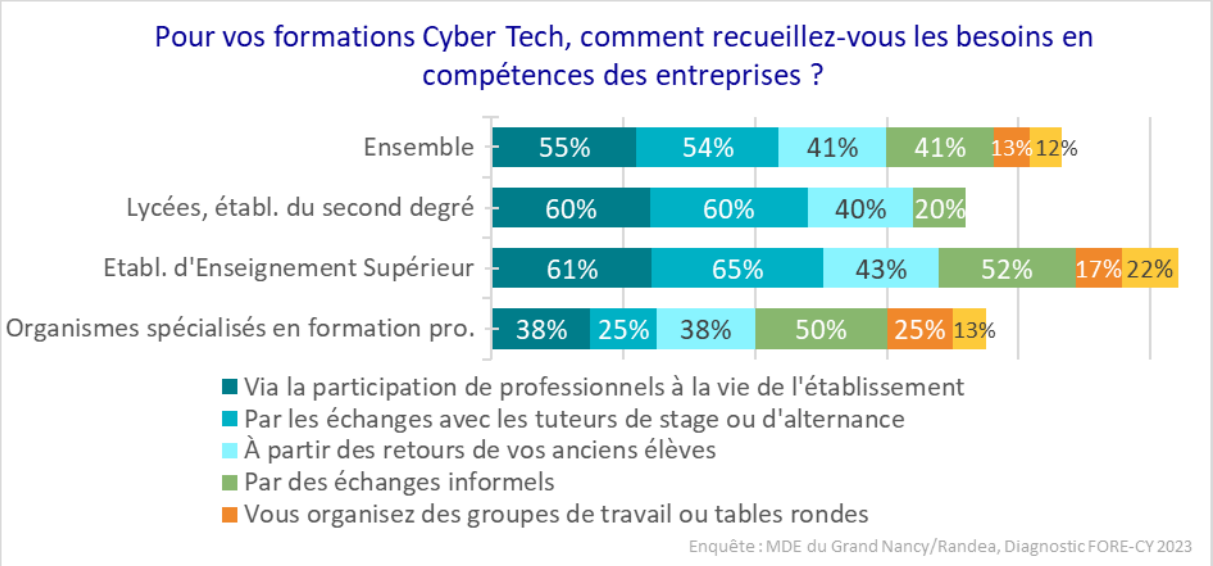
Les trois quart des organismes de formation en Cyber Tech recueillent également les besoins des employeurs afin de répondre toujours davantage à leurs besoins en compétences, le plus souvent de façon continue ou annuellement. Les établissements de l'Enseignement supérieur sont les plus appliqués en ce domaine.



Ce recueil passe avant tout par une bonne capillarité avec les entreprises, *via* la participation de professionnels

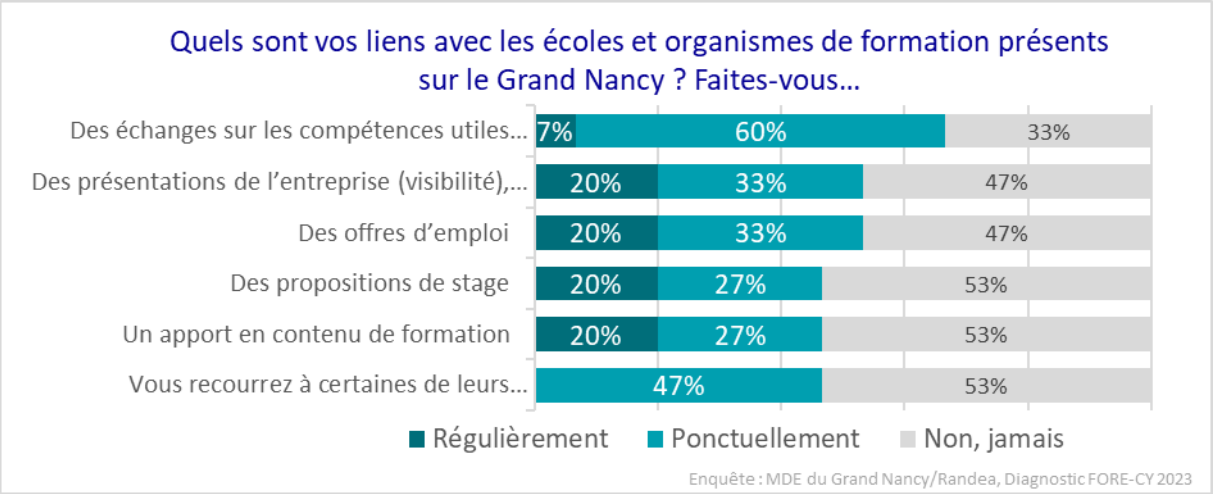
à la vie de l'établissement (55% des organismes de formation en moyenne), par les échanges avec les tuteurs de stage ou d'alternance ou encore les retours des anciens élèves restés en contact avec leur établissement de formation. Les échanges informels comptent également significativement tant pour les établissements du Supérieur que pour les organismes spécialisés de formation professionnelle (moins pour les lycées peu habitués à cette culture).

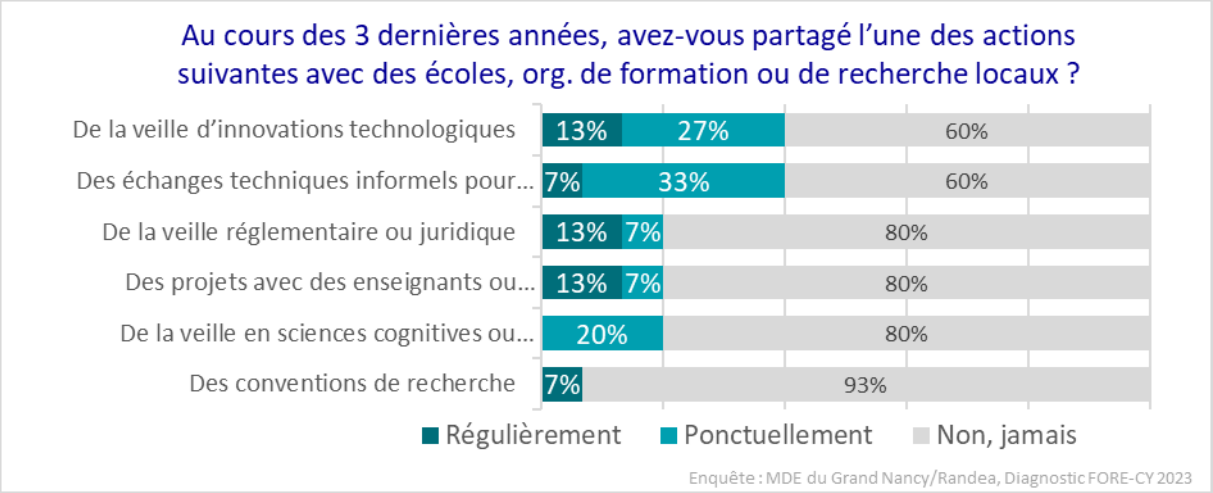
Si la présence des employeurs de profil Cyber est moins aisée à organiser pour certains organismes spécialisés de formation professionnelle, ils compensent cette moindre capillarité par l'organisation de groupes de travail ou de tables rondes (25% des organismes de ce profil).



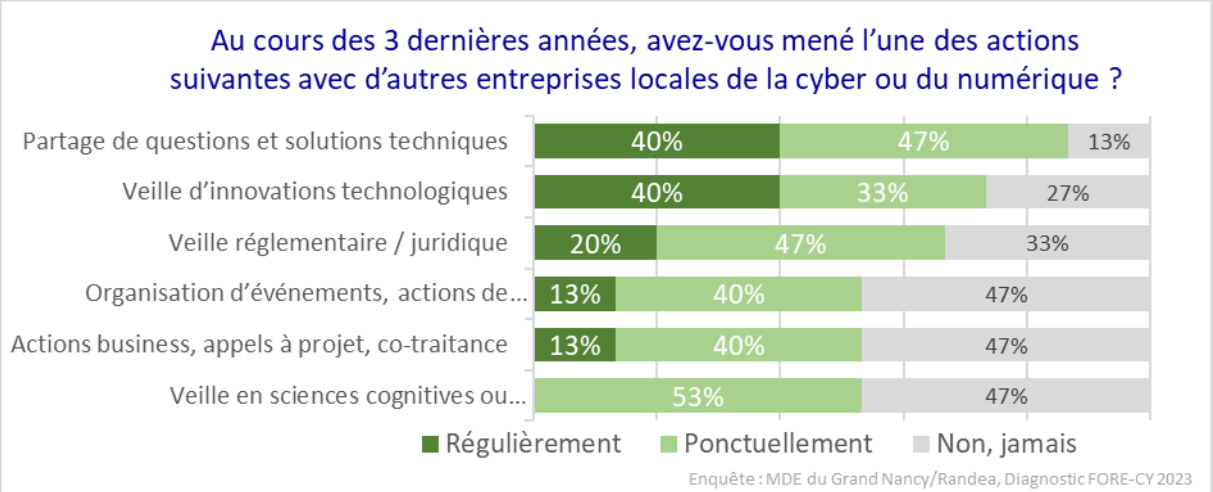
Note de lecture : Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

Les employeurs de profils Cyber interrogés sur leur capillarité avec l'écosystème de formation corroborent le retour d'expérience des organismes de formation (cf. double graphique ci-dessous) : les employeurs ayant des échanges sur les compétences utiles recherchées (67% des employeurs *a minima* ponctuellement) sont aussi ceux réalisant des présentations de leur entreprise pour gagner en visibilité auprès du vivier des candidats (~la moitié des employeurs). D'autres adressent des offres de stage et proposent des offres d'emploi ; il y a là aussi une fréquente redondance. **15% des employeurs n'ont *in fine* aucune interaction avec l'écosystème de formation.**





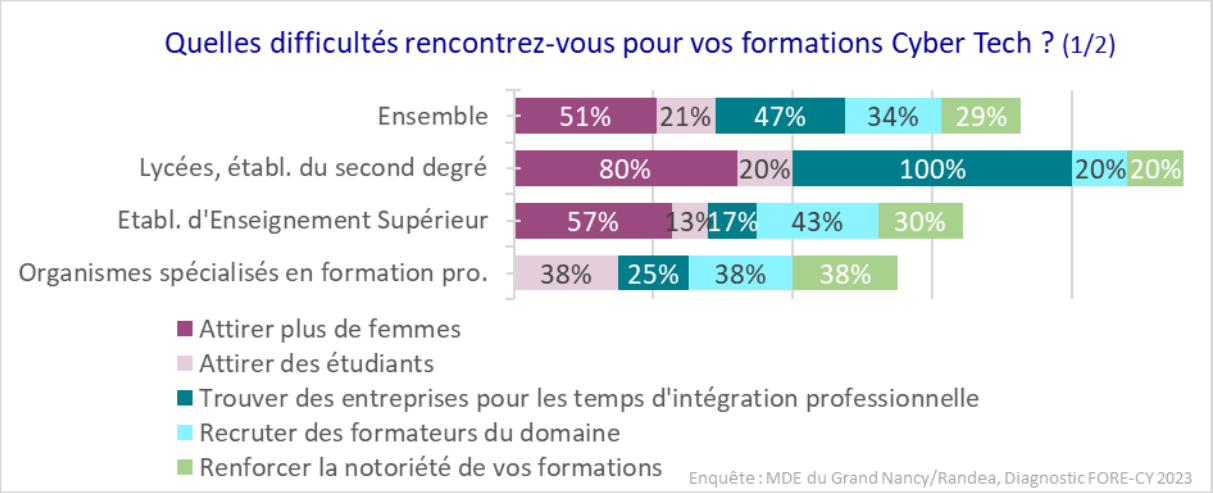
Parmi les coopérations touchant plus directement la création de valeur de l'entreprise, les interactions relevant du domaine des technologies (veille ou échanges informels) priment sur les échanges juridiques ou en sciences cognitives ou SHS. Les interactions sont en ces domaines le fait d'une minorité d'acteurs. **Les employeurs privilégient en ces domaines les interactions entre pairs particulièrement développées au sein de la filière : 40% des employeurs déclarent partager régulièrement des questions et solutions techniques entre pairs et même près de 90% au moins ponctuellement. Dans un secteur en constante évolution, le partage entre pairs de la veille d'innovations apparaît également fort développé.**



Résultats-clés : La capillarité entre l'écosystème de formation et les employeurs de profils Cyber est de bonne qualité. Les employeurs de profils Cyber nourrissent par ailleurs entre eux de fortes interactions, notamment dans le domaine technique.

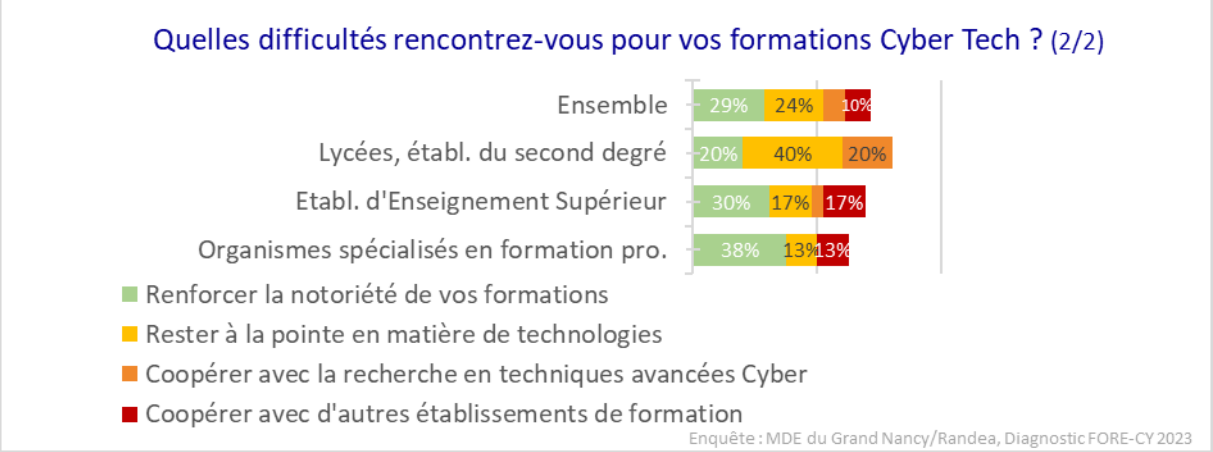
3| Les difficultés des acteurs de formation du domaine Cyber

Les interactions entre écosystème de formation et employeurs sont un enjeu clé, avec des relations porteuses mais figurent également dans le tableau des difficultés rencontrées par les structures de formation. Ce dernier est fortement différentié selon le type d'organismes : les BTS sont unanimes sur leurs difficultés à trouver des entreprises d'accueil de leurs étudiants en stage, ainsi qu'à attirer les candidates au sein de leurs formations (80% des lycées). Les établissements du Supérieur partagent cette dernière préoccupation pour près de 60% d'entre eux et peinent pour leur part pour plus de 40% d'entre eux à trouver des formateurs, notamment experts du domaine, pour dispenser leurs formations et ce faisant, renforcer la notoriété de l'établissement. Les difficultés semblent moins aiguës ou plus disparates au sein des organismes spécialisés de la voie professionnelle avec un enjeu néanmoins plus marqué que les autres acteurs d'attractivité des publics et de notoriété (près de 40% des organismes).



Note de lecture : Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

De façon plus secondaire et à l'articulation là aussi des enjeux de notoriété (reportés sur les deux graphiques de restitution du tableau des difficultés), les BTS soulignent combien rester à la pointe en matière de technologie constitue un défi pour 40% des lycées et structures formatrices. Coopérer avec la recherche en techniques avancées Cyber est aussi une gageure pour 20% des BTS.

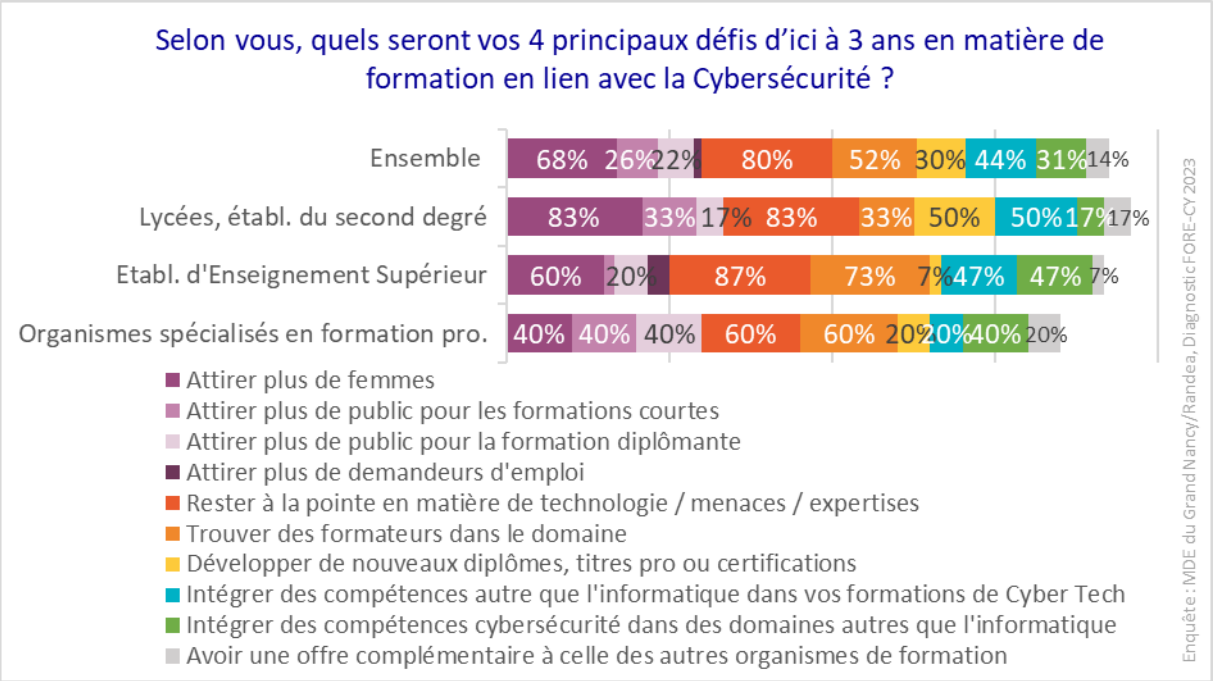


Note de lecture : Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

Face au défi de la forte évolutivité du domaine, la mobilisation d'intervenants professionnels et d'experts au sein des structures de formation est capitale, à tous les niveaux de qualification. La part d'intervention de profils experts des technologies avoisine ainsi, 50% pour les établissements d'Enseignement supérieur mobilisés dans l'enquête FORE-CY, 70% pour les organismes de formation de la voie professionnelle.

4| Les défis des acteurs de la formation en Cybersécurité d'ici 2030

Des difficultés aux défis de l'écosystème d'ici 2030, il n'y a qu'un pas.



Note de lecture : Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

- **La féminisation du vivier est un défi actuel comme à moyen terme**

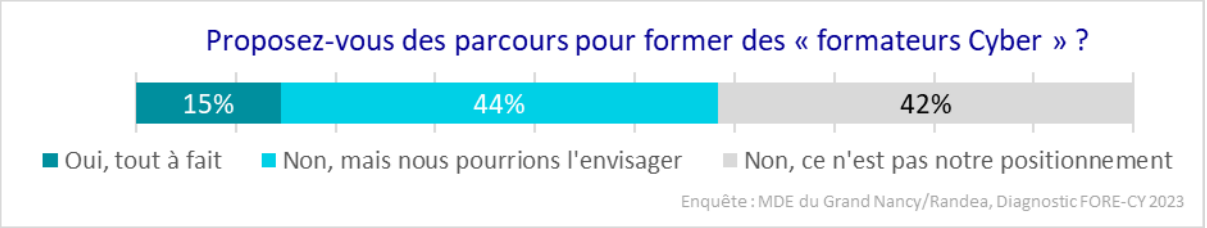
La féminisation du vivier mobilise l'ensemble des acteurs à toutes les échelles du local au national. Elle se pose avec une acuité particulière au sein des BTS, mais aussi dans l'enseignement supérieur, notamment les écoles d'ingénieur qui ont vu le flux de candidates se tarir suite à la réforme du baccalauréat. L'équipe FORE-CY est très consciente de cette problématique dont elle n'a cependant pas souhaité faire un axe prioritaire d'action, souhaitant capitaliser sur les initiatives et actions déjà en cours en ce domaine. Citons à titre d'illustration la forte mobilisation des acteurs associatifs (Femina Tech, Elles bougent…), les actions de sensibilisation et/ou de formation dans le domaine numérique dédiées exclusivement au public féminin (Les Hackeuses, HTM.Elles, Place des Compétences Numériques…)

- **L'attention insuffisante portée aux profils issus de la reconversion**

Si le défaut de féminisation du vivier mobilise les parties prenantes de la filière, **l'accompagnement des profils issus de la reconversion bénéficie de moins d'appui et brille par son absence dans le tableau des priorités des acteurs, à l'exception de quelques établissements du Supérieur**. Certes, le choix étant limité à 4 priorités, d'autres items ont pris la lumière, pour autant la problématique de l'élargissement du vivier est essentielle pour la filière. Le projet FORE-CY souhaite poursuivre l'investigation en ce domaine pour éclairer les acteurs.

- **La formation des formateurs : un enjeu de court et moyen terme**

Tout au long du diagnostic FORE-CY, **la problématique de la formation des formateurs** s'est fait entendre comme un défi lancinant, l'entretien de l'expertise technologique se posant avec une acuité particulière en matière de technologies Cyber. Il s'agit du **défi n°1 des organismes spécialisés dans la formation professionnelle (60%) et du défi n°2 des établissements de l'Enseignement supérieur** (75% des structures) avec l'exigence de rester à la pointe en matière de technologies, menaces et expertises. Si peu d'acteurs proposent aujourd'hui des parcours pour former des « formateurs Cyber », y réfléchir apparaît indispensable et même une voie possible pour 45% des organismes de formation de FORE-CY.



- **L'hybridation des parcours : un virage à réussir !**

45% des organismes de formation de FORE-CY font de l'intégration de compétences autres que l'informatique dans leurs parcours Cyber Tech un enjeu et un défi d'ici 2030. Cette proportion avoisine 50% dans le Supérieur et au sein des BTS. Or, cette vision d'avenir contraste fortement avec l'évaluation de l'existant.

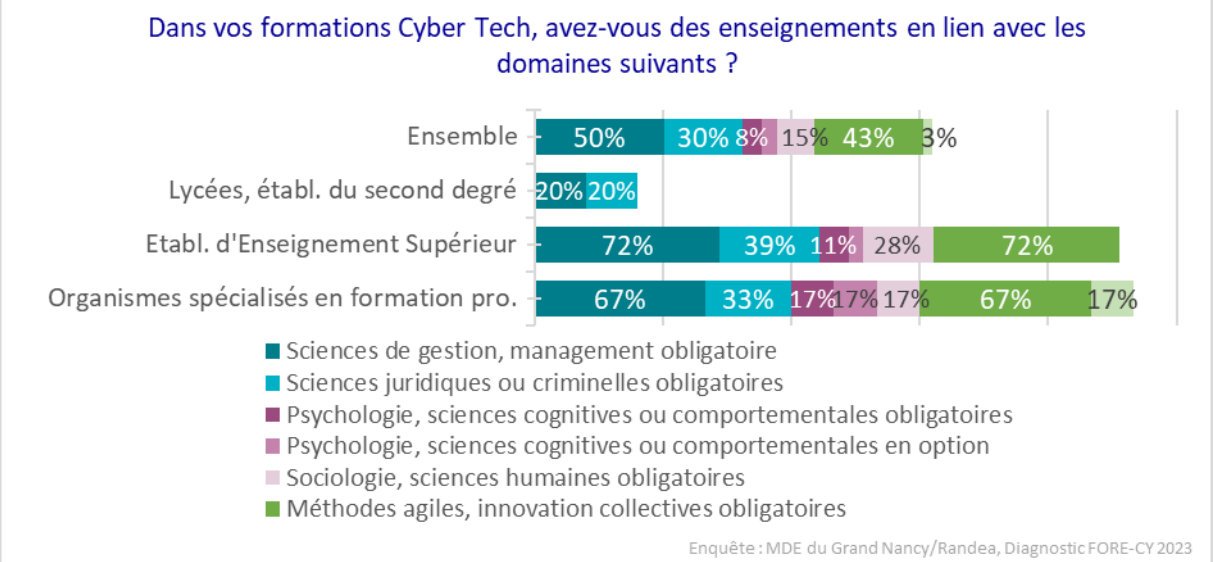
En effet, interrogés plus tôt dans l'enquête sur la propension à hybrider leurs parcours de formation, une forte dichotomie apparaît entre :

- Les lycées et établissements du second degré d'une part : **rares sont les formations de niveau 4 ou 5, principalement les BTS, à disposer d'un temps de formation sur des matières connexes à l'informatique**, qu'il s'agisse de management ou de gestion ou encore de sciences juridiques ; quelques établissements font figure d'exception dans ces deux domaines, mais aucun lycée ne dispense d'ouverture en sciences cognitives, psychologiques ou sociales, ni ne sensibilise aux méthodes d'innovation collective ;
- **Les structures formatrices du Supérieur et de la voie professionnelle** où deux champs de compétences connexes apparaissent fréquemment proposés : **70%** des établissements de ces deux écosystèmes proposent un enseignement en sciences de **gestion ou management**, ainsi qu'en **méthodes agiles** ou innovation collective. Ces deux approches sont le plus souvent une bi-composante soit présente, et ce de manière obligatoire dans les cursus, soit absente.

