Cybersécurité

Un secteur stratégique en plein essor, confronté à des défis de légitimité, de financement et de recrutement

Cybersécurité

Un secteur stratégique en plein essor, confronté à des défis de légitimité, de financement et de recrutement

La multiplication des cyberattaques, liée à la généralisation du télétravail durant l'année 2020 marquée par la pandémie de Covid-19, a confirmé l'importance des questions de cybersécurité et les lacunes en la matière. Le secteur, déjà en croissance depuis plusieurs années, a vu son activité s'accélérer tant auprès des entreprises privées que des organisations publiques. Après une transformation numérique réalisée dans l'urgence de la crise sanitaire, ces dernières devraient privilégier à l'avenir la sécurité de leurs réseaux et de leurs données, profitant ainsi au marché de la cybersécurité.

Portées par de grands groupes du numérique ou de la défense mais également par une multitude de start-up, toujours plus nombreuses, les activités de cybersécurité peuvent compter sur un soutien massif de l'État. Les acteurs se mobilisent et s'organisent en un écosystème réunissant des entreprises, des centres de recherche ou de formation et des investisseurs privés comme des structures publiques.

Le secteur doit cependant faire face à plusieurs écueils, dont un manque de personnel qualifié de plus en plus critique. Un financement parcellaire, notamment concernant les jeunes sociétés les plus prometteuses, l'expose par ailleurs à une prise de contrôle par des acteurs étrangers. Il bénéficie toutefois d'opportunités de différenciation technologique alors que la France profite de positions avantageuses dans les domaines de recherche les plus porteurs pour l'avenir du secteur.

DANS CE DOSSIER

Points-clés

Ce qu'il faut retenir

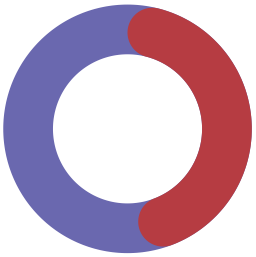
Chiffres-clés

8,3 milliards (2020)

+ 11,3 %

Produits et logiciels

4,3 milliards
+ 10,9 %



Services

4 milliards
+ 12,3 %

Moteurs

LE DIGITAL ACCROÎT LES MENACES	• Espionnage • Vol de données • Blocage des infrastructures numériques...
DE MULTIPLES SOURCES DE PIRATAGE	• Cybercriminels indépendants • Entités étatiques • Organisations autonomes soutenues par des puissances étrangères
CRISE SANITAIRE	• Plus grande vulnérabilité des organisations
DES SECTEURS PARTICULIÈREMENT TOUCHÉS	• Finance • Santé • Énergie
SOUTIEN DE L'ÉTAT	• Recrutement d'experts pour la cyberdéfense • Plan de financement (1 milliard d'euros) • Partenariats favorisant la recherche et les start-up

Points-clés

Ce qu'il faut retenir

Paysage concurrentiel

START-UP

De plus en plus nombreuses

Hausse des levées de fonds

Des solutions variées

- Systèmes basés sur l'IA
- Cybernotation
- Renforcement de la vigilance des employés...

GRANDS GROUPES

Dans le numérique et la défense

Des offres développées en interne

Des filiales dédiées et des rachats de jeunes pousses

OPPORTUNITÉS

Force de la recherche française dans les technologies d'avenir

- Supercalculateurs
- Cryptographie quantique
- Blockchain

Nombreux partenariats entre acteurs

- Solutions communes
- Accroître la formation
- Programmes de recherche

Défis et freins

FAIRE PREUVE DE PÉDAGOGIE	• Augmenter les budgets dédiés dans les organisations. • Rappeler que la sécurité repose avant tout sur l'humain
PÉNURIE DE MAIN D'OEUVRE	• Accélérer la formation d'experts et de personnel de qualification intermédiaire
MANQUE DE FINANCEMENT	• Rachats de sociétés françaises par des firmes étrangères • Réserver les marchés publics aux acteurs européens ?

Sécuriser le recrutement des talents

Pour les acteurs de la cybersécurité, **la gestion de la ressource humaine apparaît comme un enjeu déterminant**. Le fort développement de l'activité au cours des trois dernières années génère d'importants besoins de personnels qualifiés, au sein d'un secteur qui pâtit d'une pénurie de compétences. Le mouvement de recrutement massif engagé ces dernières années entraîne **une flambée des salaires**, laquelle se révèle préjudiciable pour les plus petites structures. Ces dernières peuvent voir leur développement entravé, faute de disposer de moyens financiers suffisants pour se doter de compétences toujours plus chères.

Les nouveaux acteurs disposent toutefois de leviers pour se positionner dans ce contexte de pénurie de main d'œuvre qualifiée. **Certains grands groupes ont mis en place des centres de formation spécifiques** qui constituent autant de viviers de talents potentiels. Un rapprochement avec ces derniers pourrait ainsi constituer une opportunité de recruter de jeunes diplômés. **Les partenariats avec des institutions publiques se présentent également comme un levier**, l'État mettant en place de nouvelles formations afin de limiter les difficultés de recrutement dans le secteur.

Les potentiels entrants peuvent en outre **mettre en avant la particularité de leur statut de start-up**. Les petites structures agiles et en développement sont susceptibles d'attirer certains profils intéressés par une expérience différente des postes offerts par les grands groupes. Grâce à leurs innovations dans des domaines spécifiques de la cybersécurité (solutions basées sur l'intelligence artificielle, la blockchain, la cybernotation…), les start-up disposent d'atouts **pour proposer des postes variés et des missions plus originales et novatrices**.

Il apparaît également nécessaire pour les acteurs **d'accroître leur communication à destination du grand public et des étudiants**. Pâtissant de certains clichés, le secteur demeure méconnu. Une plus grande visibilité dans les parcours d'orientation des élèves ainsi qu'une présence plus marquée dans les médias et auprès des décideurs peuvent représenter des sources non-négligeables de reconnaissance de la profession. Ces initiatives pourraient **augmenter le nombre de candidats aux formations en cybersécurité**, réduisant par la suite les difficultés de recrutement.

Renforcer les apports de capitaux

Incontournable pour se positionner, le développement de solutions innovantes **nécessite des investissements conséquents** du fait d'une main d'œuvre onéreuse et de l'usage de technologies complexes. Pour les jeunes pousses du secteur de la cybersécurité, dont les moyens financiers s'avèrent bien souvent limités, **l'accès à des financements extérieurs revêt dans ce contexte un caractère prioritaire**. Ces ressources externes doivent leur permettre d'amortir les frais de développement de leur solution et/ou d'en assurer une diffusion à plus grande d'échelle.

Les nouveaux entrants disposent de plusieurs leviers spécifiques pour obtenir des fonds et financer leurs investissements. **L'État a mis en place un plan de soutien au secteur** visant notamment à développer des technologies souveraines. Des incubateurs, publics comme privés, proposent des aides pouvant permettre aux start-up de se lancer sur le marché. Le fonds d'investissement Brienne III d'ACE Capital Partners et les structures de financement rattachées au ministère des Armées peuvent par ailleurs soutenir les entrants potentiels. **La mobilisation de capitaux auprès d'acteurs étrangers constitue également une opportunité**. Si cette option peut constituer un atout pour s'internationaliser, elle présente également des inconvénients. Les questions relatives aux transferts de technologies et à la protection des données (conformité et extraterritorialité) peuvent amoindrir le soutien public et la confiance de certains clients.

Décrocher rapidement des contrats auprès d'acteurs réputés enclenche un cercle vertueux : en gagnant en crédibilité, les jeunes sociétés attirent à elles davantage d'investisseurs et peuvent convaincre de nouveaux clients. Dans cet objectif, **elles doivent diversifier leurs cibles** et se tourner vers les multiples petites sociétés et structures publiques mal protégées des cybermenaces. Les nouveaux entrants ont également la possibilité de **nouer des partenariats entre eux ou avec de grands groupes et des cabinets de conseil**. La commercialisation de solutions globales communes ou la vente indirecte par le biais d'acteurs disposant de portefeuilles de clients conséquents représentent des canaux pertinents pour se développer.

Certains acteurs du secteur plaident par ailleurs pour **l'instauration d'une clause préférentielle dans l'attribution des marchés publics**. En soutenant ce type d'initiatives, les potentiels entrants peuvent contribuer à atténuer la pression concurrentielle des acteurs étrangers. Ils doivent de plus renforcer la communication du secteur auprès des décideurs dans les organisations. Encore perçue comme un coût supplémentaire à minimiser, la cybersécurité ne bénéficie pas toujours de budgets suffisants pour assurer un niveau de protection adéquat. Il s'avère donc nécessaire de **faire preuve de pédagogie afin de rehausser les dépenses des entreprises dans le domaine**. Elles doivent toutefois se garder de tout miser sur la technologie : **la sécurité, même informatique, repose avant tout sur l'humain** et donc l'implication de l'ensemble des collaborateurs.

