PÔLE D'EXCELLENCE CYBER

ANTICIPER LES COMPÉTENCES CYBER : CE QUE NOUS APPRENNENT LES ENQUÊTES !

Analyse internationale, européenne et territoriale au service du projet AMI CMA Cyberskills4all

Juin 2026

Région Bretagne

Ministère des Armées et des Anciens Combattants
Liberté
Égalité
Fraternité

Cet ouvrage a bénéficié d'une aide de l'Etat gérée par l'**Agence Nationale de la Recherche** au titre de **France 2030** portant la référence « ANR-23-CMAS-0026 ».

Le Pôle d'excellence cyber tient à remercier Iris Hourcade qui a contribué à la préparation et à l'élaboration de cet ouvrage, en tant que rédactrice.

Chargée de l'observatoire des compétences, coordinatrice des groupes de travail du Pôle d'excellence cyber.

SOMMAIRE

PRÉFACE

Le projet CyberSkills4All lauréat de l'AMI « Compétences et métiers d'avenir » du programme France 2030 (22M€ de budget dont 9M€ de subvention) fédère 10 acteurs en Bretagne : l'Université de Rennes (coordinateur), le Pôle d'Excellence Cyber (PEC), l'Université Bretagne Sud, France Université Numérique, l'ENSTA, Bretagne INP, Rennes School of Business, le CMQ Numérique, Photonique et Cybersécurité, le GIP FAR et Orange. Ils se sont unis pour répondre aux importants besoins de personnes formées en cyber, tant en formation initiale que continue.

CyberSkills4All a vocation à sensibiliser les lycéens et lycéennes, à créer de nouveaux parcours de formations, à former de futurs chercheurs et à produire de nouvelles ressources numériques. Il a aussi décidé de se doter d'un observatoire des compétences cyber pour éclairer les choix de création de nouvelles formations et de ressources par les partenaires. Et qui de mieux placé pour piloter cette action que le PEC, fort d'un réseau de plus de 131 membres académiques, régaliens, associatifs et entrepreneuriaux ?

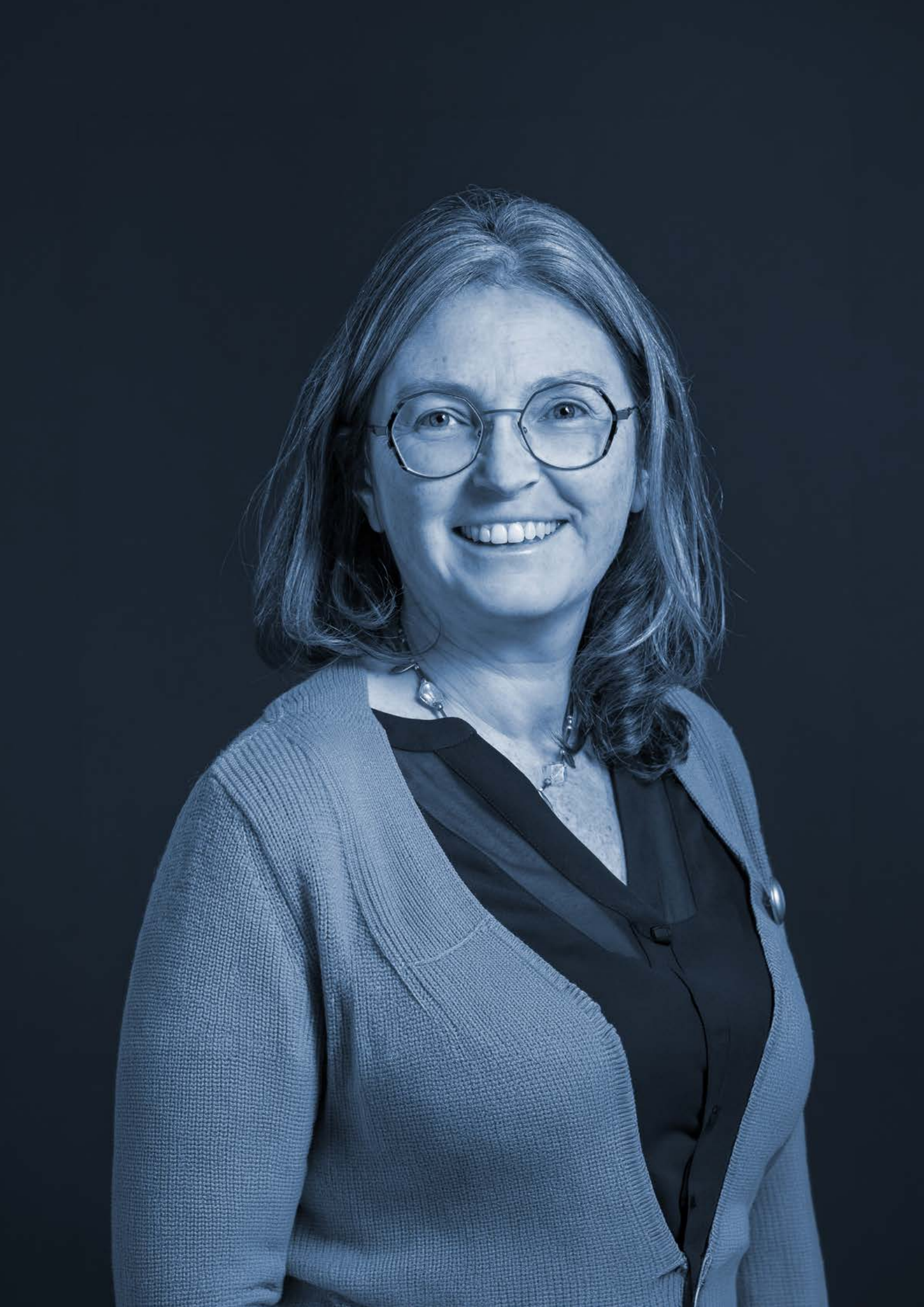
Cette première étude est nécessairement descriptive car il s'agit de faire un état les lieux des études les plus pertinentes sur les besoins en cyber. D'autres suivront. Elles seront tantôt quantitatives tantôt qualitatives, à partir d'entretiens auprès de recruteurs, de DRH et de dirigeants. L'objectif sera de se projeter au-delà du besoin immédiat pour anticiper les besoins futurs.

L'intérêt de la démarche est qu'elle s'inscrit dans la durée. L'évolution constante des technologies, des risques, des attaques, des réglementations, tout cela oblige à adopter une approche longitudinale pour se projeter, pour innover et pour toujours tenter de conserver un avantage concurrentiel. Nous le devons à nos concitoyens.

Je n'ai aucun doute que l'observatoire des compétences cyber saura alimenter la réflexion et les actions des partenaires de CyberSkills4All. Et je suis convaincu qu'il servira aussi à l'ensemble des acteurs français de la cyber.

Bonne lecture.

Jean Peeters
Directeur scientifique du projet Cyberskills4all
Professeur des universités
Université Bretagne Sud



INTRODUCTION

Face à la demande croissante de professionnels hautement qualifiés en cybersécurité, le projet CyberSkills4All, lauréat de l'Appel à Manifestation d'Intérêt « Compétences et Métiers d'Avenir » (AMI CMA) dans le cadre du plan France 2030, s'inscrit dans une ambition stratégique : contribuer activement à réduire le déficit de compétences qui fragilise aujourd'hui le secteur. À travers la création d'une offre diversifiée et structurée de formations, le projet entend répondre aux enjeux de compétences numériques de la France et participer à l'émergence d'une nouvelle génération d'experts en cybersécurité.

Afin d'adapter au mieux cette offre de formation aux besoins réels du marché — qu'il s'agisse des entreprises privées, des organisations publiques ou encore d'établissements d'enseignement supérieur amenés à faire évoluer leurs programmes — un Observatoire des emplois et des compétences a été créé. Sa mission consiste à identifier les tensions actuelles et à venir en matière de recrutement, ainsi que les compétences critiques ou rares. Les analyses produites ont vocation à nourrir les travaux du Comité d'Orientation Stratégique du consortium, notamment pour orienter et prioriser les thématiques des micro-certifications : des formations courtes, conçues par des experts en cybersécurité, à destination de professionnels du secteur et répondant à des besoins opérationnels ciblés.