  33% à 40% des établissements du Supérieur et de la voie professionnelle formant aux technologies Cyber incluent une introduction ou des modules juridiques dans tout ou partie de leurs formations ; les sciences humaines et sociales sont nettement moins souvent mobilisées au sein des cursus de formation des profils Cyber Tech. Là aussi, elles sont souvent soit proposées en bouquet, soit absentes.

L'hybridation des parcours semble « plus naturelle » pour les formations juridiques ou d'accompagnement de l'organisation en cybersécurité : la moitié des répondants de ce profil ayant un module sur les technologies informatiques de sécurisation ou les techniques de surveillance et gestion des cyberattaques.

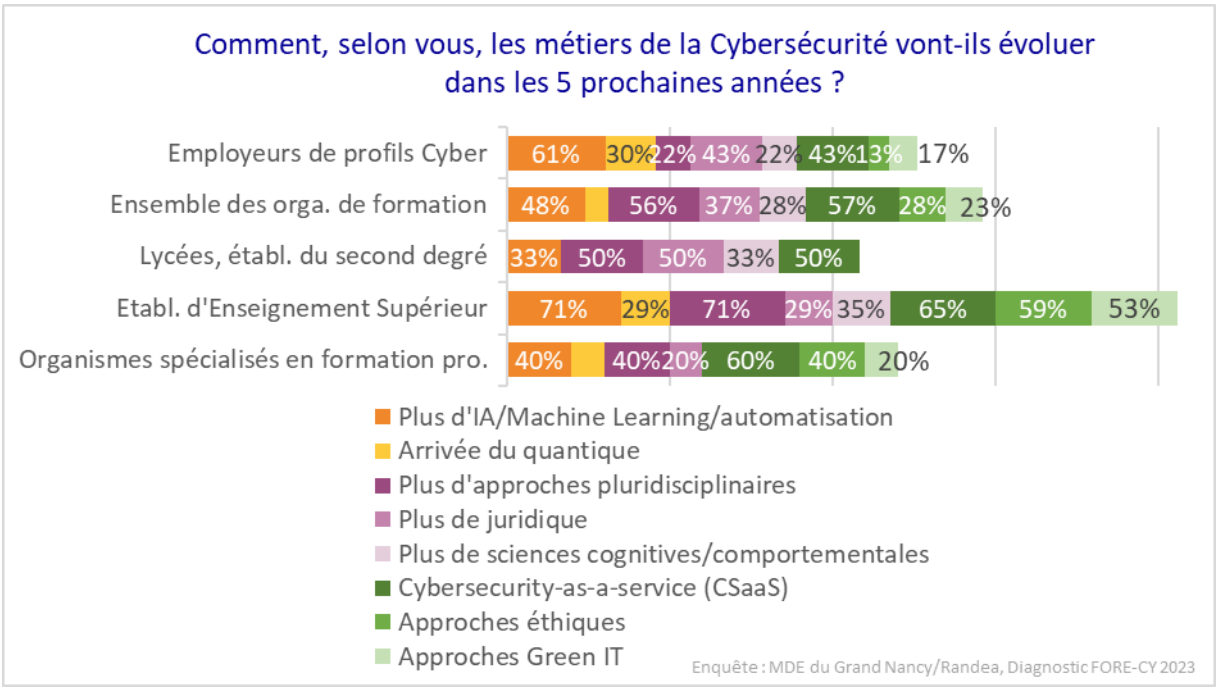
La nécessité d'aller plus avant dans l'hybridation des parcours concerne également l'intégration de compétences technologiques Cyber dans des domaines autres que technologiques. Près de la moitié des établissements de l'Enseignement supérieur de FORE-CY et 40% des organismes spécialisés en formation continue en font l'un de leurs quatre défis parmi les 10 proposés.



Note de lecture : Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

Cette priorisation des défis est à mettre en perspective avec la vision des organismes formation, ainsi que des employeurs, de l'évolution des métiers de la Cybersécurité dans les 5 prochaines années. Le domaine affrontera d'importantes évolutions et même ruptures technologiques avec l'intégration de l'IA, du Machine Learning et de l'automatisation tout d'abord, puis avec l'arrivée du quantique – problématique mise avant tout en avant par les employeurs de profils Cyber ainsi que par les établissements du Supérieur. La cybersécurité deviendra aussi toujours plus un service sur mesure, avec une forte exigence dans la posture de centration sur le client, ses besoins et sa maturité en matière de cybersécurité.

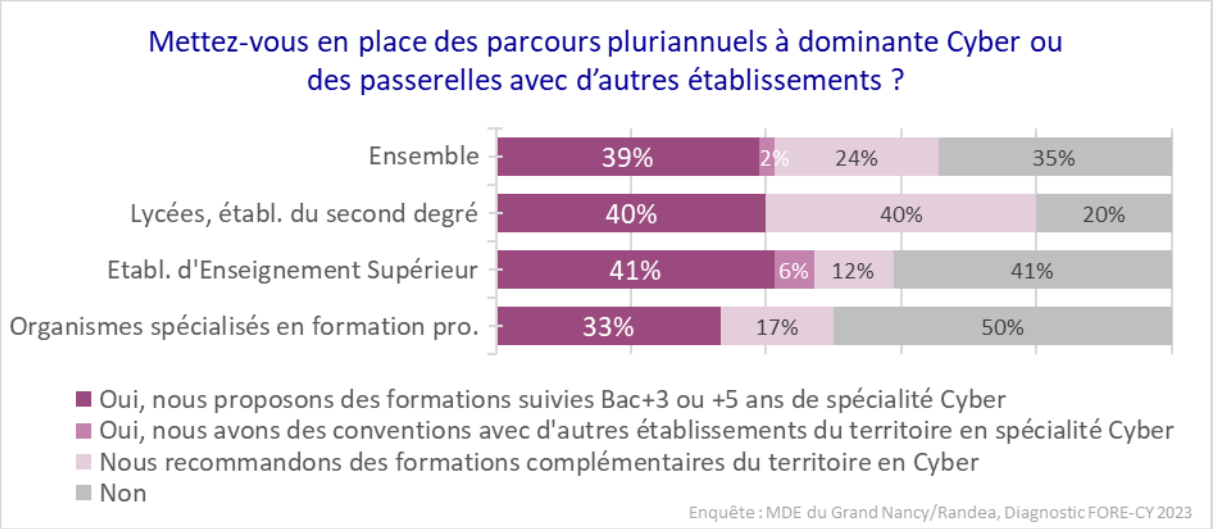
Résultat-clé : En sus de la rupture technologique de l'IA, arrive presque en tête du podium des évolutions du domaine pour les organismes de formation, l'exigence d'aller vers des approches davantage pluridisciplinaires : cette conviction est partagée par plus de 50% de l'écosystème tous types d'acteurs confondus, Enseignement supérieure en tête, BTS à leur suite pourtant aujourd'hui en marge de ces disciplines. La progression du juridique participe de cette impulsion nouvelle à donner pour près de 30% des organismes de formation, les employeurs de profils Cyber la plaçant quant à eux devant l'exigence de pluridisciplinarité.



Note de lecture : Pour faciliter l'analyse comparative, ces réponses à choix multiples ont été représentées sur une unique ligne dont le total est supérieur à 100%

- **La constitution de parcours favorisant un haut niveau d'acquisition de compétences**

Afin d'alimenter le vivier des entreprises et d'attirer des candidats à potentiel, la mise en place de parcours de formation est un atout pour le territoire. **40% des structures de formation** impliquées dans les formations Cyber à dominante technologique **proposent des parcours de formation de niveau Bac +3 ou Bac +5** donnant de la consistance aux compétences Cyber progressivement acquises (30% pour les parcours juridiques ou d'accompagnement ayant répondu à l'enquête FORE-CY).



Un autre quart des acteurs recommande des formations du territoire, complémentaires aux leurs. Rares sont en revanche les conventionnements entre établissements du territoire dans le domaine de la cybersécurité, par exemple entre établissements à dominante technologique et d'autres composantes non technologiques.

De façon cohérente, plus les organismes interviennent tardivement dans le cycle de formation (en niveau 6 ou 7) et surtout au moment de la formation continue professionnelle, moins ils ont tendance à être insérés dans un écosystème multi-acteurs facilitant les parcours pluriannuels.

Coopérer avec d'autres acteurs de formation reste une difficulté soulignée notamment par certains établissements du Supérieur (cf. graphique des difficultés 2/2). Identifier quelques voies novatrices pour faciliter des occasions de coopération serait ainsi porteur pour la filière.

Résultat-clé : Le volet « Formation » du diagnostic FORE-CY confirme cinq grands défis pour le domaine :

- La féminisation du vivier, gageur aujourd'hui comme à moyen terme ;
- L'attention insuffisante portée aux profils issus de la reconversion ;
- Le défi de la formation des formateurs ;
- L'hybridation des parcours : un virage à réussir !
- La constitution de parcours pluriannuels favorisant un haut niveau d'acquisition de compétences.

Partie III. Monographie des parcours de reconversion vers la cybersécurité : élargir le vivier et favoriser des parcours plus inclusifs

La loi pour la liberté de choisir son avenir professionnel du 5 septembre 2018 vise à faciliter l'accès de tous aux compétences, dans un contexte de mutation des modes de production, des organisations du travail, de l'emploi et des métiers. Nombreux sont les dispositifs et les outils, nouveaux ou reconfigurés, permettant d'accompagner les transitions professionnelles, dans un contexte de besoins accrus par la crise économique et sociale découlant de la crise sanitaire (Cf. Plan de relance 2020) et/ ou l'évolution de certaines attentes sociales.

Dans la perspective de rendre plus inclusifs les parcours d'accès à l'emploi et à la formation dans l'écosystème cybersécurité et d'élargir le vivier pour pallier le manque de talents et collaborateurs, le projet FORE-CY s'est attaché à étudier des parcours de reconversion professionnelle vers le domaine de la cybersécurité.

Les spécificités et la technicité des compétences déployées dans les métiers de la cybersécurité interrogent sur les possibilités et les modalités de réalisation des parcours de reconversion dans cette filière : profils et origines des candidats, dispositifs d'accompagnement mobilisés, choix et perception des métiers/compétences, engagement dans un parcours de formation, connaissance de l'écosystème d'acteurs économiques, intégration dans l'emploi, etc.

En proposant un focus sur les parcours de reconversion pour l'écosystème cybersécurité, la monographie réalisée dans le cadre du projet FORE-CY s'attache à identifier les compétences d'appui à l'œuvre et les difficultés ressenties, levées ou non, susceptibles de constituer autant de points de blocage à prendre en considération dans ces parcours spécifiques afin de les faciliter. Elle vise aussi à pouvoir proposer des parcours inspirants afin d'encourager les réinventions professionnelles capables de répondre aux besoins des entreprises prestataires de service et plus largement de l'ensemble du tissu économique et local exposé aux problématiques de cybersécurité.

Si la méthodologie de ce volet est précisée en Annexe #2, il convient néanmoins de présenter les profils rencontrés avant d'analyser leurs parcours à travers trois étapes de l'itinéraire : l'émergence du projet, la place de la formation dans le projet et enfin, la continuation du parcours jusqu'à l'intégration dans l'emploi, le cas échéant. Ce volet « Monographie de parcours de reconversion » s'achèvera par un zoom sur les compétences Cyber au prisme desdits parcours de reconversion.

1| Périmètre et profils rencontrés dans le cadre de la monographie

1.1. Notion de « reconversion professionnelle » et périmètre du diagnostic FORE-CY

Dans son rapport d'enquête sur les reconversions professionnelles, publié en février 2022[34], France Compétences définit la notion de reconversion professionnelle comme *« une évolution de la situation professionnelle se tradui[san]t par le passage d'un métier à un autre métier* ***n'ayant pas de rapport direct avec le premier ou par un changement de statut qui transforme radicalement les conditions d'exercice du métier*** *(création d'entreprise par exemple) ».* Le diagnostic FORE-CY s'est ainsi intéressé aux deux itinéraires de reconversion avec :

- **9 personnes** issues d'un cursus initial ou de premières expériences professionnelles qui n'ont aucun rapport direct ni avec la cybersécurité, ni avec la sécurité informatique ;
- **3 personnes** ayant connu une transition forte au sein de la cybersécurité ou plus globalement de l'informatique.

Ces transitions au sein du domaine Cyber ou plus largement informatique ont, en effet, nécessité une réelle conversion des pratiques professionnelles ; elles se sont parfois accompagnées d'un changement de statut et de l'approfondissement voire de l'acquisition de certains savoir-faire.

L'approche linguistique du terme de reconversion mise en avant par France Compétences y fait écho en soulignant ce qui se joue dans ces parcours : *« En anglais (retraining) ou en allemand (Umschulung), le terme de reconversion professionnelle se traduit littéralement par « reformation ». L'idée de conversion, transformer une chose en autre chose, associée au préfixe « re » qui renforce l'idée de revenir sur l'état initial ou de recommencer une conversion, pourrait traduire cette même idée que se reconvertir c'est se reformer, mais avec un sens bien plus large que retourner en formation, on pourrait dire se reconfigurer. »* Les récits du présent volet monographique sont riches de ces « re-configurations » engagées par celles et ceux qui ont accepté de témoigner de leur itinéraire.

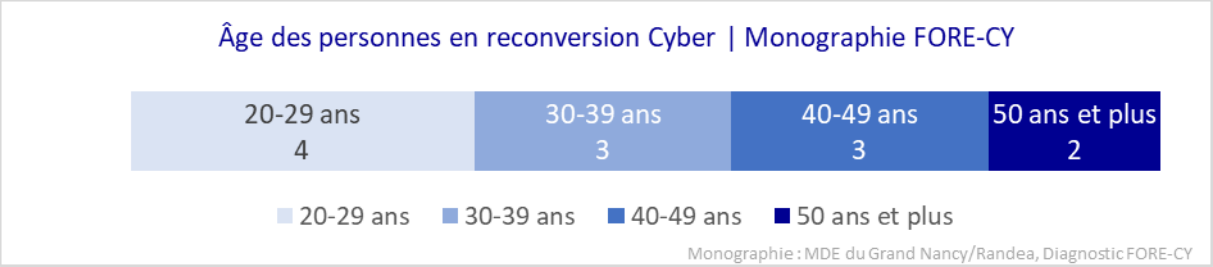
L'étude s'appuie sur le recueil et l'analyse de parcours individuels de reconversion professionnelle d'hommes et de femmes qui :

- ont finalisé leur parcours (qu'il ait ou non abouti à un emploi) au cours des trois dernières années ;
- sont en cours de réalisation de leur parcours de reconversion ;
- ont commencé mais stoppé leur parcours.

Principales caractéristiques de l'échantillon de l'approche monographique

Les entretiens ont été réalisés auprès de 11 hommes et 1 femme, âgés de 22 à 57 ans.

[34] https://www.francecompetences.fr/app/uploads/2022/02/Rapport_Reconversion_Professionnelle2021.pdf



L'avancement des projets de reconversion :

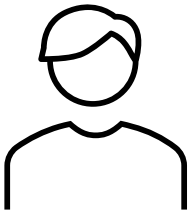
- 2 personnes amorcent leur parcours de reconversion : elles sont en recherche d'employeurs qui vont leur permettre d'entrer en formation après avoir connu une rupture dans leur parcours initial ;
- 7 personnes sont en cours de formation ;
- 1 personne est en recherche de formation pour compléter son parcours après une première formation ; 1 autre personne a réalisé une transition lente d'un métier de la cybersécurité à un autre et étudie l'opportunité de réaliser une formation ;
- 1 personne a finalisé son parcours ; elle est actu intégrée dans l'emploi.

Les diplômes visés par les personnes en cours de formation :

- 4 personnes visent un diplôme Bac +3 d'Administrateur d'infrastructures sécurisées ;
- 2 personnes sont en dernière année pour obtenir un diplôme Bac +5 comme Manager en système d'information, option cybersécurité ;
- 1 personne est en année de spécialisation cybersécurité au sein de l'école 42 à Paris ; le diplôme de cette formation n'est pas reconnu par l'État.

1.2. Présentation individuelle des personnes rencontrées

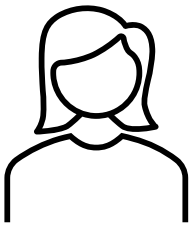
N.B. Les prénoms ont été modifiés afin de préserver l'anonymat des interviewés



SYLVAIN – 43 ANS

Après un BEP Topographie puis un Bac Pro Dessin industriel, Sylvain a finalement choisi de s'auto-former à la création de sites internet. Il est devenu webdesigner à son compte pendant 7 ans. Peu à l'aise avec le développement commercial, Sylvain a fermé son entreprise et n'a plus travaillé dans le domaine de l'informatique pendant 10 ans. Il a travaillé avec ses parents sur les marchés pendant 5 ans et s'est à nouveau auto-formé à la réalisation d'images 3D.

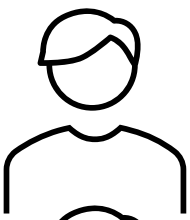
En 2021, il choisit de s'orienter vers l'informatique et reprend une première formation Bac +2 Technicien supérieur Systèmes et Réseaux (TSSR). Il suit actuellement un Bac +3 Administrateur d'Infrastructures Sécurisées.



ANAÏS – 31 ANS

Après un Bac littéraire, Anaïs qui souhaitait rapidement entrer dans le monde du travail a obtenu un CAP Coiffure complété par une Mention Complémentaire, un Brevet Professionnel puis un Brevet de Maitrise.

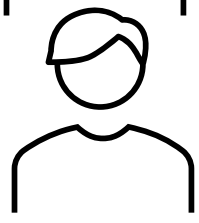
En 2017, elle fait le choix de s'orienter vers l'informatique et entame en 2018 une formation Bac +2 de Gestionnaire en Maintenance et Support Informatique. Elle suit actuellement une formation Bac +5 de Manager en Systèmes d'Information.



AMIR – 32 ANS

Après un Bac scientifique, Amir s'est formé au montage vidéo. Après plusieurs années en tant que monteur et enseignant, il se réorienter vers l'informatique.

En 2021, il intègre l'École 42 à Paris au sein de laquelle il est actuellement en année de spécialisation.

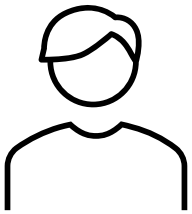


BILAL – 22 ANS

Après avoir obtenu son Bac, Bilal postule sans succès à un BTS Services Informatiques aux Organisations (SIO). Il débute une année universitaire en Maths-Info sans l'achever. Il souhaite alors

s'orienter vers une L1 Histoire mais faute de place, est orienté vers une L1 Géographie qui ne l'a pas intéressé.

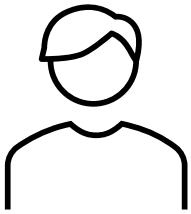
En 2021, après une expérience en tant que livreur, il décide de reprendre des études en informatique. Il a entamé une année en alternance en Bac+2 Gestionnaire en Maintenance et Support Informatique. Son contrat d'alternance ayant été rompu avant la fin de l'année, il n'a pu terminer l'année scolaire. Accompagné par la Mission Locale, il est actuellement à la recherche d'un employeur pour reprendre son Bac+2.



PASCAL – 57 ANS

Après un diplôme d'ingénieur informatique et plusieurs années en entreprises de développement de logiciels, Pascal a créé sa propre entreprise de sensibilisation à la cybersécurité.

Intéressé par l'accompagnement des organisations, la transformation des usages, la valorisation des données, il s'oriente désormais vers des prestations de conseil aux entreprises plus globales.

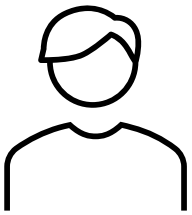


FREDERIC – 52 ANS

Après un Bac Pro en Bureautique et système informatique, Frédéric a suivi un DEUG en Sociologie « pour comprendre comment les hommes fonctionnent » et a finalisé son parcours par une licence en Informatique.

Il travaille plusieurs années dans une SSII, puis à son compte, avant de rejoindre une nouvelle entreprise comme salarié dans la domotique.

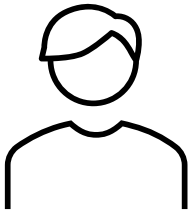
Afin de mettre à jour ses compétences et de se spécialiser dans la cybersécurité, après une prépa compétences, il a intégré en 2022 un Bac + 3 Administrateur d'Infrastructures Sécurisées.



GUILLAUME – 28 ANS

Après un BEP et un Bac Pro Cuisine, Guillaume a obtenu un CAP Pâtissier avec une Mention Complémentaire avant d'intégrer les cuisines d'un restaurant étoilé.

En 2017, il change de voie et décide de s'orienter vers l'informatique. Il entame en 2018 une formation Bac +2 de Gestionnaire en Maintenance et Support Informatique. Il est actuellement en formation Bac +5 Manager en Systèmes d'Information.

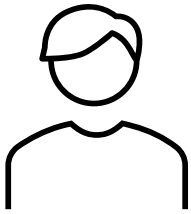


JÉRÉMY – 35 ANS

Après un Bac Pro Vente et négociation, Jérémy a obtenu un BTS Banque. Il a travaillé quelques années en intérim.

En 2013, il décide de reprendre des études en informatique et intègre une formation Bac +2 de Gestionnaire en Maintenance et Support Informatique en alternance. Il continue son parcours jusqu'à valider un Bac +5 Manager en Systèmes d'Information. A l'issue, il sera embauché par l'entreprise qui l'emploie depuis sa première année d'alternance.

Il est actuellement Responsable des SI au sein de cette entreprise.

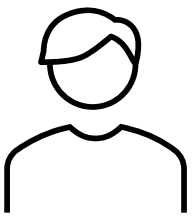


DYLAN – 41 ANS

Après un Bac Sanitaire et social, Dylan commence à travailler dans le monde du secours en tant que Pompier, Gendarme et Policier Municipal. En 2010, il passe une capacité professionnelle en transport de marchandise et ouvre son entreprise de transport d'organes. En 2019, il doit arrêter son activité pour des raisons de santé et décide de s'orienter vers le domaine de la cybersécurité.

En 2021, il intègre une formation Bac +2 Technicien Supérieur Systèmes et Réseaux et obtient un CDD dans l'entreprise qui l'emploie en alternance. Son CDD ne sera pas renouvelé.

Il recherche actuellement un employeur et envisage de consolider son parcours avec une nouvelle formation.

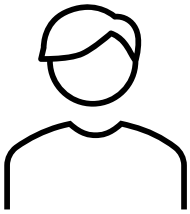


SÉBASTIEN – 45 ANS

Après un BEATEP Guide et Animateur Nature, Jérôme obtient un BTS Gestion et protection de la nature. Il travaille ensuite en tant que Chargé de mission dans plusieurs organismes.

Il est licencié en 2018 pour inaptitude. Après un bilan de compétences, il fait le choix de s'orienter vers le domaine de l'informatique et intègre en 2021 une formation Bac +2 Technicien Supérieur Systèmes et Réseaux.

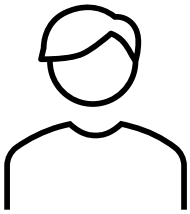
Il poursuit actuellement son parcours en Bac +3 Administrateur d'Infrastructures Sécurisées.



BACARY – 22 ANS

Après un Bac STIDD et un BTS Services Informatiques aux Organisations (SIO) option Solutions d'Infrastructure, Systèmes et Réseaux (SISR), Bacary s'inscrit en 2022 dans une formation Bac +3 en alternance mais n'a pas trouvé d'employeur.

Dans l'attente de la rentrée prochaine, Bacary a effectué un CDD de 2 mois en tant que chargé de clientèle. Il poursuit sa recherche d'employeur pour mener à bien son projet d'obtention d'un diplôme Bac +3.



TRISTAN – 28 ANS

Après un CAP Vente obtenu en 2013, Tristan connaît plusieurs années de chômage.

En 2016, après quelque temps en chantier d'insertion, il reprend les études en vue de l'obtention d'un BEP informatique puis d'un Titre professionnel de Technicien assistance informatique.

Il continue son parcours et intègre en 2022 une formation Bac +3 Administrateur d'Infrastructures Sécurisées.

1.3. Les perceptions contrastées du domaine de la cybersécurité

L'échantillon de la monographie des parcours de reconversion s'avère varié tant par les parcours initiaux que par les métiers cibles visés au sein du domaine de la cybersécurité. **Cette diversité nourrit également des perceptions différentes de son périmètre même et de la technicité à maîtriser pour en relever.**

Dès les prises de contact pour réaliser les entretiens, plusieurs personnes ont été surprises d'être sollicitées et perçues comme réalisant « un parcours de reconversion dans le domaine de la cybersécurité ». En effet, de leur point de vue, la cybersécurité cible un petit nombre de métiers axés sur la cyberprotection, à l'image du *pentester* ou de l'analyste SOC. **En tant que futurs administrateurs réseaux, ils ne considèrent pas intégrer le monde des professionnels de la cybersécurité.**

> *« Le côté cybersécurité c'est un autre monde, un autre métier que ce qu'on fait ici » (Anaïs, 31 ans)*

> *« Si demain vous me parlez d'un poste d'admin système qui doit inclure dans ses process la cyber dans son environnement, je suis armé. Mais si demain je dois faire du pentest, pas du tout. » (Guillaume, 28 ans)*

> *« Je suis pas sorti en tant qu'expert cybersécurité. » (Jérémy, 35 ans)*

Ces écarts de perception mettent en évidence deux types de projets professionnels en lien avec le domaine. D'une part, les projets professionnels orientés informatique et réseaux qui ne comptent qu'« une pointe de cybersécurité » considérée comme *« indispensable quand on travaille dans l'informatique »* sans être pour autant un professionnel du domaine.

