Michael Page
Technology

LES NOUVEAUX ENJEUX DE LA

CYBERSÉCURITÉ :

Quels **profils et compétences** recruter ?

LES **CHIFFRES-CLÉS** DE LA **CYBERSÉCURITÉ**

Taille du marché européen[1]

2020
8,56
milliards $

2027
22,67
milliards $

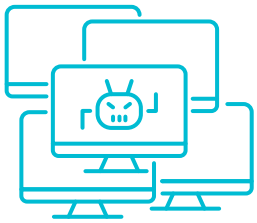
Taux de croissance estimé
+15% par an
2020-2027

Panorama des cyberattaques en 2021[2]

Panel : 6 042 entreprises dans 8 pays (Royaume-Uni, États-Unis, Espagne, Pays-Bas, Allemagne, France, Belgique et Irlande)

43%
des entreprises **ont été visées par une cyberattaque**

49%



28%
des entreprises visées **l'ont été plus de 5 fois**

22% plus de 25 fois

21% du **budget informatique** des entreprises a été **dédié à la cybersécurité** (vs 13% en 2020)

+63% en 1 an

TOP 5 SECTEURS LES + ATTAQUÉS

1. IT/Media/Télécom (56%)
2. Finance (55%)
3. Énergie (54%)
4. Construction (46%)
5. Logistique (45%)

TOP 5 PRINCIPAUX POINTS D'ENTRÉE DES ATTAQUES

1. Serveurs de l'entreprise (37%)
2. Serveurs cloud de l'entreprise (31%)
3. Site web (29%)
4. Salariés (28%)
5. Téléphones portables de l'entreprise (26%)

Conséquences des cyberattaques[2]

1 entreprise sur 6 déclare que **sa viabilité a été menacée** par une cyberattaque en 2020

6 700€
Coût médian par cyberattaque dans les TPE

250 000€
Perte moyenne subie par 5% des entreprises

1 entreprise sur 6 a reçu **une demande de rançon** suite à une cyberattaque › **58%** d'entre elles l'**ont payée**

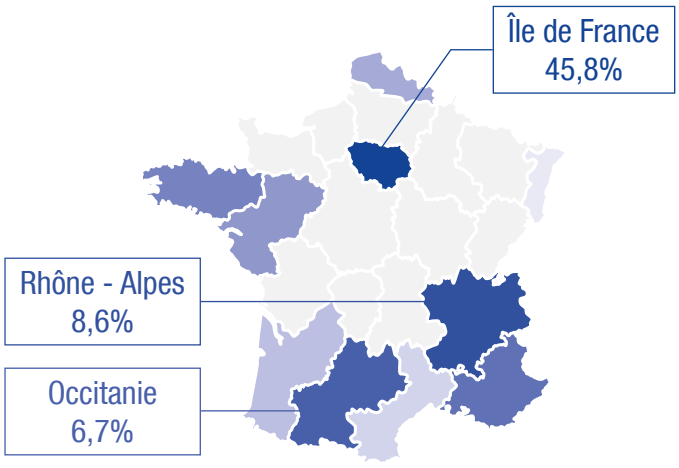
9% des entreprises affirment avoir réussi à repousser ou à remédier aux attaques dont elles ont fait l'objet avant qu'elles ne causent des dommages

Marché de l'emploi français : quelques chiffres[5]

16 048
offres d'emplois publiées en 2021
(hors stages/alternances)

+30%
vs 2020

RÉPARTITION DES OFFRES PAR RÉGION



Sources
(1) ResearchAndMarkets.com
(2) Etude Hiscox Cyber Readiness Report
(3) Page Insights – Jobfeed

Sommaire

Éditorial

Nous vivons dans un monde hyper connecté où des pans entiers de notre société sont régis par les nouvelles technologies de l'information et de la communication (NTIC). Dématérialisation des documents, hébergement de tous types de données sur le Cloud, sacre des réseaux sociaux, avènement du métavers etc., si **les NTIC sont principalement symboles de progrès et de croissance, elles n'en sont pas moins faillibles et peuvent devenir une véritable source de vulnérabilité et de forte dépendance pour les individus, les entreprises et les Etats**, comme en témoigne la hausse constante de la cybercriminalité.

La crise sanitaire, catalyseur de la digitalisation des entreprises et des cyberattaques

Ces deux dernières années, la pandémie mondiale a encore renforcé les enjeux autour de la cybersécurité car elle a non seulement imposé un recours massif au télétravail, mais elle a aussi contraint les entreprises à digitaliser leurs offres de produits, de services et leurs modes de distribution.

Ainsi, selon une étude du cabinet McKinsey [1], **la crise sanitaire aurait accéléré d'environ 7 ans la transformation digitale des entreprises**. A la sortie du premier confinement (juillet 2020), **55% des interactions clients en Europe étaient digitales** soit un bond en avant de 3 ans par rapport aux prévisions pré-crise et une augmentation de 71% depuis décembre 2019.

En parallèle, à fin 2020, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), estimait que **le nombre de victimes de cyberattaques avait été multiplié par 4 en un an** [2].

Motivations multiples et disparition des frontières : la cybersécurité est devenue un enjeu mondial

Aujourd'hui les entreprises ou les Etats sont quotidiennement victimes de cyberattaques. Au-delà de la simple volonté de nuire, ces dernières sont devenues des armes redoutables et s'enracinent dans **différentes motivations : financières, concurrentielles mais aussi doctrinales ou encore géopolitiques**, comme en témoigne la cyberguerre menée entre l'Ukraine et la Russie.

Par ailleurs, comme l'ANSSI le rappelait en mars 2022, les frontières en termes de cybersécurité ont **désormais totalement disparu**. Les organisations et les gouvernements du monde entier sont donc dorénavant tous confrontés à des défis majeurs afin de préserver l'intégrité de leurs systèmes informatiques.

Cet enjeu essentiel a d'ailleurs été bien compris par le géant du numérique Google qui a réalisé en mars 2022 l'acquisition pour 5,4 milliards de dollars de la société américaine Mandiant, spécialisée dans la détection des menaces et la réponse aux incidents en cas d'attaque.

Le capital humain au cœur des nouvelles transformations

A la lueur de ces évolutions, Michael Page Technology, entité spécialisée sur les métiers de l'IT et de l'informatique de PageGroup, leader mondial du recrutement, a interviewé des experts afin de mettre en lumière les dernières évolutions en matière de cybersécurité.

Quelles sont les tendances de fond susceptibles d'affecter la protection des données et des systèmes ? Quels sont les métiers émergents et pourquoi privilégier une approche centrée sur l'humain ? **Quels profils et quelles compétences recruter pour transformer la cybersécurité en une véritable ressource stratégique ?** Éléments de réponse dans notre livre blanc.

