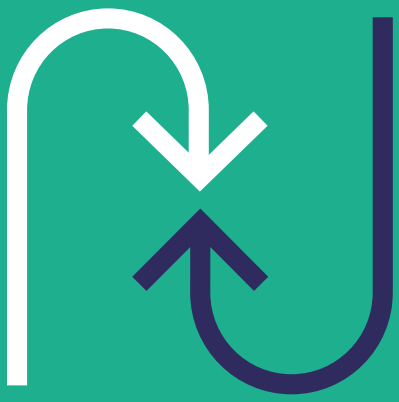


Cybersécurité

Un marché de l'emploi cadre diversifié et de plus en plus porteur

En 2021, 7 000 offres d'emploi cadre ont été publiées sur apec.fr dans le champ de la cybersécurité

→ La multiplication et la diversification des cyber-attaques obligent les entreprises à protéger toujours plus leurs systèmes d'information. Aussi, le volume des offres d'emploi cadre exigeant des compétences dans le champ de la cybersécurité a quasiment doublé entre 2017 et 2021, passant de 3 650 à 7 000 offres.

→ Les entreprises du secteur informatique sont les premiers recruteurs.

La cybersécurité en Bretagne : un écosystème riche et dynamique

→ La Bretagne est une des régions qui diffuse le plus d'offres d'emploi cadre en cybersécurité. Aussi, elle est celle qui en concentre le plus en proportion sur son territoire.

→ La présence d'infrastructures étatiques, d'ESN et d'importants acteurs des télécoms en fait un territoire propice au développement de la filière.

Une grande diversité de profils sont recherchés par les entreprises

→ 46 % des profils recherchés par les entreprises sont des spécialistes de la conception d'architectures sécurisées, du développement de solutions sécurisées et de l'administration des systèmes d'information.

→ Des cadres de la gouvernance, de la gestion des risques et de la conformité sont aussi recherchés mais dans une moindre proportion. Les besoins de cadres pour gérer des incidents sont quant à eux plus rares.

Ces profils sont difficiles à recruter

→ La pénurie de profils disponibles sur le marché oblige les entreprises à se tourner vers la chasse pour approcher des cadres déjà en poste. Les partenariats avec les écoles sont aussi de mise pour recruter de futurs diplômés.

→ Dans un univers très concurrentiel, la rémunération et les opportunités d'évolution proposées aux candidats sont des facteurs d'attractivité non négligeables. Mais d'autres leviers peuvent permettre de faciliter les recrutements.

→ À l'avenir, les besoins et les tensions vont s'accentuer. Former aux risques cyber reste une des priorités.

Juin 2022

Région Bretagne

Préfet de la Région Bretagne — Direction régionale de l'économie, de l'emploi, du travail et des solidarités

Pôle d'excellence cyber

apec

Sommaire

Méthodologie

Cette étude a été réalisée en partenariat avec le Pôle d'excellence cyber (PEC). Elle s'inscrit dans le cadre d'un programme de réflexion plus ample, portant sur les enjeux en matière de cybersécurité. L'Apec, la DREETS (Direction régionale de l'économie, de l'emploi, du travail et des solidarités) et la Région Bretagne en sont les cofinanceurs. Différentes données ont été exploitées pour réaliser cette étude :

Des données qualitatives

Celles-ci sont le résultat d'entretiens menés auprès d'experts d'associations et de centres de formation, et d'interviews conduites auprès d'entreprises ayant diffusé une offre d'emploi cadre sur apec.fr pour recruter un spécialiste de la cybersécurité (tous secteurs confondus). 12 entreprises implantées pour la plupart en Bretagne et en Île-de-France ont été interrogées.

Des données quantitatives

Elles s'appuient sur l'exploitation des offres d'emploi cadre publiées sur apec.fr par des entreprises du privé et du public entre 2017 et 2021. La requête pour identifier les offres en cybersécurité a été réalisée à partir de mots clés issus du référentiel du Pôle d'excellence cyber (ex : cyber, sécurité informatique, *pentest*, SOC, CERT, *forensic*, etc.)[1]. Ces mots clés ont été recherchés dans les intitulés des postes à pourvoir, les missions proposées aux candidats, et les compétences recherchées par les entreprises.

[1] https://www.pole-excellence-cyber.org/wp-content/uploads/2021/06/Brochure-Referentiel-V6.pdf

Le mot du Pôle d'excellence cyber et de l'Apec

Stratégique pour l'économie et les institutions, la cybersécurité s'est imposée ces dernières années à tous ceux qui utilisent des outils numériques. En effet, les systèmes d'information et de communication (matériels et logiciels) conçus pour nous aider à produire, créer, échanger, accélérer le monde l'ont été à une époque où la sécurité n'était pas une priorité pour les concepteurs et développeurs.

De fait, nos systèmes d'information sont, pour la plupart, faillibles, et les préjudices d'une attaque peuvent être immenses pour une organisation : mise à l'arrêt d'une chaine de production ou d'une supply-chain, sabotage des machines, vol, perte, destruction ou revente de données, déficit d'image, coût de restauration, couverture assurantielle incertaine, etc. Pour faire face à ces problématiques, les entreprises et les administrations ont aujourd'hui l'obligation (légale pour les OIV[2]) d'employer des cyber-spécialistes possédant les compétences nécessaires pour protéger leurs réseaux, leurs serveurs et administrer au mieux les nombreuses données qui y transitent ou y sont stockées.

Fort de ce constat et de ces besoins, le Pôle d'excellence cyber (PEC) avait souhaité en 2017 dresser une première photographie du marché de l'emploi cadre dans ce domaine. Créé en 2014 à l'initiative du ministère des Armées et de la Région Bretagne pour accompagner le développement d'une filière souveraine d'excellence en cybersécurité, le PEC réunit les meilleures compétences françaises du domaine cyber (chercheurs, enseignants, personnels des grands groupes spécialisés ou utilisateurs de la cyber, ETI, PME/PMI, experts militaires de la cyberdéfense). De par ses expertises « marché » et « métiers », l'Observatoire de l'emploi cadre de l'Apec l'avait accompagné dans cette première démarche.

Aujourd'hui, le fort développement du numérique, la dématérialisation, la systématisation du télétravail, l'usage d'équipements informatiques personnels dans un contexte professionnel, et inversement, démultiplie les risques cyber. D'où la nécessité de dresser un nouvel état des lieux de ce vaste marché en pleine expansion et des domaines d'expertise qui intéressent les entreprises. Ce document apporte les éléments de réponse et analyse les tensions observées pour recruter les profils cadres spécialisés.

[2] OIV : « Opérateurs d'importance vitale », soit « plus de 200 opérateurs publics ou privés dont les activités sont indispensables au bon fonctionnement et à la survie de la Nation. » Ils sont regroupés dans « une liste gardée confidentielle pour des questions de sécurité nationale », Source ANSSI (Agence nationale de la sécurité des systèmes d'information)

01. Les besoins en compétences cadres « cyber » ont doublé en cinq ans

En 2021, 7 000 offres d'emploi cadre ont été publiées dans le domaine de la cybersécurité

Face au risque de cyber-attaques, les profils cadres possédant une expertise en cybersécurité sont de plus en plus prisés par les recruteurs. En 2021, un peu plus de 7 000 offres d'emploi cadre leur ont été destinées, soit quasiment deux fois plus (+90 %) qu'en 2017.

Cette augmentation est d'autant plus forte qu'elle est très largement supérieure à l'évolution du nombre d'offres d'emploi cadre publiées au global sur apec.fr au cours de cette même période (+20 %).

Les besoins sont portés pour moitié par les entreprises de services numériques (ESN)

L'enjeu de la cybersécurité concerne toutes les entreprises. Toutefois, 51 % des offres d'emploi cadre publiées dans ce domaine en 2021 sur apec.fr, l'ont été par des entreprises de l'informatique, et 34 % par l'ensemble des autres sociétés de services. Ceci inclut notamment les sociétés d'ingénierie-R&D (14 % des émetteurs d'offres) ainsi que les banques et assurances. Figurant parmi les cibles privilégiées des cyber-attaquants, celles-ci ont représenté 4 % des pourvoyeurs d'offres. Autre acteur important, l'administration publique a publié en 2021 près de 420 opportunités d'emploi cadre sur apec.fr dans le domaine de la cybersécurité. Ceci la place au 4e rang des diffuseurs d'offres en cybersécurité sur apec.fr[3].

