Cité de l'Economie et des Métiers de Demain

ÉTUDE PROSPECTIVE

MÉTIERS DE DEMAIN POUR LA CYBERSÉCURITÉ EN OCCITANIE

Décembre 2021

Réalisé avec :

Avec l'appui du cabinet

L'étude prospective « Métiers de demain pour la Cybersécurité » menée de septembre à décembre 2021 par la Cité de l'Economie et des Métiers de Demain et la Région Occitanie, en partenariat avec Cyber'Occ / ADOCC, présente trois phases :

1 - L'état des lieux de la filière et des tendances de fond qui impactent et impacteront la filière
2 - Une cartographie des métiers pour la filière
3 - Un descriptif des offres de formation et des passerelles

1.
ÉTAT DES LIEUX ET DES TENDANCES DE LA FILIÈRE

Pour la réalisation de cette phase, les moyens suivants ont été mobilisés :
• Réalisation d'entretiens avec des experts nationaux ayant une vision transverse et globale de la cybersécurité
• Analyse de documents de références

1.1.
PREMIER ÉTAT DES LIEUX DE LA FILIÈRE CYBERSÉCURITÉ

> Au niveau national

Dans un contexte où l'espace numérique mondial peine à se réguler et où des pans entiers de la société se digitalisent, nous observons un nombre croissant d'attaques cyber sur tous les acteurs.
De ce fait, les besoins en cybersécurité ne cessent d'augmenter. Entre 2014 et 2020, cela s'est traduit par plus du doublement du chiffre d'affaires des acteurs cybers français.

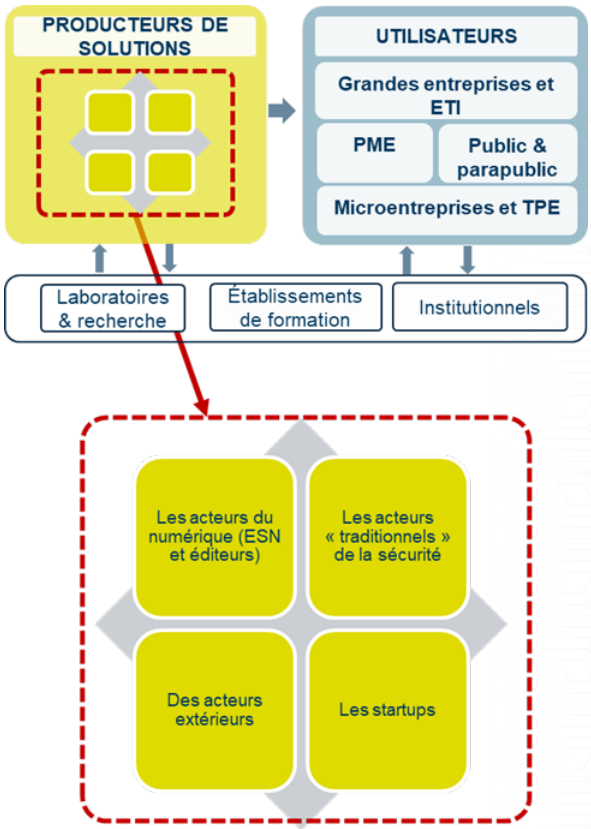
Cette tendance devrait logiquement se poursuivre, avec notamment un plan gouvernemental ambitieux de 1 milliard € à horizon 2025, qui a pour ambition de faire passer les effectifs territoriaux **de 37 000 à 75 000 ETP.**

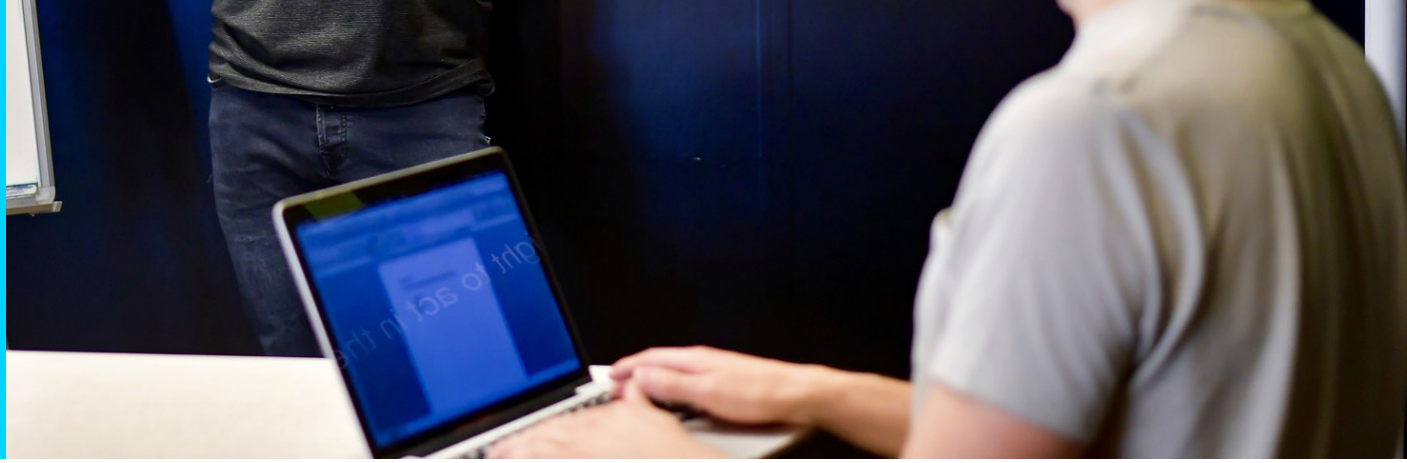
La filière cybersécurité comprend :