SACHA KALUSEVIC
Directeur Senior
Michael Page Technology

ADRIEN LEROY
Partner
Michael Page Technology

PRÉSENTATION DES EXPERTS

N.B : les experts qui partagent leur regard dans ce livre blanc s'expriment à titre personnel et non au nom de l'entité ou entreprise pour laquelle ils interviennent à titre professionnel.

KARIM SLIMANI

Business Information Security Officer
& Senior Manager
Cognizant Technology Solutions

MAX AGUEH

Directeur du Programme
« Cybersécurité, Réseaux
et Systèmes Embarqués »
EFREI*

N

Directeur Cybersécurité Opérationnel
dans le secteur du transport

H

Manager Cybersécurité
dans un grand cabinet de conseil

SACHA KALUSEVIC

Directeur Senior
Michael Page Technology

ADRIEN LEROY

Partner
Michael Page Technology

* EFREI = École d'Ingénieurs Généralistes du Numérique - ex : École Française en Électronique et Informatique. L'EFREI forme 120 étudiants en cyber et propose des programmes Experts en cybersécurité en programme continue.

Comprendre les tendances et enjeux de la cybersécurité

Un des principaux enjeux technologiques pour les entreprises et les institutions publiques réside dans la protection des données personnelles, métiers ou financières car celles-ci irriguent désormais les organisations à tous les niveaux et dans tous les secteurs.

Si les données sont violées, corrompues, subtilisées ou détournées, l'impact sur l'activité d'une entreprise peut se révéler désastreux : ralentissement ou interruption de sa production, indisponibilité temporaire ou totale de son site web professionnel, perte de chiffre d'affaires. Par ailleurs les conséquences d'une cyberattaque peuvent être amplifiées selon la place de l'entreprise dans la chaîne de valeur d'un secteur stratégique (transport de personnes, énergie, santé, ...).

UNE FINALITÉ VOIRE UN PRÉALABLE : LA PRISE DE CONTRÔLE DU SYSTÈME

La prise de contrôle à distance d'un système informatique reste une finalité voire un préalable de nombreuses attaques informatiques constatées par l'ANSSI. L'attaquant exploite des vulnérabilités généralement bien connues ainsi que les faiblesses de la sécurité des systèmes informatiques : mauvaise configuration, non-application des mises à jour de l'éditeur... , qui constituent une surface d'exposition importante aux attaques.

1 Cyberattaques : des menaces de plus en plus sophistiquées

Les menaces cyber ont considérablement évolué au cours des vingt dernières années. Alors que les virus (programmes qui attaquent d'autres ordinateurs) représentaient la principale source d'inquiétude en l'an 2000, aujourd'hui, avec l'apparition des malwares, des ransomwares, du phishing etc., **les attaques de cybersécurité deviennent chaque jour plus complexes**. Les entreprises doivent se tenir constamment à l'affût de toute tentative qui pourrait nuire à leur activité, à la sécurité de leurs clients, salariés ou à leur image.

« Prenons un exemple concret et imaginons une cyberattaque de grande ampleur au sein d'un important groupe de distribution d'électricité en France. Imaginons que le pays soit confronté à une coupure d'électricité massive et de longue durée… Pas d'éclairage, plus de chauffage, impossibilité d'utiliser les appareils électroménagers mais aussi plus d'équipements de sécurité, de téléphone, de télévision, de radio ou d'internet, … La plupart des magasins resteraient fermés, les stations essences ne fonctionneraient plus et les hôpitaux seraient dépendants de groupes électrogènes de secours. **Des catastrophes en cascade qui conduiraient à une désorganisation progressive et totale du pays.** » explique N., Directeur Cybersécurité Opérationnel dans le secteur du transport.

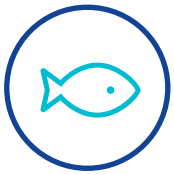
En France, suite aux attentats du 11 septembre 2001, des réflexions ont été menées au plus haut niveau de l'Etat pour définir les activités essentielles et difficilement substituables ou remplaçables, produisant et distribuant des biens ou des services indispensables au pays. En 2006, **une liste de 12 secteurs d'activité à importance vitale (SAIV) a été dressée** parmi lesquels on peut citer : l'électricité, les transports, les télécoms, la santé ou encore la gestion de l'eau. Au sein de ces derniers, **près de 250 Opérateurs d'importance vitale (OIV) ont été identifiés**. Ces acteurs publics ou privés sont **jugés indispensables au bon fonctionnement et à la survie de la Nation** et leur liste est gardée confidentielle pour des questions de sécurité nationale.

En France, la sécurité des OIV est un enjeu majeur pour l'ANSSI, qui a pour mission d'accompagner ces opérateurs cruciaux dans la sécurisation de leurs systèmes d'information sensibles. Leur cybersécurité est inscrite dans le code de la Défense et la France est d'ailleurs le premier pays à être passé par la réglementation pour mettre en place un dispositif efficace et obligatoire de cybersécurité de ces infrastructures critiques.

DÉCODER LES MENACES DE CYBERSÉCURITÉ COURANTES

MALWARE

Un « malware », aussi appelé « logiciel malveillant », s'introduit dans un réseau grâce à une vulnérabilité, généralement lorsqu'un utilisateur clique sur un lien douteux ou ouvre une pièce jointe infectée. Une fois dans le système, ce malware peut bloquer l'accès à des composantes critiques du réseau, installer des logiciels dangereux ou récupérer des informations sensibles.



PHISHING

Situation dans laquelle une communication frauduleuse se fait passer pour une communication émanant d'une source connue et réputée afin de voler des données sensibles telles que des identifiants de connexion ou des coordonnées bancaires.

ATTAQUE PAR DÉNI DE SERVICE

Ce type d'attaque submerge des systèmes, des services ou des réseaux entiers grâce à de fausses requêtes, ce qui empêche ensuite les requêtes légitimes d'aboutir. Cela entraîne un effondrement du service dans son intégralité et le rend inutilisable.

INJECTION SQL

Une injection de code SQL (Structured Query Language) est une attaque par laquelle l'auteur injecte un code malveillant dans le serveur, le forçant ainsi à révéler des informations sensibles.

ATTAQUE «MAN-IN-THE-MIDDLE»

Lors de cette attaque, des pirates interceptent des communications ou des données entre deux entités afin de les voler, les altérer ou les détruire. Elle survient généralement sur des réseaux Wi-Fi publics non sécurisés et en quelques instants.

