CAP MÉTIERS
Nouvelle-Aquitaine

Métiers stratégiques

Contrat régional de filière Activités de service numérique et jeux vidéo

CRF

Métiers de la sécurité informatique

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

RÉGION Nouvelle-Aquitaine

17 000 **professionnels**[1]

1% de l'emploi régional
4% des professionnels français

+3,6%/an (+0,3% tous métiers confondus)

Principal secteur d'exercice

Activités informatiques et services d'information (48%), essentiellement dans le conseil en systèmes et logiciels informatiques (plus de la moitié des emplois hors secteur)

Profil des actifs

21% de femmes
(49% tous métiers confondus)

40 ans de moyenne d'âge
(42 ans tous métiers confondus)

72% de Bac +3 et plus
(23% tous métiers confondus)

Le professionnel de la cybersécurité assure la sécurité des systèmes d'information/communication et des données qu'ils contiennent (fiabilité, intégrité, disponibilité…). Pour ce faire, il définit les règles de sécurité, analyse les risques potentiels, identifie les vulnérabilités, traite les menaces d'intrusion, élabore les plans d'action nécessaires à leur anticipation/correction, répare et renforce le système en cas de cyberattaque, installe le matériel adéquat, sensibilise les utilisateurs aux enjeux, procédures et bonnes pratiques… La cybersécurité recouvre de nombreux métiers, structurés autour de cinq grandes familles :

Le pilotage, l'organisation de la sécurité et la gestion des risques, qui regroupent les métiers à fortes responsabilités en termes de management de la sécurité des systèmes d'information. Ces métiers jouent un rôle direct dans la définition de la stratégie de sécurité d'une entreprise. Ils sont responsables de l'évolution du corpus documentaire, notamment en ce qui concerne les politiques de sécurité. Ex. : Responsable de la Sécurité des Systèmes d'Information (RSSI), spécialiste en gestion de crise cyber, Responsable du Plan de Continuité d'Activité (RPCA)…

Typologie des contrats de travail

CDI
96%

Temps plein
94%

Salaire mensuel net médian

3 120 euros

(salaire indicatif pour un ingénieur informatique salarié, hors apprenti et stagiaire, à temps complet)

[1]PCS : 388a Ingénieurs et cadres d'étude, recherche et développement en informatique, 388b Ingénieurs et cadres d'administration, maintenance, support et services aux utilisateurs en informatique, 388c Chefs de projets informatiques, responsables informatiques et 388e Ingénieurs et cadres spécialistes des télécommunications.

Le management de projets et du cycle de vie de la sécurité, qui rassemble les métiers participant à l'évolution de la sécurité des systèmes d'information. Ex. : chef de projet sécurité, architecte sécurité, développeur solution de sécurité…

Le maintien en condition opérationnelle, qui couvre les métiers ayant en charge l'application de mesures de sécurité sur l'infrastructure technique et le déploiement de correctifs. Ex. : administrateur sécurité, technicien sécurité…

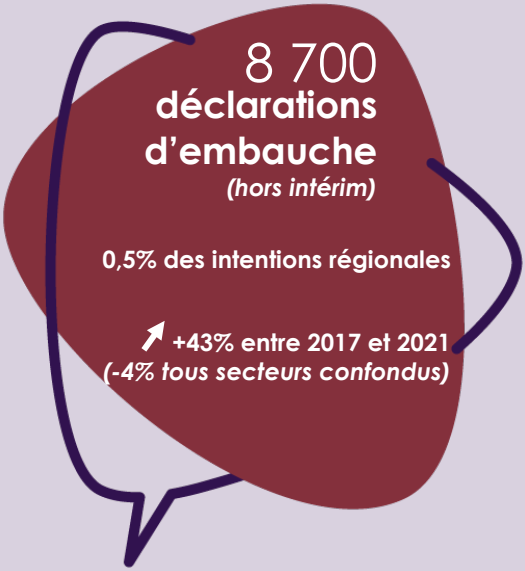
Le support et la gestion des incidents, constitués des métiers intervenant directement sur les incidents de cybersécurité (fuite d'informations, infection virale, ransomware ou rançongiciel…). Ils participent également à l'amélioration continue des méthodes de détection et de prévention. Ex. : analyste SOC (Security Operation Center) …