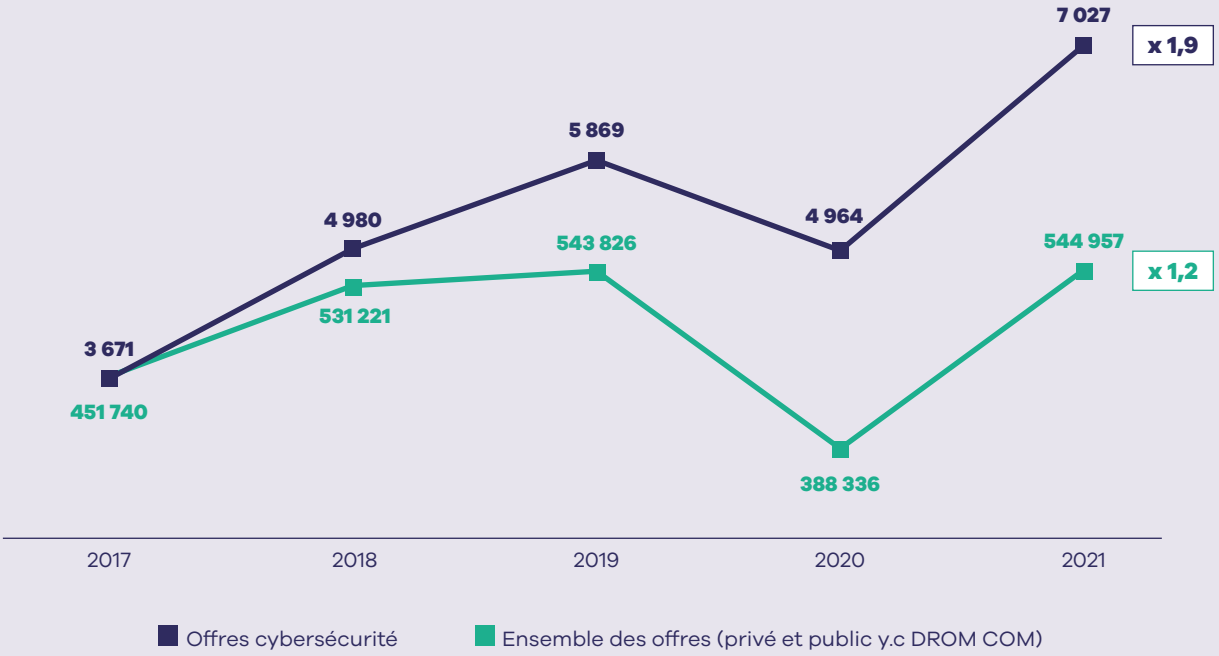
Les entreprises industrielles émettent peu d'offres « cyber ». Ainsi, les fabricants d'équipements électriques ou électroniques qui conçoivent des solutions embarquées ne sont à l'origine que de 2 % des offres en cybersécurité, et les industriels de l'aéronautique, de l'automobile, du naval et du ferroviaire guère plus. Quant aux constructeurs, le nombre d'offres d'emploi qu'ils diffusent en cybersécurité sur apec.fr est plus marginal encore. Pris dans leur ensemble, industriels et constructeurs n'ont représenté que 6 % des diffuseurs d'offres sur apec.fr.
De leur côté, les acteurs de la distribution ne sont à l'origine que de 3 % des offres, et ce quand bien même les possibilités d'achats en ligne les obligent à une extrême vigilance en matière de sécurité informatique.

Si la demande en profils « cyber » peut paraître faible dans ces entreprises, la sécurité de leurs systèmes d'information reste toutefois un de leurs enjeux majeurs. Mais plutôt que de recruter des spécialistes et de renforcer leurs ressources internes pour y parvenir, elles préfèrent souvent avoir recours à des prestataires externes.

[3] Le site de l'Apec n'est pas un canal très utilisé par les administrations publiques qui souhaitent recruter. En conséquence, leurs offres d'emploi qui ne transitent pas sur apec.fr ne sont pas prises en compte dans cette analyse.

En 5 ans, le nombre d'offres d'emploi cadre en cybersécurité a quasiment doublé

Évolution du nombre d'offres d'emploi cadre en cybersécurité, en comparaison de celui du total des offres (Base 100 en 2017*)

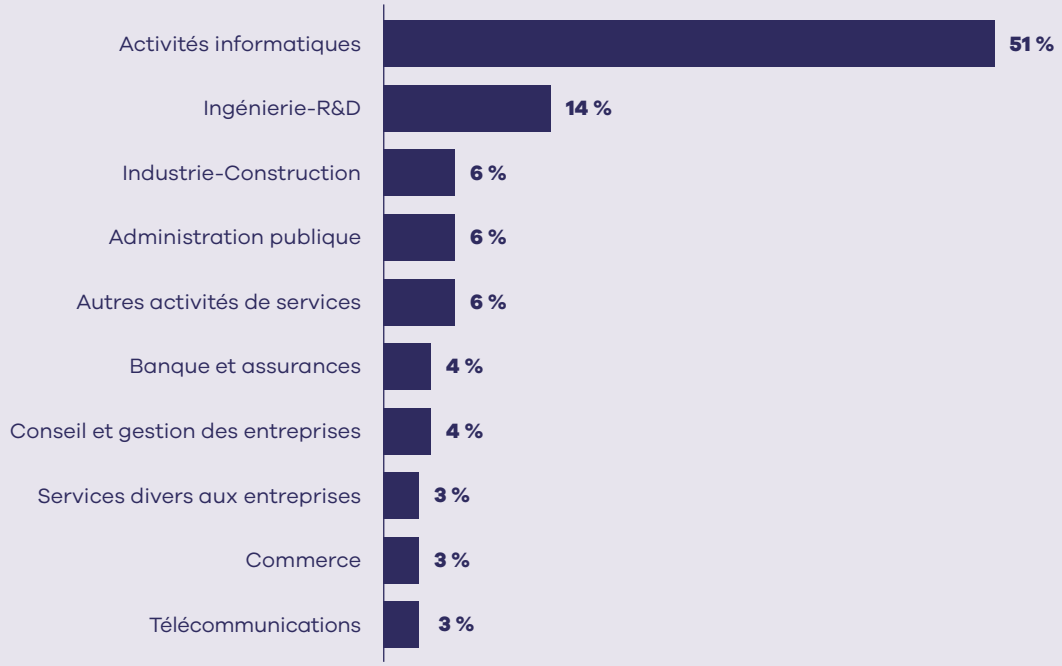


Hors Offres doublons et partenaires

Source : Apec.fr

Des offres d'emploi cadre essentiellement portées par des ESN

Répartition du nombre d'offres d'emploi cadre publiées en 2021 par secteur (hors ETT)*



Hors Offres doublons et partenaires

Source : Apec.fr

02. La cybersécurité en Bretagne : un écosystème riche et un marché dynamique

La Bretagne figure parmi les premières régions pourvoyeuses d'offres d'emploi cadre en cybersécurité

Avec une forte concentration d'ESN et de sociétés de conseil, l'Île-de-France est la région qui exprime le plus de besoins en cybersécurité, et ce, devant la région Auvergne-Rhône-Alpes. Toutefois, la Bretagne se démarque fortement. En effet, avec 540 offres d'emploi cadre publiées en 2021, la Bretagne se hisse au 5e rang des régions qui publient le plus d'opportunités d'emploi dans le domaine. En comparaison, la région n'arrive qu'au 9e rang de celles qui publient le plus d'offres en général. Dans le domaine de la cybersécurité, la Bretagne talonne de peu les régions Provence-Alpes-Côte d'Azur (550 offres) et Occitanie (590 offres). Ces deux régions représentent chacune 8 % des émetteurs d'offres en cybersécurité.

L'écosystème breton est favorable à la montée en puissance de la cybersécurité

En matière de cybersécurité, la Bretagne est la seule région (hors Île-de-France) à disposer sur son territoire d'une infrastructure aussi riche que complexe. Elle bénéficie d'une part de l'implantation ancienne de centres étatiques : direction générale de l'Armement-Maîtrise de l'information (DGA-MI), École des transmissions, École navale, Écoles de Saint-Cyr Coëtquidan, etc.). Elle bénéficie d'autre part de centres de formation civils et militaires dans le domaine (Université de Bretagne Sud, Cnam Sécurité Défense). Ceci explique pourquoi tant d'offres d'emploi « cyber » sont émises dans la région par des administrations publiques (30 % en sont issues vs. 6 % au national).

À ceci, s'ajoute la présence de filières pour lesquelles la cybersécurité constitue depuis toujours un enjeu majeur. C'est le cas des télécoms implantés depuis les années 1970 dans la région.
La puissance de cet écosystème fait que 2,8 % des offres émises en Bretagne sont dédiées à la cybersécurité, contre 1,3 % en moyenne. À ce titre, la Bretagne est la région qui concentre le plus d'offres en cybersécurité sur son territoire.

La Bretagne est plus dynamique qu'en moyenne dans le domaine de la cybersécurité

Des cinq régions ayant diffusé le plus d'offres en cybersécurité en 2021, la Bretagne est celle où le nombre d'opportunités d'emploi dans le domaine a le plus augmenté, celui-ci ayant triplé en 5 ans. Ce dynamisme est essentiellement porté par les administrations publiques, puisque celles-ci ont publié 5 fois plus d'offres sur apec.fr en 2019 qu'en 2017. On peut supposer que face à l'expansion de leurs besoins, celles-ci ont élargi leur recours à des plateformes d'emploi telles qu'apec.fr pour recruter.

Enfin, la région se montre particulièrement attractive pour les jeunes diplômés, 44 % des offres d'emploi en cybersécurité leur étant ouvertes, contre seulement 22 % au niveau national (que ce soit dans la cybersécurité ou tous domaines confondus). Cette attractivité est portée non seulement par les promesses d'embauche qui sont offertes aux candidats, et par la région qui en fait une priorité matérialisée par de nombreux investissements dans la filière. Elle l'est aussi par son cadre de vie que beaucoup jugent plaisant.