2 … qui n'épargnent aucune entreprise ni aucun secteur

« La cybersécurité est aujourd'hui l'affaire de tous. Entre l'accélération du tournant numérique et les nouvelles méthodes de travail, **les cybermenaces se sont diversifiées et toutes les entreprises, quelle que soit leur taille, sont maintenant l'objet d'attaques malveillantes**. Ce risque n'est plus réservé qu'aux grands groupes. » annonce Max Agueh, Directeur du Programme « Cybersécurité, Réseaux et Systèmes Embarqués ».

En effet, face à la hausse permanente des risques cyber, les grandes entreprises et les ETI mettent progressivement en place des mesures de protection qui compliquent la tâche des cybercriminels. Ces derniers se rabattent donc de plus en plus sur les entreprises de petite taille, souvent moins bien équipées et plus fragiles.

43%

des PME ont connu au moins un incident de cybersécurité en 2020 (3)

71%

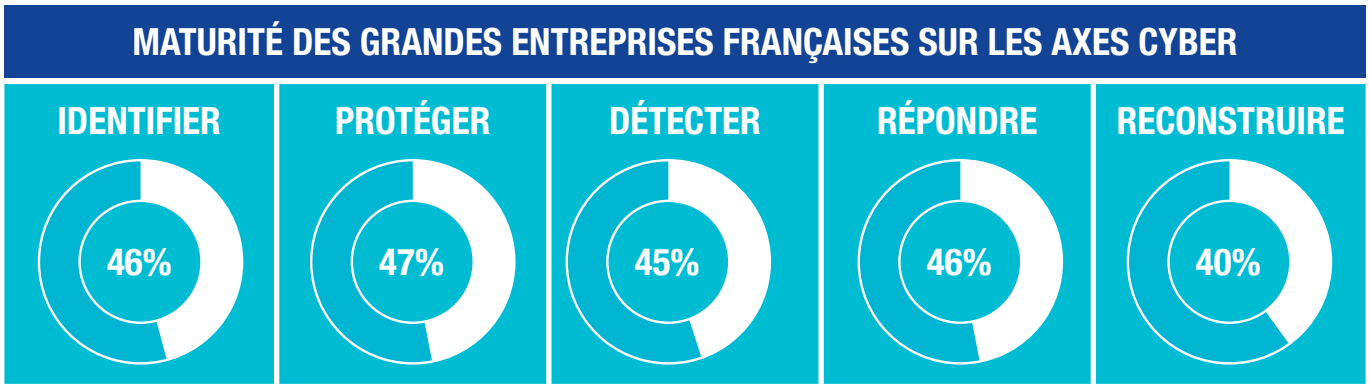
des TPE et PME qui font l'objet d'une cyberattaque ne s'en remettent pas (4)

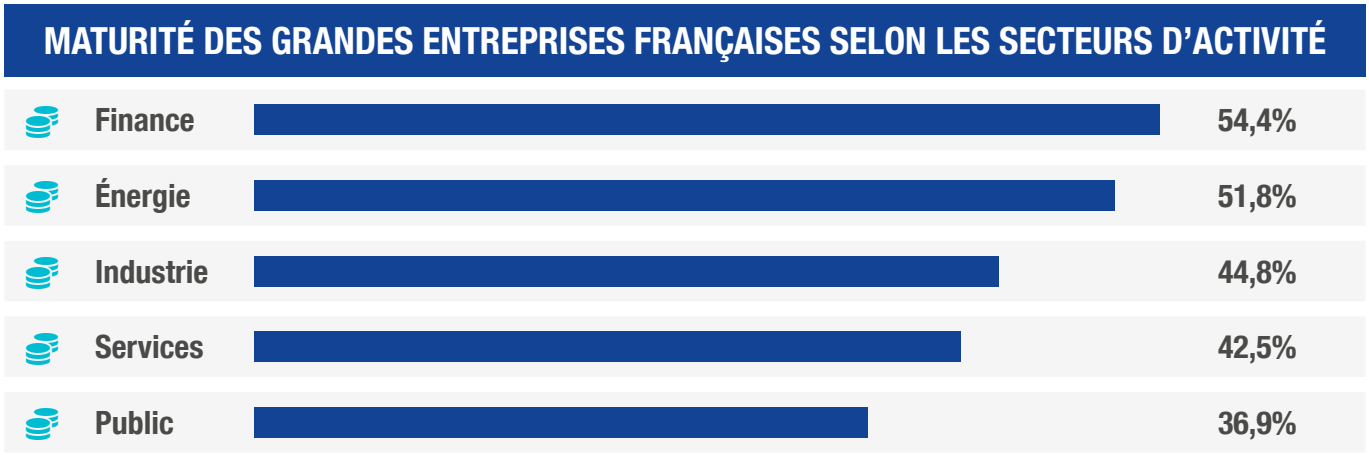
« Les attaques sur les PME représentent également un risque supplémentaire pour les entreprises de plus grande taille dans le sens où celles-ci sont bien souvent les fournisseurs ou les sous-traitants des secondes. Cela crée un effet domino dangereux qui peut en rebond affaiblir la cybersécurité des grands groupes ou ETI. » explique Adrien Leroy, Partner Michael Page Technology.

4 entreprises sur 5 ont expérimenté une compromission de cybersécurité due à une vulnérabilité touchant l'écosystème de leurs fournisseurs tiers (5)

Si à première vue, les grandes entreprises semblent moins vulnérables que les petites, elles sont pourtant loin d'être exemptes de tout cyber risque. « Certes, en cas d'attaque malveillante, les grands groupes ont une capacité de réaction supérieure à celle d'une PME mais le risque intrinsèque de voir son activité amputée ou totalement stoppée par une cyberattaque est le même pour tous. De plus, par leur notoriété, ils sont davantage visibles et donc plus exposés. Aujourd'hui, leur niveau de protection est loin d'être suffisant. » explique, N, Directeur Cybersécurité Opérationnel dans le transport.

Dans sa dernière étude [6], le cabinet Wavestone estime ainsi que le niveau de maturité cyber des grandes organisations françaises atteint seulement 46%. Une donnée moyenne qui cache par ailleurs des disparités assez importantes selon les secteurs.





3 Accélération de la décentralisation de la cybersécurité

Au cours de la décennie écoulée, les progrès technologiques tels que la 5G, l'Internet des objets, le Cloud ainsi que la transformation numérique ont accéléré la décentralisation de la cybersécurité. « La cybersécurité était plutôt simple avant. Vous placiez tout ce que vous souhaitiez protéger sur un ordinateur ou un serveur puis vous bâtissiez une muraille virtuelle, ou un pare-feu, tout autour. Aujourd'hui, il ne suffit pas de sécuriser un périmètre donné car les frontières des réseaux disparaissent peu à peu et la mise en place de certains outils habituels devient caduque. » explique Sacha Kalusevic, Directeur Senior Michael Page Technology.