Le conseil, l'audit et l'expertise, composés des métiers généralement missionnés par les entreprises ne disposant pas des compétences en interne, pour répondre à un besoin ponctuel ou obtenir un avis indépendant. Ex. : cryptologue, consultant sécurité, évaluateur sécurité, juriste cybersécurité, Délégué à la Protection des Données (DPD) ou Data Protection Officer (DPO), formateur en sécurité…

Perspectives et difficultés de recrutement

1 600 projets de recrutement

Plus de 1 600 projets de recrutement d'ingénieurs et cadres prévus en 2022, essentiellement des **ingénieurs et cadres d'études, recherche et développement** et des **chefs de projets.** Les deux tiers des projets sont concentrés sur le **bassin d'emploi de Bordeaux.** 68% sont jugés difficiles, proportion comparable à celle enregistrée tous métiers confondus. Ces difficultés semblent plus prégnantes dans le Pays Basque (100%), sur Limoges (83%) et Bordeaux (72%).



46% des embauches dans le **conseil en systèmes et logiciels informatiques**

32% dans la **programmation informatique**

Projections emploi

Selon les projections d'emploi réalisées avec l'outil Proj'EM (Cap Métiers) à partir des tendances passées, il faudrait environ **1 260 entrées annuelles** dans la famille professionnelle des ingénieurs de l'informatique pour compenser, chaque année, les 530 départs en cours ou fin de carrière et satisfaire aux 730 postes créés.

Un besoin croissant de professionnels

Les enjeux autour de la sécurité informatique ouvrent de nombreuses opportunités de créations d'emplois. La multiplication des attaques renforce les besoins en matière de cybersécurité notamment. L'étendue de la région, la diversité de ses activités et la densité d'entreprises de taille intermédiaire, souvent peu dotées en équipes informatiques, mal protégées, voire non équipées, offrent un large panel clients aux métiers concernés. De plus, les problématiques de cybersécurité gagnent tous les secteurs d'activité, élargissant un peu plus encore le champ possible des recrutements.

Pour l'ensemble des métiers du numérique, le potentiel d'embauches est très important hors secteur : d'après une étude de l'OPIIEC, la moitié des compétences produites en région intègrerait véritablement la filière, tandis que l'autre moitié serait distribuée dans l'industrie, les services et l'administration. De nombreux secteurs d'activité (banque, santé, automobile...) internalisent ou vont devoir incorporer des compétences numériques, en complément de leurs compétences « métier ». Au niveau national, cela représenterait trois établissements sur cinq, tous secteurs confondus. Les compétences en sécurité des données sont parmi les plus recherchées, dans l'informatique et les télécommunications, mais également dans les activités scientifiques et techniques (comptabilité, services juridiques…), les activités financières et d'assurance et le commerce de gros.

Les métiers adossés aux technologies SMACS (Social, Mobile, Analytics, Cloud and Security), parmi lesquels les **chefs de projet**, les **architectes sécurité**, les **administrateurs** et les **analystes SOC**, sont particulièrement prisés pour concevoir et optimiser les systèmes d'information. Avec le développement de l'internet des objets (IoT), les entreprises aéronautiques et automobiles comptent parmi les plus gros diffuseurs d'offres d'emploi sur ces postes. Dans le contexte actuel de déploiement du RGPD, **RSSI** et **DPD** sont des métiers également amenés à se développer.