Un marché dynamique, stimulé par la pandémie de Covid-19

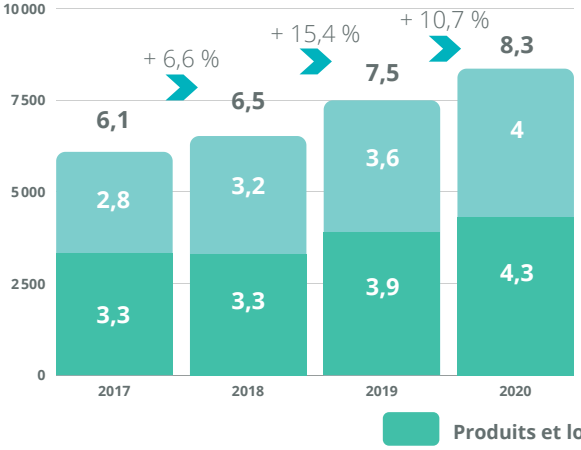
La cybersécurité se développe fortement

Une progression soutenue depuis 2016

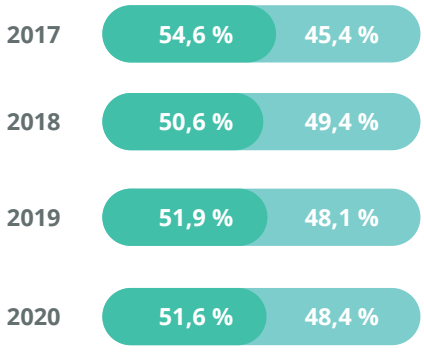
Le marché de la confiance numérique, qui regroupe la sécurité numérique et les activités de cybersécurité, s'est considérablement accru ces dernières années. Il a ainsi **augmenté d'environ 8 % par an entre 2016 et 2020** pour atteindre à cette date **13,4 milliards d'euros en France** selon l'Observatoire de la Confiance Numérique. Les entreprises françaises du secteur ont réalisé 8 milliards d'euros de chiffre d'affaires grâce à leurs activités à l'étranger en 2020. Le reste du monde a suivi la même tendance, le marché mondial étant passé de **75,5 milliards de dollars en 2016 à près de 129 milliards en 2020**, soit une hausse de plus de 70 %. Celui-ci devrait croître de 14,5 % chaque année d'ici 2025 d'après Business France. Le marché de la cybersécurité, qui représente 62 % de la confiance numérique, a quant à lui atteint **8,3 milliards d'euros en France en 2020**. Il s'est accru de 11,5 % cette même année, tandis que les activités de sécurité numérique ont reculé de 1 %. La moindre croissance de la confiance numérique en 2020 (+ 6,4 % contre + 8,8 % l'année précédente) explique cette diminution. La cybersécurité représente en outre **une part considérable dans la valeur ajoutée de la confiance numérique : 68 % en 2020,** soit une proportion supérieure à son poids dans le chiffre d'affaires. Avec 39 % de part dans la valeur ajoutée, les produits cyber figurent comme l'origine de cette différence.

Un marché français en progression

Chiffre d'affaires de la cybersécurité en France, en milliards d'euros, et évolution



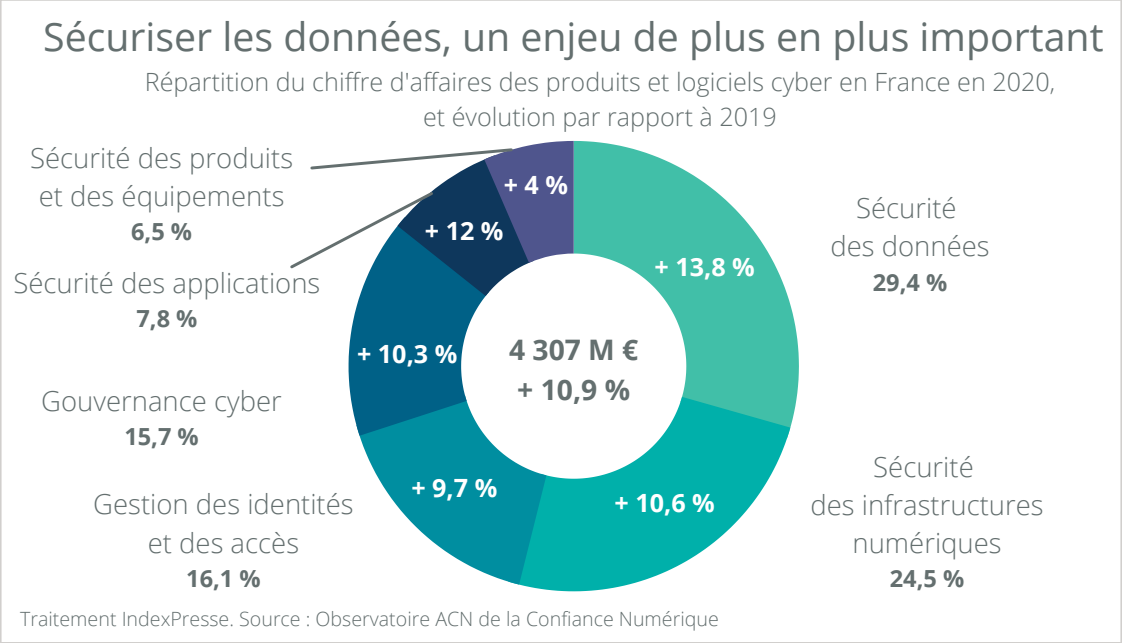
Évolution de la répartition du chiffre d'affaires de la cybersécurité en France



Produits et logiciels — Services

Traitement IndexPresse. Source : DECISION Études & Conseil, via ACN

Une forte croissance des produits et logiciels de cybersécurité portée par la sécurité des données



Les produits et logiciels de cybersécurité représentent 51,6 % du marché, s'établissant à environ **4,3 milliards d'euros en 2020** en France. Leur croissance a atteint 10,9 % cette même année, portée en particulier par celle de **la sécurisation des données (+ 13,8 %)**. Celle-ci constitue le premier segment des produits cyber, avec une part s'élevant à près d'un tiers du chiffre d'affaires. Second segment avec un quart des ventes en valeur, **la sécurité des infrastructures numériques a également connu une croissance soutenue (+ 10,6 %)**. La catégorie plus modeste de la sécurité des applications, représentant 7,8 % du chiffre d'affaires des produits cyber en 2020, a elle aussi bénéficié d'une forte dynamique. Ses revenus se sont ainsi accrus de 12 % en valeur sur l'année.

Les produits de cybersécurité ont généré **57 % de la valeur ajoutée totale du marché en 2020**, signe de leur haut degré de technicité. Elle a atteint 2,5 milliards d'euros cette même année. À elle seule, **la sécurité des données a compté pour 765 millions d'euros, soit 30,4 % du total du segment**. C'est plus que son poids dans le chiffre d'affaires, ce qui montre le caractère stratégique de cette activité pour les acteurs du marché. **La gestion des identités et des accès semble également bien valorisée** (17,5 % de la valeur ajoutée contre 16,1 % du chiffre d'affaires). De son côté, la sécurisation des infrastructures numériques a représenté 23,8 % de la valeur ajoutée avec près de 600 millions d'euros. Avec une part de 5,2 % dans la valeur ajoutée contre 6,5 % dans le chiffre d'affaires, **la sécurité des produits et des équipements fait figure d'activité moins valorisée** sur le segment. Sa croissance, de 4 %, apparaît également comme la plus faible du segment.

Les services cyber tirent la croissance du marché

Second segment de la cybersécurité avec 48,4 % de parts de marché, **les services ont progressé de 12,3 % en valeur, atteignant un chiffre d'affaires de 4 milliards d'euros** en France, en 2020, selon l'Observatoire de la Confiance Numérique. La croissance se portait déjà à 11,9 % en 2019. Les missions d'audit, de planning et de conseil s'avèrent surreprésentées, leur part du chiffre d'affaires du segment dépassant 43 % en 2020. Elles ont **enregistré la plus forte hausse (+ 13,6 %)**, suivie par la mise en œuvre cyber, (+ 11,9 %) et par la sécurisation de l'infogérance et l'exploitation (+ 11,2 %). De leur côté, **les formations en cybersécurité demeurent modestes** avec une part du chiffre d'affaires s'élevant à 2,9 %. Elles se sont outre développées de façon plus limitée que les autres catégories, avec une hausse de 5,6 %. **En termes de valeur ajoutée, l'audit et le conseil représentent une part plus faible** des services cyber (38 %). C'est également le cas avec la mise en œuvre de la cybersécurité, avec 29 % de la valeur ajoutée contre 31,7 % du chiffre d'affaires. La sécurité relative à l'infogérance et l'exploitation des infrastructures se présente quant à elle comme **une activité fortement valorisée sur le segment**. En 2020, sa part dans la valeur ajoutée atteignait ainsi 28,6 % alors qu'elle représentait 22,3 % du chiffre d'affaires. Sa croissance s'est montrée soutenue, à 11,2 %.