La Bretagne : 5e région qui recrute le plus de profils « cyber »

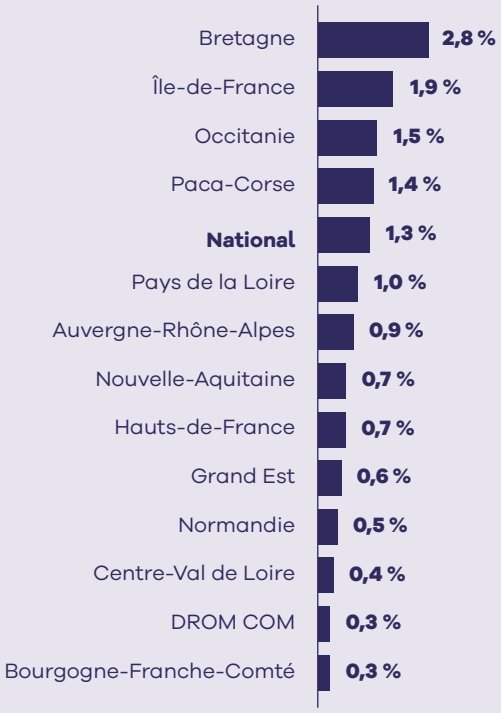
Volume des offres « cyber »* par région et leur poids par rapport au national

	Volume d'offres en 2021	Répartition des offres par région
Île-de-France	3 516	50 %
Auvergne-Rhônes-Alpes	680	10 %
Occitanie	595	9 %
Paca	551	8 %
Bretagne	**542**	**8 %**
Pays de la Loire	330	5 %
Nouvelle-Aquitaine	234	3 %
Hauts-de-France	209	3 %
Grand Est	166	2%
Normandie	85	1 %
Centre - Val de Loire	73	1 %
Bourgogne-Franche-Comté	34	1 %
DROM COM	12	Ɛ
Corse	0	Ɛ
Total	**7 027**	100 %

**Hors Offres doublons et partenaires*
Source : Apec.fr

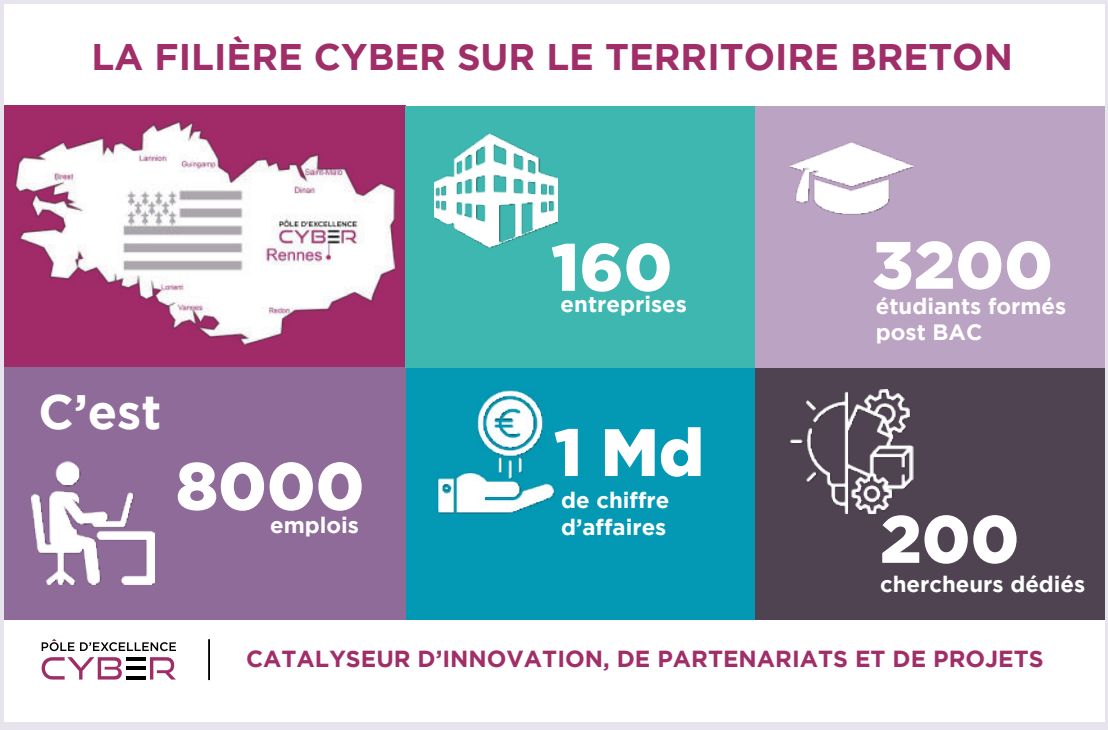
Les offres d'emploi cadre en cybersécurité sont plus fortes proportionnellement en Bretagne

Poids des offres « cyber »* par région en 2021



**Hors Offres doublons et partenaires*
Source : Apec.fr

La région dispose d'un écosystème propice au développement de la filière cybersécurité



Source : Pôle d'excellence cyber, 2022

03. Six familles de métiers structurent les besoins cadres « cyber »

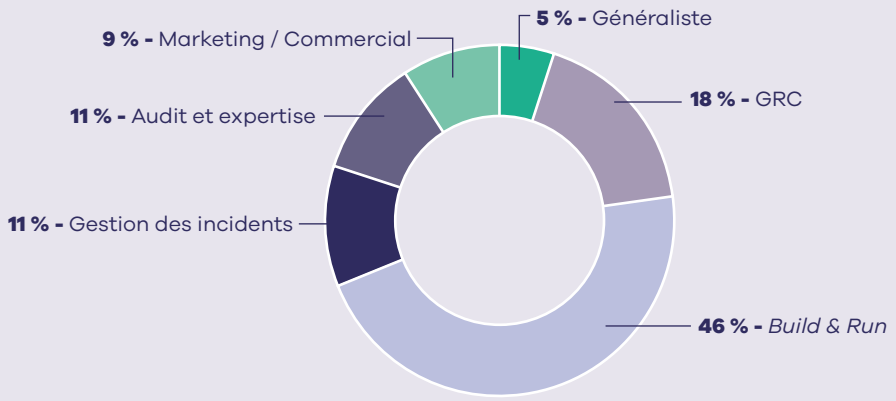
Une lecture approfondie des offres d'emploi cadre proposées en cybersécurité permet de répartir celles-ci en six grandes familles de métiers. Celles-ci correspondent aux différents champs d'action sur lesquels peuvent intervenir les spécialistes de la cybersécurité, que ces domaines soient clairement identifiables dans l'intitulé du poste à pourvoir ou bien dans le descriptif des missions qui y sont rattachées. Jamais déconnectées les unes des autres, ces familles réunissent une diversité de profils. Ces familles de métiers cadres sont :

- La gouvernance, les risques et la conformité (GRC),
- La conception, le déploiement et la maintenance informatique (*Build & Run*),
- La gestion et la réponse à incidents,
- L'audit et l'expertise,
- L'ingénierie généraliste en cybersécurité,
- Le commercial et le marketing.

Parmi ces familles de métiers, celle du *Build & Run* est celle qui concentre le plus d'offres d'emploi cadre (3 200 offres en 2021, soit 46 % de l'ensemble), avec une répartition des offres quasi-équivalente entre les deux sous domaines qui la composent. Vient ensuite celle de la GRC (1 250 opportunités d'emploi cadre en 2021, soit 18 % du marché). Les autres familles de métiers regroupent des profils moins recherchés (moins de 1 000 offres chacune en 2021).
Le volume d'offres d'emploi cadre en cybersécurité a fortement augmenté en 5 ans dans chacune de ces familles. Il a même été multiplié par 2,4 pour les métiers de la gestion et de la réponse à incidents et par 2 pour les métiers du commercial et du marketing ou encore ceux de l'expertise. Toutefois, la répartition des offres d'emploi par famille de métiers est restée à peu près la même en proportion, ce qui montre que les profils recherchés ont, en structure, peu évolué.

Les opportunités d'emploi cadre en cybersécurité

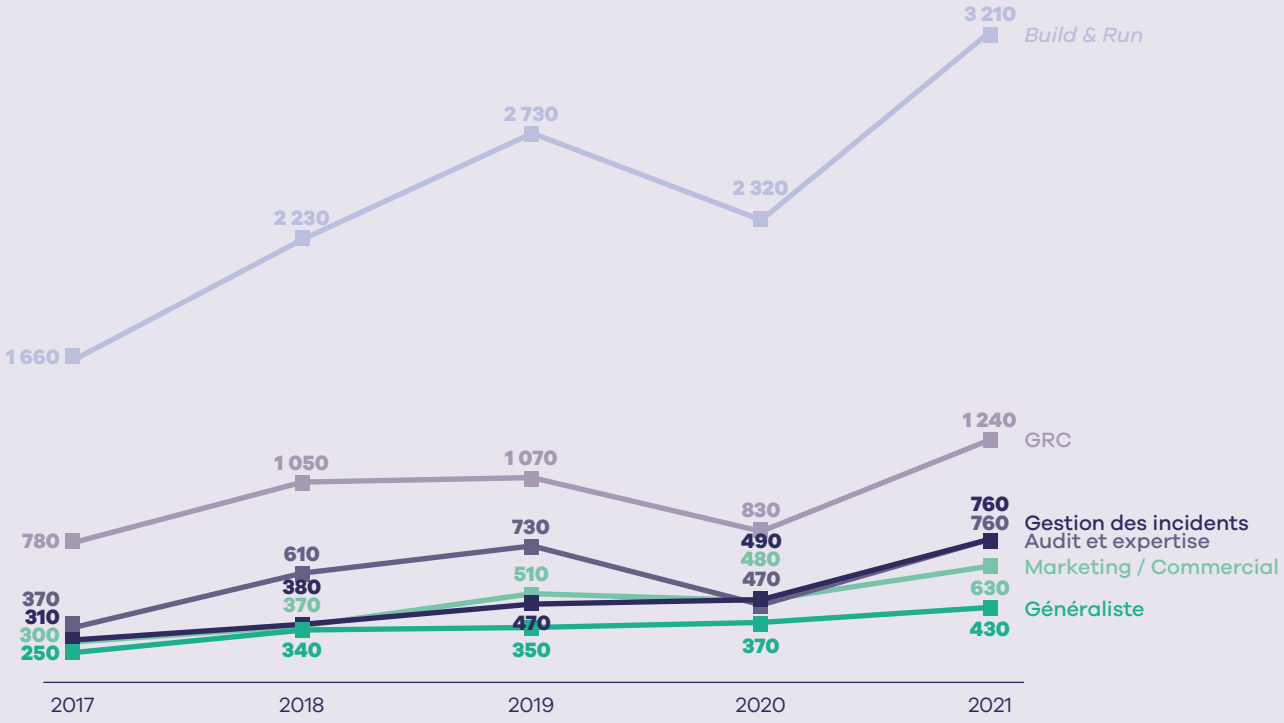
Répartition des offres d'emploi en cybersécurité en 2021