Au-delà du périmètre strict du projet, les travaux de l'Observatoire ont également vocation à alimenter les réflexions de l'écosystème de la cybersécurité - autres initiatives et AMI CMA en cybersécurité, des entreprises et des pouvoirs publics - en contribuant à une meilleure identification et adaptation des besoins en compétences.

Le présent document propose une synthèse d'enquêtes conduites par diverses organisations. Il ne prétend pas à l'exhaustivité : de nombreuses études de qualité existent, mais leur recensement intégral dépasserait l'objectif poursuivi ici. Les enquêtes retenues ont été sélectionnées selon plusieurs critères complémentaires :

- La couverture géographique, allant de l'échelle internationale et européenne jusqu'aux niveaux national, régional et métropolitain. Dans une logique d'analyse différenciée, le territoire français a été appréhendé selon quatre grands ensembles (Nord, Sud, Est, Ouest), afin de mettre en évidence certaines spécificités territoriales.
- La méthodologie mobilisée, certaines études reposant sur des enquêtes qualitatives ou quantitatives, tandis que d'autres s'appuient sur des analyses structurelles du tissu économique d'un territoire.
- L'angle d'analyse, qu'il porte sur les métiers, les macro-compétences, les dynamiques sectorielles ou encore les dimensions économiques.
- Le public ciblé, certaines enquêtes s'adressant aux acteurs spécialisés (« pure players ») de la cybersécurité, d'autres aux entreprises utilisatrices dites « à sécuriser », voire au secteur numérique dans son ensemble.

Chacune des études présentées apporte un éclairage spécifique sur les enjeux d'emplois et de compétences en cybersécurité, avec des niveaux de granularité et des prismes d'analyses variés, contribuant ainsi à enrichir la réflexion stratégique.

Ce travail de synthèse constitue une base structurante pour les futures investigations de l'Observatoire. Il ne s'agit pas de dupliquer des travaux existants, mais de positionner l'Observatoire comme un dispositif complémentaire, cohérent avec l'écosystème d'études déjà en place, et pleinement aligné avec les objectifs du projet CyberSkills4All.

Afin de garantir une lecture structurée, la présentation et l'analyse des enquêtes adoptent une approche progressive, allant de l'échelle internationale jusqu'aux dynamiques territoriales.

Solene Chevreau
Coordinatrice projet cyberskills4all
Pôle d'excellence cyber

ISC2 : Cybersecurity Professionals Navigate Evolving Workplaces While Seizing New Opportunities

International Information Systems Security Certification Consortium ((ISC)²) est le nom d'une organisation américaine à but non lucratif. Cet organisme est reconnu pour ses certifications (CISSP).

Date : 2025
Champ de l'étude : Toutes les entreprises.

Méthodologie de l'enquête : Questionnaire en ligne quantitatif
Échantillon : 16,029 professionnels cyber ou décideurs cyber.
Périmètre géographique : International dont 34% USA et 2% France.

Résumé

Le rapport 2025 de l'ISC2 montre les effectifs de la cybersécurité sous tension mais en voie de stabilisation, avec un enjeu désormais centré sur le manque de compétences plus que sur les effectifs. Au-delà du contexte économique actuel (gels d'embauche, réductions budgétaires et licenciements dans le secteur de la cybersécurité), le rapport met en lumière le besoin de compétences en intelligence artificielle et en sécurité du « cloud ».

1. L'IA, un levier d'opportunités pour les professionnels de la cybersécurité

L'IA s'impose comme un levier clé pour aider les équipes de cybersécurité, souvent limitées par les budgets et les ressources, à faire face à l'explosion des alertes et des tâches de surveillance. Son adoption est déjà bien engagée : 69% des organisations utilisent, testent ou évaluent des outils de sécurité basés sur l'IA, avec des bénéfices concrêts en termes de productivité pour une majorité d'utilisateurs.
Les impacts les plus rapides sont attendus dans le monitoring réseau, les opérations de sécurité, les tests de sécurité et la gestion des vulnérabilités, des domaines particulièrement adaptés à l'automatisation. L'IA est perçue non comme une menace pour l'emploi, mais comme un accélérateur de carrière, générant de nouveaux rôles, des compétences plus spécialisées et un besoin accru de profils stratégiques et transverses.
Les compétences clés concernent l'usage de l'IA pour la détection et la réponse aux menaces, le threat modeling, ainsi que la sécurisation des systèmes d'IA eux-mêmes (modèles, données, gouvernance, conformité). En parallèle, l'IA crée de nouveaux vecteurs d'attaque, déjà largement observés, renforçant la nécessité pour les professionnels d'adopter une approche orientée IA afin de sécuriser durablement les organisations.

2. Le Cloud Security : une compétence indispensable.

Avec la généralisation du cloud dans les systèmes d'information et la chaîne logicielle, la sécurité cloud est devenue une compétence incontournable en cybersécurité.
Elle vise à protéger des environnements distribués où infrastructures, services, identités et données sont étroitement interconnectés. Les priorités portent d'abord sur l'architecture cloud et la conception sécurisée, qui conditionnent la robustesse globale des environnements, puis sur la sécurité des plateformes et des infrastructures. Le déploiement sécurisé et la gestion rigoureuse des configurations sont également essentiels, notamment pour limiter les risques liés aux erreurs de configuration, encore fréquentes. La gestion des identités et des accès (IAM) joue un rôle central dans la prévention des intrusions, tandis que la protection des données cloud, à travers le chiffrement, l'obfuscation et la tokenisation, demeure un enjeu clé pour garantir la confidentialité des informations sensibles.

3. Zéro Trust, informatique quantique et Soft Skills : quelles tendances sur 2025 ?

A l'inverse, certaines compétences sont en léger recul par rapport au rapport de l'an dernier : le Zero Trust ou l'informatique quantique jugée encore peu mature et peu accessible. Les compétences transversales sont quant à elles de plus en plus demandées.

Le Zero Trust, bien qu'en légère baisse de priorité en 2025, reste un axe stratégique étroitement lié au cloud et à l'IA. Les compétences clés portent principalement sur la conception d'architectures Zero Trust, la sécurité centrée sur l'identité, le moindre privilège, la gouvernance, ainsi que la segmentation réseau et l'authentification continues.

Les compétences non techniques ou Soft Skills sont désormais centrales en cybersécurité : résolution de problèmes, communication, esprit d'équipe, capacité d'apprentissage, pensée stratégique, intégration des enjeux métiers ..., autant de compétences qui font la différence lorsqu'elles sont associées à des profils techniques.

Conclusion

La cybersécurité entre dans une phase de rééquilibrage, où la montée en compétences, l'IA, la sécurisation du cloud et la gestion humaine des talents deviennent centrales. Les organisations qui sauront investir dans leurs équipes et particulièrement dans ces compétences clés, malgré les contraintes économiques, seront les mieux armées pour faire face à un paysage de menaces toujours plus complexe.

Point d'intérêt pour cyberskills4all :

- Cette étude donne une vision de l'évolution des besoins en compétences cyber au niveau international avec une forte prédominence des USA. Cet aspect permet d'anticiper les tendances à venir en europe car très souvent les USA sont pionniers et une tendance qui est repérée aux USA arrive en Europe et en France avec un décalage.
- De plus, cette étude comprends de très nombreux participants, de tous les continents : ce qui lui donne une forte représentativité et donc une légitimité.
- Enfin l'étude réalise un zoom sur les besoins en compétences en IA et cloud security, Zero trust et compétences transversales : La création de micro-certifications sur l'IA et le cloud security permettraient d'être en avance de phase et d'anticiper efficacement les besoins à venir.

Lien vers l'enquête complète : https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

Flash Eurobaromètre 547 – Cybercompétences

Étude réalisée par Ipsos European Public Affairs à la demande de la Commission européenne, Direction générale des réseaux de communication, du contenu et des technologies (DG Connect) ; et coordonnée par la Direction générale de la communication.

Ipsos European Public Affairs (EPA) est une division spécialisée d'Ipsos, leader mondial des études de marché et des sondages d'opinion.