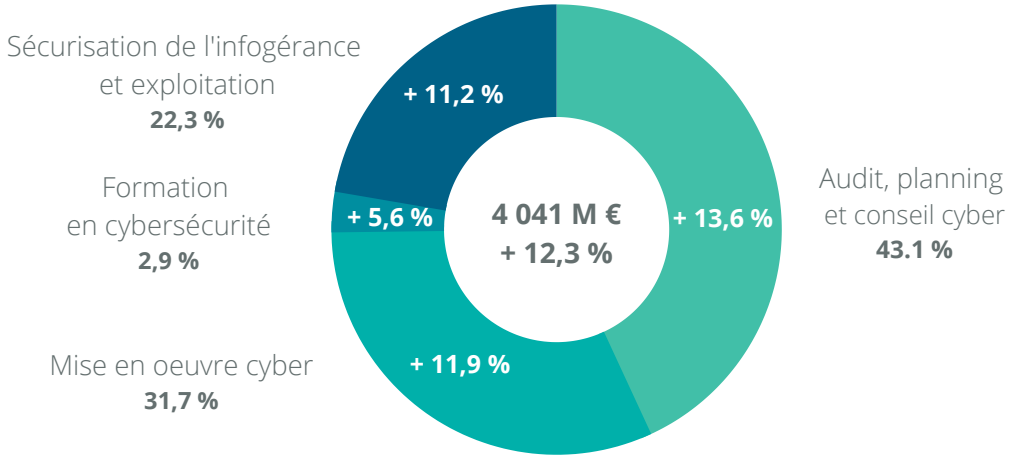
46,4 %

La part de la valeur ajoutée par rapport au chiffre d'affaires des services cyber

Source : Observatoire de la Confiance Numérique, 2021

Une croissance des services portée par le conseil

Répartition du chiffre d'affaires des services cyber en France en 2020, et évolution par rapport à 2019



Traitement IndexPresse. Source : Observatoire ACN de la Confiance Numérique

Les menaces s'intensifient avec la crise sanitaire

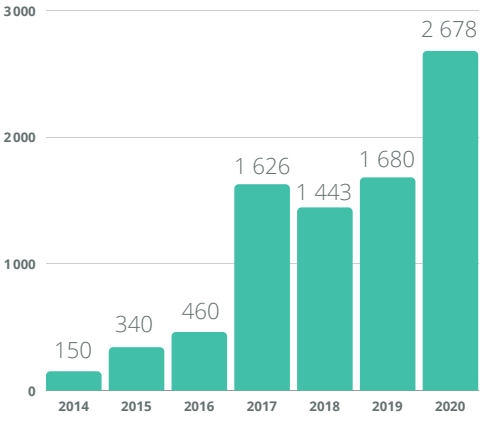
La numérisation croissante génère des vulnérabilités

Le numérique, omniprésent

L'usage de plus en plus répandu des technologies digitales accroît les risques de cyberattaques et la gravité de leurs conséquences. Le développement de l'intelligence artificielle, des plateformes ou encore de la collecte massive de données dans des domaines variés ont favorisé le développement du numérique. Le chiffre d'affaires du e-commerce a ainsi doublé en sept ans en France. **Les objets connectés (Internet of Things, IoT) se diffusent de façon croissante** tant dans les villes avec les projets de *smart city* que dans les usines ou chez les particuliers. Ces derniers ont acheté pour près de **2,7 milliards d'euros d'objets connectés en 2020**, un montant multiplié par 17 depuis 2014. Le nombre d'utilisateurs de visioconférence a quadruplé depuis 2011, selon une enquête du Crédoc de 2021. La part des individus déclarant utiliser des services administratifs en ligne a **gagné six points entre 2018 et 2020**, tandis que l'usage des réseaux sociaux s'est accru de huit points sur la période. Il atteignait 67 % en 2020. L'étude du Crédoc indique que **83 % des Français interrogés se connectent à Internet tous les jours**. Plus de la moitié des sondés consultent la presse sous format numérique. Dans le domaine de la sécurité, le nombre de caméras de surveillance dans les 50 plus grandes villes de France a été **multiplié par 2,4 entre 2013 et 2020** selon *La Gazette des communes, des départements et des régions*. À cette date, le pays comptait ainsi plus de 11 400 caméras. Le secteur énergétique se numérise également avec les réseaux intelligents : 30 millions de compteurs connectés Linky étaient ainsi installés sur le territoire en 2020.

Une numérisation multidimensionnelle

Évolution du chiffre d'affaires des objets connectés (BtoC) en France, en millions d'euros



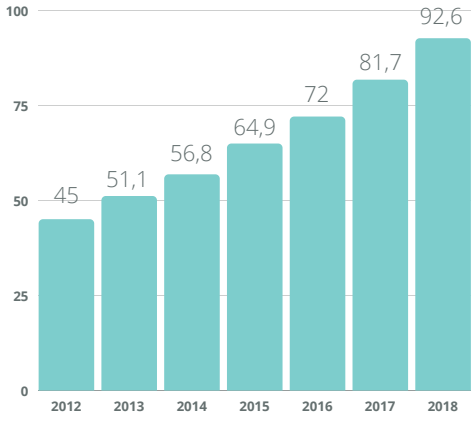
71 %

Part des Français ayant recours à l'administration en ligne en 2020

45 %

Part des Français ayant communiqué par visioconférence en 2020

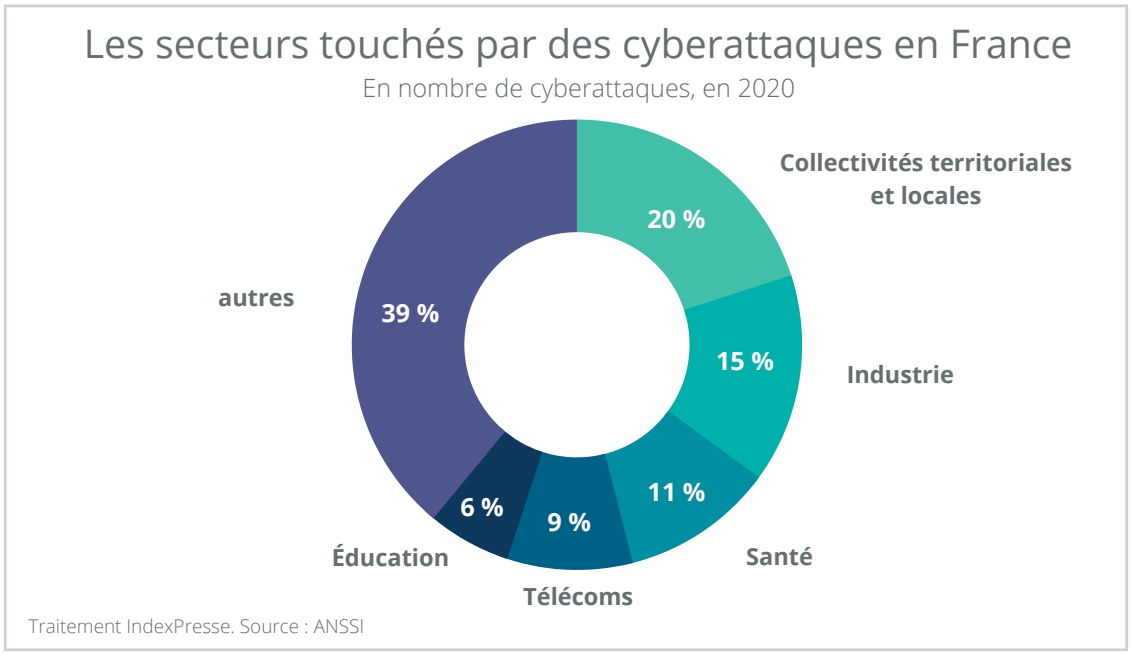
Évolution du chiffre d'affaires du e-commerce en France, en milliards d'euros



Traitement IndexPresse. Sources : Statista, Baromètre du numérique 2021 du Crédoc

De multiples secteurs touchés par la cybercriminalité

La ville intelligente et les bâtiments connectés présentent des vulnérabilités au risque cyber. Deux ingénieurs ont rapporté, lors de la conférence de cybersécurité Le Hack en 2019, être parvenus à **se connecter à un réseau de caméras de surveillance via la gestion des feux de signalisation**. La même année, une étude de l'éditeur de logiciels russe Kaspersky a montré que **37,8 % des 40 000 bâtiments connectés analysés dans le monde avaient subi des cyberattaques**. En 2017, l'hôtel quatre étoiles autrichien Romantik Seehotel Jägerwirt a vu l'accès à ses chambres bloqué par des cybercriminels. Le système de réservation avait par ailleurs été désactivé. L'établissement avait dû payer une rançon de 1 500 euros en bitcoins pour que cesse l'attaque informatique. Les failles permettant ce type d'intrusion **proviennent notamment des objets connectés des smart buildings** : 57 % d'entre eux se montrent vulnérables à des cyberattaques de gravité moyenne ou supérieure selon une étude de la société américaine Palo Alto Networks publiée en 2020. Directeur des ventes BtoB chez Kaspersky, Bertrand Trastour regrettait à cette période dans la revue *Le Moniteur des travaux publics et du bâtiment* que "le plus souvent, **ces produits sont conçus sans intégrer la moindre couche de sécurité**, sans respecter la moindre bonne pratique sécuritaire". Emmanuel François, président de la Smart Building Alliance, rapportait dans le même magazine qu'**aucun bâtiment testé en France pour le label Ready2Services n'atteignait 55 % de conformité**. Créé en 2018, ce label vise à définir des règles de sécurité pour les objets connectés du domaine, tant au niveau de leur structure que de leur installation et de leur utilisation. Or, il indiquait que "le jour où les pirates s'intéresseront aux bâtiments intelligents et à la smart city, **les dégâts pourront être bien plus importants qu'une simple rançon** (...) il suffit d'une variation de 3 GW pour provoquer un effondrement du réseau électrique à l'échelle européenne." Selon Emmanuel François, une telle hausse de la consommation énergétique équivaudrait à celle de 10 000 bâtiments tertiaires subissant une augmentation brusque du chauffage ou de l'éclairage. L'étude de Kaspersky de 2020 avait noté que de nombreux immeubles de bureaux disposaient d'**un seul appareil permettant de contrôler à la fois les accès et les systèmes de ventilation, d'eau ou encore les ascenseurs**. Bien que les réseaux IT (liés à l'activité de l'entreprise) et OT (énergie, capteurs, gestion opérationnelle) s'avèrent séparés du fait d'une approche dite "ségrégative", **le développement des objets connectés tend à accroître les interactions entre eux**. Expert en cybersécurité industrielle chez Kaspersky, Samy Tadjine expliquait en 2020 dans *Le Moniteur des travaux pu-*



blics et du bâtiment : "si toutes les technologies convergent vers un protocole de communication commun, les deux réseaux pourront à terme être interconnectés, voire fusionner".