1. Les « producteurs de solutions », qui regroupent les prestataires et sociétés spécialisées dans les prestations ou dans les produits de cybersécurité

2. Les « utilisateurs », qui regroupent tous les acteurs utilisant des services et/ou produits de cybersécurité

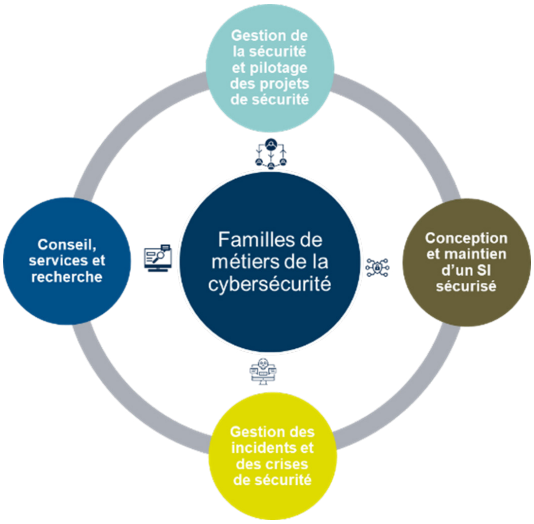
3. Et tous les acteurs connexes de l'écosystème comme les organismes de formation ou encore les acteurs institutionnels





Les métiers qui composent ce secteur peuvent être regroupés au sein de 4 familles. Bien que différents dans les compétences et savoir-faire requis, tous ces métiers partagent des similitudes :

- Un niveau de qualification élevé, BAC+5 est la norme
- Une concentration majeure de ressources en Île-de-France
- Des profils jeunes, de moins de 10 ans d'expérience
- Des tensions structurelles de recrutement



> Une tendance forte à l'externalisation

On observe certaines pratiques clés, comme la tendance forte à l'externalisation pour les acteurs privés à l'exception de certains secteurs (ex. : télécoms, énergie, défense / industrie navale) ayant la volonté de garder une partie en interne. Le secteur public a un modèle plus hybride, avec notamment l'ANSSI qui apporte son expertise.

Focus Occitanie

Avec une présence majeure de secteurs comme la santé, l'aéronautique ou encore les équipements électriques & électroniques, l'Occitanie est fortement concernée par les problématiques cyber. Ceci a conduit la Région à définir la cybersécurité comme l'un des 8 domaines de spécialisation intelligente de la Stratégie Régionale d'Innovation (SRI).

Le secteur numérique régional constitue le 3ème de France en termes d'emplois.

La filière régionale de cybersécurité regroupe aujourd'hui un écosystème dense et dynamique composé d'entreprises et d'acteurs à tous les niveaux (producteurs de solutions, utilisateurs, recherche…) et de leaders nationaux (Apsys, Orange Cyber Défense, Thalès …)

Forces

- Un **écosystème régional dense,** avec des acteurs à tous les niveaux, mais qui doit encore se renforcer pour prendre une position forte au niveau national et européen
- Des **champions du cyber sur le territoire régional** avec des leaders de l'industrie comme Airbus Cyber Defense...
- Une **forte collaboration entre les différents acteurs et une communauté qui émerge, fédérée par Cyber'Occ**

Faiblesses

- Un **éloignement de l'Ile de France,** qui reste le principal bassin cyber avec plus de la moitié des effectifs
- **Peu (ou pas ?) d'acteurs de taille intermédiaire au rayonnement international**

1.2.
META-TENDANCES ET IMPACTS SUR LA FILIÈRE RÉGIONALE

Dans un exercice d'anticipation des évolutions de la filière, des grandes tendances qui impactent, ou impacteront, fortement la filière de cybersécurité ont été identifiées dans le cadre de l'étude. Celles-ci se catégorisent autour de 5 axes :

Évolutions de marché / économiques :

• Une intensification de la concurrence internationale avec la poursuite du développement des leaders de la Tech qui profitent de leur position dominante exacerbée par transition vers le cloud et l'intensification de la concurrence cyber au sein des grandes puissances mondiales
• Une **demande qui s'intensifie** face à la recrudescence des attaques et l'exposition aux risques des entreprises
• Une démultiplication du recours aux services SAAS et cloud qui augmente les risques avec l'interconnexion des réseaux et la démultiplication des points à contrôler qui demande la création de solutions innovantes (IA, machine learning…)