Date : Avril et mai 2023
Champ de l'étude : entreprises hors secteur de la cyber

Méthodologie de l'enquête : Entretiens téléphoniques
Échantillon : 1 2 916
Périmètre géographique : Europe

Résumé
Le Flash Eurobaromètre 547 analyse les besoins en compétences en cybersécurité des entreprises de l'Union européenne à partir d'une enquête menée au printemps 2024 auprès de 12 916 sociétés. Il montre que la cybersécurité est devenue une priorité stratégique pour une majorité d'organisations, mais que les niveaux de maturité varient fortement selon la taille et le pays. Le rapport identifie les compétences et rôles les plus recherchés, avec une forte importance accordée à la protection des données, à la gestion des risques et à la conformité réglementaire. Il met également en évidence des difficultés de recrutement liées à la pénurie de profils qualifiés et à l'évolution rapide des technologies. Enfin, il aborde les enjeux de formation, de certifications, de cadre européen de compétences (ECSF) et de diversité dans les métiers de la cybersécurité.

1. Une demande de compétences centrée sur la protection des données, l'analyse technique et la gestion des risques

L'enquête fait apparaître une hiérarchie nette des compétences en cybersécurité attendues par les entreprises européennes. La priorité est donnée à la mise en œuvre des pratiques liées à la protection des données et au respect de la vie privée, citée par 25 % des entreprises. Ce résultat souligne le poids structurant du cadre réglementaire européen et la centralité des enjeux de données dans l'activité économique.

Les compétences techniques arrivent ensuite : 21 % des entreprises mentionnent l'analyse et l'évaluation de la sécurité des logiciels et des matériels, et 20 % la capacité à identifier et résoudre des incidents de cybersécurité. Les organisations recherchent donc des profils capables d'auditer les systèmes, de détecter les vulnérabilités et d'intervenir efficacement en cas d'attaque, dans une logique à la fois préventive et corrective.

La gestion des risques et la conformité réglementaire occupent également une place importante, citées par 19 % des répondants. Les compétences cyber s'inscrivent ainsi dans une perspective de gouvernance, dépassant la seule dimension technique pour intégrer des enjeux de pilotage stratégique et de conformité aux normes.

D'autres compétences complètent ce socle, comme la définition d'exigences de sécurité (17 %), l'identification des besoins en sensibilisation et formation (15 %), l'intégration de solutions de cybersécurité (14 %) ou l'analyse des menaces (11 %). À l'inverse, les expertises très spécialisées, telles que le développement de code sécurisé (7 %) ou le social engineering (4 %), sont moins citées, ce qui suggère que les entreprises privilégient des compétences opérationnelles et transversales.

Il est également notable que 24 % des entreprises ne considèrent aucune des compétences proposées comme prioritaire, proportion qui diminue fortement avec la taille de l'entreprise. Cela révèle un écart de maturité significatif entre petites structures et grandes organisations.

Enfin, les rôles jugés les plus importants confirment cette hybridation des attentes. Aux côtés des fonctions stratégiques comme le Chief Information Security Officer, les entreprises valorisent des profils spécialisés en gestion de crise, réponse aux incidents, audit, investigation numérique et conformité juridique. La place accordée à l'expertise en conformité illustre l'intégration croissante des enjeux réglementaires dans le champ des compétences cyber.

2. Un déficit de formation continue malgré des besoins identifiés

L'enquête révèle un paradoxe notable. Alors que les compétences identifiées sont multiples et évolutives, une majorité d'entreprises n'a pas organisé de formation ou d'actions de sensibilisation en cybersécurité au cours des douze derniers mois. Parmi celles qui n'ont rien mis en place, 68 % estiment qu'aucune formation n'était nécessaire. Cette perception contraste avec l'importance accordée à la protection des données et à la gestion des risques.

D'autres freins sont mentionnés : 16 % déclarent ne pas savoir quel type de formation serait pertinent, 10 % ne savent pas où trouver des formations adaptées et 9 % évoquent le temps nécessaire pour les identifier. Le coût de la formation et l'absence d'offres adaptées sont chacun cités par 8 % des entreprises. Ces résultats mettent en évidence un besoin d'accompagnement et de structuration de l'offre de formation, ainsi qu'un enjeu d'orientation des entreprises vers des parcours clairs et certifiants.
La question des certifications et des qualifications formelles apparaît également en filigrane comme un levier d'harmonisation des compétences. L'existence du European Cybersecurity Skills Framework (ECSF) s'inscrit dans cette logique de standardisation, visant à rapprocher les environnements d'apprentissage des exigences du marché du travail.

3. La compétence réglementaire comme pilier stratégique

Parmi les éléments les plus saillants de l'enquête figure la place centrale accordée aux compétences liées à la protection des données, à la conformité et à la gestion des risques. La mise en œuvre des pratiques de protection des données et de respect de la vie privée constitue la compétence la plus citée à l'échelle européenne. De plus, la capacité à assurer la conformité aux réglementations et aux standards est explicitement identifiée par près d'une entreprise sur cinq, et même davantage dans certains États membres.

Ces résultats montrent que la cybersécurité est désormais indissociable de la maîtrise du cadre normatif européen. Les entreprises attendent des professionnels capables d'interpréter et d'opérationnaliser les exigences réglementaires, d'intégrer la conformité dans les processus métiers et d'articuler gouvernance, gestion des risques et architecture technique. La compétence réglementaire devient ainsi un facteur de compétitivité et de résilience, au même titre que l'expertise technique.

Conclusion

Le Flash Eurobaromètre 547 met en évidence une demande européenne de compétences cyber structurée autour de trois axes complémentaires : la maîtrise opérationnelle de la protection des données, l'expertise technique d'analyse et de résolution d'incidents, et la capacité à intégrer la gestion des risques et la conformité réglementaire dans la stratégie de l'entreprise. Les difficultés de recrutement, la rapidité d'évolution technologique et le déficit de formation continue confirment l'existence d'un écart persistant entre les besoins du marché et l'offre de compétences disponibles.

Point d'intérêt pour cyberskills4all :

- Cette étude est particulièrement intéressante de par son ampleur : presque 13 000 répondants à travers toute l'Europe. Elle est ainsi très représentative de la situation de l'Europe à un instant T, et par rebond de celle de la France. Par exemple, en comparaison avec les autres pays européens, la France recrute et

forme très peu de professionnels cyber (la France est placée en dernière position pour les formations et sensibilisations effectuées en cyber dans les 12 derniers mois).

- Le sujet de la formation continue y est abordé de manière très directe, ce qui constitue un panorama très intéressant pour Cyberskills4all : cela met en valeur le marché potentiel pour les micro certifications qui sont en cours de création, certains pays sont plus friands que d'autres de ce type de contenus pédagogiques. Le projet Cyberskills4all, via FUN, peut donc s'adresser à des apprenants à l'échelle européenne, et pourquoi pas s'inspirer des problématiques identifiées dans cette étude.

Lien vers l'enquête complète : https://europa.eu/eurobarometer/surveys/detail/3176

Étude sur les besoins en compétences, emplois et formations en matière de cybersécurité en France

L'Observatoire paritaire des métiers du Numérique, de l'Ingénierie, des Études et du Conseil, et des métiers de l'Événement (OPIIEC), créé en 1998 anticipe les mutations des compétences via des études prospectives sur l'emploi et la formation, fournissant des données clés aux entreprises et institutions.

Date : Avril 2025
Champ de l'étude : Toutes les entreprises

Échantillon : 51 entretiens qualitatifs
Périmètre géographique : France
Méthodologie de l'enquête : Entretiens qualitatifs et enquête en ligne quantitative

Résumé :

L'OPIIEC a conduit une étude approfondie afin d'identifier les besoins en compétences, emplois et formations liés à la cybersécurité en France, dans un contexte de hausse continue des cybermenaces, de complexification des attaques et d'une évolution et accélération de l'utilisation de nouvelles technologies, notamment l'intelligence artificielle.