« Le monde de l'entreprise a accueilli à bras ouverts le mode de fonctionnement tout numérique mais n'a pas forcément mis en place les contrôles appropriés, ce qui a multiplié les cyber risques. Les nouveaux enjeux sécuritaires requièrent maintenant un **système de défense qui met l'accent sur l'articulation de la protection entre plusieurs équipements**, ce qui renforce le système dans son intégralité. » ajoute H, Manager dans un grand cabinet de conseil.

Récemment, **la pandémie du COVID-19 a contraint les salariés à utiliser massivement leurs équipements professionnels à leur domicile**, ce qui a multiplié les points d'attaque potentiels, **les connexions internet privées faisant maintenant partie du réseau des entreprises**. Les organisations doivent donc s'armer à plusieurs niveaux en renforçant à la fois la sécurité de leurs outils informatiques mais aussi en sensibilisant et formant leurs salariés pour faire évoluer leurs comportements.

« Il faut également noter que les nouvelles technologies font sans cesse évoluer les usages des objets. Ainsi un téléphone portable, qui servait autrefois uniquement à téléphoner, a aujourd'hui de multiples nouveaux usages : surfer sur le web, consulter ses comptes, acheter en ligne, … Autant de possibles brèches de sécurité qui n'avaient pas été anticipées au moment de leur conception, celle-ci étant, parfois antérieure à l'émergence de la cybercriminalité, ou à la prise en compte des risques réels. » explique N, Directeur Cybersécurité Opérationnel dans le transport. « Les nouveaux usages entraînent automatiquement de nouveaux risques et forcent à développer de nouveaux systèmes de protection. Il existe trois axes de veille technologique : les nouveaux scenarii d'attaques, les nouvelles menaces, les nouveaux usages. Cela amène les experts en cybersécurité à constamment innover sur les usages et à constamment anticiper les nouveaux modes de consommation ».

Demain, avec le développement de la 5G et des objets connectés par exemple, nous devons nous préparer à de nouveaux risques. « Imaginez les conséquences du piratage d'une flotte de véhicules autonomes, cela pourrait porter directement atteinte à l'intégrité physique des personnes. Instrumentalisé, ce scénario pourrait être motivé par des fins terroristes » cite H.

4 Migration Cloud : sécuriser le recours à des prestataires externes

Avec l'avènement du Cloud, **nous assistons à une révolution au niveau du stockage des données** des entreprises. Si auparavant, la plupart des sociétés géraient ce patrimoine informationnel sur des serveurs internes, localisés dans leurs locaux et gérés par leurs équipes informatiques, elles sont aujourd'hui de plus en plus nombreuses à **s'orienter vers des prestataires externes ou des services numériques externalisés insuffisamment sécurisés** et qui représentent une faille que les attaquants ne manquent pas d'exploiter. Les entreprises ne peuvent donc pas s'exonérer de ressources spécialisées afin de veiller à la bonne sécurisation des flux gérés par les partenaires externes.

« Afin de limiter les risques de sécurité inhérents au Cloud, les bonnes pratiques recommandent aux entreprises d'évaluer régulièrement l'étendue des services confiés aux prestataires du nuage. Ces revues doivent être effectuées en fonction des évolutions des technologies adoptées pour accéder et exploiter les services du Cloud, des nouvelles typologies de cyberattaques et surtout des nouvelles formes de menaces. » déclare Karim Slimani, Business Information Security Officer & Senior Manager.

5 Un enjeu national et international

Le 15 mars 2022, le président des États-Unis, Joe Biden, a signé une nouvelle loi en matière de cybersécurité. Celle-ci oblige maintenant les entreprises traitant des infrastructures critiques sur le territoire américain à signaler toute cyberattaque importante à la CISA (Certified Information Systems Auditor) dans les 72 heures et tous les paiements de rançongiciels dans la journée. Par cette nouvelle législation, la cybersécurité n'est définitivement plus considérée comme l'affaire privée d'une seule entreprise mais bien comme une menace publique pouvant nuire à tous.

« Aujourd'hui, plusieurs pays sont réputés pour leurs technologies en matière de cybersécurité. On peut citer les États Unis, Israël, la Chine ou encore la Russie qui dispose du plus grand contingent d'experts en ce domaine. Le problème est qu'il est pour le moment impossible d'envisager une union ou coordination mondiale tant les motivations régionales sont divergentes. La guerre entre la Russie et l'Ukraine en est le parfait exemple. » déclare Sacha Kalusevic.

Face à la menace cyber, certaines zones ou pays arrivent toutefois à se regrouper pour unir leurs forces et mettre en place des réglementations qui visent à protéger les entreprises et les citoyens. C'est le cas de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis qui à travers l'agence Five Eyes (FVEY), l'alliance des services de renseignement de ces pays créée après la seconde guerre mondiale, échangent maintenant des informations et des recommandations en matière de cybersécurité. « En Europe, l'Allemagne et la France sont largement moteurs sur le sujet et le RGPD, Règlement européen sur la protection des données, entré en vigueur en 2018, est un bon exemple d'initiative locale de contrôle des données. » explique N.

Plus récemment encore, à la demande de l'Ukraine, les équipes européennes de la Cyber rapid response team and mutual assistance in cybersecurity (CRRTs), se sont mobilisées pour aider les institutions du pays victime de cyberattaques. Une dizaine d'experts en cybersécurité ont ainsi été réunis par six États membres de l'UE - Croatie, Estonie, Lituanie, Pays-Bas, Pologne et Roumanie.

Face à des cybermenaces de plus en plus importantes et ne connaissant pas de frontières, un des défis majeurs reste de réussir à faire travailler les états ensemble.

Sources :

(1) Etude McKinsey

(2) Etude ANSSI

(3) Rapport Sénat - La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?

(4) Etude Symantec

(5) Rapport Acronis

(6) Etude Wavestone

Quels recrutements et quelles compétences clés pour protéger son entreprise ?

Entre l'accroissement de la digitalisation des échanges et des transactions et la complexification des cyberattaques, **le besoin de professionnels qualifiés n'a jamais été aussi important**.

« La menace sur les systèmes d'informations n'a jamais été aussi forte. Face à notre dépendance aux nouvelles technologies et à la hausse de la cybercriminalité, les entreprises et les institutions gouvernementales n'ont pas d'autre choix que de recruter massivement des experts en cybersécurité afin de garantir la disponibilité, l'intégrité et la confidentialité des données qui leurs sont confiées. » explique Karim Slimani.