Source : Apec.fr

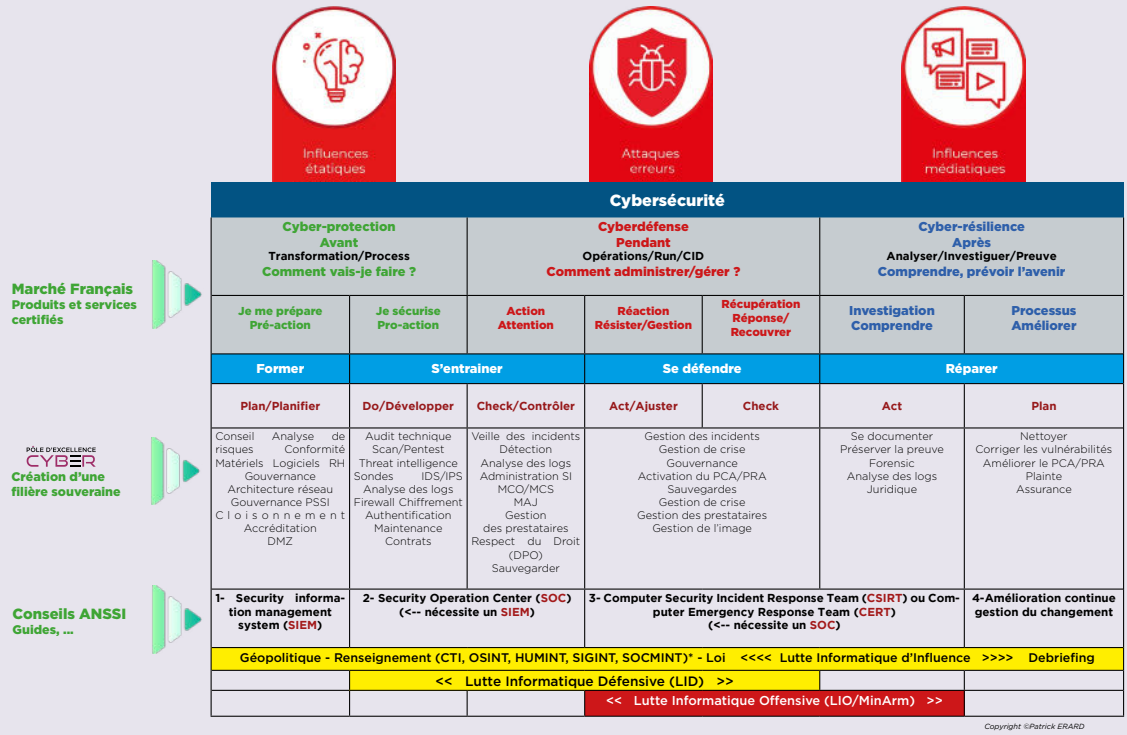
Les opportunités d'emploi cadre en cybersécurité

Évolution des offres d'emploi par famille de métiers entre 2017 et 2021



Source : Apec.fr

Que ce soit avant l'attaque, pendant celle-ci ou après, la cybersécurité mobilise des expertises diverses, toutes interdépendantes les unes des autres



** **CID** : Confidentialité, intégrité, disponibilité • **PSSI** : Politique de sécurité du ou des systèmes d'information (Norme ISO 27001/SMSI) • **DMZ** : Demilitarized zone ou zone démilitarisée • Sonde **IDS IPS** : Systèmes de détection des intrusions / système de prévention des intrusions • **MCO** : Maintien des conditions opérationnelles • **MCS** : Maintien des conditions de sécurité • **DPO** : Data Protection Officer ou Délégué de la protection des données • **PCA/ PRA** : Plan de continuité de l'activité / Plan de reprise de l'activité • **CTI** : Cyber Threat Intelligence • **OSINT** : Open Source Intelligence • **HUMINT** : Human intelligence • **SIGINT** : Signal intelligence • **SOCMINT** : Social media intelligence*

Source : Pôle d'excellence cyber (PEC)

Focus sur les métiers cadres de la gouvernance, des risques et de la conformité (GRC)

En 2021, 18 % des besoins exprimés par les entreprises dans le champ de la cybersécurité ont concerné ce type de profils cadres, soit légèrement moins qu'en en 2017 (22 %). Conscientes de la sensibilité de leurs données et des menaces qui pèsent sur elles, nombre d'entreprises se tournent vers des responsables de la sécurité des systèmes d'information, pour guider et encadrer leurs actions de protection et de surveillance. Elles comptent aussi sur des ressources (internes ou externes) capables d'évaluer les risques dans leur globalité (risques de pénétration, risques consécutifs à l'intrusion, risques de manquement aux principes de sécurité, etc.). Elles misent par ailleurs sur des cadres capables de faire certifier la robustesse des systèmes d'information. Dans les entreprises les plus matures sur le sujet de la cybersécurité, d'autres profils tout aussi stratégiques peuvent intervenir, que ce soit pour définir la ligne de conduite à tenir en cas d'attaque, mais aussi pour impulser des actions de sensibilisation auprès de l'ensemble des collaborateurs de l'entreprise.

Pour ces métiers de la GRC, des compétences techniques et/ou réglementaires sont sollicitées. En outre, les profils recherchés par les entreprises doivent posséder une bonne vision de l'écosystème interne à l'entreprise ainsi que des compétences en matière de conduite du changement. Une bonne compréhension des problématiques « cyber » est également de mise, notamment du fait de l'évolution constante des menaces. Pédagogie et leadership sont aussi requis pour ces métiers. La capacité à travailler avec des auditeurs externes et à intégrer leurs préconisations constitue un autre impératif de leurs fonctions.

Exemples d'offres (extraits)

RSSI • Télécomunications • Pays de la Loire • Salaire proposé : entre 45 et 55 K€ • H/F

Missions : Définir et faire évoluer la politique de sécurité des systèmes d'information • Validation technique des outils de sécurité • Assurer la mise en œuvre des méthodes et outils de sécurité adaptés • Mettre en place des actions de communication et de formation auprès des collaborateurs sur les différentes normes de sécurité • Assurer une veille technologique et réglementaire, de manière à garantir la sécurité du SI • Mettre en place et assurer le suivi des tableaux de bord techniques de votre périmètre technique. **Profil recherché :** Expérience d'au moins 5 ans • Bonne connaissance du système d'information, de l'urbanisation et de l'architecture du SI et des interfaces en applications • Maîtrise des normes et procédures de sécurité et des outils et technologies qui s'y rapportent • Bonne connaissance des outils d'évaluation et de maîtrise des risques (EBIOS) • Rigueur • Capacité d'anticipation et sens de la méthode pour mettre en place des programmes de sécurité efficients • Diplomatie, écoute, sens du dialogue, persuasion pour convaincre les utilisateurs des risques encourus et du bien-fondé des procédures mises en place • Curiosité, veille juridique, se tenir au courant des nouveaux risques.

Ingénieur analyste / management des risques • Occitanie • Salaire proposé : entre 32 et 43 K€ • H/F

Missions : Analyse de risques (identification, évaluation et suivi des risques) • Traitement des risques (design et déploiement des solutions ou procédures de sécurité) • Études de sécurité (études d'impact sécurité et évaluation sécurité de systèmes d'information notamment dans le cadre de procédures d'homologation ou d'accréditation de systèmes ou d'outils) • Veille des vulnérabilités et menaces. **Profil recherché :** 3 ans d'expérience en cybersécurité, idéalement dans le monde des systèmes techniques critiques ou des systèmes d'information complexes • Excellente communication et capacités pédagogiques • Rigueur, pragmatisme et discrétion • Curiosité technique, capacités d'autoapprentissage et de veille technique • Autonome • Capacité à travailler en équipe • Bon niveau d'anglais • Maîtrise des suites logicielles Microsoft • Très bonne connaissance de méthodologies d'analyse de risques sécurité (ISO 27005, EBIOS, etc.) • Bonne connaissance en *threat intelligence* et gestion des vulnérabilités • Bonne connaissance de sécurité système / réseau / communication / données • Idéalement : connaissance des réglementations européennes applicables aux systèmes d'information et à la cybersécurité, etc.

Source : Apec.fr

Focus sur les métiers cadres de la conception, du déploiement et de la maintenance informatique *(Build & Run)*

En 2021, 46 % des besoins exprimés en cybersécurité ont concerné ce type de profil, soit autant en proportion qu'en 2017.
Possédant une expertise technique forte dans le champ de l'informatique, ces cadres ont pour vocation de concevoir (*Build*) des infrastructures, des systèmes et des réseaux qui résistent aux cyberattaques.
Des chefs de projets encadrent les processus de sécurisation qui y sont associés. Relais de la gouvernance, ces derniers doivent pouvoir garantir la conformité des solutions sécurisées conçues par les architectes, les développeurs et les intégrateurs. Ils peuvent aussi orienter, dans la phase de déploiement (*Run*), les missions des ingénieurs systèmes et réseaux ou celle des administrateurs cybersécurité qui sont d'autres profils propres à cette famille de métiers.