D'autre part, les projets professionnels spécifiquement et volontairement dédiés à la cybersécurité qui nécessitent au préalable une solide formation *« socle dans l'informatique » :*

> *« Le niveau en matière de cybersécurité est hyper élevé. Je pense qu'on peut pas directement entrer dans ce domaine sans avoir les bases en système et réseau » (Sylvain, 43 ans)*

2| L'émergence des projets de reconversion

À l'exception de deux personnes contraintes d'interrompre leur précédente expérience professionnelle pour **raisons de santé**, les parcours de reconversion de FORE-CY relèvent d'une **démarche volontaire**. **Une décision est prise, élaborée dans le temps ; un choix est posé ; des actes concrétisent la prise de décision dans les faits. Autant de stades de maturation d'un projet dont il est précieux de comprendre la genèse.**

2.1. L'insatisfaction vis-à-vis des cursus initiaux ou de la situation de travail : un point de départ

Lorsque le parcours de reconversion relève d'une démarche volontaire, il trouve son origine chez nombre d'enquêtés dans une **insatisfaction vis-à-vis de l'activité professionnelle précédente, son contenu, les conditions de travail précédentes et/ou leurs répercussions sur la vie personnelle :** rémunération, équilibre entre vie professionnelle et vie personnelle.

> *« C'était par volonté de me challenger un peu plus intellectuellement et de changer. Je m'ennuyais un petit peu » (Anaïs, 31 ans)*

> *« Je me suis rendu compte que ça ne me convenait pas trop en termes de rythme, de perspectives d'évolution, de salaire. » (Amir, 32 ans))*

> *« Je m'étais rendu compte que je n'avais pas de vie privée. Je ne voyais pas ma famille, ni ma compagne. » (Guillaume, 28 ans)*

Le domaine de formation initiale et les premiers choix d'orientation professionnelle sont synonymes pour un certain nombre de « choix par défaut », voire de voie « imposée ».

> *« La vente… J'avais pas trop choisi ma voie à ce moment-là. Il fallait que je choisisse un truc à tout prix donc je suis allé là, par défaut. » (Jérémy, 35 ans)*

> *« Je voulais faire du dessin artistique et on m'a envoyé faire du dessin industriel. J'ai dit oui parce que je savais pas trop quoi faire non plus. On m'a mal orienté. » (Sylvain, 43 ans)*

Pour Anaïs, le choix de la coiffure renvoie certes à des premières expériences positives mais il lui est difficile de réélaborer les arguments de la décision, comme si cette dernière avait été prise de manière instinctive sans poser un choix clair, point déterminant dans le parcours de reconversion.

> *« J'étais au lycée, je ne savais pas trop ce que je voulais faire. Je savais que je voulais commencer à travailler rapidement et je sais pas trop comment l'idée est venue, mais j'ai fait plusieurs stages et ça m'a bien plu donc je me suis orienté comme ça » (Anaïs, 31 ans)*

La dynamique processuelle qui sous-tend les parcours de reconversion s'ancre ainsi sur une forme de « creux » qu'il s'agisse d'un « par défaut » ou d'un « je ne sais pas trop comment ». De manière plus ou moins consciente, ces « creux » constituent une force motrice des projets, la reconversion professionnelle ayant tout autant un objectif professionnel que personnel : s'engager vers un métier plus en phase avec ses aspirations personnelles afin, pour un certain nombre, d'éprouver de la satisfaction au travail voire pour avoir/faire « un travail-passion».

> *« Je voulais avoir un travail qui me plait. » (Guillaume, 28 ans) | « Je n'avais pas envie de faire un travail alimentaire, je voulais travailler par passion. » (Jérémy, 35 ans)*

A l'insatisfaction professionnelle d'hier ou à l'impossibilité de poursuivre pour raisons de santé, la reconversion doit répondre par un horizon professionnel positif, porteur d'une forme de validation pour soi-même.

2.2. Le choix du domaine cible de la reconversion

Trajectoires ou arguments-types A : l'appétence ou les qualités personnelles

Le domaine cible de reconversion – l'informatique ici – est **choisi par un premier profil de personnes davantage en référence à leur monde personnel qu'en fonction de références professionnelles.** A tout le moins, le choix

du domaine de reconversion est **légitimé dans la narration en convoquant une forme de genèse personnelle :** l'appétence ancienne pour l'informatique, le goût pour « les énigmes », la curiosité à vouloir « comprendre comment les choses fonctionnent », le plaisir de « bidouiller »…

L'ancrage et l'alignement avec soi-même sont tout à la fois la finalité du projet de reconversion et la raison ou la motivation pour un domaine professionnel cible.

> *« Ça a commencé depuis tout petit, j'étais intéressé par le poste informatique. Au fur et à mesure j'ai commencé à démonter des PC, j'adorais ça. » (Tristan, 28 ans)*

> *« C'est un truc que j'aime bien depuis tout petit, quand je suis chez moi c'est moi qui bidouille. J'aime bien bidouiller, voir ce qu'il y a à l'intérieur, comprendre comment ça marche. » (Sylvain, 43 ans)*

> *« Pour moi l'informatique c'était un peu comme un casse-tête et j'aime bien les énigmes. Le côté logique des choses me plaisait bien. » (Anaïs, 31 ans)*

L'appétence ancienne pour « l'informatique » ou plus largement la référence à l'enfance, à ses qualités personnelles, ses goûts soulignent le travail entrepris de légitimation, de fondation du projet du reconversion dans une histoire personnelle. Au sentiment de « par défaut » ou simplement du « pourquoi pas » ou du simple enchaînement dont les individus se sont sentis l'objet, ces derniers répondent par un projet convoquant l'univers personnel, signal du processus de réappropriation qui s'est opéré.

L'appétence et le rapport électif au métier cible sont également de mise dans les parcours de reconversion pour nécessité de santé : Sébastien (45 ans) chargé de projet en gestion et protection de la nature, s'occupait déjà du parc informatique de l'association qui l'employait ; quant à Sylvain, il *« a passé [son] enfance à bidouiller du matériel informatique ».*

L'appétence et la genèse personnelle convoquées sont facteurs de confiance bien au-delà de toute compétence acquise par l'expérience qui serait capitalisable. Ainsi, plusieurs interviewés s'accordent à dire qu'ils avaient surestimé leurs compétences : après quelques mois de formation, ils ont découvert *« qu'ils n'y connaissaient rien », contrairement à leur opinion en début de formation.*

Trajectoires ou arguments-type B : un travail de projection de soi, inspiré ou facilité par les exemples de l'entourage

Parmi les personnes interrogées, plusieurs connaissaient des personnes ayant engagé une reconversion. **L'exemple a pu être rassurant, voire un facteur déclenchant jouant un rôle moteur** pour engager elles-mêmes leur reconversion. Ces personnes s'inspirent des parcours qui les entourent ; **elles se mettent en situation, se projettent ou non dans le domaine professionnel de ces « prédécesseurs ».**

> *« J'ai des collègues, anciens gendarmes, qui sont reconvertis dans l'informatique. » (Dylan, 42 ans)*

> *« Mon beau-frère est programmeur informatique donc il m'a montré, je me suis rendu compte que c'était pas du tout ce que je voulais faire. » (Dylan, 42 ans)*

> *« Ce qui m'a fait prendre conscience que je devais quitter le monde de la restauration, c'est un camarade qui avait 10 ans de plus que moi et qui venait d'avoir un enfant et qui a fait ça. » (Guillaume, 28 ans)*

L'entourage et le conseil de personnes ayant déjà engagé des reconversions sont une **source importante d'informations :** aide pour le choix du métier, renseignements sur les formations, connaissance des dispositifs, etc. **Ils sont des facilitateurs crédibilisant le projet de reconversion.**

> *« J'ai été mis en contact par un ami commun avec une personne qui était dans le même cas que moi, qui faisait une reconversion à un stade plus avancé. J'ai beaucoup discuté avec et lui et c'est là que je me suis dit que c'était ce que je voulais faire. […] C'était pour découvrir plutôt ce qu'il faisait, le ou les métiers potentiellement qui s'ouvriraient derrière une formation. » (Guillaume, 28 ans)*

> *« J'ai beaucoup de personnes autour de moi qui ont fait des reconversions et qui ne travaillent pas du tout dans leur domaine initial. Donc je savais que ce serait pas un frein pour moi de reprendre des études. » | « Je connaissais des personnes de mon entourage proche, famille et ami qui ont suivi le même parcours CESI, en tout cas au début +2 et +4 et qui se sont arrêtés après. […] Ça a joué dans le choix de mon parcours. » (Anaïs, 31 ans)*

L'engagement dans la reconversion prend appui sur les exemples de l'entourage, se nourrit d'échanges et **s'opère par projection interpersonnelle**. **Le témoignage d'alter ego passé par la reconversion joue comme l'élément de preuve et de pertinence de la démarche.**

Ainsi, alors que certaines personnes rencontrées avaient déjà réalisé au cours de leur carrière d'autres reconversions, ils n'ont pas paradoxalement mis en avant cette expérience lors des entretiens. **Cela souligne combien dans ces projets-types de reconversion, un travail personnel projectif s'élabore dans l'interpersonnel.**

Trajectoires-type Bbis : un projet d'évolution né des constats sur le terrain professionnel et de la volonté d'y répondre

Pour les personnes rencontrées qui évoluaient déjà professionnellement dans la cybersécurité ou en informatique, **la reconversion se joue davantage sur le terrain professionnel.** La réorientation de l'activité se nourrit des constats faits au regard de leur pratique professionnelle.

> *« Je me suis rendu compte qu'on laisse les experts faire leur sauce et qu'il manque un truc dans le dialogue avec les non experts. » (Pascal, 57 ans)*

> *« Je me suis rendu compte qu'y avait plein de jeunes qui arrivaient et qu'il fallait que je mette à jour mes compétences et que je m'oriente vers un secteur qui se développe, donc la cybersécurité. » (Frédéric, 52 ans)*

Le projet de reconversion vise **à compléter leurs compétences actuelles en *« ajoutant plusieurs cordes à [leur] arc »* en capitalisant sur les expériences passées, tout en se réinventant pour rester maître de demain.** Il s'agit ici de projets de croissance.

Trajectoires ou arguments-type C : dépasser l'idée reçue de l'informatique, domaine inaccessible

Si la majorité des personnes interrogées ont évoqué leur appétence ancienne pour le domaine de l'informatique, peu avaient envisagé de se former dans cette filière : *« Ça ne m'était pas venu à l'idée. » (Sylvain, 43 ans).* La perspective de faire des études dans ce domaine semblait inaccessible et réservée à d'autres profils socio-culturels, notamment pour toutes les personnes dont le niveau initial d'études se situait entre un Bac Pro et un Bac +2 :

> *« Je pensais pas qu'on pouvait travailler dans l'informatique sans faire de grandes études. Je sors d'un milieu ouvrier, les grandes études on connaît pas et j'avais personne pour me guider là-dessus. » (Jérémy, 35 ans)*

> *« Je pensais pas que c'était accessible sans un bac. J'avais qu'un BEP au final. Pour moi c'était un monde d'ingénieur. […] C'est tellement vaste l'informatique. La partie système, réseau ou sécurité n'a jamais été dans mon spectre de recherche, je pensais que c'était pour du très haut niveau » (Sylvain, 43 ans)*

Pour que le projet de reconversion puisse prendre forme, il aura donc fallu dépasser le sentiment d'inaccessibilité du domaine informatique et être capable de s'imaginer autrement que sous les traits « en creux » de quelqu'un « qui n'a pas fait de longues études » et n'a pas les compétences techniques suffisantes.

Trajectoires ou arguments-type D : se spécialiser en cybersécurité, par pragmatisme

Le domaine de l'informatique est très large et les métiers qui y sont liés souvent méconnus. Parmi les personnes qui n'étaient pas issues du domaine de l'informatique, les témoignages mettent en avant les difficultés à trouver des informations pour s'orienter vers la bonne voie ou le bon métier.

« C'est tellement vaste l'informatique » (Sylvain, 43 ans) | « La cybersécurité c'était pas mon premier choix » (Bilal, 22 ans)

Si certains étaient sûrs de vouloir s'orienter vers la sécurité informatique, pour d'autres, cela n'a pas été un choix réalisé par passion. Il s'agit parfois d'un « second choix » raisonnable parce que le projet initial n'a pas pu se faire :

« D'abord j'ai cherché une formation dans la programmation, j'ai trouvé un organisme mais c'était une usine à formation et ça c'est scandaleux. » (Amir, 32 ans) | « J'avais hésité avec le développement. A la base je m'orientais plus vers le développement, mais je n'ai pas réussi à trouver de formation qui me convenait. » (Anaïs, 31 ans)

Le pragmatisme et la rationalité instrumentale s'immiscent aussi dans le choix du domaine cible, les candidats à la reconversion tenant comptent du marché de l'emploi et des opportunités d'embauche à l'issue : *« J'avais regardé un peu les offres et j'ai vu qu'y avait beaucoup d'offres dans ce domaine. » (Jérémy, 35 ans).* L'objectif de chacun est, en effet, de pouvoir travailler à l'issue du projet de reconversion.

Résultat-clé : Le choix du domaine de reconversion est un élément structurant du projet de reconversion. Il s'élabore dans le temps à la croisée des mondes personnels, interpersonnels et professionnels. Quatre lignes de forces complémentaires ont pu être mises en évidence que les candidats à la reconversion gagneront à expliciter sous la forme d'une grille d'aide à la décision :

- **l'appérence et les goûts personnels** permettant d'ancrer son projet en soi-même et dans sa biographie ;
- **la capacité à la projection de soi dans un métier donné en s'inspirant des exemples de l'entourage ou en capitalisant sur son parcours professionnel** dans le cas d'une reconversion sans changement de domaine professionnel ;
- **la capacité à dépasser les idées reçues** notamment celle selon laquelle l'informatique est un domaine inaccessible ;
- **l'indispensable pragmatisme vis-à-vis du marché de l'emploi, des facilités ou difficultés d'embauche, ou encore de l'accessibilité de l'offre de formation et de son adéquation au candidat.**

2.3. L'importance des recherches personnelles et l'appui sur les acteurs d'accompagnement

Quel que soit le profil de la personne interviewée, **les recherches personnelles pour identifier les métiers envisageables et éventuellement les formations disponibles ont une place importante dans l'initialisation de la reconversion et l'engagement dans le parcours**.

« J'ai fait beaucoup de travail personnel de recherche pour trouver des formations, sur internet notamment, qui pouvaient mener à la cybersécurité. » (Dylan, 42 ans)

« J'étais allé sur des salons de l'emploi, je me suis renseignée de mon côté sur les possibilités en alternance. » (Anaïs, 31 ans)

Les recherches personnelles ont parfois été rendues difficiles par la méconnaissance des métiers évoquée précédemment, ainsi que par la méconnaissance des lieux (physiques ou sur internet) où trouver l'information.

Point-clé : Hormis quelques personnes ayant réalisé leurs recherches en toute autonomie, en contactant directement des organismes de formation, la plupart des candidats à la reconversion se sont rapprochés de structures d'accompagnement comme Pôle Emploi, Transition Pro (ex-FONGECIF), la Mission Locale, Place des Compétences Numériques ou encore Cap emploi. **Ces structures sont bien identifiées comme pouvant répondre aux besoins en matière d'orientation dans l'emploi et la reconversion, avec un retour d'expérience variable.**

« Je suis allé me renseigner partout, y compris à la mission locale et Pôle emploi. » (Tristan, 28 ans)

« J'ai contacté la mission locale, j'ai rencontré ma conseillère avec laquelle je suis toujours en contact. Elle m'a aidé à m'orienter. » (Bilal, 22 ans)

« Je suis passé par le Fongecif et j'ai cherché à droite, à gauche des formations. Je suis passé par leur biais pour trouver une formation auprès du CNAM. » (Guillaume, 28 ans)

Si certaines personnes regrettent de ne pas s'être approchées plus tôt de structures d'accompagnement pour éviter de *« tourner en rond »,* les expériences d'accompagnement sont parfois moins satisfaisantes.

« Au final, j'ai fait les démarches moi-même. A l'usage, je trouve que les échanges qu'on peut avoir avec les personnes de Pôle Emploi sont pas très intéressants. Ils poussent plutôt à avoir un emploi. » (Amir, 32 ans) | « Je suis passé par la mission locale. J'ai rien trouvé de spécifique. Côté ANPE, j'ai pas spécialement été aidé non plus. Et après internet. » (Jérémy, 35 ans)

« Je m'étais renseigné de mon côté et je voulais aller vers le côté système et réseau. La personne de Pôle Emploi m'a dit qu'elle avait justement reçu un mail pour une session de renseignement pour ça. Et tout s'est enchainé » (Sylvain, 43 ans)

Notons que les deux personnes ayant engagé des reconversions pour raisons de santé, n'ont pas bénéficié d'accompagnement renforcé lié à la spécificité de leur situation. L'un a anticipé les difficultés et engagé un parcours classique en tant que demandeur d'emploi : il a engagé sa reconversion en recherchant par lui-même les formations disponibles, puis en contactant Pôle Emploi pour obtenir l'AIF (Aide Individuelle à la Formation).

Pour le second, après un licenciement pour inaptitude, et dans l'attente d'un diagnostic définitif en matière de santé, il a engagé un bilan de compétences avec Cap Emploi dont les conclusions sont intervenues avant le bilan santé. Il a donc recherché par lui-même ultérieurement un métier adapté à sa situation médicale.

3| La place de la formation dans le parcours

Sur l'ensemble du panel de personnes interviewées, nombreuses sont celles qui ont, ou qui comptent engager une formation dans le cadre de leur projet de reconversion. Il est donc intéressant de s'intéresser à la place de la formation dans les parcours de reconversion :

- Comment la formation s'intègre-t-elle au parcours de reconversion dans le domaine de la cybersécurité, notamment en termes de temporalité ?
- Les formés en reconversion sont-ils des « étudiants » comme les autres ou gagneraient-ils à bénéficier d'un accompagnement spécifique ?

3.1. La formation : un passage, si ce n'est indispensable, à tout le moins essentiel et structurant dans le parcours de reconversion

Point-clé : Pour les personnes dont l'expérience professionnelle précédente n'a pas de lien avec la cybersécurité, le passage par une formation est un indispensable pour *« obtenir des compétences ».* Ces compétences très techniques et spécifiques ne pouvant pas, selon eux, être exclusivement obtenues par l'auto-formation. La formation est alors le marqueur du « démarrage » du parcours de reconversion.

Pour ceux qui jugent avoir les compétences nécessaires, mais constatent qu'elles ne sont pas reconnues sur le marché de l'emploi, l'étape de la formation permettra d'obtenir une *« reconnaissance de leurs compétences via un diplôme »* afin de faciliter leur intégration professionnelle. **La formation intervient alors plutôt comme une consolidation de « fin de parcours » de reconversion face aux difficultés d'insertion professionnelle** :

« On me propose des postes de technicien niveau 1 parce que c'est le diplôme que j'ai. Mais ça m'intéresse pas du tout. C'était ce que je faisais chez mon ancien employeur mais j'avais aussi un large panel de missions qui me permettait de faire d'autres choses, notamment de développer toute la partie sécurité. Donc il va falloir que je reprenne une autre formation. » (Dylan, 42 ans)

Dans les parcours de « transitions » d'un champ de la cybersécurité vers un autre, le passage par une formation représente aussi un moyen d'aller *« au bout de la logique de reconversion »*, de *« mettre à jour leurs connaissances »*. **La formation intervient, là aussi, comme une consolidation mais non pas de la fin du parcours de reconversion, mais des compétences nouvelles à faire valeur et mettre en œuvre. Elle joue classiquement le rôle de renforcement et de maturation des savoir-faire.**

Quel que soit le profil de la personne interviewée, le parcours formatif apparaît pour les acteurs, être une étape très structurante, voire indispensable, pour asseoir leur reconversion.

3.2. Des délais variables, mais souvent longs, entre le projet de reconversion et l'entrée effective en formation

Point-clé : Pour celles et ceux qui sont en cours de formation ou l'ont finalisé, **les délais entre la décision d'entamer une reconversion professionnelle et l'entrée en formation sont très inégaux.** Ils se situent entre deux mois et deux à trois ans.

« Ça a été assez passif. C'est venu avec Pôle emploi en septembre 2021 et de là tout s'est enchainé très vite. Ça s'est fait en deux mois. » (Sylvain, 43 ans)

« Un an et demi entre l'envie et le démarrage de la formation. » (Anaïs, 31 ans)

Les délais longs s'expliquent principalement par le **temps de maturation nécessaire** pour identifier le projet adapté : *« Le temps de mûrir le projet »*. Pour d'autres, il s'agit de facteurs contingents externes qui ne manquent pas quelle que soit la période : « *Le COVID a décalé mon entrée en formation » (Amir, 32 ans)* ou des difficultés d'accompagnement par Pôle Emploi : *« Mon dossier de demande de financement était resté au point mort pendant plus d'un an » (Dylan, 42 ans).*

3.3. Un projet de formation qui s'allonge et se métamorphose au cours de la reconversion : dépasser les stigmates et se réaliser à Bac+5

Nombre des candidats à la reconversion n'envisageaient pas faire de longues études en prenant la décision d'entamer un parcours de reconversion. Cela ne faisait pas partie de leurs ambitions initiales. Or plusieurs d'entre eux, sont *in fine* engagés dans un cursus ou ont obtenu un diplôme Bac+5 bien qu'ayant débuté en partant *« à la base pour un Bac+2 »*.

C'est en cours de formation, en constatant « qu'ils se débrouillaient bien » et parfois avec les encouragements des équipes pédagogiques que la perspective d'un diplôme plus élevé qu'un Bac +2 a pu être envisagée.

« Finalement je me débrouillais bien, on m'a incité à rester et je suis resté. Je ne regrette pas, en arrivant au bout du tunnel » (Guillaume, 28 ans)

« A la base je voulais juste faire un BAC+2 mais ça s'est pas arrêté là. Les deux premières années se sont bien passées. Y avait encore pleins de choses à faire. Mon employeur était d'accord. Et je suis parti encore sur 3 ans. » (Jérémy, 35 ans)

3.4. La reprise d'études : un fort investissement et la pression de l'échec

Les témoignages recueillis soulignent tous l'impact important de la reprise d'étude sur la vie personnelle, ne serait-ce que par son incidence financière très significative :

> *« Les premières années c'était compliqué. Avec un appartement à 750 euros, c'était compliqué » (Jérémy, 35 ans)*

> *« Là je suis plus précaire que quand je travaille. Mais disons que je préfère être précaire dans ce cadre-là ou je fais quelque chose qui m'intéresse » (Amir, 32 ans)*

> *« Je suis retourné chez mes parents. Par rapport au chômage que je touche, je ne peux pas me permettre d'avoir un appartement. » (Tristan, 28 ans)*

L'incidence est également forte en termes d'investissement sur leur **temps personnel.**

> *« Il a fallu énormément de travail personnel. » (Bacary, 22 ans) | « Sans travail personnel, engagement et sans motivation ce n'est pas quelque chose qui est réalisable. » (Dylan, 42 ans)*

Ces investissements en temps et financier sont même considérés par certains comme un « sacrifice » nécessaire pour la réussite du projet : *« Là j'arrive à la consécration après 7 ans de sacrifices. » (Guillaume, 28 ans)*

> *« Ça demande beaucoup de temps personnel. Mais il faut parfois se couper du reste du monde pour réussir ce que l'on veut faire » (Jérémy, 35 ans)*

Difficile d'apprécier si le temps de travail personnel est d'une volumétrie usuelle ou si la reconversion joue (domaines moins maîtrisés à rattraper ou compenser, méthodes formelles à acquérir, exigence personnelle plus élevée…). Toutefois, plusieurs témoignages montrent que **leur situation spécifique de « personne en reconversion » les a amenés à ressentir une pression supplémentaire, celle de la crainte de l'échec** et de l'appréhension inhérente au retour en apprentissage à un âge plus avancé. Cette pression a conduit certains à beaucoup travailler pour favoriser leur réussite.

> *« Je me suis mis beaucoup la pression sur le fait que je devais absolument pas échouer […] Y a des moments où j'étais vraiment en souffrance par rapport à ça. » (Anaïs, 31 ans)*

> *« J'ai pu penser moi-même que j'suis trop vieux […] Et des fois je crois que j'ai pu mal gérer cette mauvaise pensée et j'ai beaucoup trop travailler. J'étais proche du burn out » (Amir, 32 ans)*

Cette pression supplémentaire est également liée dans certains témoignages en la reliant à un *« sentiment d'illégitime »* et à la nécessité de devoir *« faire ses preuves » :*

> *« Ce syndrome de l'imposteur et ce problème de légitimité, je l'ai retrouvé quelques années après avoir démarré mon parcours. Du coup je me suis donné à fond. » (Jérémy, 35 ans)*

3.5. L'importance des soutiens pendant le temps de formation

La pression ressentie et les sacrifices consentis traduisent l'intensité et les difficultés du parcours emprunté. Pour y parvenir, les interviewés mettent également en avant **l'importance des soutiens reçus tout au long de leur parcours.**

> *« Pour entreprendre ce genre de choses-là, il faut du soutien parce que c'est extrêmement difficile. » (Amir, 32 ans) | « Mes amis étaient un soutien important. J'ai toujours su que je voulais faire un Bac+5 mais y a plein de fois où je me suis dit que j'allais arrêter avant » (Anaïs, 31 ans)*

Le soutien reçu est principalement d'ordre « moral » et psychologique ; il est aussi ponctuellement d'ordre matériel ou financier, notamment s'agissant des parents (aide, logement…).

Point-clé : Si les familles, le conjoint et les amis sont régulièrement cités, le soutien moral ne relève pas exclusivement du cercle intime et familial. Les témoignages mettent aussi en avant le rôle important des professionnels côtoyés au sein des entreprises lors des alternances ou des stages, et celui des professionnels dans les structures d'accompagnement.