1 Privilégier une nouvelle approche centrée sur l'humain

« **Aucune solution n'est sécurisée à 100 %** et les efforts consentis chaque jour ne permettront jamais une sécurisation totale des systèmes d'information car le risque humain restera toujours présent et imprévisible. » explique H, Manager dans un grand cabinet de conseil. « Aujourd'hui, si la grande majorité des vulnérabilités de la cybersécurité résulte d'un comportement humain, **l'homme reste pourtant la première ligne de défense contre de telles attaques. Il est crucial de sensibiliser fréquemment l'ensemble des collaborateurs pour réduire les risques.** »

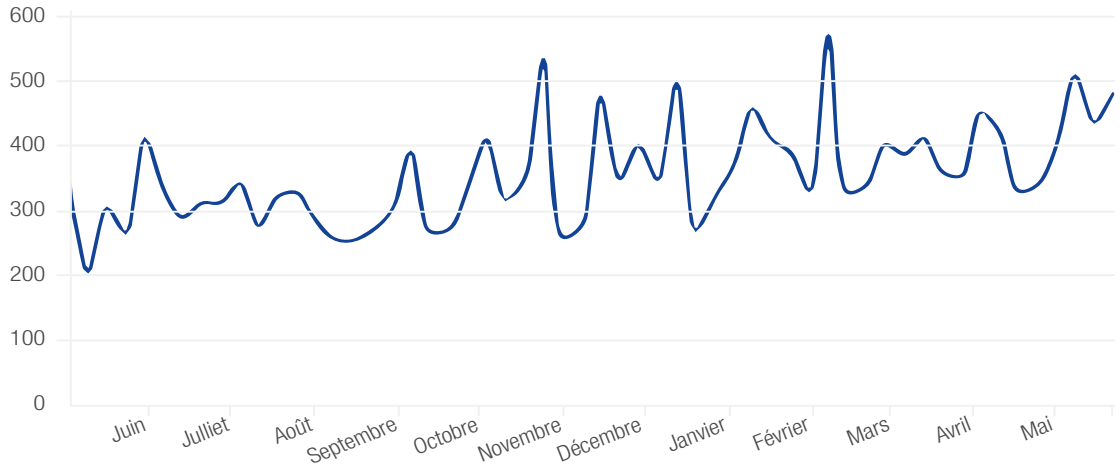
« En matière de cybersécurité, il faut investir sur l'humain. » ajoute Max Agueh, Directeur du Programme « Cybersécurité, Réseaux et Systèmes Embarqués ». « Cela va améliorer la sécurité de manière générale et donc minimiser les investissements nécessaires dans le domaine des outils. La cybersécurité ne peut pas se concentrer uniquement sur des aspects techniques, elle doit adopter une approche holistique permettant d'articuler au mieux les infrastructures et le personnel. Il est par exemple intéressant de disposer de référents métiers en interne, bien identifiés par tous les collaborateurs. **Il ne faut plus voir la cybersécurité comme un centre de coût mais véritablement comme une ressource.** »

« Les pirates utilisent des techniques de plus en plus sophistiquées et personnalisées afin de tromper les individus. Il faut donc former les salariés à reconnaître ces mécanismes et à déterminer si quelque chose sort de l'ordinaire. Il est important de faire des rappels réguliers des bonnes pratiques d'hygiène informatique au sein de l'entreprise, afin que chacun soit sensibilisé. **Les solutions doivent être invisibles et non intrusives.** » explique Sacha Kalusevic.

« La cybersécurité n'est pas un coût, c'est une assurance. Pourquoi souscrire une assurance ? Parce que si quelque chose venait à vous arriver, vous voulez avoir un filet de sécurité. Ici, c'est la même idée. Vous mettez en place des mesures de sécurité non pour éviter qu'un incident ne se produise, mais pour pouvoir y faire face le cas échéant. Ce n'est pas quand il est trop tard qu'il faut agir. » conclut Adrien Leroy.

2 Un besoin croissant d'experts cyber sur le marché de l'emploi

20 036 offres d'emploi en cybersécurité ont été publiées entre mai 2021 et mai 2022 (7)



« La tension sur les métiers cyber a toujours été importante et elle se renforce au fil des mois car il existe un **déficit de compétences cyber à tous les niveaux et dans tous les secteurs**» déclare Adrien Leroy. « Cette pénurie structurelle s'explique par deux raisons majeures : d'une part il n'y a pas assez d'experts ou de jeunes diplômés chaque année pour répondre aux demandes croissantes des entreprises et d'autre part, face aux nouvelles menaces qui apparaissent, on perçoit toujours un manque d'adéquation entre les formations et les compétences dont les entreprises ont besoin. »

« Le **phénomène de 'time to market' incompressible entre les besoins des entreprises, les cursus de formations et l'arrivée des jeunes diplômés sur le marché du travail** est particulièrement remarquable. Dans les écoles, nous ne pouvons pas constamment former les étudiants pour s'adapter aux nouvelles attentes des organisations ; **il est crucial que les entreprises misent et travaillent sur la formation continue**. » ajoute Max Agueh.

« Par exemple, avant qu'un jeune diplômé soit mature sur un poste en SOC (Security Operations Center), il faut 3 à 6 ans d'expérience. Or comme la menace est exponentielle, la demande est également exponentielle. » pointe N.

« Ce phénomène de pénurie des talents frappe tous les pays. » ajoute H. « **La cybersécurité est un enjeu global et de nombreux pays cherchent à attirer des experts étrangers.** Les pure players aux Etats-Unis offrent notamment des avantages très concurrentiels. A l'inverse, les entreprises françaises ont encore pour le moment du mal à recruter des talents à l'international. »

3 Les compétences techniques les plus recherchées aujourd'hui

« Il y a dix ans, les besoins en recrutement concernaient principalement des profils d'Architectes et de Pentesters. **Aujourd'hui, les organisations recherchent des experts avec une double casquette qui peuvent à la fois comprendre les enjeux business et maîtriser les questions techniques.** Leur quotidien va de plus en plus s'articuler autour d'une communication et d'une approche par les risques face à des populations de type C-level, ainsi que d'une réelle capacité à challenger techniquement les équipes opérationnelles. Les missions de conseil que nous gérons traitent de sujets très opérationnels jusqu'à la gouvernance des entreprises. » analyse H.