Évolutions réglementaires

• Un durcissement des réglementations à l'échelle mondiale (ex : Directive NIS)
• Des exigences accrues des autorités européennes et françaises en matière de sécurité des réseaux (SRI 2), des données (RGPD) et validation de la sécurité et de la fiabilité des outils cyber
• Un renforcement de la sécurisation des acteurs stratégiques nationaux, avec la mise en place récente des OSE (Opérateur de Services Essentiels), en complément des OIV (Opérateurs d'Importance Vitale).
• Un développement de normes et règles de conformité sectorielles. Logique du maillon le plus faible de la chaîne (Exemple : PCI-DSS dans le secteur bancaire)

Évolutions sociales / sociétales & organisationnelles

• Une prise de conscience générale du risque cyber qui le fait passer d'un sujet étiqueté DSI à un sujet transverse à toute l'organisation
• Une accélération et pérennisation du télétravail, qui augmente le risque cyber en démultipliant exponentiellement les connexions externes. Ceci pousse les entreprises à faire des compromis sur la cybersécurité pour maintenir l'activité
• La priorité opérationnelle des entreprises qui prend le pas. Ceci pousse pour des mesures cyber qui soient transparentes pour les utilisateurs, sous peine d'entraîner un non-respect ou un contournement

Évolutions technologiques

• Une digitalisation des entreprises et en particulier des usines, qui intègrent de nombreux appareils connectés IoT et migrent vers des solutions « cloud »
• Une émergence de technologies permettant la mise en place de stratégies plus intelligentes, mais qui fera aussi évoluer les menaces (IA, Machine Learning, Cryptographie quantique ...)
• Un décalage entre les « faiseurs de solutions » relativement avancés et proposant des solutions technologiques de haut niveau, et les « utilisateurs », qui manquent de compétences et de personnes en capacité d'exploiter pleinement les outils

Évolutions politiques

• Des plans structurants au niveau national et européen
• Un développement d'acteurs centraux pour le développement la filière
• Une volonté gouvernementale marquée pour soutenir l'essor de spécialistes français (contrat de filière « industries de sécurité »)
• Le renforcement des entités gouvernementales cyber (ex. ANSSI - Agence nationale de la sécurité des systèmes d'information, DRSD - Direction du renseignement et de la sécurité de la Défense) et d'une labellisation de partenaires externes de confiance pour créer un écosystème fort

1.3. QUESTIONS CLÉS POUR L'ÉLABORATION DES SCÉNARII PROSPECTIFS

Cette première phase a fait émerger un certain nombre de questions stratégiques qui détermineront en grande partie l'évolution du secteur.

Questions stratégiques :

• À quelle vitesse et à quel degré les entreprises, notamment les TPE/PME, vont-elles se digitaliser ?
• Quel niveau d'investissement des entreprises utilisatrices dans la cybersécurité ?
• Comment les règlementations et la mise en conformité vont-elles évoluer et impac er ce secteur ?
• A quel point la sécurisation des solutions logiciels et des environnements (security/ privacy by design) va-t-elle se renforcer ?

Opportunités

• Des **projets nationaux ambitieux** qui soutiennent le développement et le renforcement de la filière cybersécurité
• Une **prise de conscience forte des entreprises** du risque cyber et du besoin fort de s'équiper et de se former
• Des **besoins de personnel** formés à tous les niveaux, du BTS au doctorat
• Une **volonté affichée de souveraineté** au niveau national et européen
• Des **développements technologiques** qui vont fortement impacter la cybersécurté de demain

Menaces

• Une **bataille pour les ressources au niveau national voire international**, exacerbée par l'attrait pour le télétravail, et une pression consécutive sur les salaires
• La **démultiplication des risques** avec l'essor des nouveaux outils et la digitalisation des entreprises

2.
CARTOGRAPHIE DES MÉTIERS DE DEMAIN

2.1.
L'ACTUEL

Pour la réalisation de la cartographie des métiers et pour l'analyse de l'offre de formation, 4 sources de données ont été croisées :

- Réalisation d'une vingtaine d'entretiens auprès d'entreprises et d'acteurs de l'écosystème
- Mise en place d'un questionnaire en ligne, adressé aux entreprises (51 répondants)
- Exploitation d'une base de données sur les offres d'emplois issue de l'outil Textkernel
- Analyse documentaire