> *« J'ai reçu beaucoup de soutien de la part de mon DAF qui est aujourd'hui PDG et de mon ancien PDG. » (Jérémy, 35 ans)*

> *« Ma conseillère mission locale m'a beaucoup aidé et soutenu dans mon projet » (Bacary, 22 ans)*

Le rôle des encadrants pédagogiques doit également être mis en avant. En effet, dans plusieurs témoignages, les formateurs et les chargés de formation sont apparus à plusieurs reprises comme ayant joué un rôle de soutien, voire de moteur dans les parcours.

> *« Ils ont vu que je me débrouillais bien alors ils m'ont incité à faire une formation qualifiante […] Je me revois encore au CNAM avec un des intervenants qui me disait que le plus compliqué c'était le +2 et qu'après, ça se faisait tout seul. Je n'y croyais pas trop. Mais maintenant je vois qu'il avait raison » (Guillaume, 28 ans)*

> *« J'ai toujours été encouragé par les intervenants quand j'ai parlé de vouloir arrêter. Le chargé de formation m'a encouragée à continuer quand j'avais des petits coups de mou. » (Anaïs, 31 ans)*

Les différents dispositifs d'aides financières sont également cités comme étant indispensables pour favoriser la réussite du parcours.

3.6. L'expérience vécue du « retour en cours » : la posture spécifique des personnes en reconversion

Avec la reprise d'études, plusieurs personnes interrogées ont rejoint des promotions mixant étudiants en formation initiale et professionnels en formation continue. Toutes font le constat d'un inévitable décalage d'état d'esprit entre ceux qu'ils appellent parfois « les jeunes » et leur situation.

Au-delà des différences de maturité, des différences d'engagement et de perception vis-à-vis de la formation sont relevées :

> *« L'arrivée en Bac+3 était plus compliquée parce qu'y avait « les jeunes » qui sortaient de BTS qui pensaient avoir les plus belles capacités du monde, les plus belles compétences et qui arrivaient avec une approche un peu plus irréelle du monde du travail. » (Guillaume, 28 ans)*

> *« Quelqu'un qu'à 18 ans a pas le même état d'esprit que quelqu'un qui a 25 ans. Côté CESI, je voyais la différence. Par rapport à l'engagement vis-à-vis de la formation. Les jeunes sortaient le soir alors que moi j'avais l'objectif de l'avoir et d'y aller. » (Anaïs, 31 ans) | « Quand on était en Bac+2 j'ai l'impression qu'on avait pas tous les mêmes niveaux de motivation. […] J'avais l'impression que ça représentait plus de sacrifices pour moi que pour eux. » (Anaïs, 31 ans)*

Quant aux personnes ayant repris des études dans des promotions entièrement composées de personnes en reconversion, elles soulignent combien **la cohésion du groupe était un point positif**, apportant un soutien important dans le parcours :

> *« J'étais principalement avec des gens en reconversion, ça allait de 20 ans à 52 ans. On a été un super groupe. C'était un point fort. » (Sylvain, 43 ans)*

3.7. Le recours à l'alternance dans les parcours de reconversion : entre opportunités d'apprentissage et difficultés

Parmi les personnes interrogées, trois ont réalisé leur formation en alternance, deux sont en recherche d'employeurs pour pouvoir reprendre une formation. Une autre personne envisage de continuer ses études en master en alternance. **La moitié des projets auraient ainsi souhaité se réaliser en alternance, signe par-delà le caractère monographique de ce volet, de l'appétence pour l'alternance. Cette voie d'apprentissage a par ailleurs été très positivement appréciée.**

L'alternance répond tout d'abord pour partie à **la problématique financière**. Elle s'est parfois imposée comme une évidence pour des raisons financières :

> *« C'était indispensable pour moi de le faire en alternance pour des questions financières. Je me voyais pas revenir chez mes parents. » (Anaïs, 31 ans)*

L'alternance est appréciée pour son efficacité, **les apprentissages étant mis en pratique très rapidement, facilitant l'acquisition de compétences :**

> *« Au final, j'encourage vraiment les gens à passer par l'alternance. Ça permet de pouvoir mettre immédiatement en pratique ce qu'on a appris en cours ça permet de pas oublier. Je suis convaincue que l'alternance est pas mal du tout pour l'apprentissage. » (Anaïs, 31 ans)*

> *« C'est super, tout ce que je voyais côté formation, je le mettais vraiment en place chez mon employeur » (Jérémy, 35 ans)*

L'alternance **facilite également l'intégration professionnelle :** plusieurs personnes ont été embauchées ou vont être embauchées au sein de l'entreprise dans laquelle elles ont réalisé leur contrat d'apprentissage.

L'alternance n'est cependant pas exempte de difficultés qui transparaissent dans les différents témoignages. La première d'entre elle est **la difficulté à trouver un employeur** acceptant d'accueillir un alternant en reprise d'études, principalement pour des niveaux de qualification Bac+2, l'entrée en alternance se faisant donc avec un niveau Bac :

> *« Ca m'a pris beaucoup de temps de trouver l'entreprise, notamment parce que quand j'avais des retours, sur le peu de retours, c'était pour me dire que comme j'avais pas de connaissances c'était compliqué de tout commencer de zéro » (Anaïs, 31 ans)*

Pour pallier cette difficulté, une personne a fait le choix de commencer par une formation de préqualification en quelques mois avant d'entamer une formation en alternance.

> *« Aller vers l'alternance pourquoi pas mais le souci c'est que je ne pouvais pas commencer un cursus bac +2 sans un minimum de connaissances. C'est pour ça que je me suis rapproché du Fongecif pour avoir un salaire tout en faisant une remise à niveau qui me permettrait de prétendre pouvoir rentrer dans une formation avec une alternance » (Guillaume, 28 ans)*

Les deux personnes en recherche d'employeurs pour leur alternance sont en prospection depuis une longue période. Ils rencontrent des difficultés liées à des facteurs externes (absence de permis de conduire limitant la mobilité) et des facteurs internes (sentiment d'incompétence).

> *« Et y a des annonces sur lesquelles j'ose pas postuler parce que j'avais pas telle ou telle compétence. J'ai pas eu le courage de postuler. » (Bacary, 22 ans)*

Malgré un accompagnement par des structures comme la Mission Locale, **le temps qui passe sans trouver d'employeur les éloigne petit à petit de leur projet** et renforce leur sentiment d'incompétence.

> *« Plus les années passent, plus ça devient compliqué. Psychologiquement ça bloque, on a l'impression qu'on va plus y arriver. » (Bacary, 22 ans)*

Les difficultés à trouver un contrat en apprentissage sont renforcées par une faible connaissance de l'écosystème des entreprises employeuses dans le domaine. La stratégie utilisée par certains a donc consisté à envoyer les CV en masse.

> *« Je connaissais rien […] J'ai été à la chambre du commerce pour trouver les noms des dirigeants d'entreprise dans le domaine et j'ai envoyé mes CV » (Jérémy, 35 ans)*

> *« Je trouve que c'est difficile de devoir envoyer les CV par internet quand on connaît pas, je préfèrerais me déplacer et rencontrer les employeurs. Mais bon, j'ai quand même envoyé au moins 100 CV à différentes entreprises. Je ne sais même pas si elles ont des besoins. » (Bacary, 22 ans)*

Différents dispositifs ont été sollicités pour aider à la recherche d'employeurs : les journées coaching dispensées par le CESI avant l'entrée en alternance et le dispositif « Place des Compétences Numériques » proposé par la Maison de l'Emploi du Grand Nancy.

> *« Je suis passé par PCN. C'est la mission locale qui m'a conseillé. Ça m'a beaucoup aidé parce que ça m'a appris comment fonctionnait LinkedIn par exemple et pour connaitre l'environnement d'entreprises. » (Bacary, 22 ans) | « Et j'ai participé à des journées coaching au CESI pour trouver une entreprise en apprentissage » (Bilal, 22 ans)*

Autre difficulté, certains employeurs recrutent des alternants pour pourvoir un poste de salarié expérimenté ; une fois dans l'entreprise, l'alternant est sommé d'intervenir de manière autonome. L'un des interviewés s'est ainsi retrouvé seul intervenant du domaine de la cybersécurité au sein de l'entreprise où il effectuait son alternance ; un second a rompu son contrat pour des raisons analogues.

Pour les personnes en reconversion, qui ont déjà travaillé dans d'autres domaines, l'alternance apparait comme une étape qui nécessite une adaptation à un nouvel environnement de travail. Alors que la thématique du manque de compétences au démarrage de l'alternance apparaissait comme une inquiétude dans les différents témoignages, ce n'est finalement pas cette problématique qui a conduit à devoir **s'adapter, mais les spécificités du rythmes ou des façons de travailler de l'entreprise d'accueil par rapport à leur expérience passée**.

> *« J'ai découvert un autre monde du travail en quittant le monde de la restauration (j'étais dans un restaurant étoilé) qui demande de la rigueur. Je me suis retrouvé avec des gens qui prenaient leur temps. Et moi j'avais tendance à vouloir faire vite, trop vite pour eux. J'ai dû m'adapter à un nouvel environnement à une nouvelle façon d'agir et d'être » (Guillaume, 28 ans)*

> *« Comme je suis dans la fonction publique, la première difficulté ça a été de m'adapter à cet environnement. C'est un rythme qui est très particulier par rapport au privé, ce que j'avais connu avant. » (Anaïs, 31 ans)*

3.8. Un bilan global positif de la reprise d'étude

En dépit des difficultés liées à la reprise d'études précisées précédemment et de l'appréhension à reprendre le chemin « des cours », notamment pour les personnes de plus de 40 ans, la majorité des personnes rencontrées dressent **un bilan positif du retour en apprentissage dont ils sont très satisfaits.**

> *« La remise en apprentissage c'est ce qu'il y a de plus passionnant » (Sébastien, 45 ans)*

Les terres fertiles et leur « curiosité »

Deux profils se dégagent néanmoins en termes de retour d'expérience. Tout d'abord, comme évoqué précédemment dans les figures-types de décision, plusieurs témoignages font montre de **personnes « curieuses » et très appétentes au savoir.**

> *« J'avais je crois des qualités humaines de vouloir apprendre. Pas seulement de suivre une formation. J'ai essayé de comprendre, de pousser les choses un peu plus loin. » (Guillaume, 28 ans)*

« J'ai ce besoin perpétuel d'avancer et de vouloir apprendre. » (Tristan, 28 ans)

Ces personnes n'hésitent pas à se renseigner ou à se documenter par elles-mêmes. Certaines s'étaient déjà auto-formées dans leur précédente carrière. C'est le cas de Sylvain, 43 ans, qui s'était auto-formé en webdesign après un BEP en dessin industriel, avant de monter sa société. En entrant en formation, elles ont ***« ouvert une porte vers tout un monde de savoir »*** **constituant pour elle, un réel stimulus générant l'envie de continuer leurs études au-delà du niveau initialement envisagé :**

« Je m'interroge pour la suite, y a tout un monde qui s'ouvre à moi, alors pourquoi pas un bac +5 ! » (Frédéric, 52 ans)

« J'ai commencé par une formation de 7 mois TSSR. Et puis j'ai voulu continuer, j'étais dans mon élément. Je suis allé sur le Bac+3 » (Sylvain, 43 ans)

Pour ces profils, la reprise d'étude est particulièrement satisfaisante et gratifiante : elle nourrit leur soif de connaissances. **L'apprentissage est presque une fin en soi.** Cet intérêt pour la formation se retrouve également dans les réponses apportées à la question *« Imagineriez-vous reprendre une formation plus tard dans votre carrière ? ».* Toutes les personnes ayant ce profil répondent positivement et sont ouvertes à un nouveau projet de formation.

Les « assidus » en compétences

D'autres profils ont pu être identifiés à travers les différents parcours. **Le rapport à la reprise d'étude est plus fonctionnel ; celle-ci permet de répondre à leur besoin « d'acquérir des compétences » et sécurise le projet professionnel cible.** De manière transversale, le thème du « besoin » en connaissances et en compétences revient de manière récurrente dans leurs discours.

« Au début je passais même du temps chez moi pour essayer de rattraper le retard que j'avais accumulé avant » (Guillaume, 28 ans)

Pour ces profils, la formation a permis de surmonter la peur *« de ne pas avoir les connaissances nécessaires ».*

« J'avais vraiment aucune compétence. Je les ai acquises au fur et à mesure en recueillant les compétences des formateurs. » (Guillaume, 28 ans)

« Au niveau de mes connaissances techniques je n'ai pas eu de problème, en fait j'en ai acquis assez rapidement au cours de ma formation. » (Jérémy, 35 ans)

Pour ces profils, un lien étroit est établi entre acquisition de compétences et formation. Il se retrouve dans les réponses apportées à la question *« Imagineriez-vous reprendre une formation plus tard dans votre carrière ? »* Si cela reste envisageable, cette possibilité est limitée au besoin « d'acquérir de nouvelles compétences ».

4| Le projet professionnel cible et les perspectives d'intégration professionnelle

Tout parcours de reconversion est mu par un projet professionnel et une promesse d'amélioration de sa situation professionnelle et personnelle par rapport à la situation initiale. C'est cette promesse qui justifie les efforts consentis. Paradoxalement, comme souligné en sous-partie 2, **la Cyber en tant que telle et l'emploi cible restent très flous en début de parcours. L'ambition initiale se formule autrement que dans un projet d'insertion professionnelle précis : l'ambition est d'atteindre un niveau de qualification et de spécialisation valorisables sur le marché du travail et donnant accès à un poste « qui plaise ».**

4.1. Atteindre au moins un niveau Bac+3 : un invariant dans les profils

Point-clé : Le niveau Bac +3 est le niveau cible des parcours de reconversion en cybersécurité. Le diplôme de Technicien supérieur Systèmes et Réseaux (Bac +2) est perçu comme un *« niveau de base, alors que le Bac +3 AIS permet de se spécialiser ».* **Valider sa reconversion en pouvant faire montre d'une spécialisation est central dans l'ambition initiale.**

Le niveau Bac +3 est ainsi le niveau minimum atteint par les différents profils interviewés ou le niveau souhaité pour ceux qui débutent leur projet. La poursuite du parcours jusqu'à l'obtention d'un diplôme Bac +5 est envisagée par la moitié des personnes. Certaines personnes souhaitent poursuivre en Bac +5, immédiatement après l'obtention de leur diplôme de niveau 6 afin d'éviter une nouvelle rupture professionnelle.

> *« Je suis assez tenté de continuer pour devenir ingénieur. J'aurais peur de ressortir du travail pour revenir en formation. » (Sylvain, 43 ans)*

Les personnes envisageant plutôt de s'insérer professionnellement après l'obtention du diplôme Bac+3 visé, ne n'excluent pas de reprendre une formation pour obtenir un niveau Bac+5 ultérieurement.

> *« Pourquoi pas un Bac+5 mais plus tard. Je me vois bien me former à nouveau. » (Tristan, 28 ans)*

Une seule trajectoire faisait exception à « la règle du Bac +3 minimum en Cyber ». Il s'agit de Dylan (41 ans) ; il avait repris une formation pour une unique année sur un niveau Bac +2 comme Technicien supérieur Système et Réseau. Ayant eu l'opportunité d'intégrer une entreprise en CDD à l'obtention de son diplôme, Dylan s'implique dans sa nouvelle activité professionnelle : en complétant son BTS par de l'auto-formation, il parvient à mettre en œuvre des missions plus vastes que celles données à un technicien. Pour des raisons économiques, son employeur n'a pu renouveler son CDD. Désappointé par les emplois auxquels son Bac +2 lui permet de postuler, il est aujourd'hui à la recherche d'une formation qui lui permettrait d'obtenir un diplôme Bac +3 afin d'accéder à des postes qu'il juge *« plus adaptés à [ses] compétences »*. L'exception confirme donc la règle !

4.2. L'emploi visé : une perspective souvent floue mais néanmoins très attendue

La projection dans l'emploi est très variable en fonction du profil et de l'avancement dans le parcours de reconversion. En début de parcours, sans avoir travaillé dans le domaine de la cybersécurité, il est difficile de se projeter en matière d'intégration professionnelle.

> *« Je prendrais certainement ce que je trouverais, c'est difficile d'être exigeant. Et puis je connais encore pas trop ce qu'il est possible de faire » (Tristan, 28 ans)*

Les stages ou l'alternance au cours du projet de reconversion permettent de mieux appréhender les métiers de la sécurité informatique et son univers professionnel. Ces expériences facilitent l'intégration professionnelle : soit positivement, l'entreprise d'accueil étant susceptible de recruter, soit en expérimentant « ce que l'on ne veut pas faire ».

> *« C'est en discussion. Normalement ça devrait être possible [d'être embauchée dans le lieu où je réalise mon alternance] » (Anaïs, 31 ans)*

> *« Je compte arrêter chez mon employeur actuel et chercher ailleurs. J'ai envie dans un premier temps de rentrer dans une boite en tant qu'administrateur réseau et système. Je préfère éviter les SSII. La gestion de 30 projets j'ai testé, c'est compliqué. » (Guillaume, 28 ans)*

Les premières années en emploi sont envisagées comme un moyen de *« continuer à monter en compétences »,* y compris pour les diplômés d'un Bac +5.

L'intégration dans l'emploi est attendue avec impatience. Cette étape marque pour tous *« l'aboutissement du parcours de reconversion ».* Elle sanctionne positivement les efforts réalisés, notamment par celles et ceux qui ont repris plusieurs années d'études pour qui elle constitue une *« récompense »* eu égard aux sacrifices consentis.

Pour les personnes qui ont été éloignées de l'emploi pendant quelques temps avant d'engager leur reconversion que ce soit pour raisons de santé ou du fait de difficultés à trouver un emploi, il s'agit aussi et surtout de **la perspective satisfaisante, valorisante et rassurante de *« reprendre une activité professionnelle ».***

4.3. Une connaissance limitée des potentiels employeurs

Point-clé : Quel que soit le niveau d'avancée dans le parcours de reconversion, une grande méconnaissance des entreprises employeuses dans le domaine est à noter. **Si les individus ont une connaissance assez fine du métier visé ou de la taille de la structure dans laquelle ils souhaiteraient travailler, l'écosystème des employeurs ne leur est pas familier.**

> *« Je sais ce que je veux faire mais je crois que j'ai un vrai manque de connaissance des entreprises qui recrutent » (Sébastien, 45 ans) | « Si je devais changer d'employeur, j'ai pas de projection très claire. » (Jérémy, 35 ans)*

Certains savent par ailleurs que **la notion de réseau professionnel** est importante, mais n'ont pas encore engagé de moyens pour s'investir sur cet aspect.

> *« J'ai connaissance de ça mais c'est un travail qu'il faut faire tout le temps, réseauter tout ça. Et je le fais pas. » (Amir, 32 ans)*

Les personnes interrogées savent également ce qui fait la différence entre une entreprise de services numériques (ESN)[35] et d'autres types d'employeurs. **La plupart souhaiteraient rejoindre en tant qu'administrateur système, l'équipe interne d'une structure plutôt que d'intervenir au sein d'une ESN :** *« J'essayerais d'éviter une ESN. » (Sylvain, 43 ans)*

L'appétence à **l'entreprenariat** varie également en fonction des profils et paraît dans l'ensemble plutôt éloigné, sauf parcours personnel particulier, du projet d'intégration professionnel en cybersécurité.

4.4. Retour subjectif sur le parcours de reconversion réalisé

En fin de témoignage, les personnes ont été invitées à qualifier leur parcours et à apprécier *« ce qu'elles auraient fait autrement »* si c'était à refaire. En dépit des difficultés et des sacrifices réalisés, la plupart disent que *« si c'était à refaire, [ils] referaient la même chose. »*

Certaines personnes ayant réalisé leur reprise d'études en alternance évoquent pour certaines un choix différent d'entreprise d'accueil, non pas parce que l'expérience s'est mal passée mais avec l'idée de découvrir d'autres environnements.

> *« J'aurais peut-être changé d'entreprise en cours de route pour voir différents fonctionnements. » (Anaïs, 31 ans) | « Peut-être trouver d'autres entreprises. Les expériences auraient été différentes. » (Guillaume, 28 ans)*

Découvrir, expérimenter sont les maîtres mots avec le sentiment dominant pour ceux qui sont allés au terme de leur projet, d'un parcours réussi.

[35] Une ESN (Entreprise de Service Numérique) ou SSII (Société de Services et d'Ingénierie en Informatique) est une société prestataire de services dans le domaine informatique (définition LAROUSSE)

5| Les compétences Cyber et la reconversion

Les personnes en reconversion n'arrivent généralement pas dépourvues de compétences. Leur formation initiale et leurs premières expériences professionnelles leur ont permis d'acquérir des connaissances et de développer des compétences potentiellement remobilisables dans leur nouveau projet professionnel. Lorsque les univers initiaux et cibles sont très éloignés, les compétences transférables sont plus généralement des savoir-faire transversaux ou des aptitudes.

L'étude monographique s'attache dans cette avant-dernière partie, à identifier les compétences de la trajectoire initiale qui ont pu être mobilisées dans le parcours de reconversion en vue du projet professionnel cible.

Les compétences du parcours initial remobilisables dans le domaine de la cybersécurité

Le panel des cursus initiaux (formations ou expériences professionnelles) des personnes interrogées dans le cadre du projet FORE-CY brille par son extrême variété : pâtisserie, coiffure, secours à la personne, environnement, géographie, enseignement, vente, banque, dessin industriel, webdesign, montage vidéo, etc. Autant de premières expériences ayant permis de développer des compétences utiles dans leur nouveau projet :

> *« Dans ma précédente expérience ce que j'ai acquis c'est notamment la rigueur et l'organisation. Aussi le relationnel client, parce que dans la première formation que j'ai fait en Bac+2 on faisait beaucoup d'assistance utilisateurs, des choses comme ça. » (Anaïs, 31 ans)*

> *« Un des gros avantages de mon ancienne vie c'est la gestion du stress : savoir prendre de la hauteur et du recul. Savoir réagir rapidement et trouver une solution dans l'urgence. » (Dylan, 42 ans)*

> *« Les marchés ça m'a appris à communiquer avec les gens. On doit s'en rendre compte quand je communique avec les clients. » (Sylvain, 43 ans)*

> *« J'ai toujours été timide, mais le fait d'avoir fait chargé de clientèle ça m'a beaucoup aidé. » (Bacary, 22 ans)*

Pour certaines personnes, c'est le parcours de reconversion lui-même qui leur a permis de prendre conscience de certaines aptitudes, avantageux pour leur reprise d'études, comme pour intervenir dans le domaine de la Cyber :

> *« J'ai tendance à penser que je suis quelqu'un qui n'est pas vraiment résistante à la pression, mais je sais pas pourquoi parce que si plutôt, je suis assez réactive. Je remarque maintenant qu'en situation de stress j'arrive à garder la tête froide et à réagir sans trop paniquer. » (Anaïs, 31 ans)*

A travers les différents témoignages, plusieurs compétences utiles au parcours de reconversion en Cyber ont pu être repérées comme étant des points d'accroche facilitant :

- la **gestion du stress** et la **capacité à réagir** rapidement,
- la **rigueur** et le sens de l'**organisation**,
- le **relationnel client** et la vente,
- la **gestion de projets**,
- l'envie et la **capacité à apprendre**,
- et enfin, bien sûr, **la curiosité**.

Point-clé : Nombreux sont ceux à évoquer *« la curiosité »* comme une compétence extrêmement utile dans le domaine professionnel de la cybersécurité, point tout à fait corroboré par les employeurs de profils Cyber qui en font même un critère de sélection au recrutement (cf. I.). **Il apparaît dès lors utile que les acteurs de l'accompagnement professionnel identifient bien cette aptitude, qui couplée, peut permettre de repérer au sein d'un vivier de candidats en recherche d'emploi, des profils d'intérêt** pour la filière.

Un domaine qui nécessite de se former constamment et où l'accompagnement des utilisateurs a une place importante

Les représentations convergent également sur certaines caractéristiques du domaine : **en premier lieu, la cybersécurité est perçue comme un domaine dans lequel *« il est toujours nécessaire de se former »***.

> *« C'est de la veille permanente » (Amir, 32 ans) | « C'est un truc ou il faut se documenter au quotidien, ça change à chaque fois » (Bacary, 22 ans)*

Les personnes « naturellement curieuses » et qui « ont une soif d'apprendre constante » rencontrés dans le cadre de l'étude monographique FORE-CY y trouve donc un vaste territoire répondant à leur appétence.

La cybersécurité est, en second lieu, associée aux **enjeux de relation à l'usager** et **d'accompagnement de l'utilisateur.** Ainsi, **« le relationnel client »** a été plusieurs fois cité comme une compétence transférable importante dans les métiers de la cybersécurité. Cette thématique est même centrale dans deux parcours de reconversion, deux personnes ayant une appétence particulière pour l'accompagnement des usagers non experts dans le domaine de la cybersécurité. Il s'agit donc du domaine visé par leur projet de transition professionnelle.

> *« Il y a un vrai enjeu d'adaptation à la technologie pour les gens qui ne sont pas experts. » (Pascal, 57 ans)*

> *« Dans ma formation initiale, j'avais fait un DEUG de sociologie parce que je m'intéressais à l'utilisateur. Je pourrais plutôt m'orienter vers l'accompagnement. Même si l'expertise technique est importante pour faire les choses correctement, le plus important c'est de réussir à les vulgariser » (Frédéric, 52 ans)*

* * *

Qu'il s'agisse d'une démarche de reconversion ou de transition professionnelle, la formation s'ancre comme un passage structurant et pour le moins essentiel dans les parcours de reconversion. L'engagement dans les cursus formatifs des personnes en reconversion diffère pourtant de celui des étudiants en formation initiale : davantage de pression, la peur de l'échec, les sacrifices à consentir.