Mais des difficultés de recrutement multiples

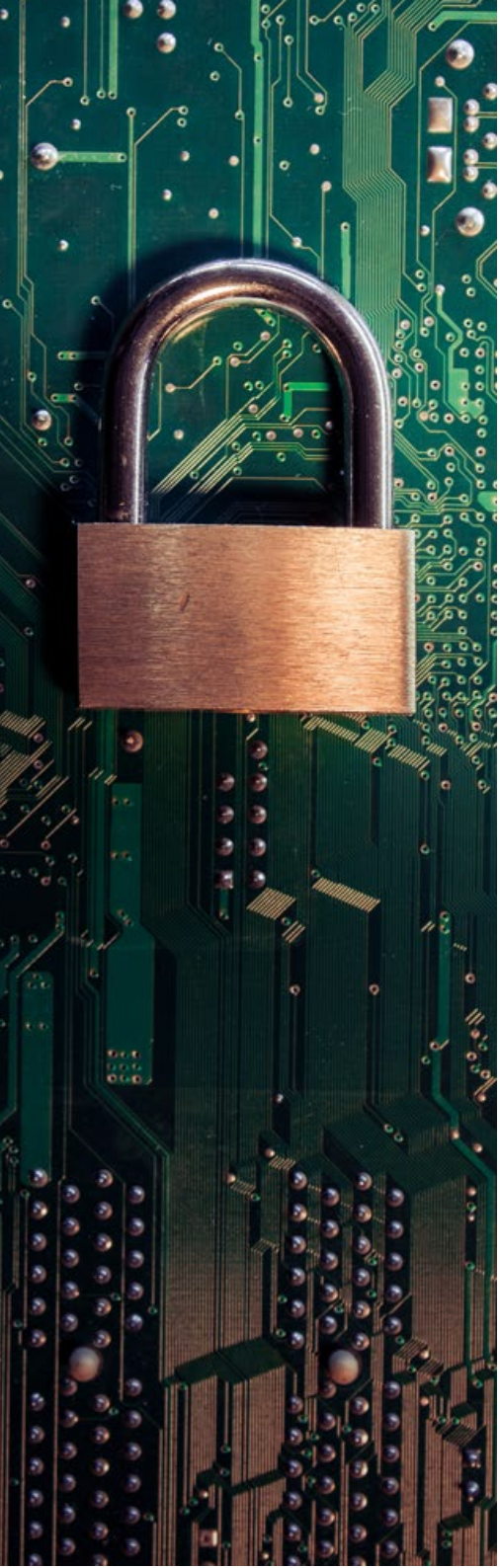
Mais si les perspectives de recrutement sont réelles, les difficultés rencontrées le sont tout autant et concerneraient, selon l'étude de l'OPIIEC sur les formations et les compétences en cybersécurité, deux entreprises sur trois au niveau national. Pami les principaux métiers en tension identifiés, citons notamment les **chefs de projet** et **analystes,** mais également les **consultants.** Les raisons de cette pénurie de candidats sont diverses :

Manque de formations. La formation initiale constitue le principal vivier de recrutement, aussi parce que ce sont des métiers de niveau ingénieur, nécessitant souvent un Bac +5, auquel il est plus difficile d'accéder via la formation continue. Mais les universités, les écoles d'ingénieurs et le CNAM ne proposent pas de formations spécialisées en nombre suffisant. Certaines formations, parmi les plus anciennes et/ou les plus (re)connues, bénéficient d'une certaine légitimité dans le domaine et se retrouvent saturées, incapables de former davantage d'étudiants.

Déficit d'attractivité. Le nombre de jeunes s'orientant vers les formations aux métiers de la sécurité informatique est globalement insuffisant. Si quelques-unes affichent un taux de remplissage important, la plupart souffrent d'un manque de notoriété, voire d'une image négative. Elles accordent beaucoup de valeur à la compétition et sont très largement composées d'hommes. Cet univers a tendance à dissuader les femmes, dont les candidatures sont particulièrement rares. Les métiers auxquels elles mènent sont méconnus du grand public et/ou réduits à leur dimension technique. On les juge pointus, tournés vers les procédures et le contrôle. Les prescripteurs manquent parfois d'informations sur les métiers en lien avec la sécurisation des systèmes et la protection des données.

Concurrence intersectorielle. Les compétences sont captées par des secteurs d'activité en mesure de proposer des rémunérations supérieures. Les candidats font jouer la concurrence et tirent les salaires vers le haut, nuisant aux capacités d'embauche de certaines structures. Interrogées sur les raisons des difficultés de recrutement rencontrées, 36% des entreprises évoquent le manque d'attractivité salariale (source OPIIEC, étude nationale). S'ils ne connaissent pas de difficultés d'insertion, les diplômés en cybersécurité peuvent aussi changer facilement d'emploi, au gré des propositions qui leur sont faites. Le débauchage chez les concurrents est fréquent.

Les recrutements à venir sont essentiellement anticipés dans l'industrie lourde (aéronautique et automobile), avec de plus en plus de demandes autour des systèmes embarqués, tant au niveau des produits (véhicules) que des process (chaîne d'assemblage). Les étudiants sont formés en cybersécurité ou en cryptographie, mais ne possèdent pas toujours les codes pour intégrer un secteur autre que le numérique. Il leur faut donc acquérir des compétences « métier » spécifiques. Bien que les intervenants extérieurs soient issus de nombreux secteurs d'activité, on ne peut pas former des spécialistes dans tous les domaines.