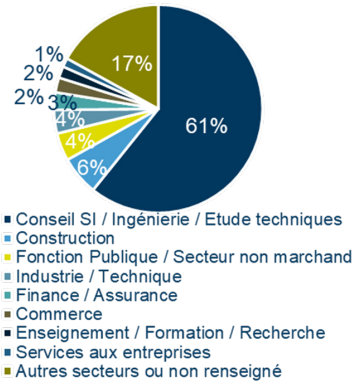
2.1.1
PANORAMA RÉGIONAL

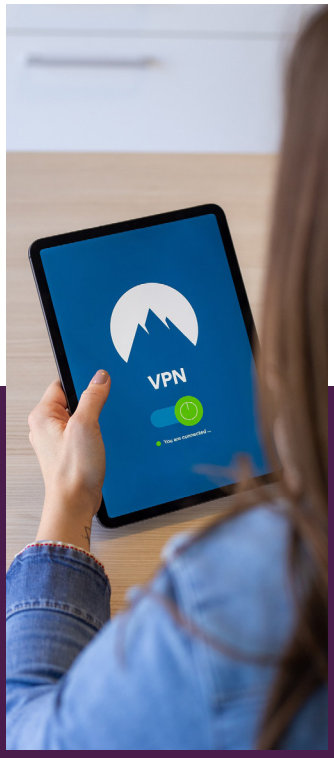
En Occitanie, bien que près de **500 entreprises** aient posté des offres de recrutement pour des postes de cybersécurité en 2019 et 2025, les besoins du secteur se regroupent autour d'un noyau dur d'environ **85 acteurs**.

En effet, l'analyse du nombre d'offres sur 2 ans fait ressortir 85 acteurs avec plus de 5 offres diffusées et fait surtout ressortir des besoins majeurs autour de quelques grands acteurs comme Thales, Apsys Airbus, Sopra Steria ou encore Capgemini, pour ne citer qu'eux. (top 10 des entreprises regroupent 39% des besoins).

REPARTITION DES OFFRES D'EMPLOIS PAR SECTEUR

Source : Textkernel, retraitement Katalyse





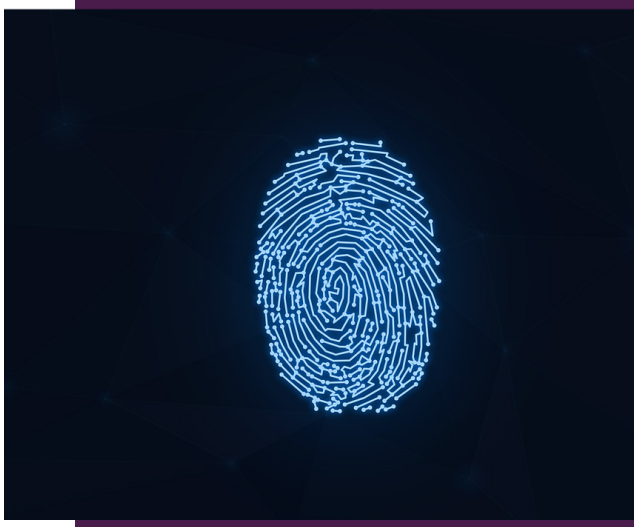
Ces acteurs sont principalement des sociétés de conseil, d'ingénierie et d'études techniques (61% des offres publiées). Ceci est cohérent avec la tendance nationale à l'externalisation de la cybersécurité et donc à une structuration de la filière autour de prestataires spécialisés.

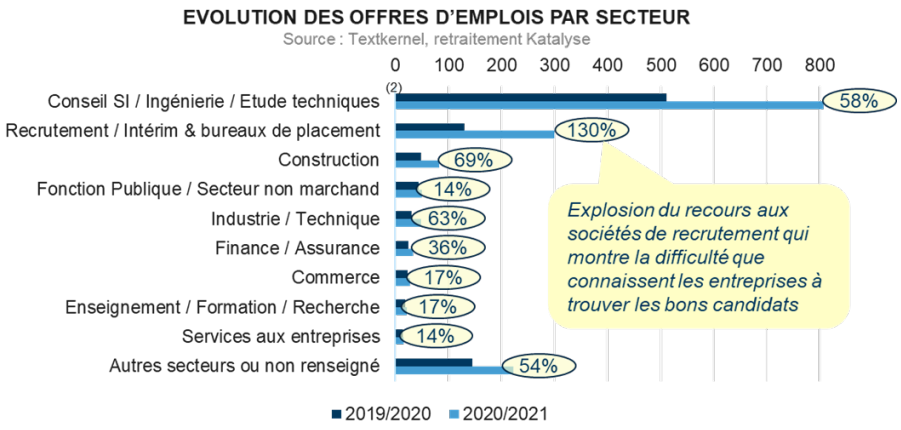
Au niveau de la répartition géographique, **71% des offres d'emploi diffusées recherchent pour des postes au niveau de l'agglomération toulousaine, suivi de 13% autour de Montpellier. Les autres zones qui ressortent sont Nîmes (5%) et Perpignan (3%).**

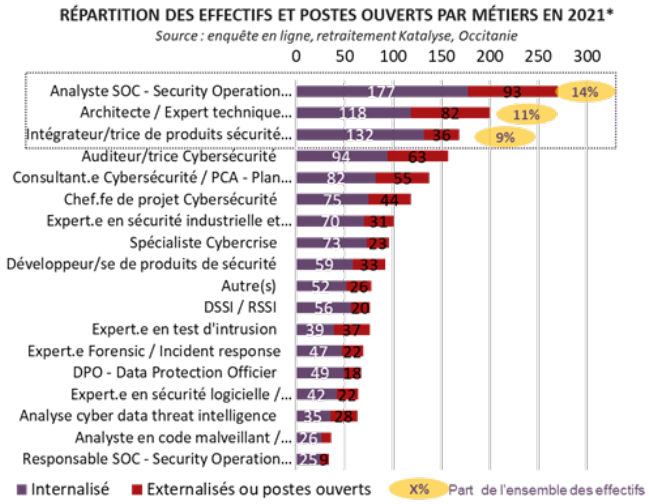
2.1.2 RÉPARTITION ET ÉVOLUTION DES BESOINS