Le domaine de la santé voit également **le nombre de cyberattaques augmenter** de façon considérable : + 14 % en 2020 dans le monde d'après F-Secure. **Le coût de tels actes malveillants s'est accru** la même année de 10,5 % pour le secteur selon IBM Security. La France a subi plusieurs atteintes récentes de ce type : 60 % des incidents recensés en 2020 par l'Agence numérique de santé avaient une origine malveillante, contre 43 % en 2019 et 41 % en 2018. Les hôpitaux de Dax (Landes) et de Villefranche-sur-Saône (Rhône) ont ainsi été visés par des rançongiciels début 2021, paralysant les systèmes d'information. Ceux de Narbonne, dans l'Aude, et d'Albertville-Moûtiers, en Savoie, avaient été touchés deux mois plus tôt. À l'été 2020, **les données de santé de plus de 1,4 million de patients ont été dérobées** à l'Assistance publique-Hôpitaux de Paris (AP-HP). En fin d'année, les usines du français Fareva, destinées à produire le vaccin anti-Covid de la société allemande CureVac, ont été **mises à l'arrêt à cause d'un virus informatique**. Le CHU de Rouen avait également subi une attaque en 2019. Des cybercriminels avaient par ailleurs infiltré les bases de données de l'Agence européenne du médicament en décembre 2020. Cette vulnérabilité accrue est étroitement liée au **manque de moyens financiers et humains du secteur public**. Christophe Corne, président du directoire de l'éditeur de logiciels Systencia, expliquait dans *L'Informaticien* en mars 2021 : "on a des clients dans le domaine hospitalier chez qui **les infrastructures sont gérées par des équipes trop limitées**, des centres névralgiques qui devraient être gérés par le double, voire le triple d'effectifs."

Le secteur bancaire se révèle aussi particulièrement ciblé par les cyberattaques. La Banque centrale européenne (BCE) a placé en 2020 le risque cyber parmi les trois principales menaces pour les institutions financières. Environ 20 % des attaques informatiques concernent le secteur bancaire, selon un article de *La Tribune* paru la même année. Alessandro Roccati de l'agence de notation Moody's expliquait dans une étude en 2020 : "**les banques détiennent beaucoup d'argent et de données**. Ces données, protégées par le règlement général sur la protection des données en Europe (RGPD), ont beaucoup de valeur car sans elles, les banques ne peuvent pas comprendre les besoins des clients." Les attaques informatiques visant les institutions bancaires **se sont multipliées en 2020 : + 238 %** selon l'entreprise de cybersécurité VMware Carbon Black. Parmi ces dernières, **57 % ont observé une augmentation des fraudes** au niveau des virements électroniques. De son côté, Kaspersky a identifié les types d'incidents concernant les fraudes pour l'année 2020. Plus de la moitié d'entre elles ont été conduites via un piratage de comptes bancaires, tandis que le blanchiment d'argent a représenté 16 % des transactions frauduleuses. Celles liées à des appareils infectés représentaient 4 % du total. IBM Security a chiffré à environ **5 millions de dollars pour le secteur bancaire le coût de chaque intrusion** dans les bases de données clients en 2020. La même année, l'éditeur de logiciels américain Infoblox évaluait à **4,2 millions de dollars le coût de chaque attaque pour les établissements européens**. Dans son étude, celui-ci indiquait que **44 % des institutions sondées avaient subi une violation des données hébergées dans le cloud** au cours des douze derniers mois. Leur part s'élevait à 37 % concernant les attaques de logiciels malveillants visant un serveur distant. Malgré des avancées réelles du secteur en termes de cybersécurité, des progrès restent à effectuer chez les acteurs européens. Alessandro Roccati affirmait dans son rapport : "**L'Europe accuse un léger retard** par rapport aux États-Unis même si certains pays comme les Pays-Bas ou l'Angleterre ont des régulateurs très à cheval sur la cybersécurité." En 2021, l'Autorité bancaire européenne a subi une cyberattaque liée à ses serveurs de messagerie Microsoft Exchange. La BCE avait quant à elle été touchée en 2019, déplorant un vol de données sur l'un de ses sites Internet d'information. Le spécialiste britannique du change, Travelex, et la banque maltaise Bank of Valletta avaient eux aussi été atteints par des cyberattaques la même année. Mickaël Bittan, responsable cybersécurité chez Accenture, considérait en 2021 que les petites banques privées et, dans une moindre mesure, les banques régionales, devaient **accroître leurs efforts en cybersécurité**. Il notait cependant que quelle que soit leur taille, toutes doivent continuer d'investir pour contenir une menace en constante évolution.

La crise sanitaire de Covid-19 a accentué les risques

La pandémie, un contexte favorable aux cybercriminels

Le nombre de cyberattaques visant des entreprises françaises a considérablement augmenté du fait de la crise de Covid-19. Entre mars et juin 2020, elles ont été ainsi été de **20 % à 25 % plus nombreuses que l'an passé** selon Nicolas Arpagian d'Orange Cyberdefense. Les attaques par déni de service ont connu une hausse de 50 %, et **le taux de réussite des attaques a doublé sur la période**. De son côté, la plateforme publique Cybermalveillance a identifié une augmentation drastique des tentatives de phishing (ou hameçonnage), qui ont quintuplé en mars 2020. Sa fréquentation a plus que doublé par rapport à 2019. Au sujet des rançongiciels, les demandes d'assistance émanant de structures professionnelles ont **vu leur nombre s'accroître de 30 %**. L'éditeur de logiciels McAfee a quant à lui indiqué que les attaques ciblant les services cloud se sont **accrues de 630 % dans le monde en 2020**. Sur l'année 2020, l'Agence nationale de la sécurité des systèmes d'information (Anssi) révèle que les signalements pour les attaques par rançongiciels ont augmenté de 255 %. De faux sites dédiés à la commande de masques, à des outils de visioconférences ou encore aux attestations de sortie ont également fait leur apparition : plus de 4 000 la première semaine du confinement de mars 2020 d'après le centre de supervision (CERT) d'Orange Cyberdefense. **La généralisation du télétravail** a conduit à affaiblir la sécurité des réseaux. "Beaucoup d'entreprises se sont concentrées sur l'autorisation des accès, en négligeant l'aspect sécurité. Il en résulte **une explosion des voies d'accès non sécurisées dans les entreprises**", expliquait début 2021 dans *L'Officiel des transporteurs* Juliette Rizkallah, directrice marketing chez le spécialiste SailPoint. Un sondage d'Infopro Digital Études a montré fin 2020 que **la transformation numérique s'est réalisée au détriment de la cybersécurité**, avec un écart élevé en termes de budget consacré. Un quart des sondés (occupant des postes de direction, notamment dans les départements numériques) estimaient ainsi que leur entreprise avait réduit ses exigences concernant la sécurité informatique pour garantir la poursuite de ses activités.

400 %

L'augmentation du nombre de tentatives de phishing en France en mars 2020

Source : Cybermalveillance.gouv.fr, *2020.*

192

Le nombre d'attaques par rançongiciels contre des entreprises en France en 2020

Source : ANSSI, 2021.

Procédés

Des méthodes variées pour mener des actions de cybermalveillance

La technique la plus répandue, le **phishing**, consiste à envoyer un email ou un sms d'apparence trompeuse. Comportant un lien ou une pièce jointe, il infecte le terminal avec un virus lorsque la victime clique sur l'un deux. Le criminel pourra ainsi récupérer des informations telles que des mots de passe. Les attaques par **rançongiciels** visent de leur côté à infiltrer un réseau afin de le rendre inaccessible ou de crypter ses données. Une somme d'argent est alors demandée pour le rétablissement du système. Quant aux **attaques par déni de service** (DDoS, pour *distributed denial of service*), elles cherchent à paralyser un système en lançant un nombre de requêtes trop important. Ce type de cyberattaques requiert au préalable l'infection d'une multitude de terminaux, les machines contrôlées par les hackers permettant d'amplifier leur force de frappe.

Une impréparation des entreprises françaises

Les moyens mis en œuvre et la sensibilisation des salariés à la cybersécurité demeurent insuffisants. Une enquête de 2021 du Cesin (association de responsables de la sécurité des systèmes d'information de grandes entreprises et d'ETI) a indiqué que **seulement 5 % du budget IT des sondés est dédié à la cybersécurité**. Mi-2021 dans *Archimag*, Arnaud Deschavanne, associate partner du cabinet spécialisé Magellan Consulting, estimait **difficile "d'assurer un niveau de sécurité satisfaisant en allouant moins de 10 %"** du budget informatique à la sécurité. Seules 43 % des entreprises interrogées dans l'enquête du Cesin prévoyaient d'augmenter cette part. Près d'un tiers ne disposaient pas de moyens de prévention suffisants contre les cyberattaques, et 41 % ne se déclaraient pas en mesure de les détecter. Les services cloud apparaissaient comme **un point de vulnérabilité majeur**. Ces derniers "sont parfois considérés avec un excès de confiance de la part des sociétés clientes. **Elles estiment souvent à tort que les questions de sécurité sont le problème des hébergeurs**", expliquait Philippe Rondel, senior security architect chez CheckPoint, fin 2020 dans *Décision Achats*. Il soulignait que "dans la réalité, **les volets applications, les infrastructures restent généralement la responsabilité du client final** qui doit lui-même mettre en place et financer un niveau de sécurité qui lui est adapté et suffisant".