Parmi les métiers cadres du *Build & Run*, figurent aussi des ingénieurs IAM[4] chargés de gérer les droits d'accès aux ordinateurs, serveurs et applications, ainsi que des spécialistes du maintien en condition opérationnelle des systèmes et réseaux (MCO). Lorsqu'un incident majeur intervient, ces derniers travaillent en interface étroite avec les spécialistes de la gestion de crise.

Tous ces profils nécessitent une extrême rigueur. Ils impliquent également de savoir travailler en mode projet, notamment avec des cadres fournissant une expertise en matière de cryptographie ou d'identification de failles. Dans les ESN, ils doivent aussi pouvoir dialoguer avec les cadres commerciaux. La réactivité et la disponibilité sont aussi exigées pour toutes les missions relatives à la maintenance.

[4] *« Identity and Access Management » :* gestion des identités et des accès.

Exemples d'offres (extraits)

Architecte cybersécurité • ESN • PACA • Salaire proposé : entre 50 et 70 K€ • H/F

Missions : Définir les exigences de cybersécurité pour les systèmes • Définir des architectures de sécurité • Contribuer à l'architecture des systèmes • Maîtriser les engagements en termes de qualité, coûts et délais • Reporting des activités de pilotage • Test de sécurité (tests spécifiques, validation, maturité incL, scans de vulnérabilité, *pentests*, *fuzzing*) • Réalisation du dossier de conformité.

Profil recherché : Bac+5 (logiciel, informatique ou systèmes de communication) • Expérience sur système logiciel d'au moins 10 ans • Connaissances en sécurité des systèmes de défense • Maîtrisez des principales technologies des infrastructures des SI • Connaissance de normes de sécurité.

Responsable IAM • Industrie • Île-de-France • Salaire proposé : entre 50 et 60 K€ • H/F

Missions : Contribuer à la conception, à la livraison et à l'exécution des services de gestion de l'identité et de l'accès • Gérer, administrer et améliorer le service de l'*Active Directory* • Gérer la mise en oeuvre efficace de la gouvernance des accès et analyse des processus entrants / sortants des employés • Gérer l'image standard des ordinateurs portable/de bureau • Assurer le déploiement des correctifs de sécurité et vulnérabilité appliqués aux postes de travail • Maintenir la documentation des procédures en conformité avec les processus qualités de l'entreprise • Communiquer en interne toutes modifications liées aux différents services • Gérer, administrer et assurer le support de niveau 3 des services Office 365.

Profil recherché : Bac+3 en informatique • 5 ans d'expérience min. sur un poste similaire • Excellent niveau de francais et d'anglais • Certifications Microsoft exigées • Compétences organisationnelles • Autonome • Orienté service client • Esprit d'équipe et collaboratif • Excellentes compétences en communication écrite et orale • Capacité d'analyse et de rédaction.

Source : Apec.fr

Focus sur les métiers cadres du traitement et de la gestion des incidents

En 2021, 11 % des besoins exprimés par les entreprises en matière de cybersécurité portaient sur ce type de profils cadres. Dotés d'un fort bagage informatique (analyse de logs, virtualisation, etc.), ces spécialistes interviennent lors de la survenue d'une intrusion (ou suspicion d'intrusion). Il leur faut généralement rechercher et collecter les preuves d'une cyber-attaque, mais aussi analyser la manière dont son auteur a réussi à pénétrer un système, à bloquer ses fonctionnalités, à aspirer des données, etc. Dans cette optique, tous les fichiers, les applications, les terminaux et les équipements réseaux susceptibles d'avoir été infectés doivent être analysés. Cette analyse dite « forensic » est nécessaire aussi pour identifier le cyber-attaquant et enclencher des actions juridiques à son encontre. Elle permet également de chiffrer le préjudice.
Qu'ils travaillent dans des *Security Operation Center* (SOC) ou non, ces profils sont en lien avec les équipes chargées de la maintenance des systèmes d'information et de la gestion de crise. Les experts capables de mettre en œuvre des solutions curatives et préventives de haut niveau (telles que des actions de cryptographie par exemple) ou de détecter des zones de vulnérabilité, font aussi partie de leurs interlocuteurs privilégiés.
La réponse à incidents mobilise également des ingénieurs intégrés à des CERT (ou CSIRT)[5]. Ces CERT/CSIRT sont, selon la définition de l'ANSSI, des unités ayant pour vocation de centraliser les demandes d'assistance consécutives à des incidents de sécurité. Elles ont également pour mission de traiter des alertes et de définir des actions de prévention visant à réduire les risques.

Pour tous ces profils, la réactivité, la résistance au stress, la rigueur et la capacité d'analyse sont des compétences essentielles.

[5] CSIRT : *Computer Security Incident Response Team* / CERT : *Computer Emergency Response Team*- Équipes d'experts en sécurité informatique.

Exemples d'offres (extraits)

Analyste SOC • ESN • Bretagne • Salaire proposé : entre 35 et 40 K€ • H/F

Missions : Vous assurez la sécurité défensive de nos clients grands comptes et devenez un acteur majeur de sa cyberdéfense. Vous aurez en charge : la surveillance et le traitement des évènements et des alertes de sécurité • l'analyse des données et l'investigation avancée des incidents • l'amélioration continue des systèmes de corrélation de la sécurité, la mise en œuvre de nouveaux périmètres et les optimisations en matière de détection des menaces • le *reporting* des incidents de sécurité, de l'activité opérationnelle et la fourniture d'indicateurs • la coordination avec le client pour la résolution des incidents et l'accompagnement à la remédiation • la recherche proactive de menaces avancées • la veille technologique des menaces, des attaques et des vulnérabilités • Vous participerez aussi à l'évolution du CyberSOC. **Profil recherché :** Ecole d'ingénieur ou licence d'informatique • Première expérience en cybersécurité • Passionné.e, dynamique, curieux.se et faisant preuve d'initiative • Vous aimez travailler en équipe, partager vos connaissances et avez envie de travailler dans un contexte international.

Ingénieur investigation numérique *forensic* • Bretagne • Administration publique • Salaire proposé : entre 34 et 55 K€ • H/F

Missions : Vous serez intégré à des projets de recherche et développement dans leur partie analyse et interprétation de traces suite à des attaques informatiques • Vous évoluerez dans un environnement à fortes contraintes sécuritaires où vos travaux et les informations manipulées sont classifiés « Défense ». **Profil recherché :** Bac+5 • Vous justifiez de compétences sur l'un ou plusieurs des sujets suivants : investigation numérique de support de données numériques (mémoire morte, vive, magnétique ou flash) : *dump*, extraction, analyse de traces, interprétation et corrélation, localisation des traces d'activités système d'un système d'exploitation, chaîne de confiance forensic, protocoles réseaux publiques et propriétaires • Langages de programmation de type script • Autonomie et curiosité • Notions en *pentest* et analyse de *malware* appréciées • Lors de votre première année de travail, si besoin, vous serez accompagné par un collaborateur plus expérimenté pour que vous puissiez monter en compétence en toute sérénité.

Source : Apec.fr

Focus sur les métiers cadres de l'audit et de l'expertise en cybersécurité

Cette famille de métiers regroupe des profils cadres hétéroclites en termes de missions ou de niveau d'intervention dans la « chaîne de valeur » de la cybersécurité. Concentrant 11 % des besoins en 2021, elle comporte deux types de métiers :

- Les premiers interviennent à titre d'experts pour des audits techniques ou organisationnels. Il s'agit de consultants qui soit travaillent en ESN, soit sont intégrés chez le client final. Ils doivent être rigoureux et faire part d'une grande capacité d'analyse. Le sens de la relation client leur est aussi nécessaire, tout comme l'éthique, indispensable pour garantir la confidentialité des données.
- Les deuxièmes occupent des fonctions émergentes. C'est le cas des délégués à la protection des données qui ont un profil relativement hybride entre les métiers du juridique, de la conformité, et de l'informatique. Parmi les profils d'experts que compte cette famille de métiers, figurent aussi les ingénieurs-R&D. Ils peuvent être sollicités pour concevoir des solutions d'analyse et de recherche de menaces. Enfin, des profils de professionnels experts dans le recrutement de profils cyber, de formateurs cybersécurité viennent compléter ce groupe de métiers. Tous ces profils, qui sont rares, nécessitent une grande ouverture d'esprit et une capacité à avancer sur des problématiques innovantes.

Pentester (Client final) • Éditeur de logiciel • Occitanie • Salaire proposé : entre 40 et 55 K€ • H/F

Missions : Réaliser des tests intrusifs conformes aux attentes du client, dans le respect des délais, des engagements et du code de déontologie • Maîtriser les méthodologies et outils d'intrusion • Se tenir informé des bonnes pratiques de sécurité afin de développer ses compétences • Évaluer les risques, les menaces et les conséquences, proposer un plan d'action, rédiger des rapports • Participer à l'activité avant-vente pour apporter sa compétence technique dans la qualification, la rédaction ou même la soutenance d'un dossier client. **Profil recherché :** Diplôme d'ingénieur ou master orienté IT et/ou sécurité informatique • Expérience en intrusion informatique • Maîtrise de l'anglais technique • Bonnes compétences en Scripting python/Bash, développement, réseau, etc. • Solides connaissances sur les méthodologies d'audits reconnues • Bonnes compétences rédactionnelles • Excellent relationnel.