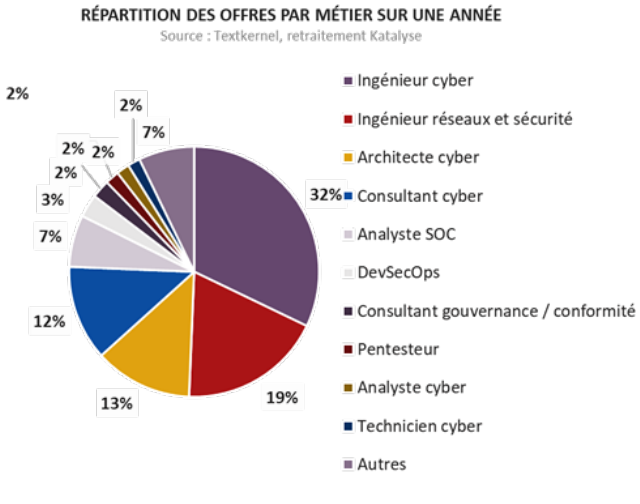
Sur les deux dernières années (12/2019 à 12/2020 et 12/2020 à 12/2021) les analyses ont confirmé la macro-tendance de croissance de la filière. Passant d**e 989 à 1609 offres publiées sur la région**, c'est in fine une croissance de **+63% d'une année sur l'autre**, chiffre révélateur de l'expansion des besoins qui touchent tous les acteurs, indifféremment des secteurs.

Cette rapide et forte croissance est un des facteurs expliquant les difficultés de recrutement des entreprises. Ceci s'est traduit en partie par un recours accru aux sociétés de recrutement spécialisées (+130%). Les entreprises acceptent de payer un surcoût pour trouver des ressources.









* Somme dés éléments supérieure au total des effectifs car certains ETP identifier sur plusieurs postes, intégrations des postes ouverts et certaines entreprises non répondantes à la question

Répartition par métier

Les analyses font ressortir une concentration d'effectifs autour de **métiers techniques** (Analystes SOC par exemple) dans les entreprises répondantes. L'analyse des offres d'emploi vient nuancer ces résultats sans pour autant les infirmer. En effet, un nombre important de recrutements sur des **métiers plus transverses**.

Ces profils transverses représentent une part importante des besoins des ESN, car ces dernières ont besoin de personnes ayant une vision large des fonctionnements des entreprises et des implications cyber qui en découlent.

Concernant le niveau de qualification, ce sont sans surprises des personnes ayant un **niveau bac +4/5 et une expérience moyenne située entre 3 et 5 ans** qui sont recherchées, tout comme au niveau national. Ces profils représentent environ 70% des offres analysées.

Difficultés de recrutement

Bien que tous les métiers puissent être considérés comme étant en tension, une situation d'ailleurs qui s'étend à une grande partie des métiers du numérique, nous observons néanmoins un besoin particulier remonté autour de **8 métiers identifiés** comme « très difficiles à recruter » (source : questionnaire).

Analyste SOC, Pentesteur, Développeur de produit de sécurité, Architecte cybersécurité, Formateur cyber, Expert Forensic, Analyse data threat intelligence

Estimation des effectifs régionaux

En croisant deux méthodes estimatives, l'une dite « ascendante » à partir d'offres d'emploi régionales, l'autre dite « descendante » à partir de grands chiffres nationaux, la taille des effectifs régionaux a été estimée à environ **3 000 ETP cyber** (pour plus de détail, se référer à l'étude détaillée).

Pour précision, cette estimation ne prend pas en compte les personnes avec une double casquette ou ayant un vernis cybersécurité dans leur métier. Nous nous sommes concentrés sur les effectifs de cybersécurité purs.

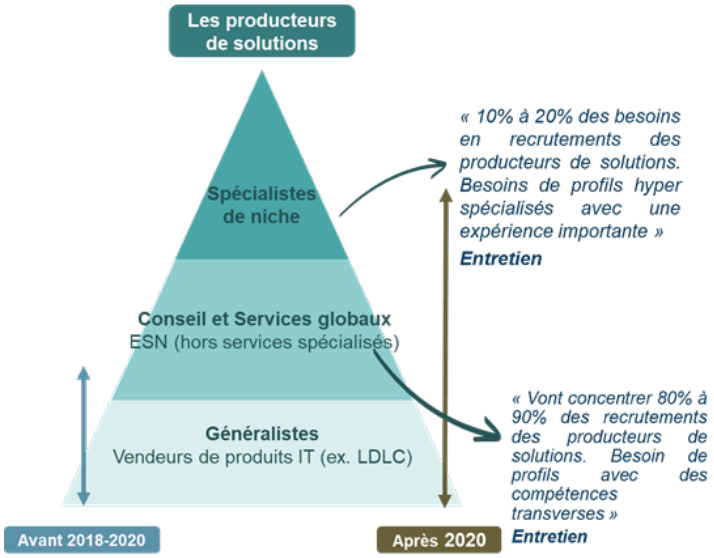
Cette estimation a été présentée lors du comité technique le 11/01/22 regroupant un panel d'acteurs régionaux. Ces éléments ont été validés et n'ont pas soulevé de débats.