La faible protection fournie par les prestataires de services cloud constitue une réalité pour les sondés, 86 % d'entre eux estimant que des dispositifs additionnels sont nécessaires. Ces derniers peuvent toutefois être **établis de façon incohérente**. Ghaleb Zekri, architecte senior chez VMware, décryptait ce phénomène dans *Décision Achats* : "**l'interopérabilité est alors l'un des grands obstacles**. Pour chaque problème de sécurité, on a proposé une solution, ce qui fait que les clients se retrouvent au fil du temps avec une multitude de couches produits qui ne sont pas corrélées".

De nombreux salariés se révèlent par ailleurs **négligents quant aux questions de cybersécurité**. Une étude réalisée en 2020 par l'entreprise japonaise Trend Micro auprès de 13 200 télétravailleurs de 27 pays a montré que **les Français accordent moins d'attention à ce domaine**. La part de ceux affirmant prendre au sérieux les directives de leur service informatique s'élevait à 79 %, contre 85 % au niveau mondial. **Seuls 73 % des employés français considéraient être en partie responsables de la cybersécurité** de l'entreprise, alors que cette proportion atteignait 81 % pour l'ensemble des sondés. Ils étaient également 44 % en France à accéder régulièrement à des données de la société via un appareil personnel, contre 39 % dans le monde. Les Français se montraient en outre **légèrement plus nombreux à télécharger des applications personnelles sur des terminaux professionnels**. Ils s'avéraient en revanche moins nombreux à considérer que ce comportement constituait un risque pour la sécurité informatique (62 % contre 64 %). La part des employés français utilisant leur ordinateur de travail pour un usage privé s'établissait à 81 % (+ 1 point que la moyenne mondiale). Dans ce dernier cas, les salariés s'imposant des limites quant aux sites visités affichent une proportion plus faible (– 2 points).

5 %

La part du budget IT dédiée à la cybersécurité des entreprises membres du Cesin

Source : Cesin, 2021.

10 %

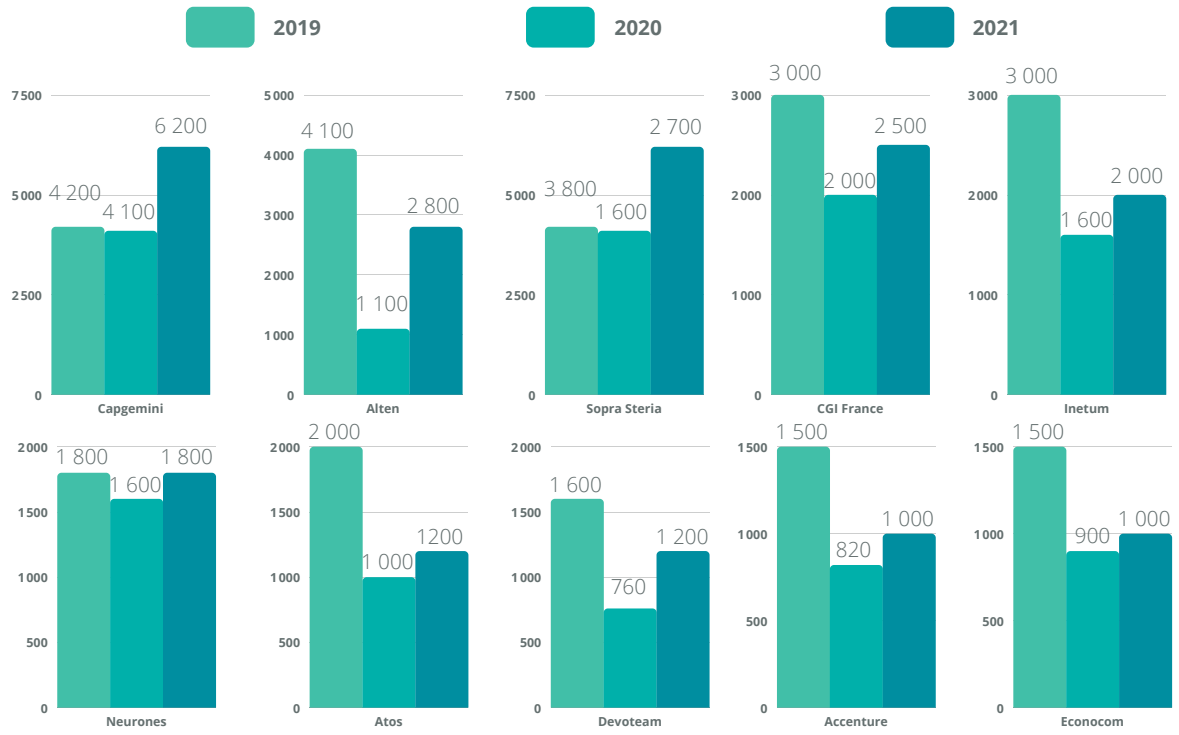
La part du budget IT devant être dévolue à la cybersécurité pour assurer une protection suffisante

Source : Arnaud Deschavanne, Magellan Consulting, 2021

Des besoins en recrutement qui s'accentuent

Signe de l'importante croissance du marché et des besoins, **les offres d'emploi relatives à la cybersécurité bondissent**. Près de 15 700 offres d'emplois en cybersécurité ont été publiées en 2019 selon l'Anssi, soit 39 % du total des effectifs recensés cette année. Le réseau professionnel LinkedIn a de son côté établi en 2020 un classement des métiers émergents entre 2015 et 2019 en se basant sur l'évolution des recrutements. **Le poste de délégué à la protection des données est arrivé en première position**, suivi par celui d'ingénieur en intelligence artificielle. **La fonction de spécialiste en cybersécurité atteignait la septième place**, tandis que la quatorzième place était représentée par le métier de recruteur IT. Parmi les individus occupant un métier identifié comme émergent, 42 % d'entre eux opéraient dans les services informatiques ou liés à Internet et chez les éditeurs de logiciels. Directrice de la communication de LinkedIn France, Esther Ohayon décrivait en 2020 dans *Stratégies* la tendance de recrutement, soulignant "**l'énorme bond en avant du secteur de la sécurité informatique et réseau** avec 63 % de talents en plus par rapport à l'année dernière." En 2019, l'Association pour l'emploi des cadres (Apec) a constaté **un doublement du nombre d'annonces** postées par les recruteurs entre 2016 et 2018 concernant le métier de consultant en cybersécurité. Sur la même période, celles portant sur un emploi d'architecte en cybersécurité ont **augmenté d'environ 40 %**. Alain Bouillé, délégué général du Cesin, expliquait

Les perspectives d'embauches en CDI des principales ESN* en France en 2021



Traitement IndexPresse. Source : *L'Informaticien*. *entreprises de services numériques

début 2020 à *L'Usine nouvelle* que "les entreprises de taille moyenne, de 2 000 à 3 000 salariés, qui n'avaient pas les moyens de se payer un responsable de la sécurité des systèmes d'information (RSSI) commencent à en recruter." Les diplômés du domaine profitent en outre de **la reprise partielle des offres d'emploi provenant des sociétés du secteur numérique**. Ces dernières recrutent dans de nombreuses branches de l'informatique, proposant notamment des postes d'architectes réseau, d'ingénieurs et de chefs de projets en cybersécurité ou encore de consultants. L'Apec prévoit d'ailleurs **une augmentation des recrutements dans l'informatique de 15 % en 2021**. De son côté, l'État a accéléré l'accroissement de ses effectifs dans la cyberdéfense. **À l'origine, 1 100 recrutements étaient prévus** dans la loi de programmation militaire (LPM) de 2021, en particulier pour renforcer le pôle cybersécurité de Rennes. Face à la forte hausse des attaques informatiques, le ministère des Armées a **décidé de relever son objectif de recrutement, le passant à 1 800 créations de postes** d'ici 2025.

L'attractivité du secteur se manifeste également dans **les salaires élevés proposés aux jeunes diplômés comme aux spécialistes aguerris**. Le cabinet de recrutement PageGroup a observé dans son évaluation de 2021 des rémunérations comprises entre 45 000 et 70 000 euros bruts pour les analystes en cybersécurité. Les directeurs de la sécurité des systèmes d'information pouvaient quant à eux prétendre à des salaires allant de 100 000 à 200 000 euros. "**Les banques et les entreprises de service numérique, qui recrutent en masse**, déroulent le tapis rouge et proposent des salaires de 10 000 à 20 000 euros supérieurs aux grilles habituellement pratiquées", expliquait Amélia Fanchette, manager au cabinet de recrutement Michael Page, dans un article du site *Emploi-Pro* de 2021. Elle ajoutait par ailleurs que les besoins s'établissaient aussi au niveau de postes plus transversaux : "**nous sommes beaucoup sollicités pour des recrutements de cadres expérimentés**, qui savent communiquer, comprennent les métiers de l'entreprise et puissent expliquer à chacun les enjeux de la cybersécurité." L'étude de PageGroup indique que le poste d'ingénieur en cybersécurité devrait connaître l'une des plus fortes augmentations de salaire de 2021.