Cryptographe cyberdéfense • Administration • Bretagne • Salaire proposé : entre 34 et 50 K€ • H/F

Missions : Produire des algorithmes cryptographiques répondant aux contraintes des programmes d'armement • Assurer un soutien technique auprès des équipes chargées de leur implémentation • Assurer une expertise technique en cryptographie auprès des équipes chargées du développement des produits de sécurité • Évaluer des algorithmes existants • Réaliser des travaux de recherche • Assurer le suivi de contrats de recherche contractualisés avec des universitaires ou des industriels. **Profil recherché :** Master ou doctorat • Connaissance de la cryptographie • Connaissances des techniques liées à la sécurité prouvable (modes d'opérations et/ou mécanismes asymétriques et protocoles interactifs) • Programmation en langage C.

Adjoint DPO • Banque-Assurances • Auvergne-Rhône-Alpes • Salaire proposé : entre 45 et 56 K€ • H/F

Missions : Identifier les risques cyber des métiers santé/prévoyance, épargne, retraite complémentaire et services financiers • Définir et mettre en œuvre les plans d'action SSI et RGPD • Conseiller les métiers dans l'évolution de leur SI • Proposer des solutions de remédiations techniques ou organisationnelles • Répondre aux sollicitations SSI des directions métiers • Accompagner la prise en compte des exigences règlementaires en matière de cybersécurité • Participer au déploiement du SMSI 27001 • Contribuer au maintien à jour du corpus documentaire SSI PCIT • Contribuer à l'élaboration et aux tests du plan de continuité d'activité : gestion de crise, plan de continuité métier et technique • Réaliser le retour d'expérience de chaque test et proposer des évolutions du PCIT, etc. **Profil recherché :** Bac +5 • Expérience minimum de 5 ans dans les domaines de la RGPD • Connaître les normes et réglementations : ISO27001, RGPD • Maîtriser les fondamentaux de la SSI • Savoir partager et diffuser l'information aux interlocuteurs clés.

Source : Apec.fr

Focus sur les métiers cadres d'ingénieur cybersécurité généraliste

Lors de la publication d'offres, certaines entreprises indiquent vouloir rechercher des « ingénieurs cybersécurité », des « experts en cybersécurité », ou bien des « consultants en cybersécurité ». Cette pratique correspond à quatre cas d'usage.

Premièrement, l'entreprise ne sait pas quel profil recruter car elle est novice dans le domaine de la cybersécurité. L'édition d'une offre labellisée « ingénieur cybersécurité » ou « expert cybersécurité » peut lui permettre de recruter dans un premier temps tous types de profils, pour dans un second temps, mieux affiner ses besoins. Dans ce cas, le descriptif du poste annoncé comme étant à pourvoir n'éclaire pas sur le contenu des missions proposées.
Deuxièmement, l'entreprise a un besoin constant de profils en cybersécurité pour développer son activité. C'est le cas des *pure-players* ou des ESN qui proposent en permanence des offres de services dans le domaine de la cybersécurité pour se constituer un vivier. D'où des offres très généralistes, et pour lesquelles il n'est pas possible de relier l'intitulé ni le contenu du poste à pourvoir à un champ précis d'intervention.
Troisièmement, l'entreprise est à la recherche d'un profil spécifique, mais celle-ci préfère publier un intitulé d'offre générique pour attirer un maximum de candidats et ne pas donner à ces derniers l'impression de chercher à les enfermer dans un poste. Dans ce cas, le descriptif du poste peut éclairer sur le type de mission proposé.
Quatrièmement, l'entreprise recherche un profil plus ou moins spécifique, mais elle préfère mettre en avant dans l'intitulé du poste à pourvoir le contexte d'exercice du métier, que ce soit « pour un client » ou « chez un client ». L'usage de l'intitulé « Consultant en cybersécurité » est alors de mise, avec un descriptif du poste à pourvoir qui peut renseigner ou non sur les missions proposées.

Les offres d'emploi pour lesquelles ni l'intitulé du poste à pourvoir ni le descriptif des missions proposées ne donnent d'indications claires sur le contenu du poste, et empêchent donc d'affilier les profils recherchés à l'une ou l'autre des familles de métiers présentées ci-avant, restent une minorité. Ainsi, elles ont représenté 5 % des besoins en cybersécurité en 2021 (contre 9 % en 2017).

Exemples d'offres (extraits)

Consultant cybersécurité • ESN • Bretagne • Salaire proposé : 40 K€ • H/F

Vous êtes amené(e) à travailler sur différentes thématiques de cybersécurité, telles que : Gestion de crise et plan de continuité d'activité • Sécurité de la transformation digitale (ex. *cloud, big data, IoT*) • Analyse de risques et déploiement de mesures compensatoires • Gouvernance de la sécurité du SI • Gestion des menaces • Gestion des identités et des accès • Mise en conformité réglementaire • Prévention des fraudes, etc.

Consultant cybersécurité • ESN • Occitanie • Salaire proposé : entre 25 et 40 K€ • H/F

Nous recherchons actuellement plusieurs profils. Après une période de formation professionnalisante, vous intégrerez notre entreprise sur un poste de consultant en cybersécurité et vous interviendrez sur nos différents projets : SOC, Analyse de risque, RGPD et autres domaines de la cybersécurité.

Source : Apec.fr

Focus sur les métiers cadres du commercial et du marketing spécialisés en « cyber »

Le marché de la cybersécurité est essentiellement porté par les ESN et les autres sociétés de services. Dans ces structures, des profils plus orientés « commercial » et « marketing » sont nécessaires pour faire vivre l'activité de sous-traitance. En 2021, 9 % des offres d'emploi cadre éditées dans le champ de la cybersécurité concernaient ce type de profils (contre 5 % en 2017).

On y retrouve tous les métiers de l'avant-vente et de la vente qui permettent à ces entreprises de conquérir le marché, *via* l'approche directe ou la réponse à des appels d'offres. Pour ces profils, disposer d'aptitudes commerciales (techniques de prospection et de vente, sens de la négociation, etc.) est un prérequis. Témoigner d'une aisance relationnelle également. La connaissance de l'écosystème « cyber » (les différents acteurs, l'état de la concurrence, les tendances émergentes, etc.) est aussi plus que souhaitable. Cette polycompétences (cyber et commercial) est aussi recherchée pour les managers opérationnels du *Build & Run* qui doivent épauler commerciaux et technico-commerciaux lors du chiffrage et de la qualification de leur offre de prestation.

Les entreprises de services recrutent également des cadres en capacité de développer, d'entretenir et de fidéliser leur portefeuille de clients. C'est pourquoi les *Account manager* ou les *Business Manager* sont des profils très demandés. Les responsables de la relation client ou les cadres chargés de garantir la bonne exécution des contrats de service, tant au niveau des délais que de la qualité (*Service Delivery Manager*) sont également recherchés. Il en va de même des chefs de produit cybersécurité. Plus orientés marketing, ils ont pour rôle d'identifier des opportunités de marché et de développer les offres de l'entreprise en conséquence.

Exemples d'offres (extraits)

Consultant avant-vente cybersécurité • Bretagne • Salaire proposé : entre 45 et 55 K€ • H/F

Mission : Identifier les besoins client • Présenter les offres aux clients • Analyser le cahier des charges • Conseiller sur les aspects techniques • Vous serez amené à évoluer dans des contextes variés (secteur privé, public, grands groupes, PME, etc.) et à proposer des prestations diverses en fonction des besoins du client (conseil, audit, évaluation, études, etc.).

Profil recherché : Au moins 2 ans d'expérience dans le conseil en cybersécurité • Appétence pour la vente de prestations de services • Qualités de conseiller • Des connaissances de la réglementation nationale (LPM, RGS, etc.) voire européenne (RGPD, eIDAS, etc.) seraient un plus • Motivation et dynamisme • Travail en équipe • Anglais impératif.

***Account Executive Manager* en cybersécurité • Éditeur de logiciel • Île-de-France • Salaire proposé : plus de 100 K€ • H/F**

Mission : Développer le marché des grands comptes en direct et au travers de partenaires intégrateurs. **Profil recherché :** Minimum 5 ans d'expérience commerciale chez un éditeur logiciel avec des résultats probants • Une expérience de la vente de solutions logicielles (infrastructures IT, sécurité, stockage, etc.) est indispensable • La connaissance des environnements réseau et/ou cybersecurité sera un plus à votre candidature • L'expérience de la gestion des partenaires (intégrateurs, VAD, etc.) est fortement recommandée • Un tempérament commercial fort, orienté *new business* • Force de conviction, dynamisme, sens du challenge • Autonome, organisé, vous savez adresser des interlocuteurs CxLevel (DSI, CTO, RSSI, Responsable réseau/sécurité, etc.) • Excellente capacité à présenter et à convaincre • Bon niveau rédactionnel • Chasseur dans l'âme, vous vous épanouissez dans la conquête de nouveaux clients • Connaissance générale des méthodologies de vente (Ex: MEDDIC ou autres) • Maîtrise de la langue anglaise est indispensable et une autre langue serait un plus.

Source : Apec.fr

04. Des recrutements sous tension

Certaines entreprises sont plus fragilisées donc plus vulnérables

Face aux problématiques de cybersécurité, le comportement des entreprises est très inégal. Certaines sont sensibilisées depuis longtemps aux enjeux de la cybersécurité, soit parce que leur activité est vitale pour la sécurité nationale, soit parce qu'elles ont déjà subi des cyber-attaques, soit encore parce qu'elles ont décidé de faire de la cybersécurité leur cœur d'activité.