1. Une montée en compétences devenue critique

L'étude met en évidence une augmentation rapide et durable des besoins en compétences en cybersécurité, directement liée à l'intensification des cybermenaces et à leur sophistication croissante. Les entreprises sont confrontées à des attaques de plus en plus automatisées, notamment les attaques DDoS dont une large majorité est désormais appuyée par des outils d'intelligence artificielle. Cette évolution impose une adaptation continue des compétences, aussi bien techniques qu'organisationnelles.
Les PME apparaissent particulièrement vulnérables, notamment en raison de difficultés à restaurer leurs données après un incident, ce qui souligne l'importance de compétences opérationnelles solides en gestion de crise, continuité d'activité et reprise après sinistre.

2. Évolution des compétences techniques prioritaires

L'évolution rapide des technologies redéfinit les compétences techniques attendues. Le développement du cloud et des approches DevSecOps impose une intégration de la sécurité dès la conception, nécessitant des compétences en automatisation, en codage sécurisé et en tests de sécurité continus.
La diversité des compétences techniques recherchées reflète le besoin d'une approche globale et intégrée de la cybersécurité, couvrant la protection des systèmes, des réseaux, des applications et des données. Cette exigence d'expertise est renforcée par l'émergence de technologies telles que l'intelligence artificielle, la blockchain et, à plus long terme, l'informatique quantique, qui appellent des compétences de plus en plus spécialisées.

3. Compétences en gouvernance, risque et conformité

La montée en puissance des cadres réglementaires, notamment NIS2, renforce les besoins en compétences en gouvernance, gestion des risques et conformité (GRC). Les entreprises doivent avoir la capacité de structurer leurs démarches de sécurité, de piloter des audits, de produire des rapports et de dialoguer avec les autorités compétentes.
Ces compétences dépassent le champ strictement technique et supposent une bonne compréhension des normes, des obligations légales et des enjeux organisationnels, tout en maintenant une articulation étroite avec les équipes opérationnelles.

4. Tensions sur les compétences et limites de l'offre de formation

Malgré une offre de formation en forte croissance, l'étude souligne plusieurs freins majeurs à la montée en compétences. Les entreprises font face à un manque de budgets dédiés, à une insuffisance de spécialisations dans les parcours de formation, à un temps limité consacré à l'apprentissage et à une absence de formations certifiantes reconnues.

Ces contraintes freinent l'adaptation des professionnels aux nouveaux enjeux et contribuent à la persistance d'une pénurie de compétences dans le secteur de la cybersécurité.

5. Diffusion des compétences cyber au-delà des experts

Le rapport insiste sur la nécessité de diffuser des compétences fondamentales en cybersécurité à l'ensemble des salariés, afin de renforcer la résilience globale des organisations. La sensibilisation aux risques, en particulier face au phishing, constitue un levier clé pour réduire l'exposition aux attaques exploitant les failles humaines.

Cette diffusion élargie des compétences permet de compenser partiellement le manque de profils spécialisés et participe à l'ancrage durable d'une culture cybersécurité dans les entreprises.

6. Orientations prioritaires en matière de développement des compétences

Les recommandations mettent en avant l'importance de structurer et de rendre lisible l'écosystème des compétences. Cela passe par l'évolution des cartographies métiers, l'intégration de nouveaux rôles liés à la sécurité dès le développement des solutions, et la mise en place d'attestations de niveau de maîtrise en cybersécurité, sur le modèle de certifications standardisées.

La sensibilisation précoce des jeunes publics et l'acculturation continue des salariés sont également identifiées comme des leviers majeurs pour répondre durablement aux besoins en compétences du secteur.

Conclusion

Les éléments du rapport montrent que la cybersécurité n'est plus seulement une affaire d'experts techniques, mais un enjeu de compétences global, combinant savoir-faire techniques avancés, capacités comportementales et maîtrise des dimensions stratégiques et réglementaires. La structuration de ces compétences constitue un facteur clé de résilience et de compétitivité pour les entreprises françaises.

Point d'intérêt pour cyberskills4all :

- Elle identifie les profils critiques (DevSecOps, analystes SOC, experts en security by design, reverse engineering, etc.) et met en lumière les lacunes du marché, fournissant ainsi une feuille de route précise pour concevoir ou adapter les formations aux besoins réels des entreprises.
- Elle dresse une prospective complète des compétences à développer, couvrant à la fois les savoirs techniques (gestion des SOC, conformité NIS 2, etc.), les soft skills (gestion de crise, collaboration interdisciplinaire) et l'impératif d'une diffusion large des connaissances pour répondre aux défis futurs.
- Enfin, elle insiste sur l'urgence d'une acculturation massive, visant tous les publics : salariés, jeunes en formation, actifs en reconversion ou seniors, afin d'ancrer la cybersécurité comme une compétence collective et accessible, et non plus comme un domaine réservé aux experts.

Lien vers l'enquête complète : https://www.opiiec.fr/sites/default/files/OPIIEC_RAPPORT_COMPLET_CYBERSECURITE.pdf

Stratégie Métropolitaine de Développement économique Questionnaire GPEC – Brest Métropole

La Gestion Prévisionnelle des Emplois et des Compétences (GPEC) est une démarche stratégique de gestion des ressources humaines qui vise à anticiper les besoins futurs de l'entreprise en termes d'effectifs, d'emplois et de compétences, en phase avec ses objectifs stratégiques et l'évolution de son environnement (économique, technologique, social, juridique).

Date : novembre 2025
Champ de l'étude : Pure players (5) et entreprises à sécuriser

Échantillon : 79
Périmètre géographique : Brest Métropole
Méthodologie de l'enquête : Entretiens quantitatifs

Résumé :

L'étude analyse la manière dont les organisations de Brest métropole appréhendent le risque cyber et les compétences associées. Elle met en évidence une prise de conscience large, mais encore centrée sur des actions de cybersécurité de premier niveau. Les compétences cyber restent peu internalisées, avec une forte dépendance à des profils expérimentés et à des prestataires externes. Les besoins portent autant sur la sécurisation technique que sur la gouvernance, l'analyse des risques et l'intégration aux métiers. Enfin, l'essor de l'IA renforce les enjeux de compétences cyber liées à la protection des données, à l'éthique et à la maîtrise des usages.

1. Des compétences cyber inégalement réparties et difficiles à internaliser

La moitié des organisations brestoises n'ont aucun poste dédié à la cybersécurité, un chiffre qui atteint 80% au sein des petites structures. Autre chiffre révélateur du niveau de maturité des entreprise : 42% des répondants ne savent pas si leur police d'assurance couvre le risque cyber. Les ETI et grands groupes internalisent davantage, avec des RSSI expérimentés, mais ces profils seniors sont rares, coûteux et difficiles à fidéliser en raison d'une forte concurrence sectorielle. Les difficultés de recrutement concernent surtout les compétences hybrides alliant expertise technique et gouvernance. Malgré des besoins identifiés, deux tiers des organisations n'envisagent pas d'élargir leurs équipes, privilégiant l'externalisation ou la formation interne. L'offre de formation locale, bien que jugée adaptée, reste méconnue de 77% des répondants, révélant un défaut de visibilité et d'accessibilité des dispositifs. Une approche différenciée est nécessaire pour répondre aux enjeux spécifiques des TPE/PME, des grandes entreprises et du secteur public.

2. L'IA : un levier de transformation aux risques sous-estimés

Plus de 50% des organisations utilisent officiellement l'IA, principalement pour automatiser des tâches administratives ou améliorer l'expérience client. Cependant, ces outils sont souvent déployés sans cadre sécurisé, exposant les données à des fuites ou à des biais algorithmiques. Un point de vigilance majeur réside dans les lacunes des compétences des utilisateurs : le manque de sensibilisation limite une utilisation maîtrisée de l'IA, aggravant les vulnérabilités. De plus, les formations actuelles séparent encore trop souvent IA et cybersécurité, alors que les organisations recherchent des profils capables de maîtriser ces deux domaines.

3. Vers une stratégie territoriale intégrée

Les organisations brestoises (77% des répondants) affirment méconnaitre les organismes de formation et leurs offres. Pourtant, elles peinent à couvrir les besoins critiques en sécurisation des systèmes et analyse des risques, qui exigent une double expertise technique et métier, ainsi que des savoir-faire transversaux comme la veille stratégique ou la rédaction de documents opérationnels. Pour combler ces lacunes, les entreprises et organisations du territoires utilisent les leviers de l'alternance et les partenariats avec les écoles afin d'attirer des profils opérationnels.