Le secteur s'avère déjà un employeur conséquent. En 2020, **près de 44 000 personnes travaillaient dans la cybersécurité** en France d'après l'Observatoire ACN. Les produits et logiciels comptaient pour environ 20 000 emplois tandis que les services représentaient un peu moins de 24 000 postes. **Les activités d'audit, de planning et de conseil en constituaient une part importante**, avec plus de 10 600 personnes. Avec respectivement 7 800 et 5 800 employés, la mise en œuvre de la cybersécurité et la sécurisation des données complétaient le podium.

44 000

Le nombre de personnes travaillant dans la cybersécurité en France en 2020.

Source : Observatoire ACN de la Confiance Numérique, *2021*

1 800

Le nombre de postes à créer dans la cybersécurité par le ministère des Armées pour la période 2021-2025

Source : Ministère des Armées, *2021*

La France et l'Union européenne se mobilisent pour renforcer le secteur

L'État français s'engage pour la filière

Considérée comme incontournable dans la protection des intérêts économiques comme dans le domaine militaire, **la cybersécurité fait l'objet d'une attention particulière de l'État**. Celui-ci met en place plusieurs projets et investit dans le secteur afin de l'aider à se développer.

En février 2021, le gouvernement a dévoilé un programme de financement d'**un milliard d'euros dédié à la cybersécurité**, dont 720 millions d'euros de fonds publics. Le soutien à la création de solutions souveraines (non dépendantes d'acteurs étrangers) représente un apport de 515 millions d'euros, un peu plus de la moitié (290 millions) venant de l'État. Ce dernier propose aux entreprises une aide en fonds propres pour un montant total de 200 millions d'euros. **Faciliter l'adoption de systèmes de cybersécurité** constitue un autre axe du programme, financé par la puissance publique à hauteur de 156 millions d'euros. Dans ce domaine, la contribution du secteur privé se porte à 20 millions. Enfin, **le renforcement des liens entre les acteurs** se montre soutenu à parts égales par la puissance publique et les entreprises pour environ 148 millions d'euros.

1 milliard d'euros

Le montant du plan gouvernemental dédié à la cybersécurité

Source : Ministère de l'Économie, des Finances et de la Relance, *2021*.

Cette volonté de fédérer l'écosystème de la cybersécurité se traduit par **la création du Campus Cyber, une structure de près de 26 000 m²** située à La Défense (Paris) et rassemblant des grandes sociétés du secteur, des start-up, des chercheurs et des administrations. Le groupe Thales, la Gendarmerie nationale, l'Institut national de recherche en sciences et technologies du numérique (Inria) ou encore l'entreprise Citalid ont prévu de s'y installer. **L'État y a investi 130 millions d'euros**, dont 25 millions pour la création d'un incubateur dévolu aux jeunes pousses de la cybersécurité. **Le partage de données, le développement commun d'innovations et l'animation de l'écosystème** en constituent les principaux objectifs. Le Campus doit également favoriser la formation du personnel des différentes entités présentes, ce domaine bénéficiant d'ailleurs, à l'instar des Armées, de crédits supplémentaires spécifiques. Michel Van Den Berghe, alors directeur d'Orange Cyberdefense, affirmait dans *Challenges* début 2021 : "au total, **plus de 60 entreprises et administrations se sont engagées** dans ce projet qui ne doit pas ressembler à une galerie marchande, mais à un campus très opérationnel et innovant." **Un premier appel à projet pour le développement de nouvelles technologies** a été lancé en septembre 2021 pour un montant de 250 millions d'euros.

Plusieurs objectifs ont été établis pour le programme, tels que **le triplement du chiffre d'affaires du secteur d'ici 2025**, le doublement de l'emploi dans la filière sur la période ou encore faire émerger trois licornes (start-up valorisées plus d'un milliard d'euros) à cet horizon. Ce plan s'ajoute aux **136 millions d'euros provenant du plan de relance** lancé suite à la crise sanitaire et dévolus à accroître le budget de l'Anssi sur la période 2021-2022. La moitié de ces nouveaux crédits visent à consolider la protection numérique des collectivités territoriales, tandis que 30 % sont destinés aux ministères. Les 20 % restants doivent permettre d'améliorer la cybersécurité des organismes publics.

De multiples initiatives portées au niveau européen

Une évolution législative majeure

L'Union européenne a pris conscience des enjeux liés à la cybersécurité et met en œuvre de nouvelles réglementations visant à la développer.

En 2019, le Parlement européen a adopté **le Cybersecurity Act**, permettant notamment d'uniformiser les protocoles de certification en matière de sécurité informatique. Cette démarche **favorise la création d'un marché commun**, limitant les coûts pour les entreprises souhaitant opérer dans plusieurs pays membres. La définition de standards et d'une politique à l'échelle de la zone **renforce en outre la coopération entre les États**. L'ENISA, l'agence européenne dédiée à la sécurité des infrastructures et des réseaux, s'est par ailleurs vu renforcée par le Cybersecurity Act. Elle a ainsi **bénéficié d'un mandat permanent et de ressources supérieures**. Son rôle est de plus étendu, l'organisme devenant le "point de référence" du domaine pour toutes les parties prenantes de l'Union européenne.

Fin 2020, l'Union européenne a dévoilé **sa nouvelle stratégie pour la cybersécurité**. Thierry Breton, commissaire au marché intérieur et au numérique, expliquait dans un communiqué : "Les cybermenaces évoluent rapidement, et leur complexité comme leur capacité d'adaptation ne cessent de croître. Pour garantir la protection de nos citoyens et de nos infrastructures, il nous faut anticiper". Cette démarche européenne a abouti à la formalisation d'**une nouvelle version de la directive SRI, relative à la sécurité des réseaux et des systèmes d'information**. Celle-ci avait été mise en place en 2016. La directive a élargi le champ des secteurs concernés et durci les obligations en termes de sécurité informatique. De nouvelles contraintes s'appliquent également aux fournisseurs. Le volet répressif se révèle en outre renforcé, avec **des amendes pouvant monter jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires** annuel mondial. La directive SRI 2 a été suivie par deux autres textes plus ciblés fin 2020 : le CIR, portant sur les infrastructures critiques, et le DORA, qui concerne le secteur bancaire. Ce dernier fait suite à **la directive DSP 2 de 2019, qui ciblait spécifiquement les systèmes de paiement digitaux**. Ces différents textes ont tous accru les exigences en termes de cybersécurité pour les entreprises. Un "Cyber Resilence Act" devrait par ailleurs voir le jour afin notamment de **renforcer la sécurité des objets connectés**.

De nouvelles entités dédiées

La Commission européenne a également mis en place **des structures spécialisées dans la lutte contre les cybermenaces**. Début 2021, le Cyber Crises Liaison Organisation Network (CyCLONe) a été créé dans l'objectif d'assurer **une coordination efficace entre les États membres en cas de cyberattaque** de grande ampleur. Il est doté de 4,5 milliards d'euros de budget. Un autre projet a été dévoilé mi-2021 par l'UE. Il s'agit de **la Joint Cyber Unit, une structure de préparation et de coordination face aux cyberattaques**, prévue pour être opérationnelle en 2023. Son action s'étendra aux domaines de la résilience, de la répression, de la défense et de la diplomatie. Elle aura notamment pour but de **travailler avec le CyCLONe et les différentes agences nationales et communautaires**. La Joint Cyber Unit sera financée par la Commission européenne ainsi que des contributions éventuelles du Fonds européen de la défense.

La France souhaite par ailleurs **renforcer ses différentes initiatives dans le cadre de sa présidence du Conseil de l'Union**, qu'elle occupera début 2022. L'Anssi a détaillé plusieurs propositions lors du Forum international de la cybersécurité en septembre 2021, comme la mise en place d'un Centre européen de compétences industrielles, technologiques et de recherche dans le domaine. Un exercice de grande envergure concernant la gestion d'une cyberattaque avec l'organisation CyCLONe pourrait également être mis en place.

Mi-2020, **l'Union européenne a pour la première fois sanctionné des entités étrangères** (russes, chinoises et nord-coréennes) pour des faits d'atteinte à la sécurité numérique. Elle a instauré un gel des avoirs ainsi qu'une interdiction d'entrée sur le territoire européen.

UN ÉCOSYSTÈME EN VOIE DE STRUCTURATION

De grands groupes français innovants

La France consolide ses positions dans le secteur

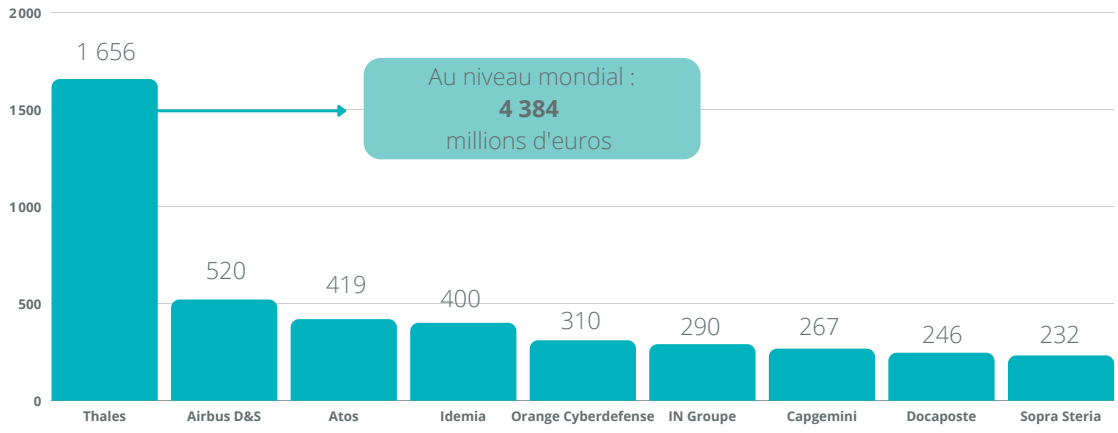
L'économie française peut compter sur un grand nombre de groupes dans les domaines de la défense, des communications ou encore des services numériques pour développer une offre performante en cybersécurité.