La technicité attendue, ou supposée, dans les métiers du champ de la cybersécurité est également susceptible de créer des craintes supplémentaires, faisant naître un sentiment d'illégitimité en dépit de profils finalement adaptés aux attentes du métier et à l'aise dans le processus d'apprentissage.

Identifiés comme indispensables dans les différents témoignages, l'accompagnement et le soutien des personnes en reconversion dès le démarrage de la démarche et tout au long du parcours, méritent d'être consolidés et adaptés dans l'ensemble des structures ouvrant leurs formations à ces profils.

Partie IV. Prospective territoriale

Le diagnostic prospectif territorial constitue le quatrième volet de l'étude. Il prolonge le tableau statistique et l'analyse des besoins en compétences des employeurs de profils Cyber restitués dans la Partie I. par un cadrage des perspectives en emplois du secteur, à l'horizon 2030. La simulation se nourrit de scénarios contrastés esquissés collectivement en séminaire avec le comité de pilotage élargi aux parties prenantes en décembre 2022 et enrichis par la veille sectorielle réalisée dans le cadre de la mission. La politique territoriale régionale en matière de cybersécurité y est prise en compte ; elle constitue un facteur de dynamisation significatif du secteur.

En se projetant vers l'avenir, les parties prenantes de FORE-CY ont aussi souhaité tirer les enseignements du diagnostic territorial. En capitalisant sur les forces du territoire, elles ont imaginé par un travail d'intelligence collective, des offres nouvelles porteuses pour les candidats du domaine, la filière Cyber et le territoire. S'il reste de nombreuses étapes pour passer de cette esquisse collective à la « première rentrée », cette créativité est signe d'une bonne émulation collective et de l'intérêt des parties prenantes territoriales à collaborer à un projet à finalité concrète et d'envergure.

Une politique régionale dynamique en matière de cybersécurité

Approuvé par les élus lors de la séance plénière du 23 mars 2023, **le Plan régional cybersécurité 2023-2025** s'articule autour de cinq objectifs[36] :

- **Prévenir les cybermenaces** par la sensibilisation de tous les acteurs régionaux (publics et privés, grand public, lycéens notamment) ;
- **Préparer les acteurs aux cybermenaces** *via* notamment un diagnostic Cybersécurité financé par la Région aux entreprises, élargi depuis lors aux acteurs publics et associatifs et aux établissements de santé ;
- **Accompagner la gestion de la crise cyber** avec l'appui de Grand Est Cybersécurité, service piloté par la Région et avec le soutien de l'Agence Nationale de sécurité des systèmes d'information (ANSSI) ;
- **Animer et développer la filière régionale de la cybersécurité,** en développant les partenariats vertueux entre la recherche, les forces académiques et les offreurs de solution pour répondre à la demande régionale et profiter de la dynamique d'un marché mondial de la cybersécurité en forte croissance ;
- **Développer les compétences en cybersécurité** pour répondre aux besoins croissants des entreprises et de la filière (formations, actions d'orientation et de promotion). Le projet FORE-CY s'inscrit pleinement dans ce 5e axe du Plan régional.

La Région Grand Est a également pour objectif de lancer au second semestre 2023 un **Campus Cyber Grand Est** ouvert à tous les acteurs de la cybersécurité du territoire. Destiné à devenir à terme la référence sur le sujet, ce Campus coordonnera et mutualisera les efforts et ressources de la communauté régionale en matière de sensibilisation, de développement des compétences, de partages de données, d'innovations et de **coopérations transfrontalières**. L'échelle européenne est d'ores et déjà prise en compte par certaines formations du territoire en ce domaine, notamment par **le DU Sécurité Intérieure de l'Université de Lorraine à Nancy** qui a ainsi noué des partenariats avec les universités allemande de la Sarre et belge de Louvain-la-Neuve[37].

A travers son plan cybersécurité, **la Région ambitionne de devenir un territoire de confiance** où l'ensemble des organisations publiques et privées peuvent profiter des bénéfices du numérique, en maîtrisant les risques sur leurs systèmes d'information, en s'appuyant notamment sur des forces académiques et des offreurs de solutions

[36] https://www.grandest.fr/actualites/un-plan-regional-pour-la-cybersecurite/
[37] https://fac-droit.univ-lorraine.fr/content/diplome-duniversite-securite-interieure

régionaux.

Perspectives de l'activité Cyber : des scénarios d'avenir contrastés

Dans la continuité du plan régional et parce que Nancy est une place forte en matière de cyberdéfense depuis 2010, l'un des scénarios imaginés par le Comité de pilotage élargi des parties prenantes lors du séminaire du 08/12/22 est **une accélération de la prise de conscience par les entreprises et les administrations des menaces et le rehaussement de leur protection Cyber** pour accroître leur résilience et celle de l'ensemble du territoire aux attaques Cyber.

Scénario A. 2030 | Vers un territoire de confiance et de résilience numériques

Créativité collective | Synthèse du séminaire du 08/12/22

La Métropole du Grand Nancy s'est mobilisée de façon prioritaire sur le sujet de la résilience numérique afin d'éviter que les acteurs du territoire ne pâtissent après la crise sanitaire, puis la crise énergétique et inflationniste, de nouvelles difficultés Cyber dont ils ne pourraient se relever, à tout le moins sans graves préjudices.

Fédérant les différentes initiatives, la Métropole mobilise l'ensemble de l'écosystème local pour cette *Bataille de Nancy* ultra-technologique : agissant par plans d'action de filière animés et suivis par un référent Cyber, orientant les budgets disponibles pour soutenir le renforcement Cyber des services et établissements publics du territoire et procédant par allègement de la fiscalité locale pour motiver les entreprises à solliciter les prestataires locaux, le niveau de protection Cyber progresse. Les entreprises prestataires gagnent chaque année davantage en lisibilité, l'offre de services est bien structurée.

Malgré la mobilisation, les cyberattaques coûtent cher à ceux qui les subissent, certains témoignages sont saisissants. Les décideurs économiques et administratifs du territoire sont toujours plus convaincus de l'opportunité de se défendre « en meute » pour éviter des déstabilisations successives de l'écosystème local. Les appels d'offre publics comme privés ont, du reste, introduit un critère de « résilience cyber » dans la notation des soumissionnaires. Chacun s'aligne donc progressivement sur les standards de place attendus, d'autres s'engagent dans la voie d'une certification cyber, facteur de différentiation et de compétitivité.

Capitalisant sur « les pépites cyber » du Grand Nancy, start-ups et pôles de R&D développent des outils performants pour les acteurs locaux. **Nancy s'affirme toujours davantage comme une terre de développement d'outils Cyber d'excellence.** Cette notoriété attire des talents prometteurs, l'innovation permet de répondre à l'évolution très rapide des menaces.

Dans ce scénario de mobilisation générale, les ESN connaissent un pic de demande et la **terre fertile nancéienne** voit s'implanter et se développer sur son territoire des acteurs nombreux et en forte croissance de leurs effectifs. **Les acteurs de la formation du domaine se mobilisent eux aussi et parviennent à fournir en nombre et qualité les talents** dont les entreprises ont besoin. Le taux de rétention sur le territoire progresse.

Scénario B. Scénario fil de l'eau : *« Pourvu que l'orage tombe plus loin… »*

Malgré le boom du télétravail à la suite de la crise sanitaire et les appels à la vigilance relayés à toutes les échelles, les entreprises et administrations du Grand Nancy sont nombreuses à se donner d'autres priorités, remettant à demain le *« dossier cybersécurité »* bien ardu techniquement et somme toute anxiogène. Chacun pense ne pas être la cible d'une cyberattaque, « l'orage devrait tomber plus loin… ».

Le CHU de Brabois a pourtant fait l'objet d'une demande de cyber-rançon et plusieurs sites industriels ont été en difficultés au cours des 6 derniers mois. L'appui du CSIRT permet d'apprendre à gérer en direct la crise et d'en limiter les conséquences.

Les entreprises les plus structurées, soucieuses de l'efficacité de leur plan de continuité d'activité en cas de crise,

effectuent un diagnostic de risques Cyber et prennent les premières actions de renforcement qui s'imposent, sollicitant les entreprises prestataires du territoire, très mobilisées.

Ce scénario correspond peu ou prou à la situation actuelle telle que décrite par les entreprises prestataire dans l'enquête FORE-CY ; **il s'agit du scénario dit « fil de l'eau »**. Dans ce scénario à l'échelle de la place nancéienne et au-delà de la disparité d'un acteur à l'autre, les acteurs locaux poursuivent une croissance relativement modérée de leurs effectifs. De jeunes créateurs d'entreprise continuent de s'installer en cybersécurité, à la sortie des formations de qualité validées à l'Université de Lorraine ou dans les grandes écoles du territoire. Le marché étant structurellement orienté à la hausse, chacun trouve son espace.

Scénario C. L'IA, une révolution, de nouveaux risques à accompagner

La révolution de l'IA bat son plein et bouleverse les organisations de service : comptables, services juridiques, assurances, traduction, agences de communication… l'emploi sur les postes les moins qualifiés s'effondre. L'IA apporte avec elle de nouvelles menaces, à un rythme effréné…

Les ETI, grandes entreprises et services publics renforcent leurs services de Cybersécurité internes et sollicitent l'appui des ESN pour répondre de manière appropriée à l'explosion des menaces et dompter l'IA et le *Machine Learning* au service de la Cyber.

« Les pépites cyber » du Grand Nancy, start-ups et pôles de R&D, savent faire la différence et développer en cycle court des outils performants pour les acteurs locaux : ***« Non inultus premor | Qui s'y frotte s'y pique ! »*** La maîtrise de l'IA, de la cryptographie et des architectures intelligentes nouvelle génération permet de tenir en respect les IA malveillantes des différents pays ennemis et réseaux mafieux internationaux. **L'excellence académique et de recherche attire des talents prometteurs,** l'innovation permet de répondre à l'évolution très rapide des menaces.

Les ESN connaissent un pic de demande, mais s'inquiètent d'un potentiel retournement de cycle (cf. scénario D) très difficile à anticiper. Les équipes sont mises sous forte pression, malgré les mesures d'aguerrissement et l'adaptation des postes, les démissions se multiplient dans le domaine. **L'outil de formation est fortement sollicité pour fournir en nombre et en qualité les talents** dont les entreprises ont besoin : **la situation est sous haute tension.** Dans l'attente d'une rupture qui se fait craindre mais constitue aussi une opportunité pour les plus experts, des acteurs de pointe s'implantent et se développent sur le territoire métropolitain avec une stratégie mixte de croissance modérée de leurs effectifs et d'appui sur de la cotraitance.

LE QUANTIQUE : MENACE ET OPPORTUNITÉ À LONG TERME

Le quantique, par le changement de paradigme qu'il implique et les résultats potentiellement impressionnants qu'il présente pour le numérique, peut être une menace pour la cyber (e.g. de part sa capacité à casser plus simplement les méthodes de chiffrement utilisées actuellement). Mais, il représente aussi une opportunité pour repenser la cybersécurité. Dans ce contexte, le Campus Cyber devra suivre de près ces évolutions.

→ **Aujourd'hui, nous observons les premières utilisations des propriétés quantiques pour améliorer la cybersécurité, en particulier sur la transmission des clés de chiffrement.**
Le processus est déjà fonctionnel et utile dans certains cas. Consciente de ces nouvelles capacités, la France a lancé en 2021 son plan quantique visant à renforcer la coopération entre les industriels, universités, organismes de recherche et startups en matière de recherche sur les technologies quantiques, qui inclut des éléments sur la cybersécurité. L'Europe est également engagée dans des démarches similaires.

Source : Horizon Cyber 2030. Perspectives et défis | Campus Cyber

Scénario D. L'IA, révolution et rupture pour la Cyber : « l'effet pointe de diamant »

La révolution de l'IA bat son plein… si les menaces numériques explosent, **l'IA est mobilisée au sein même des solutions de cybersécurité et impacte fortement le domaine lui-même. Les emplois de premier**

niveau se font rares, le niveau de qualification moyen continue de se concentrer sur **les pointes de diamant des Bac +6 et docteurs.** Certains start-uppeurs continuent de tirer leur épingle du jeu avec un parcours atypique, sans lien aucun avec l'informatique ou la gouvernance des risques, mais rares sont les élus.

Précaution méthodologique. Les quatre scénarios brossés matérialisent l'amplitude du spectre des possibles pour le secteur de la Cyber à 2030. Le niveau d'incertitude limite la portée de tout exercice de réelle simulation quantitative des besoins. Néanmoins, à titre illustratif de cadrage, des « tirs sous hypothèses » normatifs ont été réalisés sur la base des deux modèles étalonnés dans le volet I de la mission. Ils n'ont d'autre vertu que de tester la sensibilité des effectifs aux jeux d'hypothèses introduits.

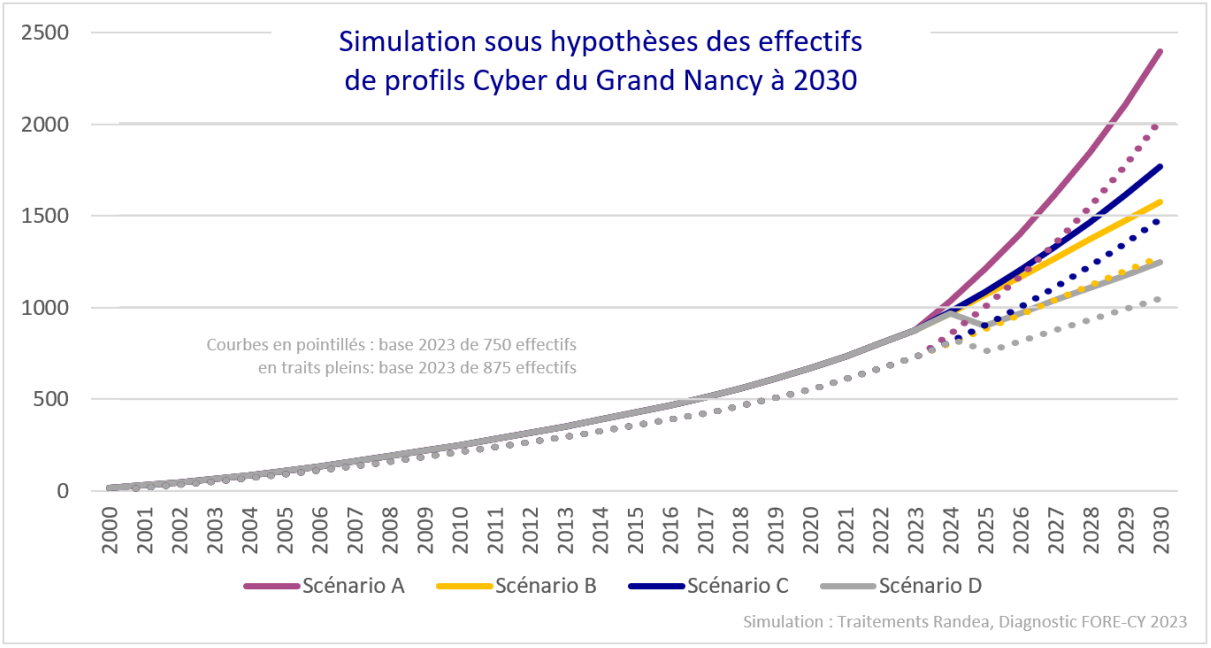
Les scénarios ont été traduits ou transposés sous la forme de jeux d'hypothèses cohérents en paramétrant :

- *l'évolution du nombre d'acteurs* offrant des services de cybersécurité ou se dotant d'une équipe interne en ce domaine sur le territoire métropolitain ;
- *la dynamique des effectifs,* raisonnée de façon différentiée selon les différents profils (techniciens, profils Tech de type Bac +5 à 8, profils conseil).

Les simulations ont été réalisées selon les hypothèses et résultats-tests suivants :

	Nombre d'employeurs de profils Cyber à 2030 (N.B. 104 en 2023)	*Dynamique des effectifs*	*Effectifs Cyber en 2023 (base 2023 : 750)*	*Effectifs Cyber en 2023 (base 2023 : 875)*	*TCAM* des effectifs*
Scénario B | Fil de l'eau « Pourvu que l'orage tombe plus loin… »	135	Effet de concentration de l'écosystème avec dynamique RH calée pour retrouver le TCAM historique	1 270	1 575	9%
Scénario A | Un territoire de confiance et de résilience numérique	200	Accélération de la dynamique RH (x1,5 à 2,5 selon les profils)	2 000	2 400	15%
Scénario C | L'IA et ses dangers	180	Légère accélération de la dynamique RH (x1,1 à 1,3 selon les profils)	1 475	1 775	11%
Scénario D | L'IA, rupture pour tous, même la Cyber	115	Chute brutale des effectifs Techniciens, hausse des effectifs Conseil (x1,5) et dynamique intermédiaire pour les profils Tech Bac+5 à 8	1 045	1 245	5%

*TCAM = taux de croissance annuel moyen



Sous ces hypothèses, les effectifs de profils Cyber pourraient connaître une croissance de 40% à 175% en 7 ans,

soit une croissance annuelle moyenne de +5% dans le cas du scénario D simulant une chute des emplois de techniciens dans la Cyber *sous le coup de l'IA*, à +15% dans le scénario A dit *de mobilisation générale*. Le vivier de professionnels impliqués en Cyber pourrait atteindre plus de 2 000 talents.

Notons que le scénario A de mobilisation générale n'est pas forcément le plus désirable : il mettrait très fortement en tension l'outil de formation à court terme et conduirait à gérer une forte et rapide croissance des effectifs avant une décélération significative. Les scénarios *fil de l'eau* et *les dangers de l'IA* donnent une trajectoire assez proche avec des moteurs très différents. Un vivier cible de 1 500-1 700 talents impliqués sur des projets de cybersécurité d'ici 2030 paraît raisonnable pour disposer d'un scénario de référence sans oublier la forte variation potentielle autour.

S'il est acquis que la menace numérique ne peut qu'aller croissante à court ou moyen terme, l'anticipation des besoins en emplois et compétences est délicate dans un domaine soumis à de rapides évolutions technologiques, au seuil même de ruptures voire d'une révolution. **Plus l'incertitude est élevée, plus l'agilité des organisations, la coopération et la créativité des professionnels et des équipes doivent être entraînées pour les rendre capables de faire face aux défis.**

Il apparaît donc essentiel non seulement de former les professionnels de la Cyber aux meilleurs outils technologiques et au management des risques, mais aussi de les mettre le plus possible en situation, de les projeter, les défier pour stimuler leurs capacités d'adaptation et de prise de décision. En ces domaines, l'entraînement doit prendre le pas sur la formation et la compléter.

Attentes et perspectives d'avenir pour les organismes de formation

Ainsi, interrogés sur l'école de la cybersécurité de demain, les organismes de formation convergent fortement. Pour aller plus loin aujourd'hui et pour répondre aux défis de demain, ils mettent en avant les apports de « la mise en situation réelle », « l'accès à des plateformes de simulation », « des travaux sur plateforme de démonstration cybersécurité industrielle ou tertiaire seraient un plus ».

Certains soulignent les apports qui pourraient être obtenus de la « mise en place d'un laboratoire de tests », de la possibilité de « participer à une plateforme d'open innovation en cyber ». Ainsi, l'école de la cybersécurité de demain est décrite comme « un croisement entre un living lab et un fab lab tout en laissant du temps à l'approche théorique » ou encore « comme ayant une part importante en immersion via une plateforme cyber-range, l'alternance en entreprises… », « Une école où tous les étudiants pourraient s'entraider et où il y aurait des formations sur la cybersécurité interactives et ultra réalistes ».

Le besoin de mise en situation opérationnelle faciliterait aussi l'hybridation des profils non issus de la technologie : « l'accès à des logiciels du marché pour permettre à des juristes ou des professions de santé d'approcher concrètement les sujets » est différenciant.

Le développement de « coopérations avec des formations à l'international » et le renforcement « des partenariats avec différents experts dans différents domaines » sont mis plus ponctuellement en avant comme leviers d'innovation et de renforcement de l'offre de formation. Les outils de e-formation sont également cités pour faciliter l'apprentissage des notions plus théoriques : disposer d'un « campus digital avec une plate-forme d'apprentissage personnalisée avec des parcours individualisés » ou « de vidéos et de modules e-learning à réaliser à distance et en autonomie pour maîtriser les concepts théoriques » sont envisagés comme des plus.

Veille des outils de mise en situation dans le champ de la cybersécurité

En matière de cybersécurité, les exercices de simulation et d'entrainement permettent d'améliorer la coopération des équipes et d'accompagner la montée en compétences des publics en apprentissage comme des salariés en

poste. La veille réalisée met en évidence différents types d'outils en fonction du degré de technicité ou des compétences visées.

Ainsi pour la sensibilisation à la cybersécurité, au phishing, à la sécurité informatique ou encore à la bonne « hygiène numérique », de nombreuses structures privées ou publiques proposent des **méthodes ludo-pédagogiques inspirées des « escape game »** à destination de publics variés : élèves, étudiants, salariés, etc. Ces jeux pédagogiques sont proposés en format physique ou entièrement digitalisé.

- L'offre « d'escape game » **à destination de salariés** est bien fournie. De nombreuses structures proposent ce type de service.
- **L'offre est plus émergente dans l'enseignement.** Des expérimentations émergent progressivement : l'ANSSI travaille d'ailleurs depuis 2019, en lien avec le Ministère de l'Éducation nationale, de la Jeunesse et des Sports, à développer des expérimentations pour mieux former les jeunes aux enjeux et aux filières de la sécurité numérique. En 2021 a été élaboré le kit CyberEnJeux38, disponible en version Beta en libre ressource. La Direction de Région Académique du Numérique pour l'Éducation de la Région Occitanie propose également, en ressource en libre accès, un jeu appelé le « Le chronocrypteur »[39] à destination des élèves de seconde.

Dans le domaine du **développement de compétences plus techniques, des plateformes de simulation d'incidents de sécurité**, appelées « Cyber Range » ou « Gammes Cyber » sont mises en place. Il s'agit d'*« environnements virtuels utilisés pour la cybersécurité, la formation à la cyberguerre, la simulation ou l'émulation et le développement de technologies liées à la cybersécurité. Leur échelle peut varier considérablement, d'un simple nœud à un réseau de type Internet ».*[40]

Parmi les **propriétaires de plateforme de simulation**, se trouve :

- Des **entreprises prestataires de services**, spécialisées dans la cybersécurité, qui proposent de développer des infrastructures et/ou des prestations scénarisées à destination des entreprises, des écoles ou des universités (ex : Soteria Lab[41], DIATEAM[42]) ;
- Des **entreprises de l'aéronautique** offrent également cette prestation à des entreprises externes et l'utilisent pour leurs propres équipes (AIRBUS[43] en France, ou LEONARDO[44] au Royaume Uni) ;
- Des **gouvernements** : aux Pays-Bas, le cyber commando du ministère de la Défense et Thalès ont conclu un contrat pour la création d'un « Cyber Range », pour l'entraînement et la formation du personnel du ministère.[45] Aux Etats-Unis, la DARPA (Defense Advanced Research Projects Agency), agence de recherche et de développement du département de la Défense développe le National Cyber Range[46]. La Fondation CR14[47] établie par le ministère de la Défense d'Estonie a également installé un Centre d'excellence de la cybersécurité à Tallinn et possède son « Cyber Range ».
- Des **universités, des écoles ou laboratoires de recherche** (« Cyber Expérience » proposée par Galileo Global Education[48] installée au Campus Cyber à Paris ; plateforme déployée par Télécom Nancy[49] ; « Cyber Range » de l'université de Belfast au Royaume Uni[50])

Ces plateformes peuvent également naître de la **collaboration entre différents acteurs,** parfois à l'initiative de pouvoirs publics. Ainsi, en Bretagne, un groupe de travail piloté par le Pôle d'excellence Cyber s'est constitué fin

[38] https://www.ssi.gouv.fr/actualite/au-college-et-au-lycee-former-a-la-cybersecurite-par-le-jeu/
[39] https://pedagogie.ac-toulouse.fr/drane/usage-dun-jeu-devasion-pour-sensibiliser-la-cybersecurite
[40] Source : Wikipédia
[41] https://soteria-lab.com/blog/article/cyberrange-les-scenarios-dentrainement-par-soteria-lab/
[42] https://www.diateam.net/fr/cyber-range-hybride/
[43] https://www.cyber.airbus.com/fr/cyberrange/
[44] https://uk.leonardo.com/en/cyber-and-security/cyber-advantage/cyber-range-cyber-trainer
[45] https://www.thalesgroup.com/fr/monde/press-release/thales-cree-le-cyber-range-un-centre-virtuel-devaluation-et-dentrainement-en
[46] https://obamawhitehouse.archives.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf
[47] https://www.cr14.ee/
[48] https://www.ggeedu.fr/revue-de-presse/communique-de-presse-salle-cyber-experience-by-galileo-global-education-une-salle-de-simulation-cyber-unique-au-monde-ouvre-ses-portes-au-campus-cyber/
[49] https://telecomnancy.univ-lorraine.fr/formation/projets-et-plateformes-formation/cyber-range/
[50] https://www.qub.ac.uk/ecit//Aboutus/Facilities/CyberRange/

2020 pour proposer une solution de « Cyber Range » spécialisée dans la santé, en co-construction avec des acteurs hospitaliers publics et privés. Cette plateforme a été initiée et subventionnée par la Région[51].

Aux Etats-Unis, le consortium « Virginia Cyber Range »[52] composé de collèges, lycées, universités et institutions publiques de Virginie a développé un centre de ressources et une plateforme de simulation dédiée aux membres du consortium (étudiants et enseignants). Ce Cyber Range a pour objectif d'augmenter le nombre d'étudiants parfaitement préparés à travailler dans la cybersécurité. Le Virginia Cyber Range est une initiative du Gouverneur McAuliffe.