2.2. DEMAIN

2.2.1. L'ÉVOLUTION DES BESOINS EN CYBERSÉCURITÉ

Historiquement, la cybersécurité passait par des solutions sur étagère génériques combinées à du matériel. Ce qui fait que les premiers acteurs étaient les acteurs « généralistes » qui vendent ces produits.

Avec l'augmentation des attaques, la complexification des systèmes et la dépendance accrue au digital, les entreprises ont pris conscience que les solutions utilisées jusque-là ne sont plus suffisantes.



La cybersécurité est maintenant un sujet central, pensé comme transverse au sein des organisations mais qui ne doit cependant pas entraver le fonctionnement et les opérations. De ce fait, les nouveaux systèmes de cybersécurités doivent être « sur-mesure », adaptés à chaque entité. Le recours à des prestataires de conseil et de services globaux va donc fortement croître. Plusieurs entreprises de ce secteur ont d'ailleurs évoqué ne pas pouvoir répondre à toutes les sollicitations par manque de personnel.

Les « spécialistes de niche » regroupent, comme le nom l'indique, des sociétés spécialisées sur des compétences pointues sollicitées dans des cas particuliers. Par exemple, les services de réponse à incident, qui ne sont sollicités qu'en cas d'attaque, sur une période courte.

2.2.2 CROISSANCE DES BESOINS

Avec un **doublement attendu des ressources à horizon 2025** (une fois de plus, croisement de deux méthodes pour estimer ce taux de croissance, cf. étude détaillée), tous les métiers de la cybersécurité vont croître.

Cette croissance devrait ainsi porter les effectifs **régionaux à environ 6 000 ETP cyber, soit un ajout net de 3 000 emplois.**

Notons que bien que les besoins par métier varient, aucun métier n'a été identifié comme en particulière évolution.

Le graphique suivant, issu de l'analyse des besoins en recrutement par métier des répondants à l'enquête, permet d'observer des taux de croissance très importants pour la plupart de ces métiers. Nous pouvons observer des prévisions de croissance majoritairement située entre +50% et +200%. Peu de secteurs en France font aujourd'hui face à de tels chiffres. Une fois de plus, ceci va venir augmenter les tensions de recrutement, il apparait critique d'accompagner les entreprises sur ce sujet.

2..2.3 LES GRANDS ENJEUX ET LEURS IMPACTS

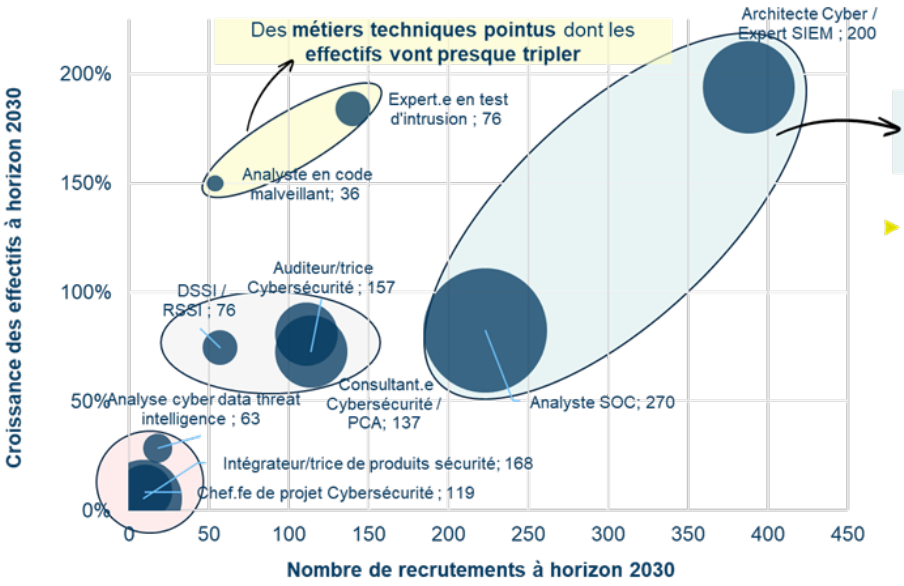
Plusieurs enjeux sont ressortis comme structurants pour l'évolution de la filière lors de la phase initiale de cette mission.
Afin de les classer, les entreprises (via le questionnaire) ont été invitées à se prononcer sur chaque enjeu, sur son importance, sur son impact pour la filière et sur son échéance (2022, 2025, 2030).
De ces réponses, 2 grands blocs d'enjeux ont émergé, regroupés autour de l'horizon temporel d'impact.