En revanche, d'autres entreprises se sont emparées du sujet plus récemment. C'est le cas de celles se considérant peu à risque car plus petites et/ou sans réel intérêt pour les cyber-attaquants[6]. De fait, ces dernières n'ont pas l'expérience des plus matures en termes de recrutement de profils « cyber ». Diffusant moins d'offres d'emploi, elles peinent à se rendre visibles sur les *job-boards* devant l'abondance des offres émises par les ESN et les *pure-players*. Aussi leur notoriété sur le marché est moins forte, ce qui complexifie leurs recrutements. De plus, elles peuvent peiner à qualifier leurs besoins (sur quel poste recruter et recruter en priorité ? pour quelle mission ?). Enfin, elles sont souvent déconnectées de l'écosystème « cyber » (associations, formations et événements dédiés), ce qui les empêche de profiter de « l'effet réseau » que cet écosystème peut générer.

La cybersécurité pâtit d'une attractivité en demi-teinte

La cybersécurité est un domaine d'activité relativement récent comparativement à d'autres métiers de l'informatique. En effet, il continue de se structurer, tant au niveau de ses métiers que du socle de formations. Décrites comme trop rares il y a 5 ans encore, ces formations se sont étoffées pour mieux satisfaire aux besoins des entreprises. Aujourd'hui, ces formations semblent aussi intéresser de plus en plus les jeunes qui sont sensibles à la certitude de débouchés professionnels.

Pour autant, cette attractivité reste relative. Tout d'abord parce que de nombreux métiers dans l'univers de la cybersécurité demeurent méconnus. Ils restent très souvent associés au « *hacking* éthique » alors que les besoins dépassent largement ce cadre. Cette méconnaissance ne permet pas aux jeunes de se projeter sur d'autres métiers de la cybersécurité comme ceux de la GRC. De plus, les métiers de la cybersécurité renvoient souvent à l'image d'un travail solitaire et renfermé sur lui-même sans mettre suffisamment en avant toutes les interactions possibles entre les différents métiers.

Enfin, comme pour les autres domaines de l'informatique ou d'autres secteurs très techniques, la cybersécurité attire peu les femmes[7]. Seule une minorité s'oriente vers ces métiers. Si des actions sont déployées dans certains établissements pour les attirer, le chemin semble encore long pour y parvenir. Ceci pose inévitablement la question des leviers à activer pour rendre plus visibles et plus lisibles les différentes facettes de la cybersécurité.

[6] TPE / PME et la cybersécurité. Ifop, décembre 2021.

[7] Les femmes ne représentent que 18 % des effectifs cadres dans les métiers de l'informatique et 26 % dans ceux de la R&D par exemple, alors qu'elles représentent 37 % des effectifs cadres au global. Portrait statistique des femmes cadres du secteur privé, Apec / Datagora, 2022.

LE POINT DE VUE DES ENTREPRISES ET DE CENTRES DE FORMATION (EXTRAITS D'ENTRETIENS)

Dans notre filière cybersécurité, nous avons près de 500 demandes par an pour 84 places par an. Donc ça attire, mais ça reste très en deçà des besoins des entreprises. Les demandes excèdent largement notre capacité à former ces jeunes. Nous recevons des candidatures féminines. Mais elles représentent moins de 10 %. Il y a des opérations à mener dès le collège, avant que les lycéens n'abandonnent les maths, les filles en particulier.

Expert, Bretagne

J'ai discuté avec des écoles ayant des cursus en cybersécurité, notamment en région et on a créé des liens avec eux. Et en fait ils me disaient que tous les candidats qu'ils ont en alternance, et même ceux en continu, même avant de rentrer sur le marché du travail, ils ont déjà tous des opportunités, ils sont déjà tous approchés et ils ont tous trouvé leur poste avant. Cela pose question et cela veut dire qu'il faut remonter très loin si on veut des profils juniors. Et même si on a des profils, on arrive à trouver des profils mais les très bons profils à fort potentiel, les talents sont déjà repérés très loin en amont, alors même qu'ils ne sont pas encore forcément visibles sur les réseaux sociaux.

Banque-Assurance, Pays de la Loire

Ces dernières années, il y a pas mal de formations qui se sont développées en cybersécurité dans les spécialisations en école d'informatique et aussi universitaires. Et, je trouve que, durant ces deux dernières années on a eu davantage de candidatures pertinentes sur des profils juniors mais avec une petite expérience d'alternance, ou même de stage, ce qui n'était pas le cas il y a encore cinq ans. Là, je trouve que ce sont vraiment des formations qui sont développées dans des établissements d'enseignement supérieur, et qui correspondent en partie à notre besoin dans les profils juniors qu'on va recruter.

Administration, Île-de-France

Globalement, c'est assez compliqué de recruter car nous sommes localisés dans un environnement cyber assez dynamique puisqu'il y a pas mal d'entreprises, d'associations. Mais c'est très concurrentiel aussi, avec pas mal d'entreprises du secteur de la cyber qui sont à Rennes. Et comme c'est un secteur très porteur, il y a beaucoup de demandes et il n'y a pas forcément non plus énormément de candidats vu que c'est assez récent. Je pense que la demande est plus forte que le nombre de candidats disponibles. Donc ce n'est pas forcément évident de recruter. Pour autant, on y arrive, mais quand on met une annonce, ce n'est pas le genre de poste où on va avoir 80 candidatures.

ESN, Bretagne

Les profils de juniors ne sont pas si difficiles à trouver car c'est très attractif pour les jeunes : tout un imaginaire s'est développé autour du sujet et qui fait que cela attire. Il y a aussi beaucoup de formations qui se sont développées avec de très bonnes filières particulièrement adaptées aux besoins. Et donc beaucoup de collaborations avec les écoles pour recruter des alternants. A côté de celà, il y a de très grosses difficultés à recruter des profils confirmés qui eux sont très pénuriques.

ESN, Bretagne

On a surtout des besoins de haute expertise pour des profils assez rares à trouver puisqu'en cybersécurité finalement, l'ancienneté n'est pas non plus exceptionnelle par rapport à d'autres domaines.

Automobile, Île-de-France

Il est difficile de se rendre visible sur les jobboards quand on a un besoin immédiat et qu'on n'est pas une ESN.

Armement, Île-de-France

La chasse et l'alternance sont les solutions jugées les plus efficaces pour recruter

La diffusion d'offres sur les *jobboards* ou sites d'entreprise est une pratique largement partagée par les recruteurs. Mais dès lors qu'il s'agit de trouver des cadres expérimentés, c'est en identifiant les bons profils sur les réseaux sociaux et en privilégiant l'approche directe que se concrétisent la plupart des embauches. Le fait que les profils les plus prisés soient déjà le plus souvent en poste explique cette pratique.

Le recours à l'alternance est aussi de mise pour les entreprises qui veulent faire le pari de la formation et de la fidélisation de jeunes recrues. La cooptation est évoquée mais en mineur, cette pratique pouvant être « à double tranchant » pour la personne qui recommande. En effet, si le coopteur peut obtenir une prime en cas de recrutement réussi, il peut aussi perdre la confiance de sa hiérarchie dans le cas contraire.

Miser sur la montée en compétences de ressources internes est également évoqué, mais avec les contraintes que cela pose. En effet, il faut disposer de ressources pour former et accompagner les personnes intéressées, ce qui manque à nombre d'entreprises. De plus, certaines passerelles métiers sont parfois difficiles à envisager.

Quel que soit le canal utilisé pour recruter, l'entreprise doit veiller à la manière dont elle approche les candidats. Comme pour tout poste à pourvoir, la lisibilité du processus de sélection, l'inscription de celui-ci dans un temps court, et la visibilité sur la date de prise de poste sont des prérequis. Toutes les entreprises n'en ont pas forcément conscience.

Plusieurs leviers peuvent être activés pour faciliter les recrutements

Les entreprises jugent que leur attractivité se joue en premier lieu sur la rémunération proposée (fixe, variable, prime, intéressement, etc.). Sur ce registre, les plus petites se sentent très souvent en décalage par rapport aux plus grosses.

Pour autant, d'autres leviers peuvent être activés pour séduire les candidats, comme promouvoir les missions proposées. En effet, nombre de cadres recherchant un emploi sont attentifs au contenu du poste à pourvoir et au sens de ce qui leur est proposé. Les entreprises gagneraient à mettre ces éléments davantage en avant, que ce soit à travers des fiches de postes ou des témoignages par exemple.

Donner à voir sur les trajectoires et évolutions professionnelles dans l'entreprise sont d'autres moyens d'attirer des candidats. Ceci intègre la capacité de l'entreprise à proposer des temps de formation pour se perfectionner.

La qualité de vie au travail et le télétravail (lorsqu'il est rendu possible) sont d'autres éléments qui peuvent plaire aux candidats dès lors qu'ils sont mis en avant lors du processus de recrutement[8].

[8] Ces leviers ne sont pas forcément spécifiques au domaine de la cybersécurité, mais ils tiennent une place importante dans ce domaine. Cf. Études régionales d'attractivité des entreprises et emploi cadre, Apec, 2021.

QUATRE LEVIERS D'ACTION POUR LES ENTREPRISES

« Les candidats expérimentés, se trouvent quasiment uniquement par la chasse et la cooptation. Ils n'ont qu'à changer leur statut sur les réseaux sociaux, et de suite, ils sont recrutés. L'entreprise peut émettre des offres par habitude, mais ce n'est pas ça qui marche.

ESN, Bretagne

« Donc beaucoup d'approche directe et de chasse et pour le coup c'est vraiment ce qui marche, c'est d'aller vraiment prospecter.