Les « Cyber Range » peuvent être des **infrastructures aux conceptions et aux tailles variées.** L'U.S. Cyber Range développé par le Virginia Cyber Range est, par exemple, une infrastructure entièrement virtuelle. Celle de Télécom Nancy est composée de deux salles avec une cinquantaine de postes et d'une salle de serveurs, qui nécessite la présence sur site pour la réalisation des simulations. L'infrastructure « Cyber Range » proposée par Soteria Lab est composée, pour chaque scénario, d'un caisson contenant un serveur, des équipements réseaux et d'un ondulateur (hébergement local).

En matière de développement d'infrastructures, DIATEAM[53] est un acteur majeur du développement de plateformes Cyber Range. Il a notamment développé les infrastructures de Thalès et de TELECOM Nancy. Il est également membre du Pôle d'excellence Cyber constitué en Bretagne.

Au-delà des infrastructures physiques, virtuelles ou hybrides, des **exercices de simulation sont organisés à grande échelle à l'occasion d'événements dédiés, notamment par les Armées, l'entraînement par la simulation étant une étape indispensable à la préparation opérationnelle.** A l'échelle internationale, **le plus grand exercice de cyberdéfense du monde** a été organisé en avril 2023 à Tallinn en Estonie. Pendant 4 jours, « Locked Shield » a regroupé plus de 3000 spécialistes de 38 pays au sein du Centre d'excellence pour la cyberdéfense en coopération (installé à Tallinn en 2010 et accrédité par l'OTAN).

Capitaliser sur les atouts du territoire : l'expérience en accompagnement de parcours atypiques et en exercices de simulation en vraie grandeur

L'écosystème du Grand Nancy est riche d'acteurs proactifs et volontaires dans la mise en place d'initiatives partenariales, notamment dans deux domaines d'intérêt susceptibles de répondre à certaines problématiques soulevées par le diagnostic Cyber réalisé :

- la sensibilisation aux métiers en tensions et l'accompagnement de parcours professionnels atypiques vers le secteur numérique ; certains dispositifs innovants pourraient être transposés à la cybersécurité ;
- la mobilisation d'outils de simulation et surtout l'expérience unique de simulation de cyberguerre en vraie en grandeur développée sur le territoire grand-nancéen en coopération avec le Ministère des Armées.

[51] https://www.amossys.fr/fr/a-propos/actualites/un-cyber-range-sante-pour-tester-les-dispositifs-medicaux-et-logiciels-de-sante/
[52] https://www.virginiacyberrange.org/about et https://www.uscyberrange.org/overview/
[53] https://www.diateam.net/fr/

Sensibiliser aux métiers et innover pour élargir le vivier de candidats

L'OPEN du Numérique de Grand Nancy

Nancy Numérique et un ensemble de partenaires ont mis en place un événement partenarial et collaboratif au cœur de l'automne : l'OPEN du Numérique[54].

Son objectif est de regrouper sous une programmation commune des animations, manifestations, tables rondes, conférences/débat, portes-ouvertes portées par des structures publiques et privées sur le territoire du Grand-Nancy afin de mettre en valeur la diversité des initiatives numériques en matière d'emploi, de formation, de responsabilité environnementale, de digitalisation de l'économie, de culture, d'innovation, d'inclusion, d'accessibilité, etc.

La première édition de l'OPEN du numérique est intervenue en 2022 avec pas moins de **55 évènements portés par 23 structures publiques ou privées.** Les événements ont permis d'offrir une vision large et concrète des opportunités professionnelles et des offres de formations offertes par la filière sur le territoire du Grand-Nancy. Citons notamment :

- La table ronde « Développer des talents dans les métiers du numérique », organisée par Nancy Numérique et ses partenaires ; la conférence « Comment recruter sur des métiers en tension ? » organisée par Tomorrow Jobs et Nancy Numérique sur les bonnes pratiques en matière de recrutement dans la filière ;
- Le « Tour de France de la Transformation Numérique » porté par CINOV Numérique et l'OPCO Atlas, qui a proposé des conférences et ateliers pratiques pour échanger sur la transformation numérique et les opportunités professionnelles de la filière ;
- Le « Joblab – Forum des Talents Numériques » organisé par la Maison de l'Emploi du Grand Nancy, occasion pour les demandeurs d'emploi et les étudiants de rencontrer des entreprises qui recrutent dans le domaine du numérique ;
- Les journées « Vis ma vie de Dév » rendues possibles par l'entreprise Adista, qui a ouvert ses portes pour offrir une immersion dans le métier de développeur web.

La Place des Compétences Numériques du Grand Nancy (PCN)

Les membres du consortium sont également partenaires de **la « Place des Compétences Numériques »[55], un parcours immersif de mentorat et d'accompagnement de personnes en reconversion** vers les métiers du numérique.

Issu d'une collaboration entre la Maison de l'Emploi du Grand Nancy et l'entreprise Tomorrow Jobs, cabinet de recrutement spécialisé dans les profils numériques, le dispositif PCN repose sur l'investissement bénévole de plus de 50 partenaires, en grande majorité des entreprises qui mentorent les candidats.

A l'image de l'incubation et de l'accélération de start-ups, chaque parcours PCN, d'une durée de 10 semaines, permet aux candidats (jeunes accompagnés par les chantiers d'insertion et les missions locales ; demandeurs d'emploi éloignés de l'emploi et de la formation) de :

- dynamiser leur projet professionnel,
- avoir accès à des ressources utiles (réseaux d'entreprises, mentorat),
- actualiser et renforcer leurs compétences professionnelles et *softskills*,
- enfin, rompre leur isolement et s'insérer dans un réseau de solidarité.

Entre 2020 et 2023, PCN a organisé **10 promotions de candidats, totalisant près de 170 personnes accompagnées** vers l'emploi ou la formation numérique :

- 25 % de femmes et 30 % de seniors (âgés de 45 ans ou plus) ;

[54] Informations sur l'Open du numérique : https://nancynumerique.com/open/

[55] Informations sur PCN : https://pcn-nancy.fr

- 50 % de non-diplômés de l'enseignement supérieur ;
- Plus de 20 thématiques abordées grâce aux partenariats développés avec les employeurs locaux : développement web et mobile, communication digitale, cybersécurité, UX/UI Design, réalité virtuelle, motion design, innovation, recrutement, création d'entreprise, etc.

L'expérience pilote mise en place a fait ses preuves avec près de **130 personnes sur la voie de la formation (cas majoritaire) ou embauchées directement à l'issue de leur parcours PCN.** Ainsi :

- 76% des candidats sont aujourd'hui sur la voie de l'emploi ou de la formation numérique ;
- 60% des participants ont rejoint une formation numérique à l'issue de leur accompagnement ;
- Les principaux domaines professionnels visés par les candidats : développement web, communication digitale, infrastructures réseaux et systèmes.

Si la « Place des Compétences Numériques » n'est pas actuellement dimensionnée pour obtenir des effets significatifs pour la cybersécurité, l'initiative pourrait être déclinée, sur cette cible plus spécialisée, à l'échelle de la Région Grand Est. L'expérience acquise par le territoire pourra être mobilisée pour imaginer les conditions et dispositifs d'un « passage à l'échelle » à rechercher dans l'accompagnement des parcours professionnels atypiques vers la cybersécurité.

Mobilisation en local d'outils d'entraînement et mise en place d'une initiative de simulation cyberattaque d'une ampleur exceptionnelle

Au-delà des capacités de formation, **le diagnostic local emploi/compétences souligne l'importance des besoins d'entraînement et de simulation en vraie grandeur**. Ces besoins s'expriment non seulement en cours de formation pour éprouver ses compétences techniques et comportementales indispensables en gestion de crise, mais aussi pour les entreprises. Plus que dans d'autres domaines, **les capacités d'entraînement et de simulation Cyber permettent un aguerrissement individuel et le développement d'un bon niveau de performance et de résilience collective.** Elles apparaissent donc clés.

Le territoire du Grand Nancy dispose en ce domaine de premiers équipements performants et autour d'eux d'une expérience opérationnelle significative.

Cesi NumériLab de Nancy

Cesi Ecole d'ingénieurs s'est doté sur le territoire du Grand Est de trois NumériLab dont l'un est situé à Nancy. Il s'agit de plateformes pédagogiques en capacité de tester à taille réelle des projets de PME et d'ETI. Elles constituent **un outil d'essai spécialisé** au cas par cas par une entreprise accueillant un stagiaire en alternance **ou d'entraînement**, notamment sur les problématiques de sécurité réseau ou d'applicatif.

Techniquement, il s'agit de laboratoires numériques interconnectés en liaisons haut débit, équipés de fermes de serveurs et de périphériques numériques variés. Chaque site dispose :

- d'une ferme de trois serveurs « lourds » en cluster pilotés sous vCenter permettant la création de machines virtuelles dédiées à chaque projet (biprocesseurs Xéon soit 96 unités de calculs & 576 Go de mémoire centrale) ;
- d'un système de stockage large et rapide permettant du traitement massif de données « big data » (40 To) ;
- d'une interconnexion à 100Mb entre sites par fibres optiques répartie entre un VPN sécurisé par l'opérateur et un flux internet direct sous le contrôle de nos firewalls ;
- de douze postes PC clients renforcés avec cartes GPU pour les traitements d'Intelligence Artificielle ;
- de deux postes clients légers pour les accès purement Terminal Serveur ;
- d'un ensemble de matériels pour des tests en mobilité, IOT, robotique, impression et imagerie 3D ;
- d'un espace créativité et d'un lieu de convivialité dans l'esprit de développement agile et d'innovations des startups.

L'outil bénéficie d'une appréciation positive des entreprises et a été conçu pour pouvoir prendre en charge des problématiques de cyberprotection. Si les capacités actuelles sont circonscrites, il s'agit d'une amorce

intéressante permettant de disposer d'un savoir-faire et de retours d'expérience locaux.

Une logique d'interopérabilité pour les Cyber range des acteurs du territoire, sur fond de coopération avec le Ministère des Armées

Nancy est une terre de coopération entre les organismes de formation et le Ministère des Armées. Dès 2010, Nancy ouvrait l'un des premiers laboratoires civils de haute sécurité informatique de France. Depuis lors, les liens se sont régulièrement renforcés avec les Armées. Le 3 juillet 2018, est intervenue la signature d'une **Convention entre la Base de Défense de Nancy et la Métropole du Grand Nancy autour des problématiques de cybersécurité** ; elle visait :

- La mise en place d'un **laboratoire cyber « cyber range »** au sein de la caserne Verneau,
- Le recrutement d'une quinzaine de **réservistes opérationnels Cyber de haut niveau,** issus du tissu industriel et académique régional. Leur emploi est du ressort du COMCYBER qui valide tout engagement ;
- **L'interopérabilité des plateformes Cyber de Nancy,** à savoir le cyber range de Nancy Telecom, le cyber range mobile de Verneau et la salle de reverse engineering de l'École Nationale Supérieure des Mines de Nancy ;
- La mise en réseau des différents acteurs régionaux Cyber dans le cadre du mandat de correspondant de la réserve Cyber pour le Grand Est donné par le COMCYBER au commandant de la Base de Défense de Nancy.

Les collaborations locales se sont encore renforcées le 24 juin 2020 par la signature d'une Convention de partenariat entre la Base de Défense de Nancy et **l'Université de Lorraine, représentée par les 11 écoles d'ingénieurs de Lorraine-INP afin :**

- améliorer la formation des étudiants des écoles d'ingénieurs de Lorraine INP, des personnels militaires ou civils ;
- en favorisant la meilleure **utilisation collective des plateformes de Nancy** dont le laboratoire Cyber Range de Verneau.

Exercices de cyberguerre : des exercices de simulation exceptionnels, un aguerrissement gage de performance

Bien conscients des enjeux et de la nécessité de se préparer au pire, entreprises, agences gouvernementales, armées et écoles ont développé des dispositifs de simulation de crise pour tester et mettre en pratique les capacités de protection et de défense de leurs équipes. Les Armées françaises comptent actuellement 3 700 cybercombattants, des effectifs qui devraient atteindre 5 200 à l'horizon 2025[56].

L'université de Lorraine, la Base de défense de Nancy et le Commandement de la cyberdéfense (COMCYBER) se sont associés depuis trois années pour organiser un exercice de cyberguerre. Celui de 2023 était baptisé *Cyber Humanum Est* ; il est intervenu du 6 au 8 février 2023, mobilisant une équipe de haut niveau de réservistes des armées, une centaine d'étudiants de six établissements nancéiens et leurs enseignants : la Faculté des sciences et technologie, l'IUT Nancy-Brabois, l'École des Mines de Nancy, Polytech Nancy, Télécom Nancy et l'UFR Sciences humaines et sociales (Master VSOC) ont été mobilisés.

L'exercice a nécessité plus de 500 jours hommes de préparation[57], la mobilisation de plus de 130 personnes organisateurs et participants, plus de 200 équipements virtuels, 1 drone militaire avec son pilote, 3 systèmes mécatroniques (scada), des robots, des attaques par les ondes radio, des malwares dédiés... Il consiste en une simulation de cyberdéfense de type « Capture the Flag » et se veut le plus immersif possible. Il constitue un exercice unique en son genre en Europe qui dote le territoire nancéien et ses étudiants d'une expérience tout à fait différenciante.

* * *

La mise en perspective à 2030 a constitué pour les parties prenantes de FORE-CY un exercice particulièrement stimulant : la conscience des enjeux de résilience et de souveraineté inhérents au domaine Cyber, la

[56] https://www.lesnumeriques.com/pro/cyber-humanum-est-un-exercice-de-cyberguerre-pour-reperer-les-talents-de-demain-a206691.html
[57] https://www.lemondeinformatique.fr/actualites/lire-simulations-de-crise-et-cyberdefense-se-multiplient-en-france-88778.html

compréhension partagée du diagnostic et des atouts du territoire en ce domaine, ont stimulé la créativité. Des idées d'offres nouvelles porteuses pour les candidats du domaine, la filière Cyber et le territoire ont émergé et ont même été préfigurées, motivant les acteurs parties prenantes à poursuivre le travail collectif. Les enseignements du diagnostic territorial ont pour ce faire, été rassemblés dans un macro-plan d'action.

Partie V. Macro-plan d'action

Les différentes approches mobilisées et leur croisement ont permis d'élaborer un diagnostic territorial prospectif fin des besoins en emplois et compétences Cyber du Grand Nancy. Les résultats clés de la mission[58] ont été discutés avec le COTECH et le Comité de pilotage élargi aux parties prenantes avec le souci d'en tirer des pistes d'action opérationnalisables.

En cohérence avec la gouvernance du projet FORE-CY et l'intention première de l'appel à manifestation d'intérêt France 2030 sur les *Compétences et métiers d'avenir*, le collectif FORE-CY emmené par la Maison de l'Emploi du Grand Nancy a structuré les enseignements du diagnostic à l'aune des problématiques de recrutement, de formation et de développement de l'emploi et des compétences.

Le macro-plan d'action s'adresse ainsi prioritairement aux partenaires mobilisés dans le cadre de la mission FORE-CY et aux parties prenantes sensibles à ces questions. Il met en lumière les principaux enjeux et propose six axes d'intervention qui seront à étayer et développer dans la suite du projet. Une attention particulière a été donnée aux actions transverses multi-acteurs qui constituent l'apport de valeur particulier du collectif. Le présent plan d'action ne se substitue pas à une réflexion plus complète sur la résilience Cyber du territoire, l'attractivité des entreprises et la politique de développement économique en ce domaine.

Axe 1. Améliorer les dispositifs d'orientation professionnelle

Proposition #1. Sensibiliser les acteurs en charge de l'orientation scolaire et post-bac afin qu'ils tiennent mieux compte de la pluralité des métiers de la chaîne de valeur Cyber, en embrassant l'ensemble des sous-filières métier :

- Concevoir des **dispositifs adaptés de présentation des métiers et des entreprises** qui ne se focalisent pas uniquement sur les technologies Cyber et mettent en avant l'idée de « métiers qui protègent » ;
- Sur la base de la cartographie des formations réalisée dans le cadre du projet FORE-CY et en l'actualisant, communiquer et mettre en valeur la **variété des parcours et organismes de formation** du domaine, implantés sur le bassin nancéien et plus largement en région Grand Est ;
- Porter une attention particulière aux **publics féminins** dans les actions et dispositifs de communication pour rendre ces métiers attractifs eu égard à leurs appétences et à l'incidence de la réforme du baccalauréat dans leurs choix d'orientation.

Proposition #2. Développer des outils de détection des profils « compatibles Cyber » :

- **basés sur les compétences transversales** identifiées comme porteuses pour les métiers de la Cyber dans le cadre du diagnostic : curiosité naturelle orientée vers la recherche de solutions, résistance au stress et qualités relationnelles tournée vers la satisfaction client ;
- basés sur l'appétence à l'informatique, à la gouvernance des risques ou à la gestion de crise, ou directement à la cybersécurité (technologies, droit, usages).

[58] Les résultats clés de la mission sont repérables tout au long du rapport par un pictogramme en forme de diamant.

Proposition #3. Valoriser l'offre de BTS en informatique appliquée à la cybersécurité ou des champs connexes qui constitue le maillage de proximité locale du domaine, en veillant au mieux à la féminisation de ces parcours d'entrée.

Axe 2. Mieux accompagner les parcours de reconversion professionnelle

Proposition #4. Sensibiliser les acteurs en charge de l'accompagnement socioprofessionnel et de la reconversion :

- **aux différents métiers de la cybersécurité** afin qu'ils tiennent mieux compte de la pluralité des métiers de la chaîne de valeur Cyber, en embrassant l'ensemble des sous-filières métier, en mettant en valeur l'idée de « métiers qui protègent » ;
- **en expliquant la réalité des différents métiers** en fonction des niveaux de formation (Bac +2 à Bac +5), à travers des témoignages, des immersions virtuelles, des échanges avec des professionnels de la filière ;
- **aux profils-types compatibles avec ces métiers** basés sur les trois grandes compétences transversales identifiées dans le cadre du diagnostic : curiosité naturelle orientée vers la recherche de solution, résistance au stress et qualités relationnelles tournée vers la satisfaction client, ainsi que l'appétence à l'informatique, à la gouvernance des risques ou à la gestion de crise, ou directement à la cybersécurité.

Proposition #5. Mieux accompagner les personnes qui engagent un parcours de reconversion en cybersécurité ou dans un domaine connexe avec module Cyber :

- **par les prescripteurs de l'accompagnement professionnel** en expliquant les métiers, en facilitant le décryptage de l'écosystème d'employeurs, en désacralisant l'informatique ;
- **par les organismes de formation qui ne sont pas spécialisés dans la reconversion professionnelle** (Grandes Écoles, Université, etc.) pour être plus soutenant tout au long de leur parcours.

Axe 3. Anticiper les expertises technologiques clés de demain

Proposition #6. Intégrer dans les maquettes pédagogiques des enseignements renforcés en IA :

- Proposer des modules complémentaires en IA dans les parcours Cyber en **partenariat avec les établissements** du bassin nancéiens positionnés sur ce segment ;
- **Encourager les parcours classiques en IA et Machine Learning à s'ouvrir davantage à des enseignements en cybersécurité** en propre ou en partenariat avec des établissements du domaine ;

Proposition #7. Renforcer les liens entre cryptographie et cybersécurité :

- Capitaliser sur les formations du territoire en cryptographie pour proposer des modules dédiés dans les parcours Cyber en **partenariat avec les établissements** positionnés sur ce segment ;
- **Encourager les parcours classiques en IA et Machine Learning à s'ouvrir davantage à des enseignements en cybersécurité** en propre ou en partenariat avec des établissements du domaine ;
- **Encourager la recherche & développement** en ce domaine.

Proposition #8. Apprécier les besoins et renforcer le cas échéant, l'offre de formation en conception et modélisation des architectures et en cyberdéfense/cyberattaque.

Axe 4. Améliorer la formation des profils Cyber

Proposition #9. Consolider et renforcer la formation en instaurant plus de pluridisciplinarité au sein des parcours technologiques (approche hybride juridique, sciences humaines et sociales, UX, design, méthodes agiles) **:**

- **À tous les niveaux du Bac +2 aux Bac +6, en l'adaptant en fonction des niveaux :** véritable innovation pour les Bac +2, l'objectif sera de développer une vision 360° des enjeux au cœur de la stratégie de l'entreprise pour les Bac +5 ;
- En encourageant les **conventions partenariales** entre composantes d'établissements et entre établissements publics et privés afin de dispenser les enseignements d'ouverture au sein des établissements tierces ;
- **En développant des parcours pluriannuels pluridisciplinaires** en partenariat.

Proposition #10. Développer les parcours hybrides pour répondre aux besoins en compétences de l'ensemble de la chaîne de valeur Cyber, au sein des établissements d'expertise non-technologique, notamment :

- Développer des **parcours de formation en Droit appliqué à l'informatique et à la Cyber** en dialogue avec les composantes juridiques du territoire ;
- Développer des **parcours appliqués en Gouvernance des risques, Gestion des risques et gestion de crise,** insuffisamment développés sur le Grand Nancy jusqu'aux métiers de remédiation.

Proposition #11. Renforcer l'acquisition et l'entretien des *soft skills* (gestion du stress, travail en transverse…) afin de limiter l'attrition des professionnels des métiers technologiques de la Cyber

- **via la formation** et **en encourageant les mises en situation réalistes** favorisant l'aguerrissement au en formation initiale (mutualisation des Cyber Range des établissements en disposant) ;
- **en encourageant les employeurs à mieux accompagner** les collaborateurs au titre de la qualité de vie au travail.

Axe 5. Faire du Grand Nancy une place forte de formation Cyber d'envergure nationale

Proposition #12. Promouvoir une offre de formation Cyber de haut niveau, cohérente, forte et attractive du Bac +2 au Bac +8 à l'échelle du bassin nancéien

- **Favoriser les continuums de parcours d'excellence,** notamment labellisés SecNumEdu
- **Favoriser des parcours Cyber avec mention de spécialisation en santé ou finance** en partenariat avec les acteurs du territoire afin de mieux répondre aux besoins de l'écosystème local et de favoriser l'insertion professionnelle des talents sur le territoire :

- Développer des **réponses innovantes aux besoins de la filière Cyber** en tirant partie des infrastructures locales et en les renforçant (ex. universités d'été de la Cyber sur le campus technologique d'ARTEM particulièrement dotés en équipements pédagogiques…)
- **Poursuivre l'exercice de simulation d'attaque en vraie grandeur Cyber Humanum Est en partenariat avec la Base de Défense de Nancy** et le Commandement de la Cybersécurité des Armées, et l'élargir à d'autres partenaires pédagogiques (Cesi, Epitech, lycées…).

Proposition #13. Mettre en œuvre une sensibilisation systématique à l'hygiène numérique des jeunes publics du bassin nancéien

- Concevoir et initier **une action annuelle cible à destination des collégiens et lycéens** du territoire permettant de diffuser les bonnes pratiques d'hygiène numérique et de faire la promotion des métiers de la Cyber avant les choix définitifs d'orientation scolaire ;
- Concevoir **un module-type d'hygiène numérique** à destination des établissements et composantes de l'Enseignement Supérieur et le tester à l'échelle des 50 000 étudiants du territoire.

Proposition #14. Doter le territoire du Grand Nancy d'une infrastructure hybride de simulation d'attaque Cyber et de gestion de crise à destination de tous les publics :

- **constituant un lieu de formation, de partage d'expériences croisées entre écoles et niveaux de formation complémentaires** en insufflant du réel dans la formation ;
- un lieu de **sensibilisation et d'entraînement pour les entreprises** utilisatrices et les acteurs prestataires ;
- **y proposer des approches intégrant « l'ensemble des étages » :** anticipation/prévention, protection, détection, remédiation avec différents niveaux d'expertise (opérationnelle, stratégie et planification, communication, etc.) ;
- **y rattacher et développer un concept innovant d'école de formateurs Cyber.**

Axe 6. Concourir à un territoire de résilience et confiance numériques en étant à l'écoute des besoins de l'écosystème

Proposition #15. Concrétiser sur le territoire nancéien le projet de Campus Régional Cyber (lieu totem ou antenne) :

- Y favoriser les **échanges et coopérations** entre les organismes de recherche, les entreprises et les organismes de formation ;
- Mettre en place un **Observatoire prospectif local et régional des emplois, métiers et compétences Cyber** doté d'un outil de modélisation afin d'étayer les enjeux RH quantitatifs et les besoins de formation.

Proposition #16. Renforcer la sensibilisation de tous les acteurs du bassin nancéien à la cybersécurité et mieux faire valoir les services offerts par le CSIRT et les ESN de la métropole auprès :

- des entreprises et administrations ;
- des étudiants et scolaires ;
- du grand public.

Annexe #1

Présentation des membres du Consortium

A propos de la Maison de l'Emploi du Grand Nancy

Chef de file du projet FORE-CY, la Maison de l'Emploi du Grand Nancy, créée en 2005 à l'initiative de la Métropole du Grand Nancy sous statut associatif, structure son activité autour de trois grands axes :

- l'accompagnement des transitions économiques, sociales, numériques et environnementales des secteurs et filières à enjeux ;
- le soutien à l'emploi local et l'appui aux employeurs ;
- l'animation du PLIE et du Contrat de Ville (volet Emploi).

La Maison de l'Emploi du Grand Nancy s'appuie sur un réseau de plus de 500 partenaires institutionnels et économiques. Ses projets s'adressent chaque année, à plus de 3 000 entreprises et à 12 000 personnes (dirigeants, salariés, demandeurs d'emploi). La Maison de l'Emploi du Grand Nancy est lauréate de nombreux appels à projets nationaux ou régionaux, financés par le Ministère du travail, la Banque des Territoires, France Num, la DGE, la Grande École du Numérique ou encore la Région Grand Est.