L'industrie de la défense investit le créneau de la cybersécurité

Les groupes Thales et Airbus Defence and Space se positionnent de plus en plus dans le domaine. Les deux entités ont annoncé en 2019 **la création d'une offre commune** basée sur la solution Cybels Sensor du premier et Orion Malware, développée par Airbus CyberSecurity. La technologie de Thales passe au crible une grande quantité de données afin de détecter les anomalies, les fichiers suspects étant ensuite analysés par la solution d'Airbus. Celle-ci fournit un rapport détaillant les risques ainsi qu'un résumé pouvant être lu et compris par des non-spécialistes. L'année précédente, Thales avait fait **l'acquisition du groupe français Gemalto**, spécialisée dans la sécurité numérique. Il souhaitait par ailleurs "devenir à court terme **le leader en Europe de la cybersécurité du véhicule autonome et connecté**", selon les mots de son vice-président chargé de la cybersécurité, Jean-Marie Lefort, interrogé par *L'Usine nouvelle*. Le groupe comptait alors environ 2 000 experts du domaine, tandis qu'Airbus CyberSecurity disposait de 850 employés.

Les leaders français de la cybersécurité

Chiffre d'affaires dans la confiance numérique, en France en 2020, en millions d'euros



Traitement IndexPresse. Source : Observatoire ACN de la Confiance Numérique

Des entreprises de services numériques bien positionnées

Plusieurs groupes, présents dans la transformation digitale, le cloud ou encore les activités de conseil, proposent également des offres dans le domaine de la cybersécurité. Numéro trois en France du marché de la confiance numérique en termes de chiffre d'affaires, Atos a poursuivi dans cette voie avec **l'acquisition fin 2020 de l'entreprise française Digital.Security**. Cette dernière s'est spécialisée dans la sécurisation des objets connectés. La branche du groupe dédiée à la cybersécurité est ainsi **passée de 150 à plus de 400 experts**. Jean-Claude Tapia, alors directeur de Digital.Security (et futur dirigeant de la *business unit* d'Atos), expliquait la pertinence de l'opération à *L'Usine digitale* : "**il y a une forme de complémentarité** : ils ont des SOC (*Security Operations Center*), nous avons un CERT ; ils sont présents dans la défense et les administrations, nous dans les secteurs bancaires et industriels…" Fondée en 2015, la firme était une filiale d'Econocom.

De son côté, Capgemini coordonne depuis 2019 **le projet européen Phoenix** visant à assurer une meilleure protection des réseaux électriques. Celui-ci est doté d'un budget de huit millions d'euros et se terminera en 2022. Le groupe a par ailleurs mis en place mi-2021 **un partenariat avec les sociétés françaises Apsys et Utac** afin de procéder à des tests et ainsi d'améliorer la cybersécurité des véhicules civils comme militaires. Deux mois plus tard, **une autre collaboration a été initiée avec l'éditeur de logiciels de cybersécurité Tehtris**. Cette dernière prend la forme d'une offre commune dans le domaine, permettant la détection des attaques et l'automatisation de la réponse. Elle comporte des outils basés sur l'intelligence artificielle ainsi qu'un centre de supervision.

Sopra Steria a pour sa part lancé en septembre 2021 **une nouvelle offre de cybersécurité** centrée sur la gestion de crise. Elle s'appuie sur plusieurs logiciels tiers comme Quarksflow et Glimps-Malware. Le groupe a en outre annoncé le mois suivant sa volonté d'**acquérir le cabinet français spécialiste de la cybersécurité EVA Group**. Le projet devrait être finalisé d'ici fin 2021. En 2020, Sopra Steria avait par ailleurs racheté l'entreprise spécialiste du numérique Sodifrance.

Orange, un opérateur télécom dans la cybersécurité

Avec la création de sa filiale Orange Cyberdefense en 2014, l'opérateur français apparaît comme **un acteur majeur du domaine**. Son offre de détection et de gestion des cybermenaces MicroSOC, lancée en 2020, a dépassé les 200 clients l'année suivante. Cette dernière **s'appuie sur des partenaires** tels que Tehtris, Palo Alto Cortex ou encore SentinelOne. Orange souhaite la développer afin de **réaliser des économies d'échelle**, comme l'indiquait le chief developement officer Benjamin Serre au site *Solutions numériques* fin 2021 : "Un SOC est coûteux à mettre en place car, pour chaque client, on doit se livrer à une analyse de risque et créer des playbooks de détection spécifiques. **L'offre MicroSOC est au contraire un modèle industriel** avec un EDR qui est opéré de la même façon pour tous nos clients. Avec l'automatisation, **c'est la clé pour abaisser les coûts**, et c'est ce qui va nous permettre d'aller vers les professionnels, les PME de moins de 10 personnes et le grand public. Cette offre sera lancée début 2022." Orange Cyberdefense a par ailleurs mené **une stratégie d'acquisitions au niveau européen** avec les rachats en 2019 de la société britannique SecureDate et de la néerlandaise SecureLink. En France, l'entreprise a **obtenu en 2021 le certificat PRIS** (Prestataire de réponse aux incidents de sécurité) délivré par l'Anssi. Elle n'est que la seconde organisation à recevoir ce label, après le cabinet de conseil en transformation numérique Wavestone en 2020. Celui-ci indique que la société propose des offres conformes aux 213 exigences édictées par la Loi de programmation militaire 2019-2025, lui permettant de **fournir ses solutions aux opérateurs d'importance vitale** (OIV, dans la santé, l'énergie, la finance…). Orange Cyberdefense pourrait être **séparé du reste du groupe afin d'entrer en Bourse**. Ce projet de cotation demeure pour l'instant en suspens, alors que les syndicats s'y opposent et que l'ancien directeur, Michel Van Den Berghe, contestait également cette volonté. Il a démissionné en 2021, officiellement pour prendre la tête du Campus Cyber.

De nombreux dépôts de brevets

Les groupes français continuent d'investir dans la recherche afin de développer de nouvelles technologies dans le domaine de la cybersécurité. **Depuis 2017, plusieurs centaines de familles de brevets ont été déposées** par ces derniers ainsi que par les centres de recherche. **Thales et Orange se présentent comme les innovateurs les plus importants** avec un portefeuille supérieur à 300 brevets en France. Ils prennent également la tête du classement en termes de dépôts de brevets durant les quatre dernières années. Issu de la fusion en 2017 entre Oberthur Technologies et Morpho (ex-Safran Identity & Security), **le groupe Idemia apparaît aussi comme un déposant majeur** avec un stock dépassant 200 brevets. Le spécialiste de l'électronique STMicroelectronics dispose lui aussi d'un portefeuille de brevets conséquents, ses marchés comme l'automobile, l'informatique, l'industrie ou les objets connectés étant fortement exposés aux cybermenaces. Bien qu'affichant un nombre de brevets total inférieur aux groupes précédemment cités, **le CEA s'est fortement engagé dans la recherche relative à la cybersécurité** avec 39 familles de brevets déposées depuis 2017. Les groupes Atos, Airbus ou Sagemcom (communications) représentent également des acteurs importants dans l'innovation en cybersécurité, chacun possédant plusieurs dizaines de brevets dans le domaine.

La communication digitale, les technologies informatiques et les télécommunications constituent **les principaux domaines techniques** auxquels se rapportent les brevets déposés. Thales et PSA se distinguent avec un nombre de brevets liés au transport plus élevé que chez les autres acteurs.

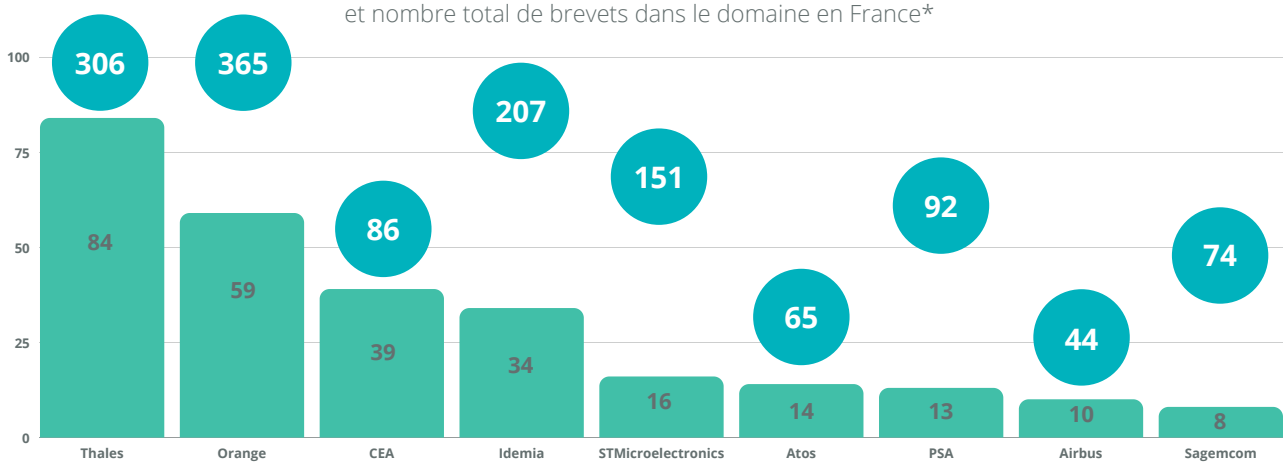
>300

Le nombre de brevets de Thales et Orange dans la cybersécurité

Source : Questel

Des groupes français impliqués dans la recherche et l'innovation

Nombre de familles de brevets déposées en France dans la cybersécurité entre 2017 et 2021, et nombre total de brevets dans le domaine en France*