Banque-Assurance, Pays-de-la-Loire

« Les leviers pour recruter en externe ? Déjà il y a l'entreprise en question, ensuite il y a les possibilités d'évolution au sein de l'entreprise et après il y a la partie rémunération aussi qui rentre en jeu. Après, le réseau cybersécurité, depuis quelques années maintenant, est assez petit au final et on se retrouve avec des personnes qui connaissent d'autres personnes de par leur réseau, ce qui fait que ça peut aussi être des leviers notamment en termes de cooptation. [Sinon, lors du processus d'embauche], le salaire, c'est un des premiers sujets qui est évoqué puisque forcément les candidats ont déjà un niveau de rémunération qui est assez élevé. Et si on n'est pas alignés dès le départ, ça ne sert à rien de perdre du temps.

Automobile, Île-de-France

« Nous, ce qu'on met en avant c'est notre terrain de jeu, parce que pour ces profils et sur ce domaine, il est vraiment intéressant. On a des problématiques qui sont extrêmement pointues, extrêmement innovantes, et c'est ce qu'on vend.

E-commerce, Province

« Nous vous offrons la possibilité d'évoluer, grâce à : • Un onboarding *que vous débuterez en participant à des « vis ma vie » avec l'ensemble des équipes pour que vous puissiez comprendre le métier de chacun, et comprendre également votre rôle • L'opportunité d'évoluer au sein d'une structure où il fait bon vivre (note de 4,7/5 obtenue sur Glassdoor) • Un suivi régulier pour vous accompagner dans votre montée en compétences • Déroulement des entretiens : durant ton processus de recrutement chez nous, tu auras l'occasion de rencontrer différents acteurs : tu mèneras en premier lieu un entretien avec notre chargée de recrutement. Par la suite, tu participeras à un entretien technique •Enfin, tu échangeras lors d'un entretien avec la direction.*

Offre d'un éditeur de logiciel breton pour un poste d'ingénieur cybersécurité H/F

05. Formation et innovation : les deux enjeux forts de demain

Les besoins de profils « cyber », et les difficultés pour les recruter vont augmenter

La multiplication des risques de cyber-attaques et d'erreurs humaines a accru les besoins en spécialistes de la cybersécurité. Cela devrait s'amplifier dans un contexte de tensions exacerbées au niveau international, notamment depuis le début de la guerre en Ukraine. La sécurité de l'État, des organisations (administrations publiques et OIV) et des entreprises privées impose en effet de continuer à recruter de manière importante dans ce domaine.

En termes de besoins, les spécialistes de la sécurité offensive et défensive pourraient devenir encore plus recherchés qu'ils ne le sont aujourd'hui. Les offres visant des cadres de la gestion d'incidents devraient aussi augmenter au regard des inflexions souhaitées par l'ANSSI. En effet, l'ANSSI favorise le financement des CERT (ou CSIRT) portés par les régions pour mettre en relation des spécialistes de la gestion d'incidents avec les entreprises victimes de cyber-attaques. Dans le cadre de cette décentralisation, les métiers de l'audit devraient également se développer tant leur rôle sera crucial pour évaluer la sécurité des systèmes d'information des collectivités et petites entreprises présentes en région[9].

Dans ce contexte, on devrait assister à un renforcement des tensions sur un marché du recrutement déjà très tendu.

Continuer de sensibiliser et de former reste plus que jamais un enjeu majeur

Aujourd'hui encore, continuer de développer l'offre de formation reste un impératif. Quand bien même celle-ci s'est étoffée au cours des dernières années, et même si elle est jugée plus qualitative qu'avant, certains acteurs déplorent un manque de formateurs pour pouvoir prodiguer des enseignements poussés dans le domaine. Il y a donc un enjeu fort de demain à trouver comment former davantage. Recourir à plus de consultants ou experts en cybersécurité pour former dans le supérieur, pourrait être un moyen de résoudre (même partiellement) cette problématique.

La cybersécurité applicative est décrite comme un parent pauvre de la sécurité informatique. Or les risques pesant sur l'industrie lourde (aéronautique, armement, automobile, etc.) sont plus que réels au vu des cyber-attaques passées. Pour certains experts, leur recrudescence et leur virulence sur des activités stratégiques pourraient finir par mettre à mal l'économie et par conséquent nombre d'emplois. Des synergies entre les établissements de l'enseignement supérieur et les entreprises sont à développer pour remédier à cela.

La problématique est également vraie pour l'agroalimentaire puisque l'intégrité même des produits de consommation pourrait être mise à mal par une attaque, de même que la chaîne d'approvisionnement qui va du fournisseur au consommateur final.

Le domaine de la santé est également concerné, notamment les systèmes de gestion des hôpitaux et les dispositifs médicaux connectés.

[9] Programme d'incubation de CSIRT, Anssi ; FIC 2021 : L'organisation locale de la cybersécurité à mi-parcours, Banque des territoires, Septembre 2021.

La sensibilisation des salariés aux problématiques de cybersécurité est aussi un enjeu fort de demain. Souvent mal sensibilisés, ils sont les principaux « maillons faibles » de la sécurité informatique, c'est-à-dire ceux par lesquels un virus pénètre un système (*via* l'ouverture d'une pièce jointe douteuse par exemple, ou un mot de passe peu robuste). Or, si les besoins d'expertise en « cyber » progressent fortement, les offres d'emploi cadre pour lesquelles des notions basiques de sécurité sont exigées, restent rares. Dans l'informatique par exemple, elles ne concernent que 7 % des postes à pourvoir et la proportion est infinitésimale dans les autres métiers.
Ceci plaide en faveur du développement d'actions pour sensibiliser aux règles d'hygiène numérique[10]. Leur normalisation est aussi essentielle à la filière, c'est à ce titre que les recrutements de cadres dans les métiers de la gouvernance, du management des risques et de l'audit technique des systèmes d'information sont essentiels.

La recherche et développement en cybersécurité devrait se présenter comme une opportunité pour réduire les coûts associés aux cyber-attaques

Enfin, et parce que l'ingéniosité des cyber-attaquants est sans limite et que ceux-ci ont toujours un temps d'avance sur leurs cibles, la nécessité d'aller plus loin et plus vite dans la détection et l'analyse des failles s'impose. En effet, poursuivre des investissements dans l'ingénierie-R&D mais aussi comme le supposent certains experts dans l'intelligence artificielle[11], pourrait permettre de réduire la vulnérabilité des entreprises et de limiter les coûts induits par les cyber-attaques (déficit d'image pour l'entreprise, couverture assurantielle incertaine, coût de la procédure juridique à engager contre l'attaquant, coût des pénalités juridiques en cas de manquements de l'entreprise aux réglementations, coût du préjudice en cas de vol de données, etc.).

[10] Ce qu'a fait le Pôle d'excellence cyber avec son Guide de sécurité numérique pour les collectivités, petites et moyennes organisations. https://www.pole-excellence-cyber.org/wp-content/uploads/2021/06/GuideSecurite_organisations-V1-1_WEB1.pdf

[11] https://www.journaldunet.com/solutions/dsi/1502747-l-ia-au-service-de-la-cybersecurite-quelle-part-de-mystification/

L'observatoire de l'emploi cadre

RECRUTEMENT
PRÉVISIONS
& PROCESSUS

TRAJECTOIRES
PARCOURS
& INÉGALITÉS

COMPÉTENCES
MÉTIERS
& SOCIÉTÉ

L'observatoire de l'Apec réalise des études pour mieux comprendre le marché de l'emploi des cadres et anticiper les tendances à venir, en matière de modalités de recrutement et de fidélisation, de processus de mobilité, d'évolution des métiers et des compétences.

Les études publiées s'articulent autour de trois grands axes :

> Analyser les besoins, les difficultés et les processus de recrutement des cadres ;

> Comprendre les trajectoires des cadres, leurs parcours et les inégalités qui peuvent en résulter ;

> Révéler les évolutions des métiers et des compétences des cadres en lien avec les transformations sociétales.

LES DERNIÈRES ÉTUDES PARUES DANS LA COLLECTION « COMPÉTENCES : MÉTIERS ET SOCIÉTÉ »

> Métiers cadres porteurs pour 2022, février 2022.
> Télétravail des cadres : entreprises et managers à la recherche de nouveaux équilibres, janvier 2022.
> Industrie et bâtiment du futur : quels besoins en compétences cadres et quels enjeux pour les entreprises, décembre 2021.
> L'industrie et les services à forte valeur ajoutée, mars 2022.

Toutes les études de l'Apec sont disponibles gratuitement sur le site www.corporate.apec.fr > Nos études

Suivez l'actualité de l'observatoire de l'emploi cadre de l'Apec sur Twitter : @Apec_Etudes

ISSN 2681-2835 (Collection Compétences)
ISBN 978-2-7336-1332-0

Juin 2022

Cette étude a été réalisée par la direction Données et études (DDE) de l'Apec.

Directeur de la DDE : Pierre Lamblin

Responsables du pôle études : Emmanuel Kahn, Gaël Bouron

Responsable du pôle valorisation des données : Sébastien Thernisien

Référent pour le PEC : Patrick Erard

Équipe projet : Caroline Legrand, Kaoula Ben Messaoud, Florence Kremer, Carole Rogel.

Maquette : Caracter.

ASSOCIATION POUR L'EMPLOI DES CADRES
51 boulevard Brune-75689 Paris Cedex 14

CENTRE DE RELATIONS CLIENTS
0 809 361 212 Service gratuits + prix d'un appel

DU LUNDI AU VENDREDI DE 9H À 19H
*prix d'un appel local (France métropolitaine)

Juin 2022