10 COMPÉTENCES EN FORTE CROISSANCE DANS LA CYBERSÉCURITÉ* (8)	
Normes ISO	+ 64%
Microsoft Azure	+ 64%
Produits Dockers	+ 49%
Règlement général sur la protection des données	+ 35%
Analyse des risques	+ 33%
Python	+ 31%
Test d'intrusion	+ 26%
Cryptographie	+ 21%
Audit sécurité	+ 20%
Gestion des identités et des accès	+ 19%

« **Les compétences les plus recherchées sur le marché aujourd'hui gravitent toutes autour de la sécurité opérationnelle.** La gouvernance cybersécurité attire quant à elle des profils beaucoup plus expérimentés donc plus dispendieux pour les entreprises. » ajoute Karim Slimani.

Si les fonctions régaliennes autour de la cybersécurité restent très prisées, « on note **une demande croissante en termes de recrutement à destination des Devsecops**, ressources dont la mission est d'intégrer la sécurité à toutes les étapes du développement continu. Il s'agit là plus d'un framework de méthodes et de process que de solutions technologiques » cite H.

4 Soft skills : un attrait grandissant pour les profils aux compétences transverses

« Soyons honnête, encore récemment, pour de nombreuses entreprises, recruter un spécialiste en cybersécurité consistait avant tout à acheter une expertise technique. Or si hier, les fonctions cyber évoluaient plutôt en vase clos au sein d'une DSI, elles sont maintenant de plus en plus exposées vis-à-vis des utilisateurs et doivent de fait **démontrer une réelle aptitude à vulgariser leur métier**. Dorénavant, les qualités humaines, et notamment la **capacité à communiquer et faire le lien avec différents services** d'une organisation, sont donc considérées avec attention par les recruteurs. » analyse Adrien Leroy.

Aujourd'hui, les directions générales cherchent à anticiper et à réduire au maximum les risques opérationnels d'une cyberattaque, elles souhaitent **des profils capables de parler GRC** (Gouvernance, Risques et Compliance) à des directions métiers. Le spécialiste cyber doit faire preuve d'une plus grande **curiosité** et s'intéresser à l'ensemble des métiers de l'entreprise afin de **bien identifier les enjeux opérationnels d'une potentielle menace cyber**. Pour avoir cette vision globale de son environnement interne, cela nécessite pour lui de prendre de la hauteur sur des sujets purement techniques et adresser les besoins entrants avec **un regard très fonctionnel, pragmatique et accessible**. Dans la mesure où la principale source de menace reste l'utilisateur lui-même, l'expert cybersécurité doit faire preuve d'une grande **écoute** et **ouverture d'esprit**, et ainsi se mettre au niveau des opérationnels pour échanger de manière audible sur leur processus métiers et les bonnes pratiques en termes d'accès et d'utilisation au SI.

Par ailleurs, inévitablement, il doit continuer à développer de solides compétences techniques pour pouvoir challenger les équipes IT ainsi que les prestataires éventuels. Il doit donc faire preuve de **prise d'initiative pour s'autoformer ou mettre en place des actions qui visent à développer ses compétences techniques** régulièrement.

QUI SONT LES PROFESSIONNELS DE LA CYBERSÉCURITÉ EN FRANCE ? (9)

89% **Hommes**

11% **Femmes**

60% **entre 30 et 49 ans**

Ils travaillent

90% en **CDI**

73% Dans le **secteur privé**

53% Dans une **structure de 1000 salariés et +**

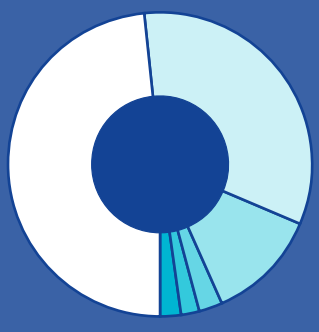
Ils sont trés qualifiés

72% ont un **diplôme équivalent ou supérieur à Bac +5**

Ils ont peu d'expérience dans le domaine de la cybersécurité

45%
Moins de 5 ans d'ancienneté

Domaine d'expertise d'origine



- Informatique numérique hors cybersécurité 48,6%
- Cybersécurité 33%
- Juridique, audit, adminstratif et qualité 11,9%
- Marketing/Vente/Communication 2,5%
- Sécurité / Sureté 2%
- Gestion du risque 2%

Ils vivent

+ de 50% en **Île-de-France**

25% en Bretagne, Occitanie, Auvergne-Rhône-Alpes et Nouvelle-Aquitaine

5 TOP 10 des métiers et des rémunérations de la cybersécurité

Si les salaires d'embauche en début de carrière se situent déjà dans la fourchette haute des salaires d'entrée sur les métiers IT, nous constatons une **véritable accélération des packages salariaux proposés aujourd'hui**.

En effet, la cybersécurité reste un sujet « récent », les professionnels présentant des expériences de plus de dix ans sont rares et cette rareté renforce leur valeur sur le marché français.

Compte tenu des transformations en cours, et des évolutions des cyber menaces, ce phénomène de rareté devrait perdurer a minima sur les cinq années à venir. De quoi encourager les plus jeunes à se spécialiser dès aujourd'hui dans les métiers porteurs de l'informatique, et plus spécifiquement la cybersécurité

TOP 10 DES POSTES DE LA CYBER (H/F)*

RÉMUNÉRATION ANNUELLE BRUTE EN K€

	0 à 2 ans	2 à 5 ans	5 à 10 ans	10 à 15 ans
Auditeur	38 - 47	45 - 65	60 - 90	90 - 120
Cryptologue	38 - 48	45 - 65	60 - 90	80 - 120
Analyste SOC	38 - 50	45 - 70	60 - 80	70 - 100
Ingénieur Cybersécurité Cloud	40 - 50	50 - 70	65 - 90	80 - 110
Pentester	40 - 55	50 - 75	65 - 90	80 - 120
Analyste CSIRT / CERT	40 - 55	47 - 75	65 - 90	80 - 110
Ethical Hacker	45 - 60	55 - 80	70 - 100	90 - 130
Devsecops	-	45 - 70	65 - 85	80 - 100
Architecte Cybersécurité	-	-	70 - 110	90 - 150
CISO (Chief Information Security Officer)	-	-	70 - 100	90 - 140

N.B : les rémunérations présentées correspondent à des salaires fixes (hors bonus et avantages annexes), pour des postes situés en région parisienne.
*Données PageGroup

La connaissance de certaines solutions propres à la cybersécurité (Vault, CyberArk, F5, Palo Alto, …) ainsi que des certifications associées peuvent aisément « booster » la rémunération d'un candidat.

Par ailleurs une spécialité dans la sécurité de flux Cloud (Azure, AWS, GCP etc.), ou la maîtrise des contraintes réglementaires propres à certains secteurs d'activité peuvent également être fortement valorisées.