D'un côté les enjeux à court terme (principalement 2022) sont ressortis comme ceux avec le niveau d'impact et d'importance le plus élevé. En particulier, la « sécurisation des outils » et le « déblocage des budgets » sont ressortis loin devant.
Ceci vient confirmer deux tendances fortes précédemment citées. La première étant la prise en compte du besoin d'améliorer la cybersécurité et donc de débloquer des budgets dédiés. Il faut aussi que ces budgets soient pérennes dans le temps.
Le second point concerne la démultiplication des objets connectés, logiciels, applications… et la nécessité de les sécuriser pour limiter les risques des entreprises. Exemple : en 2018, un casino s'est fait pirater via le thermomètre d'un aquarium. Cet exemple qui porte à sourire démontre l'interconnexion de tous les systèmes et le besoin de sécurisation de tous les éléments qui composent ces systèmes.

La seconde catégorie d'enjeux regroupe ceux ayant un impact moyen ou fort mais à horizon 2025-2030. Cette catégorie regroupe la transition cloud, la régulation de l'espace cyber ou encore les évolutions technologiques.

PRÉVISION DE RECRUTEMENT EN 2030 DES PRINCIPAUX MÉTIERS ACTUELS POUR LE PANEL DE REPONDANTS

Source : enquête en ligne, retraitement Katalyse



Les principaux métiers actuels de l'échantillon le seront aussi demain

- Par ailleurs, 3 métiers additionnels seront en forte croissance et peu présents aujourd'hui (~50 recrutements prévus par poste par l'échantillon de répondants):
  - Développeur/se de produits de sécurité
  - Spécialiste cybercrise
  - Formateur.trice cybersécurité

3.
OFFRE DE FORMATION & PASSERELLES

3.1.
L'OFFRE DE FORMATION

3.2.1.
ÉTAT DES LIEUX

Concernant la formation initiale :
• **35 cycles** (numérique, électronique, droit, relations internationales) intègrent des modules de cybersécurité au sein de leurs cursus
• **20 formations** sont dédiées à la cybersécurité (dont 10 Bac +5, 8 Bac +4)

Concernant la formation continue, plus de **650 de formations** sont référencées sur le site « Me former en Occitanie ».
Ces formations offrent des débouchés sur les principaux métiers de chaque famille.

3.1.2
BILAN DE L'OFFRE DE FORMATION

Une offre de formation en Occitanie qui semble adaptée au niveau des parcours proposés, avec 71% des répondants de l'enquête en ligne s'estimant satisfaits de l'offre actuelle, mais qui pourrait cependant être améliorée sur plusieurs points :

Manque de formations pour les métiers de « gestion des incidents / crises de sécurité »
Plusieurs sociétés spécialisées ont évoqué une offre actuelle insuffisante, voir manquante sur certains métiers.

Formations parfois trop éloignées des besoins des entreprises
La proximité avec les entreprises et leur implication dans les programmes est un point crucial pour assurer la pertinence des formations. Plusieurs entreprises estiment en effet que les étudiants recrutés en sortie de parcours ne sont pas assez opérationnels, ce qui demande des efforts supplémentaires pour les faire monter rapidement en compétences.
Pour améliorer la pertinence des programmes, il est donc crucial que les entreprises et organismes de formation collaborent étroitement à toutes les phases des programmes, de l'ingénierie à l'enseignement (intervenants externes).

Pour les organismes de formation, une des difficultés majeures est l'identification et le recrutement de **formateurs** ayant les compétences métiers et le savoir-faire pédagogique. Certains programmes n'ont pas été ouverts face aux difficultés pour trouver des intervenants qualifiés.

Volumétrie d'étudiants formés insuffisante
Le nombre d'étudiants actuellement formés sur le territoire ne permet pas de répondre aux besoins du secteur, ce qui questionne sur le dimensionnement actuel et futur de l'offre.
Un point supplémentaire est ressorti sur le taux de remplissage des formations. Bien que cela diffère parmi les établissements, certains programmes ont des difficultés à remplir totalement les sessions (« au niveau national, les formations sont proches de 80%, trop loin des 100% alors que le marché a besoin de 150% » commentaire d'expert).
Ce déficit s'explique par :
• Une mauvaise image perçue, d'un secteur de « geek » réservé à certains profils
• Une très faible part de profils féminins, qui démontre le besoin de communication auprès de ce public
• Un niveau de prérequis très élevé, qui restreint l'accès aux programmes ou qui impose une mise à niveau parfois longue qui freine certaines candidates

L'alternance, un programme qui séduit
Des retours positifs sur les formations en alternances dites longues (1 semaine par mois en cours et 3 semaines en entreprise). Les entretiens ont confirmé la pertinence de ces programmes, notamment pour les entreprises qui y voient l'opportunité de former dès le début une ressource à leurs besoins souvent spécifiques. Pour 80% des alternances, cela débouche sur un recrutement en fin de parcours.