Mobilité géographique. Si les étudiants en cybersécurité ne rencontrent aucun problème d'employabilité au terme de leur formation, la plupart sont contraints de quitter la région (Paris, Toulouse, Rennes...). Pour cause, nombre d'entre eux sont embauchés sur leur lieu de stage, rarement situé en Nouvelle-Aquitaine.

Inadéquation des profils. La plupart des entreprises mettent en exergue le manque de ressources et de compétences dans le domaine de la cybersécurité, avec des besoins en recrutement partiellement couverts, faute de candidats qualifiés. Interrogées sur les raisons de ces difficultés, un tiers des entreprises évoque l'inadéquation des formations (source OPIIEC, étude nationale). On constate parfois un décalage entre les compétences techniques et méthodologiques acquises en formation et les besoins des entreprises. Les contenus théoriques ne semblent pas toujours correspondre à la réalité des métiers, aussi et surtout parce que les technologies numériques évoluent constamment et deviennent très vite obsolètes. Le niveau d'exigence est également très élevé. La polycompétence est souvent de mise : on ne peut pas se contenter d'un seul domaine d'expertise, il faut être « spécialiste en tout ». Les entreprises recherchent des profils transversaux, capables de « parler toutes les langues » de la cybersécurité, de comprendre les différentes techniques et outils, sans forcément les maîtriser totalement, et de faire le lien entre les différents professionnels mais aussi avec la direction. Elles ont besoin d'ingénieurs, mais sur des technologies si nombreuses qu'elles peinent à trouver.

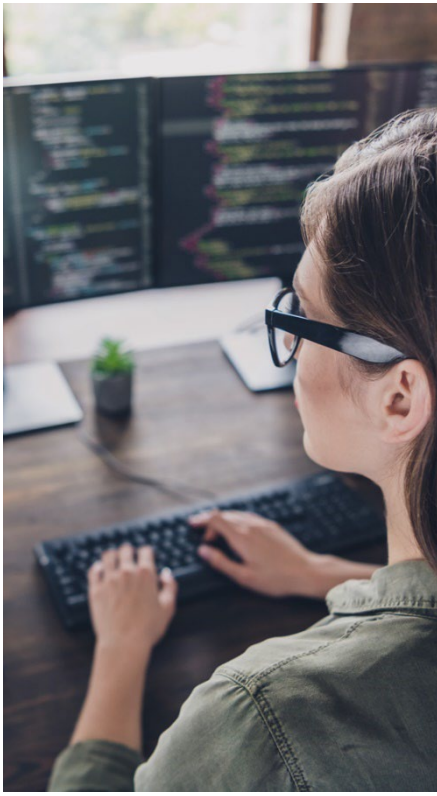
Défaillance de recrutement. Les entreprises souffrent d'un manque de structuration de la fonction RH. Nombreuses sont celles qui ne disposent pas de service dédié. Le dirigeant est souvent issu de la sphère technique. Il n'y a pas toujours d'intermédiaire entre la direction, les équipes et les clients.

Certaines entreprises méconnaissent totalement leur écosystème, les acteurs de la formation et les cursus disponibles sur le territoire. On observe aussi un vrai décalage culturel entre le monde académique et le monde économique, avec des différences de langage. Il existe une multitude de métiers, qui même s'ils relèvent d'un même environnement, sont très différents. Les enjeux de sécurité, internes ou externes, varient également d'une entreprise à l'autre. En outre, une même fonction peut avoir une appellation et/ou une définition différente selon la structure dans laquelle elle s'exerce. Cette divergence s'observe aussi par rapport aux intitulés de formation, qui ne font pas suffisamment sens pour les entreprises.

Les métiers, pour certains émergents, restent complexes à cerner au regard du foisonnement des technologies en présence. Les compétences recherchées sont nombreuses et variées. Les entreprises éprouvent des difficultés à les formaliser au sein des fiches de poste et des offres d'emploi. Pour se rassurer et recueillir un nombre suffisant de candidats, leurs offres font référence à un éventail de compétences techniques très large, renvoyant à plusieurs métiers à la fois. Autre écueil, rechercher des candidats correspondant parfaitement à leur besoin (profil technique, complété par quelques années d'expérience), mais qui sont souvent déjà en poste. Or, le coût d'un débauchage peut constituer un réel frein et sans culture RH, les TPE/PME ne sont pas suffisamment armées en interne pour mettre en place des logiques de parcours et accompagner l'intégration et la progression d'une nouvelle recrue ou d'un salarié en poste.