Pour en savoir plus : https://www.mde-ml-grand-nancy.org

A propos de Numeum

Numeum est l'organisation professionnelle de l'écosystème numérique en France. Elle représente les entreprises de services du numérique (ESN), les éditeurs de logiciels, les plateformes et les sociétés d'Ingénierie et de Conseil en Technologies (ICT).

Numeum rassemble plus de 2 500 entreprises adhérentes qui réalisent 85% du chiffre d'affaires total du secteur. Présidé par Godefroy de Bentzmann et Pierre-Marie Lehucher, Numeum souhaite mettre le numérique au service de l'humain avec deux ambitions fondatrices :accompagner le pays dans la généralisation et la démocratisation de la formation numérique ; agir au service d'un numérique responsable pour les entreprises, la société, l'Humain et la planète.

L'engagement de Numeum repose sur 4 piliers d'actions : la valorisation et la défense des intérêts de ses membres et de leurs métiers, l'incarnation de la France numérique en Europe, l'animation de l'écosystème numérique pour favoriser les synergies et l'innovation, et le renforcement du service à toutes les entreprises du numérique.

Numeum est membre de la fédération Syntec. Le secteur du numérique représente plus de 60,8 Md€ de chiffre d'affaires et 572 126 employés en France.

Pour en savoir plus : https://numeum.fr

A propos de Nancy Numérique

Nancy Numérique, association créée en 2009, et présidée par Gaspard Bergeret, a pour vocation d'animer, d'accompagner et de mettre en valeur l'écosystème numérique du Grand Nancy. L'association agit pour, et avec un ensemble d'acteurs de l'écosystème numérique local : entreprises, consultants et indépendants, institutions publiques, écoles et universités, associations, etc. Les missions de Nancy Numérique sont les suivantes :

- Connecter les acteurs de l'écosystème ;
- Mettre en lumière les compétences du territoire ;
- Aider au développement des adhérents ;
- Faciliter la transformation numérique des acteurs locaux ;
- Ancrer le numérique dans des thématiques transversales (culture, handicap, responsabilité environnementale...).

Pour en savoir plus : https://nancynumerique.com

A propos de CESI École d'ingénieurs

CESI École d'ingénieurs est un acteur majeur de l'Enseignement supérieur et de la formation professionnelle, implanté dans la cité ducale depuis 1984.

À la rentrée 2022, CESI a annoncé le développement de ses activités sous une seule marque afin d'affirmer son positionnement d'acteur majeur de l'Enseignement supérieur. Ce nouveau positionnement, comprend le développement de huit programmes de formation, dont des programmes « passerelles » afin de faciliter l'intégration du cycle Grande École d'Ingénieur grâce à des remises à niveau, ou encore des programmes pour internationaux. En 2022, ce sont plus de 26 000 apprenants qui ont rejoint les 25 campus présents sur l'ensemble du territoire français dans quatre grands secteurs d'activité : Informatique & Numérique, Industrie, BTP et Ressources Humaines & Management.

Pour en savoir plus : https://www.cesi.fr

A propos de Randea

Le consortium FORE-CY s'appuie sur l'expertise reconnue en prospective RH territoriale de Randea. Marie-Laetitia des Robert, sa fondatrice, est Docteur en sociologie de Sciences Po Paris, avec une expérience de plus de 15 ans en prospective RH forgée à la DRH du Ministère de la Défense puis comme associée senior du BIPE. Elle y a piloté plusieurs missions de prospective RH dans les services comme dans l'industrie, notamment pour l'OPCO2i dont l'une faisant de la cybersécurité, l'une des 7 activités critiques de la Branche métallurgie.

Randea est spécialisée dans l'accompagnement des transitions de filière technologique, environnementale et collective. Randea appuie les entreprises et les collectifs en déployant des approches à forte exigence méthodologique et un savoir-faire éprouvé en intelligence collective croisant les outils de la prospective quantitative, de la sociologie et de l'analyse stratégique avec ceux des approches participatives, avec le souci de résultats opérationnalisables.

Dans son actualité récente, citons :

- *L'élaboration de la Feuille de route Décarbonation de la filière pharmaceutique*, pour la FEFIS, publication prochaine par le Conseil National de l'Industrie ;
- L'animation du *Laboratoire d'innovation territoriale du GDON des Bordeaux*, en partenariat avec l'INRAE dans le cadre du projet VitiREV : expérimentation d'un changement d'échelle dans la lutte contre la Flavescence dorée affectant les vignes, avec pour objectif final de réduire l'utilisation de pesticides ;
- L'appui à l'Observatoire Régional des Compétences Industrielles (ORCI) d'Occitanie sur *les compétences nouvelles de la filière aéronautique et spatiale occitane*.

Pour en savoir plus : https://randea.fr

Liste des personnes auditionnées

Emilie BONNEFOY, CEO Open Sezam

Gaëlle BRIZION, Chargée d'affaires du Campus CESI école d'ingénieur

Christophe CHAMBET-FALQUET, Data Coach / Data Strategist

Claire DITNER, Cheffe de projets structurants, Grand E-nov+

Laurent DUEZ, Chef de projets Développement des compétences, en charge des transitions numériques et industrielles, Région Grand Est

Stéphane LAURENT, Responsable du pôle Enseignement supérieur, Région Grand Est

Franck OLIVIER, Chargé de mission numérique, Région Grand Est

Fabian OSMOND, Président de Cybi

Jean-Claude RENAUDIN, Responsable de Grand Est Cybersécurité (CSIRT)

Renaud TISSERANT, Président de la Commission « ITPME » de Numeum

Matthieu VEILLÉ, Directeur général, Chargé de développement et de projets de Nancy Numérique

Irène WEISS, Conseillère régionale déléguée à la cybersécurité

Annexe méthodologique #2

Méthodologie du volet « Employeurs de compétences Cyber »

1| Travaux amont : enjeux, périmètre des métiers et compétences cibles

L'étude des besoins en compétences de l'écosystème cybersécurité a été introduite par **des entretiens qualitatifs auprès d'entreprises et organismes spécialisés en Cybersécurité du territoire afin de dresser la toile de fond des défis des entreprises en ce domaine.** Les entretiens ont été relativement limités en nombre compte tenu de la forte convergence d'analyse des défis qui ont aussi présidé à la mise en place de la *Stratégie nationale d'accélération pour la cybersécurité*.

Ont été interrogés en décembre 2022 : les membres du Consortium (CESI école d'ingénieurs, Nancy Numérique et Numeum), la Conseillère régionale déléguée à la cybersécurité ainsi que quelques entreprises. La remontée d'information sur les problématiques locales relatives à la filière et aux besoins en emplois et compétences s'est poursuivi lors **des échanges techniques du COTECH ainsi qu'avec les parties prenantes du territoires lors des trois séminaires du COPIL élargi.**

Le diagnostic des enjeux a constitué la toile de fond de la réflexion sur **le périmètre des métiers et compétences Cyber à retenir pour répondre aux besoins du territoire et à la préparation de l'avenir**. Les référentiels métiers disponibles français (ANSSI, Région Grand Est puis le RCCP de Cybermalveillance.gouv.fr) et européens (ECSF/ENSIA, CyBok/Université de Bristol) ont fait l'objet d'une analyse comparative. Les analyses ont conduit les pilotes du projet à retenir un périmètre élargi permettant d'embarquer la diversité qui ressortait du panorama des défis à relever pour les entreprises **dans une logique de « chaîne de valeur » complète.**

Au-delà du périmètre des métiers, l'ambition du projet FORE-CY était aussi de disposer d'une **compréhension fine des besoins en compétences des employeurs,** entreprises prestataires de services Cyber ou disposant d'un service interne dédié. Pour ce faire, il a été procédé au recensement des « compétences métiers » du référentiel ANSSI (hors *soft skills*) indistinctement de la fiche-métier correspondante. Il en a résulté une liste de 36 compétences distinctes qui ont été sélectionnées et regroupées en 19 compétences cibles sensibles pour répondre aux besoins en cybersécurité (cf. *infra*) afin de rester sur une volumétrie acceptable pour un questionnaire.

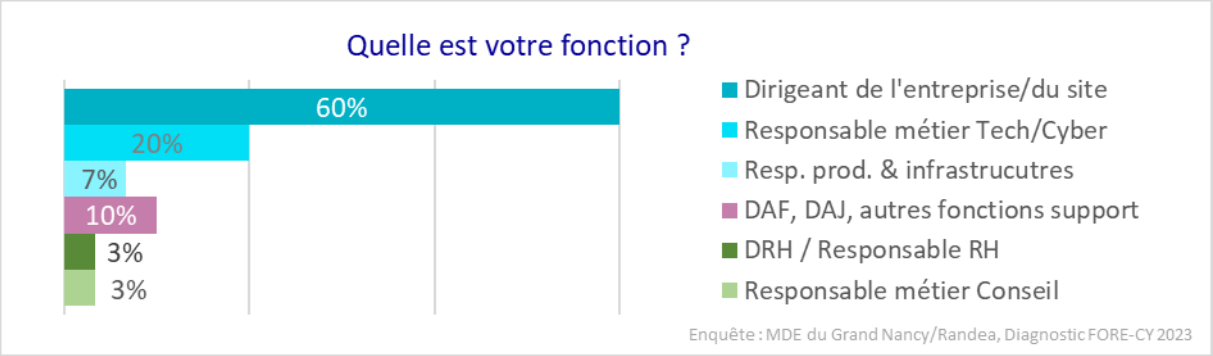
2| L'enquête auprès des employeurs de profils Cyber du territoire métropolitain

Afin d'approfondir les besoins en compétences des employeurs de profils Cyber du territoire métropolitain, une enquête par questionnaire a été mise en place.

- L'enquête a ciblé des employeurs de sociétés prestataires de service en cybersécurité et d'organisations d'autres secteurs disposant d'un service ou pôle de cybersécurité interne.

  101 employeurs de la métropole du Grand-Nancy ont été identifiés comme susceptibles d'être employeurs de profils Cyber et ont été sollicités par internet puis par relance téléphonique par l'APF de Ludres, ainsi que 13 prestaires du Grand Est, soit au total : 91 entreprises prestataires et 26 organisations des secteurs banque/assurance et industrie ou de l'administration publique dont les entités locales des Ministères de la Justice et des Armées, les services de santé. **30 entreprises ont répondu présentes, soit un taux de retour de 25% permettant une exploitation des données malgré le quorum inévitablement resserré.**

  L'enquête a été principalement renseignée par des dirigeants ou responsables métiers :



- L'enquête a prioritairement porté sur les champs suivants :
  - **Profil de l'entreprise :** activité principale, secondaire, pourcentage du CA en cybersécurité, nombre de collaborateurs mobilisés sur les prestations Cyber, R&D Cyber
  - **Effectifs et enjeux RH :** évolution des effectifs, pourcentage de femmes, jeunes/seniors en Cyber, recrutements par profil (Bac+3 +5/8 Tech +5/8 Conseil), recours à l'alternance, difficultés RH par profil
  - **Anticipation des besoins en compétences et formation :** l'approche a porté sur 8 compétences technologiques de mise en œuvre, 4 compétences technologiques dites de supervision, 7 compétences relevant du conseil et de l'accompagnement des organisations (cf. ci-dessous – intitulés proposés aux répondants ; aucune définition complémentaire n'était fournie dans le questionnaire). Elle a investigué de façon fine pour chacune des compétences ou famille de compétences les dimensions suivantes :
    - Expression des besoins à 12-36 mois (couverts ou non) et moyens de les couvrir ;
    - Niveaux et profils de recrutement envisagés, voies de formation ;
    - Vision de l'évolution des métiers Cyber et attentes en matière de formation.

Formulation des besoins en compétences proposée aux répondants		
Compétences technologiques de mise en œuvre	Compétences technologiques dites de supervision	Compétences relevant du conseil et de l'accompagnement des organisations
1| Connaissance, veille, mise en œuvre des technologies de sécurité (pare-feu, anti-virus, techniques d'authentification …)	1| Conception et modélisation des architectures liées à la sécurité	1| Connaissance de la gouvernance des risques, veille des normes et standards Cyber, méthodes d'audits
2| Exploitation des sources ouvertes de manière sécurisée (OSINT)	2| Management sécu. de l'info° (SMSI), méthodes d'analyse des risques de sécurité, stratégie cyber de l'orga°, Security-by-design	2| Gestion des risques
3| Dév. sécurité et ingénierie logicielle (vulnérabilités logicielles…)	3| Forensic : connaissance des outils d'analyse, de collecte de preuves et des procédures légales	3| Droit lié à la sécurité des SI et à la protection des données (normes, standards, PRA/PCA, RGPD, etc.), menaces
4| Dév. sécurité et ingénierie numérique (systèmes embarqués...)	4| Connaissance et veille des normes, certifications et évaluations sécuritaires de produits : ISO, PCI, DSS, Critères Communs, CPSn, etc.	4| Formateurs en cybersécurité (pour publics non experts ou initiés)
5| Cyberdéfense : techniques d'attaque et intrusion, vulnérabilités des envir., analyse des flux réseaux et de journaux		5| Évaluation des besoins clients, analyse bénéfices/risques et approche financière
6| Rétro-ingénierie, Scripting, cryptographie...		6| Sciences cognitives et comportementales, usages, confiance numérique utilisateurs, UX, etc.

7| IA et Machine Learning... 8| Anim° du processus d'innovation technologique		7| Change management, transfo°, méthodes d'intelligence collective (Living Lab…), etc.

- 10 entreprises prestataires ont poursuivi le questionnaire sur trois thèmes connexes :
  - **Bilan et perspectives d'activité en Cybersécurité :** priorités stratégiques, évolution du CA Cyber 2020-2025, intensité du niveau d'activité
  - **Rapports à l'écosystème territorial :** mutualisation d'actions de veille, liens avec les écoles et organismes
  - **Maturité Cyber de leurs clients**

  Les réponses, peu nombreuses, apportent une mise en perspective stratégique intéressante pour l'analyse, même si elles ne sont pas statistiquement suffisamment robustes pour constituer des résultats significatifs. Elles ont néanmoins fait l'objet d'une exploitation **à titre exploratoire**.

- L'enquête « Employeurs de profils Cyber » n'a pas l'objet d'un redressement compte tenu de l'aléas relatif à la connaissance de la population-mère et de la petite taille de l'échantillon. Chacune des réponses ont été considérée avec un poids identique quelle que soit la taille ou le degré de spécialisation Cyber des acteurs.

3| Les exploitations statistiques complémentaires

Le volet économique de l'étude a été complété par l'exploitation des données statistiques publiques disponibles :

- Un portrait statistique des entreprises de l'écosystème et de leurs ressources humaines a été réalisé *via* l'exploitation des données DSN suite à une commande de traitements à façon auprès des services lorrains de l'INSEE. Les données métropolitaines sont mises en perspectives sur les mêmes champs avec plusieurs régions (le Grand Est, les Hauts-de-France, la Bretagne, l'Auvergne-Rhône Alpes et l'Occitanie), ainsi qu'avec la France entière à partir des bases INSEE BTS 2020 et DADS 2020 ;

  Afin d'y procéder, ont été retenus dans la base INSEE/BTS regroupant l'ensemble des données sociales nominatives agrégées (DNS), deux agrégats : celui des **cadres informatiques** et celui des **techniciens informatiques** de droit privé sur la base des regroupements suivants :

Cadres informatiques			Techniciens informatiques	
388A	**388B**	**388C**	**478A**	**478B**
Ingénieurs et cadres d'étude, recherche et développement en informatique	Ingénieurs et cadres d'administration, maintenance, support et services aux utilisateurs en informatique	Chefs de projets informatiques, responsables informatiques	Techniciens d'étude et de développement en informatique	Techniciens de production, d'exploitation en informatique

- Une analyse du marché du travail local en cybersécurité a enfin été réalisée à partir des données Pôle Emploi et des données de l'enquête FORE-CY sur la base des périmètres suivants :

Familles professionnelles (FAP2) pour la comparaison 2018/2022				
M0Z60	**M1Z80**	**M1Z81**	**M2Z90**	**M2Z92**
Employés et opérateurs en informatique	Techniciens d'étude et de développement en informatique	Techniciens de production, d'exploitation, d'installation, et de maintenance, support et services aux utilisateurs en informatique	Ingénieurs et cadres d'étude, recherche et développement en informatique, chefs de projets informatiques	Ingénieurs et cadres des télécommunications

Codes ROME	Appellations spécifiques

M1802	M1805	M1810	038834	038915	038917	038918
Expertise et support en SI	Études et développement informatique	Production et exploitation de SI	Opérateur(trice) en cybersécurité	Analyste en cybersécurité	Expert(e) en cybersécurité	Spécialiste en gestion de crises cyber

Méthodologie du volet « Formations en cybersécurité »

La cartographie des formations de la cybersécurité a été établie selon deux focales complémentaires. Elle recense du local à l'échelle du Grand Est :

- les **formations permettant d'accéder aux métiers spécialisés de la cybersécurité aux savoir-faire technologiques :** il s'agit de formations initiales du Bac Professionnel au Doctorat, mais aussi de formations professionnelles ou de reconversion ;
- les formations incluant des modules de compétences ou de connaissances de la cybersécurité **intégrés à des parcours ayant une autre dominante de spécialité** qu'il s'agisse de formation initiale ou de modules de formations professionnelles.

Étapes de mise en œuvre

La cartographie a été élaborée selon la démarche suivante :

- Collecte extensive de données (cf. sources ci-dessous) et analyse documentaire des informations récoltées ;
- Une enquête auprès des organismes de formation pour consolider la donnée et l'enrichir d'éléments de diagnostic de maturité et une mise en perspective à partir de quelques questions de l'enquête Employeurs ;
- Le partage des résultats en séminaire avec le Comité de pilotage élargi aux parties prenantes.

1| Sources de l'approche cartographique

La cartographie a été établie par le biais d'informations croisées à partir :

- de **données communiquées par l'écosystème** numérique notamment les partenaires du consortium du projet FORE-CY, mais aussi les certificateurs et financeurs ;
- d'une **veille internet** des sites-ressources dédiés à l'orientation scolaire, post-bac et continue ainsi que sur les bases de données en ligne (Grande École du Numérique, ONISEP, Région Grand Est, Inter CARIF-OREF, ANSSI notamment les formations initiales en cybersécurité de l'Enseignement supérieur labellisées SecNumEdu) ;
- des données sur le contenu des formations retenues, recensées sur les **sites internet des organismes identifiés** ;
- l'**envoi à chaque organisme ciblé des lignes de la cartographie le concernant pour validation** et, le cas échéant, complétion des données.

Les établissements employeurs ont également été sollicités dans le cadre de l'enquête FORE-CY Employeurs, pour partager le nom des organismes de formation auxquels ils recourent .

Le travail de recensement des formations réalisé dans ce diagnostic a visé à être le plus fin possible sans pouvoir prétendre à l'exhaustivité. **La veille extensive des formations courtes a été plus difficile à réaliser,** en raison du nombre limité de données disponibles sur internet ou au sein des bases de données en ligne.

2| Enquête auprès des organismes de formation

Afin d'approfondir les besoins en compétences des employeurs de profils Cyber du territoire métropolitain, une enquête par questionnaire a été mise en place.

- L'enquête a ciblé les **70 composantes issus de 48 établissements** identifiés au sein de la cartographie des formations en cybersécurité du Grand Est

  La population-mère est ainsi composée de 23 lycées, 30 composantes ou établissements de l'Enseignement supérieur et 17 organismes spécialisés dans la formation professionnelle. 44 acteurs ont répondu à la sollicitation de FORE-CY, soit un très beau **taux de retour de 63%**. Les réponses ont été **redressées sur la base du type d'établissement, sans introduire de pondération relative au nombre de sortants** des différents acteurs. Ainsi, une fois redressé en « 70 acteurs », chaque établissement vaut 1 indépendamment du nombre de sortants.

- L'enquête a prioritairement porté sur les champs suivants :
  - **Profil de l'organisme ;**
  - **Attractivité** des formations par famille et **difficultés** rencontrées pour les formations initiales ou professionnelles longues (*versus* courtes) de spécialité technologiques *versus* autres expertises ;
  - **Démarche d'élaboration des offres de formation en cybersécurité** et modalités de prise en compte des besoins des employeurs de profils Cyber ;
  - **« Atouts » vis-à-vis des enseignements prodigués** :
    - Part d'enseignement par des professionnels extérieurs ;
    - Place faite aux approches complémentaires au champ disciplinaire principal (ex. sciences cognitives pour les formations de spécialité technologique).
  - **Vision de l'évolution des métiers de la Cyber à 5 ans** et **principaux défis** en matière de formation en lien avec la cybersécurité à 5 ans.

3| Partage et enseignements

La cartographie des formations et l'enquête auprès des organismes de formation ont fait l'objet d'un partage lors de la séance de travail associant le Comité de pilotage élargi du 6 avril 2023. **Les résultats sont également mis en perspective avec les réponses des employeurs de profils** Cyber quant à leur capillarité avec l'écosystème de formation et leurs attentes.

Méthodologie du volet « Monographie de parcours de reconversion »

Le diagnostic FORE-CY s'est intéressé à deux itinéraires de reconversion avec :

- **9 personnes** issues d'un cursus initial ou de premières expériences professionnelles qui n'ont aucun rapport direct ni avec la cybersécurité, ni avec la sécurité informatique ;
- **3 personnes** ayant connu une transition forte au sein de la cybersécurité ou plus globalement de l'informatique.

1| Profils et identification des personnes interrogées

L'étude s'appuie sur le recueil et l'analyse de parcours individuels de reconversion professionnelle d'hommes et de femmes qui :

- ont finalisé leur parcours (avec ou sans être intégré en emploi) au cours des trois dernières années ;
- sont en cours de réalisation de leur parcours de reconversion ;
- ont commencé mais stoppé leur parcours.

L'identification des profils à rencontrer dans le cadre l'étude s'est fait en lien avec :

- Des organismes de formation (AFPA, CNAM, GRETA, Web Force 3, CESI) ;
- Des structures de l'accompagnement à la reconversion et à la transition professionnelle (Transition Pro Grand Est, Place des Compétences Numériques[59] piloté par la Maison de l'Emploi du Grand Nancy) ;
- Des entreprises accueillant des personnes en reconversion sur des métiers de la cybersécurité dans le cadre de contrats en alternance ou ayant connaissance de profils répondant aux critères.

En complément, des profils ont été trouvés sur des CVthèques en ligne, notamment sur le site de l'APEC. L'étude cible en priorité des personnes situées sur le territoire de la Métropole du Grand Nancy ; toutefois, la spécificité de l'étude a rendu difficile l'identification de ces profils. Des opportunités de rencontres avec des personnes ayant engagé des parcours de reconversion sur d'autres territoires ont aussi été réalisé afin de disposer d'une base renforcée d'entretien, étant entendu que la dimension géographique n'apparaissait pas comme un critère déterminant dans le parcours de reconversion relevant de la Cyber.

2| Guide d'entretien pour le recueil de témoignages

Les témoignages sur les parcours ont été recueillis à l'occasion d'entretiens semis-directifs individuels d'environ 1h, réalisés en présentiel, visio-conférence ou par téléphone, entre le 21 février 2023 et le 28 mars 2023.

Les entretiens réalisés ont vocation à récolter de manière descriptive les parcours individuels pour comprendre de manière fine :

- Les conditions d'émergence du projet de reconversion,
- Le choix du secteur et du métier,
- Les dispositifs et aides mobilisés,
- Les différentes étapes du projet,
- Les modalités et délais de concrétisation du projet,
- Les conséquences dans les autres pans de la vie,
- La projection dans l'emploi à l'issue.

Au-delà de l'aspect narratif, le cadre des entretiens vise également à aborder les expériences vécues au travers de ce qui a rendu possible et facilité, ou à l'inverse, de ce qui a contraint, empêché ou rendu difficile la finalisation du projet de transition professionnelle.

Méthodologie du volet prospectif

Quatre scénarios contrastés ont été élaborés sur la base d'un travail de co-construction en séminaire avec le comité de pilotage élargi aux parties prenantes en décembre 2022, d'échanges en COTECH et de travaux de veille sectorielle réalisés dans le cadre de la mission. La politique territoriale régionale en matière de cybersécurité y est prise en compte. Les scénarios relèvent d'une démarche de **prospective narrative** et n'ont pas fait l'objet d'un étiage économique et sectoriel consolidé.

[59] https://pcn-nancy.fr/

Précaution méthodologique. Les quatre scénarios brossés matérialisent l'amplitude du spectre des possibles pour le secteur de la Cyber à 2030. Le niveau d'incertitude limite la portée de tout exercice de réelle simulation quantitative des besoins. Néanmoins, à titre illustratif de cadrage, des « tirs sous hypothèses » normatifs ont été réalisés sur la base des deux modèles étalonnés dans le volet I de la mission. Ils n'ont d'autre vertu que de tester la sensibilité des effectifs aux jeux d'hypothèses introduits.

Les scénarios ont été traduits ou transposés sous la forme de jeux d'hypothèses cohérents en paramétrant :

- *l'évolution du nombre d'acteurs* offrant des services de cybersécurité ou se dotant d'une équipe interne en ce domaine sur le territoire métropolitain ;
- *la dynamique des effectifs,* raisonnée de façon différentiée selon les différents profils (techniciens, profils Tech de type Bac +5 à 8, profils conseil).