Une offre large et accessible de formation continue notamment grâce au distanciel
Des programmes qui proposent notamment des :
• Formations courtes portant sur la réglementation, normes (ex.: normes ISO)
• Formations certifiantes et cours en ligne à distance via des plateformes digitales payantes et gratuites (ex.: UDEMY, COURSERA)

3.2 LES OPPORTUNITÉS DE PASSERELLES MÉTIERS

3.2.1 PASSERELLES POUR LES MÉTIERS SI

Seules passerelles identifiées, les métiers SI fortement impactés par l'évolution des usages et des pratiques (cloudification, digitalisation, télétravail…)
• Ces métiers, comme les responsables réseaux, sont en pleine mutation. De « faiseurs », ils deviennent « gestionnaires de prestataire », ce qui entraîne parfois un sentiment de relégation
Autres métiers cités : ingénieur système / administrateur de base de données

• Ces profils possèdent cependant des connaissances très pertinentes pour la cybersécurité et sont donc à même de se reconvertir rapidement vers des métiers cyber.

Pour le reste, très peu de conversions vers des métiers cyber ont été identifiées, hors coloration de quelques profils
• Certaines professions, comme dans le milieu juridique, vont développer un savoir-faire et des connaissances spécifiques à la cybersécurité, mais ne vont pas basculer vers des métiers identifiés « cyber » pur
• Globalement, la technicité et la particularité des métiers de la cybersécurité rendent très complexe la conversion de profils hors SI.

4. PRÉCONISATIONS

La présentation de l'étude au comité technique a permis de challenger et compléter les recommandations. Celles-ci se classent de 4 axes :

1 - Renforcer l'appui au recrutement des entreprises

2 - Développer l'attractivité des métiers cyber

3 - Adapter l'offre de formation sur le territoire

4 - Autres recommandations

1 - Renforcer l'appui au recrutement des entreprises

- Identifier les entreprises qui rencontrent des difficultés de recrutement
- Proposer un accompagnement (cf dispositif contrat RH Région Occitanie, accompagnement RH AD'OCC)
- Identifier les écoles, salons régionaux, nationaux, et internationaux pertinents pour aider les entreprises d'Occitanie à « chasser » les talents
- Animer des sessions collectives sur le recrutement dans la Cyber, y compris avec la vision d'acteurs RH qui interviennent régulièrement sur le sujet (ex : Manpower Talents) et créer des occasions de JOB DATING en invitant des jeunes dans la Région et hors Région (job dating existant : la Melée)
- Rendre plus visibles l'offre de formation du territoire et les personnes formées pour les entreprises

2 - Développer l'attractivité des métiers cyber

Démystifier le secteur et présenter la pluralité des métiers accessibles

- Favoriser les stages de 3ème vers les entreprises cyber (cf dispositif Région stage)
- Favoriser la présence des publics féminins via des actions dédiées (ex Digifilles, actions La Melée…)
- Construire des présentations de parcours pour accéder aux métiers de la cybersécurité à l'attention des lycéens (ex dispositif « image métiers »…), notamment dédiées aux publics féminins
- Déployer des présentations des métiers de la cyber via les actions de promotion des métiers portées par la Région : dans les lycées, dans les salons, dans les Maisons de l'Orientation Région
- Mener des actions de design de métiers Cyber dans les lycées, à la CEMD, à l'attention des publics jeunesse de lycées et lors de hackatons etc…

3 - Adapter l'offre de formation sur le territoire

- Étoffer et structurer l'offre de formation sur le territoire, en comblant notamment les « trous dans la raquette » (métier de « gestion des incidents et crises de cybersécurité »)
- Promouvoir l'alternance sur le territoire
- Poursuivre le développement de formations sur tous les métiers de la cybersécurité
- Développer des formations de reconversion pour les métiers SI proches du cyber (Ingénieur réseau / admin BDD….)
- Poursuivre l'amélioration de la relation organismes de formation / entreprises
- Renforcer le développement de cycles courts qui donnent accès à des certifications Pour beaucoup, ces certifications sont plus importantes que le diplôme

4 - Autres recommandations

- Poursuivre la veille sur l'impact des nouvelles technologies sur les métiers « techniques »
- Poursuivre le développement d'une communauté cyber forte et active
- Aider la structuration des entreprises utilisatrices, notamment les TPE/PME, actuellement très désorganisés sur le sujet cyber

CITÉ
DE L'ÉCONOMIE
ET DES MÉTIERS
DE DEMAIN

CITÉ DE L'ÉCONOMIE ET DES MÉTIERS DE DEMAIN

Cité de l'Economie et des Métiers de Demain

ÉTUDE PROSPECTIVE

MÉTIERS DE DEMAIN POUR LA CYBERSÉCURITÉ EN OCCITANIE

AD'OCC Direction de la Communication - Février 2022 - www.agence-adocc.com