Besoins en compétences : un solide socle technique complété par des compétences comportementales

Savoir-faire



La principale caractéristique des métiers du numérique réside dans leur caractère dynamique : les technologies évoluent rapidement, impactant les métiers et les compétences requises pour les exercer. Les métiers se transforment, faisant appel à de nouvelles compétences, mais aussi à un plus fort niveau de maîtrise des compétences existantes. Face à la complexification de la gestion de la sécurité, les entreprises recrutent des experts aux compétences avérées.

On distingue plus précisément les **compétences fonctionnelles** (élaboration des politiques, procédures et normes de sécurité, gestion du plan de continuité/reprise d'activité, sensibilisation et formation aux enjeux de sécurité…) et les **compétences techniques** (sécurité des réseaux, systèmes d'exploitation ou applications mobile/web, gestion des accès et identités, cryptographie…). La maîtrise des méthodes d'analyse des menaces et de recherche des vulnérabilités est requise, de même que la connaissance des principes et outils d'intrusion, des pratiques de pentesting (test de pénétration) et des produits de sécurité. Parmi les **langages informatiques à maîtriser,** citons notamment Java et Python.

La protection des données numériques étant strictement encadrée par la loi, la cybersécurité suppose par ailleurs des **connaissances juridiques.** En complément, des **notions en termes de responsabilité numérique et d'écoconception** sont indispensables, de même qu'une bonne **maîtrise de l'anglais.**

Dans les Entreprises de Services du Numérique (ESN), une **double expertise technologique et « métier », voire une spécialisation « métier »** (aéronautique, agroalimentaire…), est parfois nécessaire : la connaissance du secteur applicatif du client et la compréhension des enjeux associés sont primordiales pour développer une solution répondant parfaitement à ses besoins ou produire des recommandations.

La **maîtrise de pratiques innovantes en matière de management, gestion de projet** (méthode agile, Scrum, Kanban, Lean, cycle en V…) **ou stimulation de la créativité** (design thinking, service design…) est particulièrement importante.

Savoir-être

Conscients de la rapidité des progrès technologiques, certains recruteurs accordent davantage d'importance aux **compétences comportementales,** préférant miser sur des **profils agiles,** ouverts d'esprit et capables de s'adapter très vite. Il est nécessaire que les compétences techniques exigées soient constamment complétées et mises à jour (veille technologique, webinaires, MOOC, formations...). Si la cybersécurité exige, plus que tout autre secteur, de se former tout au long de sa carrière, cet apprentissage s'effectue souvent sans intermédiaire, nécessitant **autonomie** et **curiosité intellectuelle.** En outre, les entreprises n'embauchent pas toujours en interne, mais recourent à des sociétés de services ou des consultants indépendants, amenés à intervenir dans des contextes et sur des sujets complexes et extrêmement variables et devant, là encore, faire preuve d'une grande **capacité d'adaptation.**

Avec la transversalité des projets, la multiplication des interlocuteurs et l'essor des méthodes de travail basées sur une plus grande co-construction avec le client, les **qualités relationnelles, d'écoute et de communication** sont devenues essentielles, de même que la rigueur et le respect des engagements (confidentialité). Au niveau humain, l'ingénieur cybersécurité est un bon **pédagogue,** capable de sensibiliser efficacement aux problématiques de cybersécurité et de les présenter de manière constructive, sans heurter inutilement.

Des niveaux de qualification globalement élevés

La plupart des métiers de la cybersécurité requièrent un niveau **Bac +5 ou des compétences maîtrisées de niveau ingénieur.** Le temps de formation étant particulièrement long, les employeurs peuvent être tentés de revoir leurs ambitions à la baisse. Mais placer sur le marché des experts en cybersécurité qui n'en sont pas risque de mettre encore plus à mal les entreprises.

La formation continue peut constituer une alternative pour amener certains publics vers ce niveau (professionnels du numérique, personnes en reconversion, demandeurs d'emploi, dès lors qu'ils manifestent un intérêt pour le numérique).