Des packages de rémunérations qui varient selon la taille de la structure

Sans surprise, les **cabinets de conseils et les pure players proposent les packages de rémunérations les plus intéressants du marché**, tant sur les rémunérations fixes que par la mise en place de plans de carrière bien balisés : augmentation significative tous les ans, changement de grades et attribution de nouvelles responsabilités (notamment managériales), formations et certifications, … Des pratiques non seulement très appréciées des candidats en recherche mais qui favorisent également la rétention des talents.

Si les packages de rémunérations fixes des **grands comptes** sont souvent un peu moins élevés que ceux des pure players ou des cabinets de conseil, **ils compensent en général les éventuels écarts par des mécanismes de rémunération variable ou le financement de formations et de certifications spécialisées**. Des avantages annexes particulièrement appréciés par les candidats et qui sont aujourd'hui un levier d'attractivité significatif. Sur un marché particulièrement pénurique, on note également une alternative à l'embauche de ressources en externe, qui consiste à proposer à des collaborateurs internes une reconversion vers les métiers de la cybersécurité moyennant un plan de formation spécialisé.

Les PME, peu habituées à recruter à des niveaux de salaires aussi élevés, rencontrent parfois des difficultés à justifier auprès des autres collaborateurs la rémunération d'un spécialiste cybersécurité. « Afin d'éviter de possibles tensions en interne et de palier à la pénurie de talents disponibles sur le marché, **de nombreuses PME préfèrent aujourd'hui faire appel à des prestataires externes spécialisés**. » explique Sacha Kalusevic.

Quel salaire pour un jeune diplômé ou un profil débutant ?

Un **jeune diplômé, issu d'une école d'ingénieur ou équivalent universitaire, qui entre sur le marché du travail avec une première expérience significative** (stage de fin d'études ou une alternance probante dans le domaine de la cybersécurité) peut aisément prétendre à une **rémunération annuelle fixe entre 40 et 45K€** en fonction de sa localisation (région parisienne ou province).

Enfin, il est important de préciser qu'au sein de pure players ou de cabinets de conseil spécialisés, les salaires s'envolent très vite, même pour les professionnels en début de carrière.

Comment attirer et fidéliser les experts cyber ?

Séduire passe par le changement et l'innovation. Sur un marché en pleine mutation, l'expert cybersécurité entreprend d'abord de valider le niveau de maturité de son futur employeur en termes de sécurité. Beaucoup cherchent à contribuer à la **professionnalisation de leur entreprise** sur le sujet et il faut pouvoir les **rassurer, au-delà des ambitions, sur les moyens (organisationnels et financiers) alloués à la sécurité pour avancer**. L'autre levier de motivation exprimé est celui de l'**innovation technologique**. Les instruments et méthodologies liés à la sécurité évoluent en permanence et le collaborateur doit se sentir libre de pouvoir suggérer des pistes d'innovation pour améliorer l'existant.

LES MÉTIERS ÉMERGENTS OU EN MUTATION DE LA CYBER

CYBER CHAMPION

Rôle émergent au sein des services Dev ou Ops, le Cyber Champion a pour mission d'éduquer les équipes et de les sensibiliser aux cyber risques mais aussi de passer en revue les défauts de sécurité et de les escalader afin de les résoudre. « Ce métier devient crucial car les organisations sont de plus en plus complexes et les configurations agiles prennent de plus en plus de place dans le développement de projets. » explique Karim Slimani.

EXPERT SÉCURITÉ CLOUD

Que le modèle soit public, privé ou hybride, l'Ingénieur Sécurité Cloud a pour principale mission d'assurer la sécurisation des données et des flux hébergés dans le Cloud, quel que soit l'opérateur de services. Il doit également veiller à la bonne sécurisation des conteneurs et évaluer les risques tant opérationnels que techniques associés. De fait il est régulièrement amené à auditer ses fournisseurs sur leurs capacités à répondre aux exigences de sécurité, voire réglementaires, imposées par l'entreprise" analyse Adrien Leroy.

GRC : L'AUDITEUR ORGANISATIONNEL

L'Auditeur GRC (Gouvernance, Risques et Compliance) devient une pièce maîtresse dans l'efficacité du dispositif de sécurisation du système d'information. Il veille au respect de standards fixés par les entreprises au niveau des organisations (qui est responsable de quoi ?), des processus (notamment dans le cadre de projets de certification ISO), de la cartographie et la gestion des risques (opérationnels comme techniques), et enfin de l'adéquation des solutions avec risques identifiés. C'est l'auditeur 360° en termes de cybersécurité.

INGÉNIEUR RÉSEAU

« La fonction d'Ingénieur Réseau mute également au profit du 'Zerotrust Network Control'. Cette philosophie du 'je ne fais confiance à personne', impliquant une segmentation très forte du réseau interne, est déployée par l'Ingénieur Réseau qui doit désormais gérer de nouvelles solutions et procédures d'authentification en point à point. » ajoute H.

Sources :

(7) Page Insights – offres en CDI, CDD, Intérim ou Freelance

(8) Linkedin Talent Insights

(9) Enquête les profils de la cybersécurité

A propos de Michael Page Technology

Cabinet de recrutement leader en nombre d'offres d'emploi cybersécurité*

RÉPONDRE À VOS ENJEUX TECHNOLOGIQUES GRÂCE À NOTRE EXPERTISE HUMAINE ET À LA PERFORMANCE DE NOS OUTILS

- Nos équipes sont composées d'experts en recrutement de profils Tech/IT qui vous accompagnent dans vos recrutements en **CDD, CDI, Freelance, Management de Transition ou Intérim**.
- Pour renforcer la relation de confiance et la connaissance de votre environnement, un **seul et unique recruteur gère l'intégralité** de vos enjeux de recrutement Tech et IT.
- Vos projets sont uniques et requièrent une solution sur mesure. Nous sommes convaincus que la réussite à long terme de vos recrutements passe par l'**expertise métier** de nos équipes et par l'**intelligence émotionnelle** de nos consultants.