Conclusion :
Face à l'essor de l'IA et aux risques cyber croissants, Brest doit concilier montée en compétences techniques et sensibilisation des utilisateurs pour une adoption sécurisée des technologies.
En misant sur des formations hybrides et un écosystème collaboratif, le territoire peut transformer ces défis en opportunités pour renforcer sa résilience numérique. L'enjeu est désormais de passer d'une logique de réponse ponctuelle à une stratégie collective et durable. Une approche coordonnée entre acteurs publics et privés sera la clé pour y parvenir.

Point d'intérêt pour cyberskills4all :

- D'abord, elle identifie des besoins précis en compétences cyber et IA, comme la maîtrise des outils sécurisés ou l'analyse des vulnérabilités, qui manquent cruellement dans les formations actuelles, en s'appuyant sur une synthèse du référentiel de l'ANSSI.
- Ensuite, elle révèle un fossé entre les attentes des entreprises, notamment les plus petites, et l'offre disponible, offrant une base solide pour ajuster les programmes.
- Enfin, elle met en lumière l'importance de la sensibilisation des non-experts, un levier souvent sous-exploité mais essentiel pour une protection efficace.

Lien vers l'enquête complète : https://adeupa-brest.fr/nos-publications/les-besoins-en-emplois-et-competences-de-la-filiere-cybersecurite-brest-metropole

Formation, emplois et compétences de la filière cybersécurité du Grand Nancy.

Porté par un consortium piloté par la Maison de l'Emploi du Grand Nancy et associant Numeum, Nancy Numérique et le CESI École d'ingénieurs, le projet FORE-CY (Formation, Emplois et Compétences Cybersécurité) vise à établir le premier diagnostic territorial (du Grand Est) des besoins en compétences et formations de la filière cybersécurité. Son objectif : dresser un état des lieux précis et élaborer un plan d'action stratégique pour aligner l'offre de formation locale sur les attentes des employeurs.

Date : 31 mai 2023
Champ de l'étude : Pure players et entreprises à sécuriser

Échantillon : 30
Périmètre géographique : Grand Est
Méthodologie de l'enquête : Entretiens qualitatifs

Résumé :

Le diagnostic FORE-CY, mené dans le cadre de France 2030, analyse les besoins en compétences et en formations de la filière cybersécurité du Grand Nancy afin d'adapter l'offre locale aux évolutions rapides du marché. Il met en évidence une forte tension sur les profils cyber, en particulier sur les compétences de pointe comme la cyberdéfense, l'IA, le machine learning, la gouvernance des risques et la conformité réglementaire.
Le rapport souligne la nécessité d'une approche pluridisciplinaire des métiers, intégrant des parcours hybrides combinant compétences techniques, juridiques, managériales et organisationnelles. Il valorise les atouts territoriaux du Grand Nancy en matière de recherche, d'innovation et de coopération entre acteurs de la formation et employeurs, tout en identifiant des freins dans l'attractivité et l'accompagnement des parcours de formation et de reconversion.
Enfin, FORE-CY propose un macro-plan d'actions visant à anticiper les expertises clés à horizon 2030, renforcer les liens entre formation, recherche et entreprises, et élargir le vivier de talents en cybersécurité.

1. La sécurisation des infrastructures et des réseaux : un besoin structurant pour la filière

La sécurisation des infrastructures, des systèmes et des réseaux constitue le socle des besoins identifiés pour les entreprises de la filière. Les retours recueillis mettent en évidence une tension significative sur les profils capables d'intervenir sur des architectures hybrides, d'en comprendre les interdépendances techniques et d'en garantir la sécurité dans un cadre opérationnel.
Les compétences attendues relèvent en premier lieu de la sécurité des réseaux et des accès : administration sécurisée des équipements de filtrage, déploiement de mécanismes VPN, supervision des flux, détection des comportements anormaux et mise en œuvre de dispositifs de détection et de prévention d'intrusion. Elles impliquent également une bonne maîtrise des standards de sécurisation des communications et des services réseau, ainsi qu'une capacité à évoluer sur les principales solutions présentes dans les environnements professionnels.
Cette demande s'étend au durcissement des systèmes, à la maîtrise des configurations sécurisées et à l'industrialisation des pratiques de sécurité. Les entreprises attendent à cet égard des compétences articulant administration système, maintien en condition de sécurité, traitement des vulnérabilités et usage d'outils d'automatisation permettant de déployer et maintenir des configurations conformes aux exigences de sécurité.
L'analyse souligne une inadéquation partielle entre ces besoins et l'offre de formation. Si les cursus abordent de plus en plus les enjeux de cybersécurité, les employeurs pointent encore un déficit de mise en situation réelle, de maîtrise des environnements techniques et de préparation à l'exploitation opérationnelle des infrastructures sécurisées.

2. L'analyse et la réponse aux cybermenaces : un déficit de compétences à forte criticité

L'analyse met en évidence une tension forte sur les compétences dédiées à l'investigation et à la réponse aux cybermenaces. Les employeurs expriment des difficultés récurrentes à identifier des profils capables d'assurer la supervision des événements de sécurité, la qualification des alertes, l'investigation technique des incidents et la conduite coordonnée des actions de réponse.

Cette tension concerne à la fois les fonctions de détection opérées dans des environnements de type SOC, l'exploitation de plateformes SIEM, l'automatisation partielle des traitements via des mécanismes SOAR, ainsi que les expertises spécialisées en DFIR. Elle s'étend également à des compétences plus avancées, telles que la threat intelligence et le threat hunting, dont le développement apparaît nécessaire pour anticiper les attaques les plus sophistiquées.

Le rapport fait ressortir un décalage entre, d'une part, le niveau d'exigence opérationnelle attendu par les entreprises et, d'autre part, la disponibilité locale de profils formés à la conduite complète d'un cycle de réponse à incident, depuis la détection jusqu'au rétablissement. Cette fragilité pèse particulièrement sur les secteurs les plus exposés ou les plus réglementés comme la santé, l'énergie ou la finance, pour lesquels la maîtrise du traitement d'incident constitue un enjeu de continuité, de conformité et de confiance.

3. L'intégration des technologies émergentes, un défi technique et prospectif.

L'intégration des technologies émergentes redéfinit les besoins en compétences techniques. L'intelligence artificielle s'impose comme un levier mais également comme une menace pour la cybersécurité, avec une demande croissante pour des profils capables de développer des modèles de détection d'anomalies ou de contrer les attaques adversaires. Le Grand Nancy, avec des acteurs comme le Loria et la start-up Cybi, dispose d'un avantage compétitif dans ce domaine, mais les formations locales ne reflètent pas encore cette dynamique.

Par ailleurs, les besoins liés aux environnements cloud et à l'industrialisation sécurisée des chaînes de production numérique appellent à une clarification. D'une part, la sécurisation des services déployés dans le cloud fait émerger des attentes fortes en matière de maîtrise des configurations, des identités, des interconnexions, des journaux et de la posture de sécurité, notamment au travers d'approches de type CSPM. D'autre part, la diffusion des pratiques DevSecOps traduit un besoin distinct : celui d'intégrer la sécurité dès les phases de développement, de test, d'intégration et de déploiement, dans une logique de responsabilité partagée entre développement, opérations et sécurité.

Dans ce cadre, l'Infrastructure as Code, la gestion sécurisée des secrets et l'automatisation des contrôles doivent être analysées comme des compétences transverses, au croisement des fonctions cloud, DevOps et cybersécurité, plutôt que comme de simples sous-composantes d'un même ensemble technique. Enfin, à plus long terme, la montée des enjeux liés à la cryptographie post-quantique confirme l'émergence d'un besoin de veille, d'anticipation et d'acculturation sur les futures transitions cryptographiques.

4. Les compétences techniques de niche : un enjeu stratégique pour les infrastructures locales

L'enquête fait apparaître plusieurs compétences techniques de niche dont la rareté constitue un facteur de vulnérabilité pour le territoire. La sécurité des systèmes industriels, en particulier dans les environnements de type SCADA ou OT, représente un premier champ critique. Elle mobilise des connaissances spécifiques en architectures industrielles, en protocoles dédiés et en sécurisation de systèmes soumis à de fortes exigences de continuité de service.