Quelques offres d'emploi mentionnent des niveaux d'études inférieurs, dès lors qu'ils sont compensés par une expérience, pas nécessairement longue (pas plus de trois ans, en général). Les licences professionnelles sont notamment appréciées dans le maintien en condition opérationnelle ou le conseil, l'audit et l'expertise.

Notons que si les entreprises de la filière cybersécurité ont majoritairement besoin de profils « ingénieur », le reste du tissu économique a plutôt besoin de **bons techniciens,** spécialistes « métier », à qui il faut donner des compétences larges en cybersécurité.

Des perspectives d'évolution en interne comme en externe

Avec de l'expérience, l'ingénieur en cybersécurité évoluera vers des fonctions de management, sur des postes de **responsable ou directeur de systèmes d'information,** ou vers le conseil aux grandes entreprises. Les métiers du numérique sont multisectoriels et offrent donc de grandes possibilités de mobilité.

Formation

400
formés en 2021/2022*

180
voie scolaire
(hors ens. >)

200
apprentissage

3%
femmes

6%
femmes

100%
niveau 5

42%
niveau 6

Principal diplôme

BTS Services informatiques aux organisations

Evolution annuelle moyenne 2018-2021 :
+30% (+16% tous secteurs confondus)

Près de 1 600 contrats d'alternance signés en 2021 par des établissements dont l'activité relève du champ numérique, quelle que soit la formation préparée *(soit 2% des contrats régionaux)*

1 400 contrats d'apprentissage (88%) **+91%**

+29% **190 contrats de professionnalisation (12%)**

Deux principaux secteurs employeurs :
Conseil en systèmes et logiciels informatiques (44%)
Programmation informatique (39%)

37% des structures d'accueil comptent 1 à 9 salariés

61% des contrats signés en Gironde et 11% dans les Deux-Sèvres

51% des contrats visent un Bac +5 et plus *(15% tous secteurs confondus)*

Principaux diplômes préparés :

Titre Expert informatique et systèmes d'information (niv. 7)

Titre Concepteur développeur d'applications (niv. 6)

*En année terminale de formation, à la rentrée 2021 ou au 31/12/2021 (apprentissage). Les données relatives à l'enseignement supérieur ne sont pas précisées car non exhaustives (absence des écoles d'ingénieurs, impossibilité d'identifier les diplômes universitaires spécifiquement dédiés à la cybersécurité…).

Pistes d'action possibles

Manque de formés

Augmenter le volume de sortants (ingénieurs et étudiants de master) **et donc le nombre de formations et/ou de places disponibles, ainsi que la taille des équipes pédagogiques,** tout en restant vigilant sur la qualité des parcours proposés. Il sera probablement plus simple d'aider les formations existantes à passer à une autre échelle, pour irriguer toute la région, que de partir d'une feuille blanche, en créant des formations équivalentes, qui mettront des années à trouver une légitimité et à gagner la confiance des

Développer l'alternance et le mentorat. Le secteur compte beaucoup de prestataires de services, pour lesquels il est difficile de proposer des alternants peu expérimentés aux clients. En dépit de cette difficulté, il existe donc un fort potentiel de développement, avec de nombreuses entreprises régionales intéressées. Les alternants étant souvent embauchés par leur entreprise d'accueil, l'alternance peut, en outre, constituer une piste intéressante pour recruter et monter en compétences. Des formations par apprentissage pourraient être développées à l'université, y compris sur des niveaux « technicien ». Une mutualisation des enseignements avec les formations dispensées sous statut scolaire ne nécessiterait pas de doubler les équipes pédagogiques. De plus, bien qu'intéressées par l'accueil d'alternants, de nombreuses entreprises sont freinées par le manque de ressources internes à y consacrer (mentorat). Peut-être faudrait-il envisager une refonte des modèles d'alternance, avec une pratique en entreprise intervenant en dernière année, tandis que le début de cursus serait exclusivement dédié à l'apprentissage de la théorie, à l'école.

Accompagner la mobilité professionnelle et la montée en compétences
Proposer des parcours de formation continue aux professionnels du numérique, en identifiant les passerelles possibles entre les métiers (ex : administrateur systèmes et réseaux => ingénieur en cybersécurité) et les compétences qu'il conviendrait d'acquérir et en repérant les formations continues existantes ou en développant une offre de formation permettant l'acquisition de ces compétences.