NOUS RECRUTONS DANS TOUS LES DOMAINES TECHNOLOGIQUES :

Infrastructure, Cloud & Systèmes d'Information

Développement Front, Back, Fullstack

Intelligence Artificielle Data/Big Data, Digital

Cybersécurité & Sécurité Informatique

NOS ATOUTS :

Sur un marché de l'emploi Tech et IT particulièrement sous tension, notre position de leader et nos spécialisations vous apportent :

- Une expertise recrutement associant hard skills et soft skills
- Des outils de sourcing innovants et exclusifs sur le marché
- Une approche de recrutement/conseil bienveillante avec les candidats
- Un interlocuteur unique sur vos recrutements pour une expérience client personnalisée
- La puissance de PageGroup avec l'agilité d'une start-up

NOTRE EXPERTISE :

16 000 entretiens réalisés chaque année

1 200 recrutements par an

450 000 profils dans notre base de données

60 consultants

Grâce à notre connaissance approfondie des spécificités locales, nous vous aidons à recruter rapidement les meilleurs candidats qualifiés, sur l'ensemble du territoire grâce à nos **10 bureaux en France** : Bordeaux, Lille, Lyon, Marseille, Nantes, Neuilly-sur-Seine, Nice, Rennes, Strasbourg, Toulouse.

*Source Page Insights : nombre d'offres publiées entre Janvier-Juin 2022

PageInsights

PAGE INSIGHTS, NOTRE SOLUTION DE VEILLE

Page Insights est notre outil de business intelligence, qui exploite de nombreuses données internes et externes pour générer des informations précieuses pour nos clients sur le marché de l'emploi. Nous pouvons ainsi vous aider à prendre les décisions les plus éclairées possibles.

Nos rapports sur mesure peuvent inclure notamment :

- Cartographie du marché
- Informations sur les salaires
- Analyse des concurrents
- Rôles les plus demandés.

VOUS CHERCHEZ À RECRUTER DES PROFESSIONNELS DE L'IT ? CONTACTEZ-NOUS !

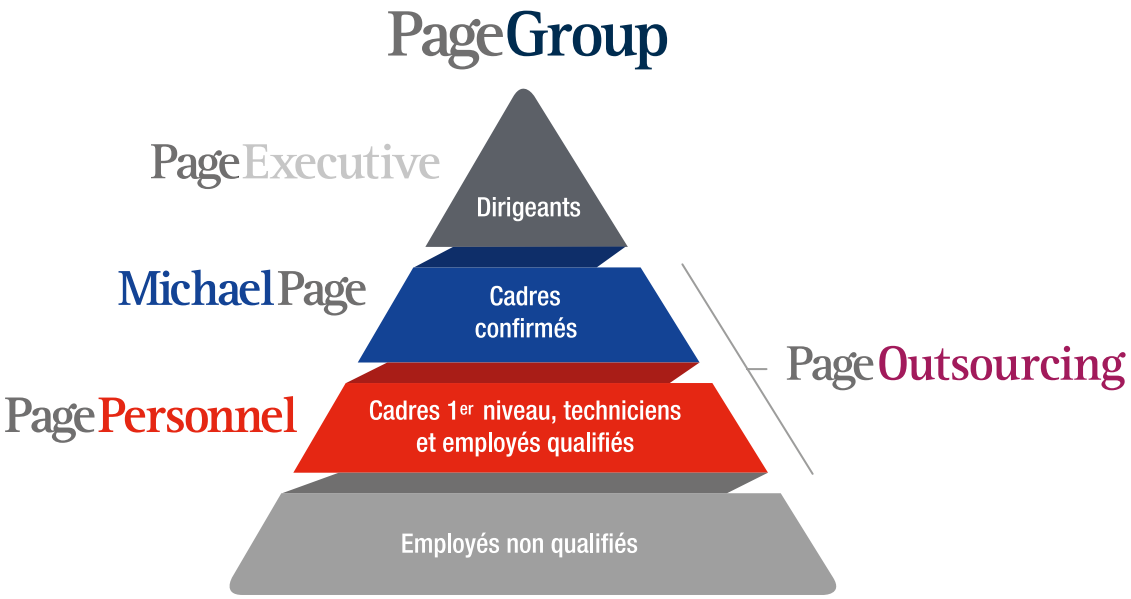
www.pageexecutive.com

www.michaelpage.fr

www.pagepersonnel.fr

www.pageoutsourcing.com

NOS BUREAUX À PARIS ET EN RÉGION



ÎLE-DE-FRANCE

Cergy
Immeuble Grand Axe
10, boulevard de l'Oise
95000 Cergy
01 30 75 31 32

Massy
Immeuble Odyssée – Bâtiment E
2-12, chemin des Femmes
91300 Massy
01 64 86 47 70

Neuilly-sur-Seine
164, avenue Achille Peretti
92200 Neuilly-sur-Seine
01 41 92 70 70
01 78 99 48 48

Noisy-le-Grand
16, boulevard du Mont d'Est
Bâtiment Maille Nord 4
93160 Noisy-le-Grand
01 55 85 12 85

Paris Bercy
Bâtiment Vivacity
151-155, rue de Bercy
75012 Paris
01 44 75 25 97
01 44 75 25 40

Roissy
Paris Nord 2 – Immeuble Le Cézanne
35, allée des Impressionnistes
93420 Villepinte
01 48 17 92 70

Montigny-le-Bretonneux
Immeuble Le Sésame
8, rue Germain-Soufflot
78180 Montigny-le-Bretonneux
01 30 84 10 84

PROVINCE

Bordeaux
Bâtiment Le Cap Horn
123 rue Lucien Faure
33000 Bordeaux
05 56 90 26 50

Grenoble
Immeuble « Les Reflets du Drac »
1er étage du Pavillon B
32-34, rue Gustave Eiffel
38000 Grenoble
04 76 70 94 00

Lille
1, rue Esquermoise
59800 Lille
03 28 04 56 20
03 20 16 10 60

Lyon
48, rue de la République
69002 Lyon
04 78 92 30 00
04 72 77 38 40

Marseille
Immeuble Astrolabe
Place Henri-Verneuil
79, boulevard de Dunkerque
13002 Marseille
04 86 94 78 50

Monaco
Talaria Business Center – Le Mercator
7, rue de l'Industrie, Fontvieille
98000 Monaco
+377 99 99 47 38

Nantes
3, rue Menou
44000 Nantes
02 72 22 98 60
02 72 22 98 80

Nice
Arenas – Immeuble l'Aéropôle – Hall A
455, Promenade des Anglais
06200 Nice
04 89 41 01 80
04 86 94 78 50

Orléans
12, rue de la République
45000 Orléans
02 34 59 33 44

Rennes
13 ter, place des Lices
35065 Rennes
02 99 78 00 10

Rouen
43 bis, rue Jeanne d'Arc
76178 Rouen
02 32 10 21 60

Strasbourg
1, place Gutenberg
67000 Strasbourg
03 90 22 70 00
03 88 22 82 30

Toulouse
36, rue d'Alsace-Lorraine
31000 Toulouse
05 34 25 56 25
05 82 74 00 10

Michael Page

Technology