À cette première dimension s'ajoute la sécurité des objets connectés et des systèmes embarqués, qui requiert des expertises distinctes mais complémentaires. L'analyse de Firmware, notamment au travers de démarches de reverse engineering, apparaît ici comme une compétence spécialisée de haut niveau, permettant d'évaluer la robustesse réelle des équipements, de comprendre leurs mécanismes internes et d'identifier d'éventuelles vulnérabilités. Cette compétence peut concerner certains objets connectés ainsi que des composants techniques présents dans des environnements industriels ou critiques.

Enfin, la cryptographie appliquée constitue une compétence transverse à forte valeur stratégique. Elle contribue à la protection des échanges, à l'authentification, à l'intégrité des communications et à la sécurisation des données sensibles, dans des contextes où la confiance technique dans les équipements et les flux devient déterminante.

5. Le décalage entre formations et besoins opérationnels : une urgence de réarticulation entre pédagogie et terrain

L'ensemble des tensions identifiées met en évidence un décalage persistant entre les formations disponibles et les compétences effectivement attendues en situation professionnelle. Les entreprises interrogées estiment que les parcours actuels restent trop souvent en retard par rapport aux réalités techniques, aux outils et aux modes d'organisation contemporains de la cybersécurité. Ce constat appelle moins une simple actualisation des contenus qu'une réarticulation plus profonde entre apprentissage académique, expérimentation technique et immersion opérationnelle.

Dans cette perspective, il est préconisé de renforcer l'utilisation de différents dispositifs pédagogiques qui méritent d'être distingués selon leur finalité :

- Les plateformes d'entraînement pratique permettant de développer des compétences techniques ciblées et répétables ;
- Les environnements de simulation réalistes confrontant les apprenants à des cas proches du terrain ;
- Les cyber ranges, enfin, pour leurs exercices complexes, l'entraînement collectif, la détection, la réponse coordonnée et les scénarios de crise.

Le renforcement des partenariats entre établissements, entreprises et acteurs de l'écosystème apparaît dès lors comme un levier prioritaire pour développer des parcours spécialisés, professionnalisants et adaptés de manière régulière pour suivre au plus près les besoins des entreprises.

Conclusion :

Le diagnostic FORE-CY révèle les défis spécifiques du Grand Nancy en matière de cybersécurité : une forte demande en compétences techniques (sécurité des réseaux, cloud, IA, systèmes industriels) et un décalage entre l'offre de formation et les besoins opérationnels des entreprises. Si le territoire bénéficie d'atouts comme la recherche (Loria) et l'innovation (start-ups), il doit renforcer les liens entre formation et monde professionnel, adapter régulièrement les cursus et élargir le vivier de talents pour éviter une dépendance externe et maintenir sa compétitivité.

Point d'intérêt pour Cyberskills4all :

- Cette étude constitue une photographie extrêmement complète des compétences actuelles existantes sur le Grand Nancy et mettant en valeur les particularités du territoire.
- C'est une mise en perspective des compétences sur lesquelles les écoles et organismes de formations locaux doivent travailler et évoluer pour répondre aux enjeux du territoire.
- Ce focus mis sur les compétences manquantes sur le Grand Nancy, avec un niveau de granularité très fin, représente autant de thématiques potentielles pour de futures micro-certifications. Le territoire a exprimé clairement des besoins de formations continues sur lesquels Cyberskills4all peut se positionner.
- Ce travail d'une grande précision gagnerait à inspirer d'autres territoires.
- Cette vision prospective des compétences et technologies émergentes va venir bousculer les pratiques actuelles cyber.

Lien vers l'enquête complète :
https://www.info.gouv.fr/upload/media/content/0001/08/b95bc1c2883c3344776b89368c5ff277ad3d34cb.pdf

La filière de la cybersécurité en Auvergne-Rhone-Alpes

Ce document a été produit par le pôle Intelligence Économique et Territoriale (IET) d'Auvergne-Rhône-Alpes Entreprises, en partenariat avec les structures suivantes : le pôle de compétitivité Minalogic, le Commissariat à l'Énergie Atomique (CEA Grenoble), l'Association pour le digital et l'IT en Auvergne-Rhône-Alpes (ADIRA), le CLUSIR Auvergne-Rhône-Alpes, Digital League, le Campus Région du numérique, ainsi que les Experts du Numérique en Entreprises (ENE)

Date : mars 2024
Champ de l'étude : Pure players

Échantillon : 314 entreprises sur le territoire
Périmètre géographique : Auvergne Rhone Alpes
Méthodologie de l'enquête : Étude quantitative se basant sur l'analyse des données des entreprises du territoire et de la veille documentaire.

Résumé :

Cette étude dresse un état des lieux de la filière cybersécurité en Auvergne-Rhône-Alpes, en s'appuyant sur l'analyse de 314 entreprises « pure players ». Elle met en évidence de forts besoins en compétences techniques avancées, notamment en sécurisation d'infrastructures hybrides (IT/OT/IoT), cloud, cryptographie, audit et tests d'intrusion. Malgré un écosystème d'excellence structuré autour d'acteurs majeurs comme le CEA et Minalogic, la région fait face à des tensions importantes de recrutement, dans un contexte national de plus de 15 000 postes non pourvus. L'enjeu principal porte sur la formation, l'attractivité des talents et la capacité à répondre aux besoins croissants de protection des systèmes critiques.

1. Des besoins marqués en compétences techniques avancées

L'étude met en évidence une demande soutenue en compétences techniques de haut niveau, en particulier dans la sécurisation des infrastructures numériques, des systèmes industriels et des environnements cloud. Les besoins portent sur la capacité à analyser des architectures complexes, à sécuriser des réseaux hétérogènes, à protéger les données et à gérer les identités et les accès dans des environnements multi-technologiques.
Ces attentes se traduisent également par un besoin accru de compétences en analyse de vulnérabilités, en audit de sécurité et en tests d'intrusion, y compris sur des systèmes industriels et embarqués. La région se distingue par une spécialisation sur ces sujets, renforçant la demande pour des profils capables d'intervenir sur des environnements IT/OT/IoT, où les enjeux de sûreté, de disponibilité et de sécurité sont étroitement imbriqués.

2. Une spécificité régionale autour de la cryptographie, du matériel et de la sécurité « by design »

L'un des enseignements majeurs du document réside dans le positionnement singulier de l'Auvergne-Rhône-Alpes sur les compétences de haut niveau en cybersécurité, notamment en cryptographie, en sécurité matérielle et en analyse de vulnérabilités. La présence d'acteurs de référence tels que le CEA, le CEA-Leti et de nombreux laboratoires académiques de rang international confère à la région un avantage stratégique sur des thématiques où la sécurité est intégrée dès la conception des systèmes. Les besoins en compétences dépassent ainsi les profils opérationnels classiques pour concerner des experts capables d'intervenir à l'interface du matériel et du logiciel, d'analyser des vulnérabilités physiques et logiques, de concevoir des mécanismes de protection intégrés aux processeurs et aux systèmes embarqués, et d'évaluer la sécurité de produits dans des cadres de certification exigeants.

3. Répartition des compétences et tensions sur le marché de l'emploi régional

Le tissu régional se caractérise par une forte concentration de compétences en gouvernance cyber, en particulier dans les domaines de l'audit, de l'analyse de risques, et de la conformité réglementaire, traduisant une spécialisation marquée des acteurs sur les fonctions de pilotage et de conseil. En parallèle, les compétences en protection cyber sont largement représentées, notamment dans la sécurisation des infrastructures, des données, des communications et des postes de travail, en réponse aux besoins opérationnels des entreprises face à la hausse des cyberattaques.

Toutefois, cette richesse de compétences s'inscrit dans un contexte de fortes tensions sur le marché de l'emploi, avec un déficit structurel de profils qualifiés. Selon Auvergne Rhone Alpes entreprises, plus de 15 000 postes en cybersécurité restent non pourvus au niveau national, une situation qui se retrouve à l'échelle régionale, en particulier pour les métiers d'ingénieurs en informatique, parmi les plus en tension dans l'Isère, le Rhône et le Puy-de-Dôme.