Développer des parcours de type « ingénieux du numérique », permettant d'amener des développeurs de niveau Bac +3 vers un niveau Bac +5, via un système d'alternance aménagé sur quatre ans (généralisation de l'expérimentation menée par le Syrpin, Digital Aquitaine et l'Université de Bordeaux).

Proposer des parcours de formation continue à un public en reconversion, en ciblant exclusivement des profils scientifiques de niveau Bac +5.

Si la plupart des métiers de la cybersécurité requièrent un niveau Bac +5, d'autres publics plus éloignés peuvent également y être amenés, dès lors qu'ils témoignent d'une certaine appétence pour les activités numériques (public en recherche d'emploi par exemple).

Déficit d'attractivité

Développer la visibilité et l'attractivité des filières de formation menant aux métiers de la cybersécurité : faire connaître et valoriser ces métiers, et notamment ceux présentant de forts besoins en recrutement, auprès des collégiens, lycéens et étudiants (campagne de communication/promotion, journées « portes ouvertes » dans les entreprises, interventions de professionnels en classe...), en insistant sur les prérequis nécessaires (compétences techniques, mais aussi comportementales) et sur la dimension positive des métiers (insertion professionnelle rapide, opportunités d'emploi en CDI et à temps complet, rémunérations attractives, perspectives de carrière…).

Faciliter l'orientation des lycéens et étudiants vers les formations en cybersécurité, en sensibilisant les acteurs de l'emploi et de la formation et les prescripteurs (enseignants, conseillers d'orientation, conseillers Pôle emploi…) aux métiers concernés (informations, formations…) et en s'assurant de la présence de la filière sur les salons et forums.

Identifier les freins à l'orientation des femmes dans ces métiers. *Cf. Etude de Cap Métiers (Représentations et processus d'orientation genrés dans la filière numérique en Nouvelle-Aquitaine, 2022).*

Augmenter le nombre de femmes orientées vers ces métiers, en recrutant dès le collège et au travers notamment d'actions de communication permettant de mettre en avant celles qui les exercent déjà. Aller vers davantage de mixité peut également passer par une structuration pédagogique intégrant des briques de formation plus attractives pour les femmes, à l'instar du double diplôme ingénieur informatique-designer créé par CY Tech et CY école de design.

Inadéquation des profils

Travailler de concert entre professionnels et responsables de formation pour adapter très rapidement les contenus de formation aux exigences du marché, via une actualisation régulière des référentiels, en lien avec les nouveaux usages, nouvelles réglementations et nouvelles menaces et répondant à la charte et aux critères définis par l'ANSSI (label SecNumEdu).

Développer l'alternance. En tant que moyen de recrutement de jeunes collaborateurs formés aux pratiques de l'entreprise, l'alternance permet de réduire l'écart entre les compétences maîtrisées en sortie d'études et celles attendues par les professionnels.

Faire découvrir la diversité des secteurs employeurs, au travers de stages par exemple.

Améliorer l'employabilité, en renforçant le socle de connaissances et de compétences des sortants, par une formation accélérée sur les process industriels. En complément, il conviendrait d'apporter une brique de compétences supplémentaire en sécurité des systèmes d'information aux salariés déjà en poste dans l'industrie.

Investir dans la formation des équipes pédagogiques et encourager les stages, pour permettre d'appréhender l'organisation et le fonctionnement internes des entreprises et d'échanger avec des professionnels.

Défaillance de recrutement

Accompagner la structuration RH des TPE/PME, pour faire le lien avec les acteurs de la formation, aider les entreprises à rédiger des fiches de poste ou à identifier l'offre de formation susceptible de répondre à leurs besoins et faciliter la mise en place de parcours type « ingénieux du numérique ».

Recenser et améliorer la lisibilité de l'offre de formation régionale, à travers des dénominations de diplômes plus explicites, tant pour les entreprises que pour le grand public, et en aidant à repérer les formations labellisées (SecNumEdu, CyberEdu…).

Développer le travail à temps partagé. Recourir au travail à temps partagé permet à une entreprise rencontrant des difficultés de recrutement, en raison de sa taille ou de ses moyens, de bénéficier d'une expertise externe pour répondre à son besoin de main d'œuvre qualifiée. L'embauche du collaborateur passe donc par une entreprise tierce, dite Entreprise de Travail à Temps Partagé (ETTP), qui peut également l'accompagner et lui apporter des conseils en matière de gestion des compétences et de formation.

Plus d'infos sur : www.cmaformation-na.fr