Les simulations ont été réalisées selon les hypothèses et résultats-tests suivants :

	Nombre d'employeurs de profils Cyber à 2030 (N.B. 104 en 2023)	*Dynamique des effectifs*	*Effectifs Cyber en 2023 (base 2023 : 750)*	*Effectifs Cyber en 2023 (base 2023 : 875)*	*TCAM des effectifs*
Scénario B | Fil de l'eau « Pourvu que l'orage tombe plus loin… »	135	Effet de concentration de l'écosystème avec dynamique RH calée pour retrouver le TCAM historique	1 270	1 575	9%
Scénario A | Un territoire de confiance et de résilience numérique	200	Accélération de la dynamique RH (x1,5 à 2,5 selon les profils)	2 000	2 400	15%
Scénario C | L'IA et ses dangers	180	Légère accélération de la dynamique RH (x1,1 à 1,3 selon les profils)	1 475	1 775	11%
Scénario D | L'IA, rupture pour tous, même la Cyber	115	Chute brutale des effectifs Techniciens, hausse des effectifs Conseil (x1,5) et dynamique intermédiaire pour les profils Tech Bac+5 à 8	1 045	1 245	5%

La vision prospective des organismes de formation quant à l'intérêt de compléter la formation proprement dite par de l'entraînement de mise en situation a été nourrie d'une **veille comparative nationale et internationale**.

Annexe cartographique #3

- Cartographie des **formations spécialisées en cybersécurité de plus de 200h** en Région Grand Est

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Manager en ingénierie informatique Option sécurité et cloud	Titre professionnel	7	CCI Alsace	Strasbourg	Oui	N/A
Manager en infrastructures et cybersécurité des SI	Titre professionnel	7	CESI	Nancy	Non	Oui
Manager de la sécurité des systèmes d'information	Mastère spécialisé	7	CESI	Nancy	Oui	Oui
Ingénieur spécialité informatique Option cybersécurité	Ingénieur	7	CESI	Nancy	Oui	Oui
Ingénieur informatique parcours cybersécurité	Ingénieur	7	CNAM Grand Est	Nancy	Oui	Oui
Sciences, technologies, santé mention Informatique Parcours Sécurité informatique, cybersécurité et cybermenaces	Master	7	CNAM Grand Est	Grand Est	Oui	Oui
Ingénieur Majeure Cybersécurité et systèmes	Ingénieur	7	EPITA	Strasbourg	Oui	N/A
MCs Pro cybersécurité	Master	7	EPITECH	Strasbourg / Nancy	Oui	N/A
Expert en cybersécurité et réseau	Titre professionnel	7	Mewo	Metz	Oui	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Mastère Spécialisé cybersécurité : attaque et défense des systèmes informatiques	Mastère spécialisé	7	Université de Lorraine	Nancy	Non	Oui
Ingénieur Telecom Approfondissement internet, systèmes connectés et sécurité	Ingénieur	7	Université de Lorraine	Nancy	Oui	Oui
Ingénieur civil des Mines parcours cybersécurité	Ingénieur	7	Université de Lorraine	Nancy	Oui	Oui
Master Informatique, parcours type Sécurité de l'Information et des Systèmes (SIS)	Master	7	Université de Lorraine	Nancy	Oui	Oui
Master Informatique, parcours type Sécurité de l'Information et des Systèmes (SIS)	Master	7	Université de Lorraine	Metz	Oui	Oui
Master Réseaux et Télécom Parcours ADMINISTRATION ET SÉCURITÉ DES RÉSEAUX - ASR	Master	7	Université de Reims	Reims	Oui	Oui
Master Réseaux et Télécom Parcours Développement d'Applications et Sécurité - DAS	Master	7	Université de Reims	Reims	Oui	Oui
Master Ingénierie et Management en Sécurité Globale Appliquée	Master	7	Université de technologie de Troyes	Troyes	Oui	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Master (DNM) Sciences, Technologies et Santé, mention Ingénierie des Systèmes Complexes, parcours Sécurité des Systèmes d'Information (SSI)	Master	7	Université de technologie de Troyes	Troyes	Oui	**Oui**
Mastère spécialisé expert forensic et cybersécurité	Mastère spécialisé	7	Université de technologie de Troyes	Troyes	Oui	**Oui**
Concepteur en architecture informatique parcours cybersécurité	Titre professionnel	6	CNAM Grand Est	Strasbourg	Oui	Oui
Administrateur d'infrastructures sécurisées	Titre professionnel	6	AFPA	Frouard	Non	Oui
Sciences, technologies, santé mention Métiers de l'informatique administration et sécurité des systèmes et des réseaux Parcours Cybersécurité et réponse à incident pour les systèmes d'information, indust. et urbains	Licence professionnelle	6	CNAM Grand Est	Grand Est	Oui	Oui
Bachelor numérique **Option cybersécurité**	Bachelor	6	ESAIP la Salle	Reims	Oui	N/A
Administrateur d'infrastructures sécurisées	Titre professionnel	6	ICAM Strasbourg	Strasbourg	Non	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Analyste en Génie Informatique et Réseaux - spécialiste Cybersécurité	Titre professionnel	6	IFIDE / Sup Formation	Strasbourg / Metz	Oui	Oui
Bachelor Réseaux & Cyber Sécurité	Bachelor	6	Metz numeric school (ancien IFAtech)	Metz	Oui	Oui
BUT réseaux et télécommunication parcours cybersécurité	Bachelor	6	Université de Haute Alsace	Colmar	Oui	Oui
BUT réseaux et télécommunication parcours cybersécurité	Bachelor	6	Université de Lorraine	Nancy	Oui	Non
Licence Professionnelle Métiers des Réseaux Informatiques et Télécommunications, Parcours Cybersécurité et Cyberdéfense (CYBER)	Licence professionnelle	6	Université de Lorraine	Nancy	Oui	Oui
Licence Professionnelle Métiers des Réseaux Informatiques et Télécommunications, Parcours Réseaux Sans Fil et Sécurité (RSFS)	Licence professionnelle	6	Université de Lorraine	Nancy	Oui	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Licence informatique et télécommunication parcours administration et sécurité des réseaux	Licence professionnelle	6	Université de Reims	Reims	Oui	Oui
Licence Professionnelle Métiers de l'Informatique : Administration et Sécurité des Systèmes et Réseaux, Parcours Administration de Systèmes, Réseaux et Applications à Base de Logiciels Libres (ASRALL)	Licence professionnelle	6	Université de Lorraine	Metz	Oui	Oui
BUT réseaux et télécommunication parcours cybersécurité	Bachelor	6	Université de Reims	Chalons en Champagne	Oui	Oui
Administrateur d'infrastructures sécurisées	Titre professionnel	6	Webforce 3	Strasbourg	Oui	Oui
BTS Cybersécurité, informatique et réseaux, électronique	BTS	5	LEGT Charles de Foucault	Nancy	Oui	N/A
			LEGT Henri Loritz	Nancy	Oui	Oui
			LEGT Raymond Poincaré	Bar-le-Duc	Oui	Non
			LPO François Bazin	Charleville-Mézières	Oui	N/A

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue

BTS Cybersécurité, informatique et réseaux, électronique	BTS	5	LPO la Briquerie	Thionville	Oui	N/A
			LPO Les Lombards	Troyes	Oui	N/A
			LPO Mangin	Sarrebourg	Oui	N/A
			LPO Pierre Mendès France	Epinal	Oui	N/A
			LPO Louis Armand	Mulhouse	Oui	N/A
			LPO François le 1er	Vitry le François	Oui	N/A
			LPO Georges Brière	Reims	Oui	N/A
			LPO Heinrich Nessel	Haguenau	Oui	N/A
Gestionnaire de la sécurité des données, des systèmes et des réseaux	Certificat professionnel	N/A	CNAM Grand Est	Oui	Oui	Oui
Analyste en cybersécurité	Certificat professionnel	N/A	CNAM Grand Est	Oui	Oui	Oui
Préventeur en cybersécurité des systèmes d'information	Certificat professionnel	N/A	Metz numeric school (ancien IFAtech)	Non	Oui	Oui
Diplome d'université sécurité intérieure Option cybersécurité	Diplôme universitaire	N/A	Université de Lorraine	Oui	Oui	Oui

- Cartographie des **formations « socles » de plus de 200h avec des modules en cybersécurité** en Région Grand Est

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Ingénieur informatique parcours informatique, réseaux, systèmes et multimédias	Ingénieur	7	CNAM Grand Est	Strasbourg Mulhouse	Oui	Oui
Ingénieur Informatique parcours Architecture et ingénierie des systèmes et des logiciels	Ingénieur	7	CNAM Grand Est	Strasbourg Mulhouse / Reims	Oui	Oui
Ingénieur informatique parcours informatique, modélisation et optimisation	Ingénieur	7	CNAM Grand Est	Strasbourg Mulhouse	Oui	Oui
Ingénieur informatique parcours informatique système d'information	Ingénieur	7	CNAM Grand Est	Strasbourg Mulhouse	Oui	Oui
Ingénieur	Ingénieur	7	EPITA	Strasbourg	Oui	N/A
Ingénieur du numérique	Ingénieur	7	ESAIP la Salle	Reims	Oui	N/A
Management en Ingénierie Informatique	Master	7	Metz numeric school (ancien IFAtech)	Metz	Oui	Oui
Master Méthodes informatiques appliquées à la gestion des entreprises (MIAGE)	Master	7	Université de Haute Alsace	Mulhouse	Oui	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Master informatique et mobilité	Master	7	Université de Haute Alsace	Mulhouse	Oui	Oui
Ingénieur ENSEM - spécialité Systèmes numériques	Ingénieur	7	Université de Lorraine	Nancy	Oui	Oui

Ingénieur Polytech Informatique, Automatique, Robotique, Réseaux Parcours Systèmes d'Information et Réseaux (SIR) et parcours systèmes intelligents et automatisation	Ingénieur	7	Université de Lorraine	Nancy	Oui	Oui
Master Informatique, Parcours type Génie Informatique et Interaction Humain-Machine (G2IHM)	Master	7	Université de Lorraine	Metz	Oui	Oui
Master Veille stratégique et organisation des connaissances	Master	7	Université de Lorraine	Nancy	Oui	Oui
Master Mention Informatique - parcours Science et ingénierie du logiciel	Master	7	Université de Strasbourg	Strasbourg	Oui	Oui
Master droit parcours droit de l'économie du numérique	Master	7	Université de Strasbourg	Strasbourg	Oui	Oui
Master Droit parcours cyberjustice	Master	7	Université de Strasbourg	Strasbourg	Oui	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Master Mention Informatique - parcours Science et ingénierie des réseaux, de l'Internet et des systèmes (SIRIS)	Master	7	Université de Strasbourg	Strasbourg	Oui	Oui
Master Mention Informatique - parcours Science des données et systèmes complexes	Master	7	Université de Strasbourg	Strasbourg	Oui	Oui
Master 2 Mention Informatique - parcours Gestion de projets informatiques	Master	7	Université de Strasbourg	Strasbourg	Non	Oui
Ingénieur spécialisé informatique et réseaux **Option réseaux et internet des objets**	Ingénieur	7	Université de Strasbourg	Strasbourg	Oui	Non
Ingénieur Parcours réseaux et télécommunication	Ingénieur	7	Université de technologie de Troyes	Troyes	Oui	Oui
Administrateur réseau NETOPS	Titre professionnel	6	AFPA	Frouard	Non	Oui
Administrateur systèmes et réseaux	Bachelor	6	CESI	Nancy / Strasbourg / Reims	Oui	Oui
Sciences, technologies, santé mention Informatique	Licence	6	CNAM Grand Est	Bar-le-Duc / Epinal / Strasbourg	Oui	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Concepteur en architecture informatique parcours réseaux et systèmes	Titre professionnel	6	CNAM Grand Est	Strasbourg / Mulhouse	Oui	Oui
Concepteur en architecture informatique parcours système d'information	Titre professionnel	6	CNAM Grand Est	Strasbourg / Mulhouse	Oui	Oui
Administrateur Systèmes et Réseaux	Titre professionnel	6	Mewo	Metz	Oui	Oui
BUT informatique	Bachelor	6	Université de Lorraine	Metz	Oui	Oui
			Université de Lorraine	Saint-Dié-des-Vosges	Oui	Oui
			Université de Lorraine	Nancy	Oui	Oui
BUT génie électrique et informatique industriel	Bachelor	6	Université de Lorraine	Nancy	Oui	Oui
			Université de Lorraine	Saint-Dié-des-Vosges	Oui	Oui
			Université de Lorraine	Longwy	Oui	Oui
			Université de Haute Alsace	Mulhouse	Oui	Oui
			Université de Strasbourg	Haguenau	Oui	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Licence informatique parcours informatique	Licence	6	Université de Reims	Reims	Oui	Oui
Licence pro mention métiers de l'informatique : applications web Parcours-type Applications mobiles et internet des objets	Licence professionnelle	6	Université de Lorraine	Saint-Dié-des-Vosges	Oui	Oui
Licence professionnelle métiers du numérique : conception, rédaction et réalisation web	Licence professionnelle	6	Université de Strasbourg	Strasbourg	Oui	Oui
Licence professionnelle systèmes automatisés réseaux et informatique industrielle Parcours industrie du futur	Licence professionnelle	6	Université de Strasbourg	Haguenau	Oui	Oui
Licence professionnelle systèmes automatisés réseaux et informatique industrielle Parcours intégration robotique industrielle	Licence professionnelle	6	Université de Strasbourg	Haguenau	Oui	Oui
Licence Professionnelle Enquêteur Technologies Numériques (N'TECH)	Licence professionnelle	6	Université de technologie de Troyes	Troyes	Non	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
Technicien supérieur systèmes et réseaux	Titre Professionnel	5	AFPA	Frouard / Strasbourg	Non	Oui
			CESI	Nancy / Strasbourg / Châlons en Champagne	Oui	Oui
			Mewo	Metz	Oui	Oui
			ICAM Strasbourg	Strasbourg	Non	Oui
			Metz numeric school (ancien IFAtech)	Metz	Non	Oui
			Webforce 3	Strasbourg	Oui	Oui
Gestionnaire en maintenance et support informatique	Titre professionnel	5	CESI	Strasbourg / Reims	Oui	Oui
Développeur web et web mobile	Titre professionnel	5	GRETA Lorraine Nord	Metz	Non	Oui
BTS Services numériques	BTS	5	LPO Condorcet	Schoeneck	Oui	N/A
			LPO Couffignal	Strasbourg	Oui	N/A
			LPO Jean Zay	Jarny	Oui	N/A
			Pôle formation UIMM	Thionville / Thaon-les-Vosges / Vitry-le-François	Oui	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
BTS services informatiques aux organisations Option : Solutions d'Infrastructures, Systèmes et Réseaux (SISR) Option : Solutions Logicielles et Applications Métier (SLAM)	BTS	5	IFIDE / Sup Formation	N/A	Oui	Oui
			LEGT Gaspard Monge	Charleville Mézières	Oui	N/A
			GRETA Lorraine Nord	Metz / Eckbolsheim / Troyes	Non	Oui
			CCI Alsace	Strasbourg / Mulhouse	Oui	N/A
			LEGT E. Bouchardon	Chaumont	Oui	N/A
			LEGT Franklin Roosevelt	Reims	Oui	N/A
			LEGT Frederic Chopin	Nancy	Oui	N/A
			LEGT Raymond Poincaré	Bar-le-Duc	Oui	Non
			LPO Blaise Pascal	Colmar	Oui	N/A
			LPO Camille See	Colmar	Oui	N/A
			LPO rené Cassin	Strasbourg	Oui	N/A
			LPO Robert Schuman	Metz	Oui	N/A
			Mewo	Metz	Oui	Oui
			Pôle formation UIMM	Thionville	Oui	Oui

Intitulé de la formation	Diplôme / qualification	Niveau visé	Organisme	Ville	Formation initiale	Formation continue
BTS services informatiques aux organisations Option : Solutions d'Infrastructures, Systèmes et Réseaux (SISR)	BTS	5	CFA la salle	Reims	Oui	Oui
Technicien d'assistance informatique	Titre Professionnel	4	Mewo	Metz	Non	Oui
			Webforce 3	Strasbourg	Oui	Oui
Administrateur système DEVOPS	Certificat professionnel	N/A	AFPA	Frouard	Non	Oui
Diplôme d'Université Coordinateur de Cellule de Crise	Diplôme universitaire	N/A	Université de technologie de Troyes	Troyes	Non	Oui

- Cartographie des **formations « cybersécurité » de moins de 200h** en Région Grand Est

Intitulé de la formation	Diplôme / qualification	Organisme	Durée de la formation
Référent cybersécurité en TPE/PME	Attestation de formation	CCI Alsace	35 h
Piloter la mise en conformité des traitements et de protection des données personnelles en TPE/PME	Attestation de formation	CCI Alsace	28 h
Sécurité informatique : mettre en place les bases de la sécurité informatique	Attestation de formation	CCI Alsace	14 h
Piloter et garantir la qualité du projet informatique	Attestation de formation	CESI	78 h
Maintenir et sécuriser les infrastructures informatiques	Attestation de formation	CESI	60 h
Technicien de maintenance micro-réseaux et internet spécialisation cybersécurité des PME	Certificat professionnel	CNAM Grand Est	N/A
Protection contre les risques	Attestation de formation	Digital TPE +	10 h
Cybersécurité	Attestation de formation	Louis pro formations	40 h
Analyste en cybersécurité	Certificat professionnel	M2i Formation	140 h
Parcours introductif à la cybersécurité	Certificat professionnel	M2i Formation	70 h

Intitulé de la formation	Diplôme / qualification	Organisme	Durée de la formation
Parcours analyste SOC	Certificat professionnel	M2i Formation	56 h
Lead Auditor - ISO 27001:2022	Certificat professionnel	M2i Formation	35 h
Techniques de hacking niveau 1	Attestation de formation	M2i Formation	35 h
Techniques de hacking niveau 2	Attestation de formation	M2i Formation	35 h
Splunk - Gestion des opérations de cybersécurité	Attestation de formation	M2i Formation	35 h
Analyste SOC	Attestation de formation	M2i Formation	35 h
Investigation numérique	Attestation de formation	M2i Formation	35 h
Préparation à la certification CCSP	Attestation de formation	M2i Formation	35 h
Rôles et missions du RSSI	Attestation de formation	M2i Formation	35 h
Lead Auditor - ISO 22301	Attestation de formation	M2i Formation	35 h
Fortinet NSE 4 - Fortigate security et infrastructures	Attestation de formation	M2i Formation	35 h
Lead Implementer - ISO 27001:2022	Certificat professionnel	M2i Formation	35 h

Intitulé de la formation	Diplôme / qualification	Organisme	Durée de la formation
RGPD / GDPR - DPO	Certificat professionnel	M2i Formation	35 h
Lead Cybersecurity Manager - ISO 27032	Certificat professionnel	M2i Formation	35 h
Risk manager - ISO 27005	Certificat professionnel	M2i Formation	21 h
Gestion des identités et sécurité des accès	Attestation de formation	M2i Formation	28 h
Stormshield Network - troubleshooting and support	Attestation de formation	M2i Formation	28 h
Cybersécurité des systèmes industriels	Attestation de formation	M2i Formation	21 h
Méthodologie de veille pour la cybersécurité	Attestation de formation	M2i Formation	21 h
Stormshield Network - administrateur	Attestation de formation	M2i Formation	21 h
Splunk - les essentiels	Attestation de formation	M2i Formation	21 h
Sécurité de l'active directory	Attestation de formation	M2i Formation	21 h
Check point - certified security administrator R81.x	Attestation de formation	M2i Formation	21 h
Check point - certified security expert R81.x	Attestation de formation	M2i Formation	21 h

Intitulé de la formation	Diplôme / qualification	Organisme	Durée de la formation
Stormshield Network - expert	Attestation de formation	M2i Formation	21 h
Méthode EBIOS RM 20128	Certificat professionnel	M2i Formation	18 h
EGERIE Risk Manager v4 avec EBIOS RM	Certificat professionnel	M2i Formation	14 h
Cours préparatoire aux techniques de hacking	Attestation de formation	M2i Formation	14 h
EGERIE Risk manager avec ISO 27005	Attestation de formation	M2i Formation	14 h
Sécurité des serveurs de noms (DNS)	Attestation de formation	M2i Formation	14 h
Stormshield Manager center - expert	Attestation de formation	M2i Formation	14 h
RGPD et cybersécurité	Certificat professionnel	M2i Formation	7 h
Introduction à la sécurité des systèmes industriels	Attestation de formation	M2i Formation	7 h
Cybersécurité - niveau 1 - sensibilisation	Attestation de formation	RGPD Academy	7 h
Participer à la démarche de conformité RGPD en tant que relais interne	Attestation de formation	RGPD Academy	7 h
Maîtriser le cadre légal du transfert de données personnelles	Attestation de formation	RGPD Academy	7 h

Intitulé de la formation	Diplôme / qualification	Organisme	Durée de la formation
Privacy by design, intégrer la protection de la vie privée dès sa conception	Attestation de formation	RGPD Academy	7 h
Exercer le métier de DPO – préparation à la certification - 2 modules	Attestation de formation	RGPD Academy	7 h
Analyse d'impact sur la vie privée / privacy impact assessment	Attestation de formation	RGPD Academy	7 h
Cybersécurité, campagne de sensibilisation à l'hameçonnage	Attestation de formation	RGPD Academy	7 h
Initiation aux fondamentaux du RGPD	Attestation de formation	RGPD Academy	7 h
Dossier médical partagé : anticiper ses impacts, accompagner sa mise en place	Attestation de formation	RGPD Academy	7 h
L'atelier du chargé de conformité secteur santé	Attestation de formation	RGPD Academy	7 h
Les bases du RGPD – niveau 1 – sensibilisation – secteur santé	Attestation de formation	RGPD Academy	7 h
Les bases du RGPD – Niveau 2 – approfondissement et mise en application – secteur Santé	Attestation de formation	RGPD Academy	7 h
Maîtriser le cadre légal de la collecte et de l'utilisation des données du secteur médico social	Attestation de formation	RGPD Academy	7 h
Dispositifs médicaux, maîtriser les impacts CNIL dès la conception du produit	Attestation de formation	RGPD Academy	7 h

Intitulé de la formation	Diplôme / qualification	Organisme	Durée de la formation
Les bases du RGPD – niveau 1- sensibilisation – secteur collectivités	Attestation de formation	RGPD Academy	7 h
Les bases du RGPD – niveau 2 – approfondissement et mise en application – secteur collectivités	Attestation de formation	RGPD Academy	7 h
Cybersécurité : formation sur mesure tout niveau	Attestation de formation	Straformation	N/A
Analyse avancée de la mémoire RAM	Attestation de formation	Université de Lorraine	30 h
Attaque par les IOTs	Attestation de formation	Université de Lorraine	12 h
Attaque, défense et IA	Attestation de formation	Université de Lorraine	12 h
Audit de sécurité interne – Outillage et test d'intrusion - LINUX	Attestation de formation	Université de Lorraine	24 h
Audit de sécurité interne – Outillage et test d'intrusion - WINDOWS	Attestation de formation	Université de Lorraine	12 h
Code malveillant et analyse mémoire avec Volatility	Attestation de formation	Université de Lorraine	24 h
Fuite de données en entreprise, s'en prémunir et réagir	Attestation de formation	Université de Lorraine	12 h
Innovation, digitalisation de la chaîne de valeur, transition numérique et cyber ? – Module avancé	Attestation de formation	Université de Lorraine	6 h

Intitulé de la formation	Diplôme / qualification	Organisme	Durée de la formation
Innovation, transitions numériques, digitalisation de la chaîne de valeur et cyber ?	Attestation de formation	Université de Lorraine	6 h
Intégration de processus de sécurité numérique au sein d'une TPE/PME	Attestation de formation	Université de Lorraine	6 h
Objets connectés orientés sécurité des systèmes cyber-physique	Attestation de formation	Université de Lorraine	12 h
Outils et techniques d'analyse de code malveillant	Attestation de formation	Université de Lorraine	18 h
PowerShell niveau 2, perfectionnement	Attestation de formation	Université de Lorraine	18 h
Programmation Python pour le hackeur	Attestation de formation	Université de Lorraine	12 h
Renseignement en Sources Ouvertes (OSINT) et Cybersécurité	Attestation de formation	Université de Lorraine	6 h
Sécurité des objets connectés	Attestation de formation	Université de Lorraine	12 h
Sensibilisation à la cybersécurité (dirigeants et cadres)	Attestation de formation	Université de Lorraine	6 h
Sensibilisation à la gestion des failles	Attestation de formation	Université de Lorraine	6 h
Sensibilisation à la protection des données à caractère personnel	Attestation de formation	Université de Lorraine	6 h

Intitulé de la formation	Diplôme / qualification	Organisme	Durée de la formation
Écriture de scripts Shell sous le système d'exploitation LINUX	Attestation de formation	Université de Lorraine	18 h
Écriture de scripts Shell sous le système d'exploitation LINUX dans le cadre d'élévation de privilèges	Attestation de formation	Université de Lorraine	18 h
Maintenance et dépannage des serveurs sous le système d'exploitation LINUX	Attestation de formation	Université de Lorraine	24 h
PowerShell niveau 1, automatiser l'administration Windows	Attestation de formation	Université de Lorraine	18 h
Procédure suite à une détection d'attaque Ransomware (isolation réseau, détection des partages, communication, restauration de backup…)	Attestation de formation	Université de Lorraine	12 h
Sûreté de fonctionnement et cybersécurité	Attestation de formation	Université de Lorraine	18 h
Transition numérique, digitalisation, cybersécurité	Attestation de formation	Université de Lorraine	30 h
VMware vSphere 6.7, optimisation et administration avancée	Attestation de formation	Université de Lorraine	30 h
Intégrer le risque cyber dans son activité	Certificat professionnel	Université de technologie de Troyes	45 h

GOUVERNEMENT

Liberté
Égalité
Fraternité

Contact

Ekaterina MINTCHEVA
Coordinatrice Emploi et Compétences
de la Maison de l'Emploi du Grand Nancy
Tél. 03.83.22.24.00
88 Avenue du XX^{e} Corps BP 90657 – 54063 NANCY CEDEX