Conclusion :

L'Auvergne-Rhône-Alpes confirme un positionnement à forte valeur ajoutée dans la cybersécurité, fondé sur une expertise pointue en cryptographie, sécurité matérielle et sécurisation des environnements complexes. Cette spécialisation, adossée à un écosystème scientifique et industriel de premier plan, constitue un levier différenciant à l'échelle nationale. Néanmoins, la dynamique de croissance se heurte à une pénurie durable de compétences, particulièrement sur les profils d'ingénierie et d'expertise avancée. La consolidation de cet avantage compétitif reposera donc sur la capacité du territoire à structurer un vivier de talents à la hauteur de ses ambitions technologiques et industrielles.

Point d'intérêt pour cyberskills4all :

- Cette étude est intéressante car elle se base sur un recensement des acteurs économiques (cf. carte dynamique), académiques, de recherche et de l'accompagnement de la région Auvergne-Rhône-Alpes.
- Nous obtenons ainsi une belle photographie des spécificités de ce territoire, en mettant particulièrement en avant le domaine d'excellence académique (Hardware security, crypto post quantique et menace quantique, souveraineté des données).
- Cela permet également de faire un lien qui n'est pas si aisé : ce n'est pas parce qu'il y a une excellence académique sur un thème en particulier qu'il n'y a pas pour autant un manque de compétences dans ces domaines dans le secteur privé.
- Cette étude fait également un focus sur le monde de l'industrie qui occupe la 5ème position en termes de préocupations avec une cinquantaine d'établissements spécialisés sur les infrastructures et systèmes industriels : secteur qui est de plus en plus touché par les cyber attaques.

Lien vers l'étude complète : https://plateforme-iet.auvergnerhonealpes-entreprises.fr/informations-economiques/publications/panorama-des-acteurs-de-la-cybersecurite-en-auvergne-rhone-alpes-edition-2026

Étude prospective "Métiers de demain pour la cybersécurité"

La Cité de l'Économie et des Métiers de Demain est un espace innovant porté par la Région Occitanie. Elle a pour ambition d'anticiper et d'accompagner les métiers de demain au service d'une économie durable, inclusive et compétitive. Le site accueille des projets d'innovation collaboratifs associant acteurs publics et privés, propose des espaces de co-conception ainsi que des événements thématiques, et rassemble des partenaires stratégiques tels qu'AD'OCC et Cyber'Occ.

Date : décembre 2021
Champ de l'étude : Pure players

Échantillon : 51 répondants
Périmètre géographique : Occitanie
Méthodologie : Étude qualitative

Résumé :

L'étude prospective « Métiers de demain pour la cybersécurité » (2021–2022) analyse l'état des lieux de la filière en Occitanie, ses tendances structurantes (transition cloud, durcissement réglementaire, intensification des cybermenaces) et leurs impacts sur l'emploi. Elle met en évidence une forte croissance des besoins, avec un doublement attendu des effectifs régionaux à horizon 2025 (environ 6 000 ETP), dans un contexte de fortes tensions de recrutement sur les profils techniques et expérimentés. L'étude dresse également une cartographie des métiers et souligne l'importance des compétences bac+4/5, notamment sur des postes comme analyste SOC, pentesteur ou architecte cybersécurité. Enfin, elle analyse l'offre de formation régionale, globalement adaptée mais perfectible, et formule des préconisations pour renforcer l'attractivité, l'adéquation formation-emploi et l'appui au recrutement des entreprises.

1. Un socle de compétences techniques de haut niveau

L'étude met en évidence un besoin massif et structurant en compétences techniques avancées dans le domaine de la cybersécurité. Les recrutements observés se situent majoritairement à un niveau bac +4 / bac +5, avec une expérience intermédiaire de trois à cinq ans attendue pour une large part des postes. Environ 70 % des offres analysées correspondent à ce niveau de qualification, ce qui traduit une exigence élevée et une professionnalisation croissante du secteur.

Les tensions concernent particulièrement les profils opérationnels capables d'intervenir directement sur la protection des systèmes d'information. Les analystes SOC, les pentesteurs, les architectes cybersécurité, les développeurs de solutions de sécurité ainsi que les spécialistes en forensic et en threat intelligence figurent parmi les métiers les plus recherchés et les plus difficiles à recruter. Ces fonctions supposent une maîtrise approfondie des architectures systèmes et réseaux, des mécanismes d'attaque, des outils de supervision et de détection, ainsi qu'une capacité d'analyse technique avancée.

Le déficit observé ne relève pas uniquement d'un manque quantitatif de candidats, mais également d'un écart qualitatif entre les compétences disponibles et le niveau d'expertise requis. Les entreprises expriment un besoin de profils immédiatement capables d'intervenir sur des environnements complexes et critiques, ce qui accentue la tension sur les compétences expertes.

2. Un besoin critique en gestion d'incident et en réponse à crise

L'étude met en lumière un déficit particulièrement marqué dans le domaine de la gestion d'incident et de la réponse à crise cyber. Alors que la fréquence et la sophistication des attaques augmentent, les organisations doivent renforcer leurs capacités de détection, de réaction et de remédiation.

Les compétences attendues ne se limitent pas à l'identification technique d'une intrusion. Elles incluent la

capacité à analyser rapidement la situation, à coordonner les équipes internes et les prestataires externes, à assurer la continuité d'activité et à piloter les actions correctives. La gestion de crise cyber implique également une dimension organisationnelle et stratégique, nécessitant une compréhension fine des enjeux opérationnels et décisionnels.

3. Des compétences hybrides à l'interface entre technique et stratégie

Au-delà des expertises purement techniques, la cybersécurité s'impose comme un enjeu transversal au sein des organisations. Les entreprises recherchent des profils capables d'articuler maîtrise technologique et compréhension globale des enjeux métiers, économiques et organisationnels.

Les sociétés de conseil et les entreprises de services numériques expriment un besoin particulier de professionnels disposant d'une vision systémique des systèmes d'information et de leur intégration dans les processus métiers. Ces profils doivent être en mesure d'évaluer les risques, d'accompagner les projets de transformation numérique et de formuler des recommandations adaptées aux contraintes spécifiques de chaque organisation.

Cette hybridation des compétences devient un facteur différenciant. Elle suppose des capacités d'analyse stratégique, de communication et de pédagogie, afin de dialoguer avec des interlocuteurs variés, des équipes techniques aux directions générales.

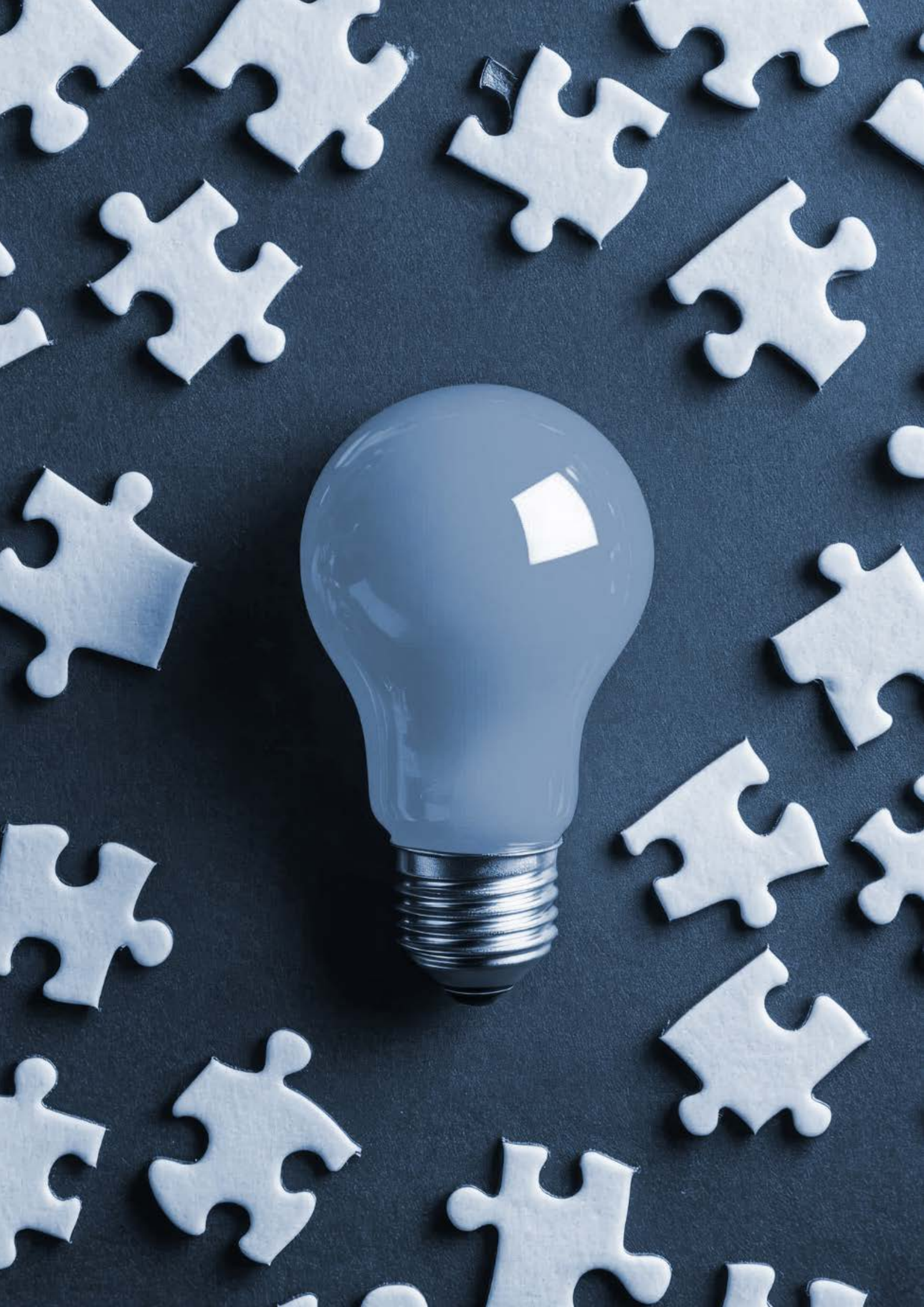
Conclusion :

En définitive, les besoins en compétences cyber se caractérisent par une forte exigence technique, une spécialisation accrue et une tension durable sur les profils expérimentés. Le déficit est particulièrement marqué dans la gestion d'incident et la réponse à crise, devenues centrales face à l'intensification des menaces. Les organisations recherchent également des profils hybrides, capables d'articuler expertise technologique et vision stratégique. Dans ce contexte évolutif, le renforcement de la formation continue apparaît indispensable pour maintenir les compétences à jour et accompagner les transformations rapides du secteur.

Point d'intérêt pour cyberskills4all :

- Cette étude permet de bien identifier les spécificités territoriales, à savoir l'aérospatiale, la santé et les équipements électrotechniques. De cette spécificité découlent des besoins en compétences particuliers.
- Un autre aspect intéressant de cette étude concerne la classification des besoins en fonction de leurs modes d'utilisations par les entreprises : certaines compétences sont internalisées quand d'autres sont externalisées (réponse à incidents et gestion de crise cyber).
- Le besoin de professionnels ayant une double compétence (technique et stratégique) est bien identifié. Cette double compétence s'acquiert également avec l'expérience professionnelle. Former des ingénieurs (qui ont déjà une compétence technique) à cette vision globale et stratégique de la cybersécurité permettrait de combler en partie le manque de profils expérimentés particulièrement recherchés actuellement.
- Les enjeux de souveraineté sont également abordés avec une volonté forte de l'écosystème de s'engager dans cette démarche. Là aussi, Cyberskills4all à travers des micro-certifications bien ciblées, pourrait apporter un élément de réponse sur les outils, les méthodes mais aussi sur l'identification des entreprises qui s'engagent dans cette voie.

Lien vers l'enquête complète : https://www.citedeleco.laregion.fr/sites/default/files/2022-07/Etudes%20prospectives%20CEMD%20-%20cybersecurit%C3%A9%20-%20complete.pdf



CONCLUSION

Ces différentes études mettent en lumière la diversité et les spécificités territoriales des écosystèmes de la cybersécurité. Elles révèlent toutefois une forte hétérogénéité, tant dans leurs objets d'analyse que dans leurs périmètres d'études et leurs méthodologies.

Les thématiques abordées varient sensiblement : certaines études portent prioritairement sur l'emploi, d'autres sur les compétences, d'autres encore proposent un état des lieux des acteurs existants — incluant les organismes de formation et les laboratoires de recherche. Si plusieurs travaux adoptent une approche globale des besoins, rares sont ceux qui atteignent un niveau de granularité suffisament fin pour identifier précisément les compétences opérationnelles en tension.

Les périmètres étudiés diffèrent également : certaines enquêtes ciblent exclusivement les « pure players » de la cybersécurité, quand d'autres s'intéressent aux entreprises utilisatrices qui doivent renforcer leur posture de sécurité. Les échelles territoriales sont tout aussi variées, allant du niveau local - ville ou métropole - jusqu'aux niveaux régional, national, européen ou international.

Par ailleurs, ces travaux soulignent l'absence de méthodologie d'enquête harmonisée. Les sources mobilisées sont multiples et les approches rarement comparables. Il en va de même pour les référentiels de compétences utilisés, qu'il s'agisse du cadre européen ECSF, du Panorama des métiers de l'ANSSI ou, dans certains cas, de classifications propres à chaque étude, voire de l'absence de référentiel structurant.

Au regard de ces constats, l'Observatoire fait le choix d'une approche différenciante.

En premier lieu, il privilégiera un niveau de granularité particulièrement fin, afin d'identifier avec précision les compétences critiques ou émergentes.

En second lieu, il adoptera une démarche résolument prospective, en projetant les professionnels sur un horizon de deux à cinq ans. Ce choix méthodologique répond aux contraintes opérationnelles du projet : la conception d'une micro-certification — même lorsqu'elle est sous-traitée — nécessite environ une année. Sans anticipation suffisante, le risque serait de proposer des contenus déjà partiellement obsolètes au moment de leur diffusion. Cette phase prospective s'appuiera prioritairement sur des entretiens qualitatifs menés auprès de professionnels reconnus et légitimes dans le domaine de la cybersécurité. Une fois les compétences émergentes identifiées, une enquête quantitative à plus large échelle pourra être déployée afin d'en mesurer l'ampleur et de prioriser les besoins. Dans cette perspective, des collaborations pourront être envisagées avec des structures conduisant déjà des enquêtes sectorielles (ACN, CESIN, OPIIEC), afin de mutualiser les expertises et renforcer la robustesse des analyses.

S'agissant du périmètre géographique, le financement du projet s'inscrivant dans le cadre de France 2030, l'enquête portera sur le territoire national afin de répondre prioritairement aux enjeux de compétences de la France. Toutefois, les contenus développés dans le cadre de CyberSkills4All seront diffusés via la plateforme France Université Numérique (FUN), dont l'audience est internationale. Ils pourront ainsi bénéficier à un public francophone plus large, notamment en Europe, au Moyen-Orient francophone, au Canada ou encore auprès des Français établis à l'étranger.

Enfin, la question du public cible mérite une attention particulière. Si les « pure players » de la cybersécurité constituent un écosystème relativement bien identifié, les professionnels exerçant des fonctions cyber au sein d'autres secteurs d'activité demeurent plus difficiles à cartographier. Une approche sectorielle pourrait s'avérer pertinente, notamment afin de couvrir les opérateurs d'importance vitale (OIV), les acteurs industriels ainsi que les secteurs concernés par l'entrée en vigueur de la directive NIS2.
Dans ce contexte réglementaire, une montée en compétences significative est attendue. Il pourrait dès lors être pertinent de développer, aux côtés des formations destinées aux experts hautement qualifiés, des dispositifs de premier niveau d'expertise permettant d'élargir le public cible, tout en maintenant l'exigence technique nécessaire aux profils les plus spécialisés. Une telle démarche contribuerait à renforcer la maturité globale des entreprises françaises en matière de cybersécurité.

PÔLE D'EXCELLENCE
CYBER

www.pole-excellence-cyber.org