Traitement IndexPresse. Source : Questel *les brevets d'entité différentes sont rassemblés sous le nom du groupe

Un vivier de start-up qui se renforce

Des jeunes pousses de plus en plus nombreuses

La création d'entreprises demeure dynamique

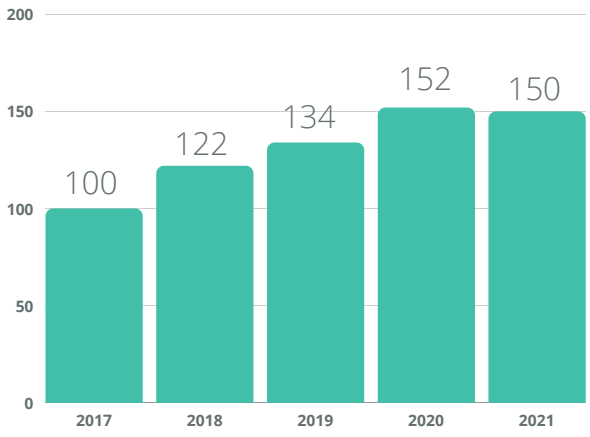
Le nombre de start-up positionnées dans la cybersécurité ne cesse de croître en France. Il est ainsi **passé d'une centaine en 2017 à environ 150 en 2021** selon le cabinet Wavestone. Ce dernier retient dans son recensement les sociétés ayant au maximum sept années d'existence et 35 employés. Wavestone a noté **la création de 19 nouvelles sociétés** dans le secteur durant l'année 2020. Le nombre global de start-up est cependant resté stable du fait de plusieurs sorties, notamment **13 entreprises à présent considérées comme "scale-up"** : elles ont perçu un financement d'au moins dix millions d'euros sur trois ans, ou ont connu un niveau et une croissance de leur chiffre d'affaires suffisamment élevés pour changer de catégorie. Reflet des recrutements massifs des petites entreprises de 10 à 20 personnes, **l'effectif moyen de cette catégorie a augmenté de 24 % en 2020**. Les jeunes sociétés disposant de plus de 20 employés ont également vu leur part augmenter de 16 %. Les plus petites équipes (moins de dix salariés) ont elles reculé de 15 %.

Un impact limité de la crise de Covid-19

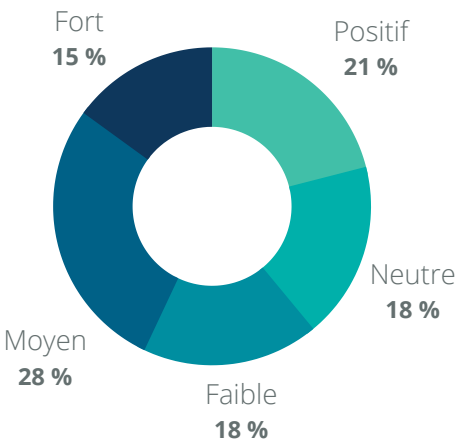
Bien qu'impactées, les start-up de la cybersécurité n'ont globalement **pas connu de difficultés majeures** avec la crise sanitaire. En juin 2020, elles n'étaient que **37 % à affirmer avoir perdu des marchés** à cause de la pandémie selon un sondage de Wavestone. Un tiers estimait que la crise n'avait pas d'effet notable sur leur activité, **21 % observant même des gains d'opportunités**. Ce chiffre s'est révélé identique en juin 2021. La part des start-up ayant subi un impact négatif significatif a **toutefois grimpé à 43 %** entre juin 2020 et le même mois de 2021, dont 15 % déplorant des conséquences fortes pour leur activité. Les jeunes pousses ayant connu de faibles difficultés et celles déclarant une absence d'effet de la crise sanitaire arrivent à égalité, à 18 %.

Un dynamisme entrepreneurial avéré

Évolution du nombre de start-up françaises dans la cybersécurité



Impact de la crise sanitaire sur les start-up françaises dans la cybersécurité, en 2021



Traitement IndexPresse. Source : Wavestone

Un financement en progression

Les levées de fonds des start-up de la cybersécurité ont **quadruplé sur la période 2017-2021**, atteignant environ 100 millions d'euros en fin de période. Certaines jeunes sociétés sont en outre **sorties de ce recensement du fait d'importantes opérations de financement**. L'entreprise Dashlane a ainsi réalisé une levée de fonds de **98 millions d'euros en 2019** auprès notamment des fonds Sequoia Capital, Rho Ventures et Bessemer Ventures Partners. De son côté, Vade Secure a rassemblé **70 millions d'euros la même année** auprès de General Catalyst. En avril 2019, la start-up Sqreen a elle **levé 12,5 millions d'euros** auprès de Greylock Partners, Y Combinator ou encore Alven. Ces opérations d'envergure aboutissent à un niveau de financement supérieur des entreprises de cybersécurité en développement : elles ont ainsi reçu **311 millions d'euros en 2019**, un montant qui dépasse nettement les 80 millions mobilisés par les seules start-up. **En 2018, ce dernier s'était élevé à 114 millions d'euros**, un niveau proche de la part dévolue aux jeunes pousses.

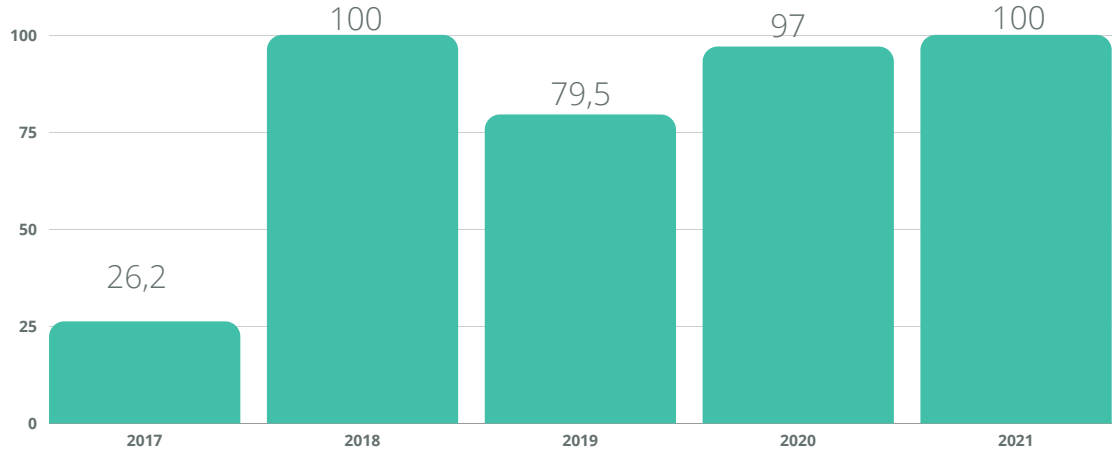
100 millions d'euros

Les fonds levés par les start-up françaises de la cybersécurité en 2021

Source : Wavestone, 2021.

Des levées de fonds régulières

Évolution des montants levées par les start-up françaises de la cybersécurité, en millions d'euros



Traitement IndexPresse. Source : Wavestone

Une multitude d'acteurs se positionnent, privilégiant le SaaS et la vente indirecte

L'attractivité du secteur se manifeste par la création de nombreuses entreprises, qui tentent de proposer des solutions de cybersécurité innovantes.

Fondée en 2014, la start-up i-Guard a mis au point **un système EDR** (*endpoint detection and response*) **basé sur l'intelligence artificielle**. Ce dernier ne nécessite pas de mise à jour pour conserver son efficacité grâce au *machine learning*, et peut **prendre des décisions de sécurité en toute autonomie**. En 2017, l'entreprise a lancé **une nouvelle offre dédiée aux TPE et aux particuliers**, "EDR pour tous". Thierry Goigoux, président de i-Guard, affirmait alors dans un article du site *MtoM Mag* : "nous sommes le seul éditeur à oser proposer aux particuliers et autres travailleurs indépendants de véritables nouveautés technologiques pour leur cybersécurité." À l'international, la start-up s'appuie sur un réseau de distributeurs.

L'entreprise Culmineo a également été créée en 2014. Elle propose un outil permettant de **se protéger contre les pics de fréquentation** d'un site afin d'assurer une continuité de son fonctionnement. Il permet de **lutter contre les attaques par déni de service** tout en évitant les problèmes de congestion liés à un trop grand nombre de requêtes. "La disponibilité fait aussi partie de la cybersécurité !", indiquait en mars 2020 dans *L'Informaticien* le dirigeant de Culmineo, Christophe Denoyer. Il expliquait le fonctionnement de la solution : "nous recueillons un ensemble de données qui permettent au système de se focaliser sur les connexions et requêtes douteuses. (...) Ensuite, nous analysons le parcours, la vitesse d'enchaînement des requêtes, et d'autres caractéristiques de la navigation." L'outil de Culmineo présente ainsi **un potentiel d'identification très fin du public**, lui permettant d'identifier avec précision les différents types de visiteurs. Il peut par conséquent favoriser la fluidité du parcours des clients potentiels au détriment des simples curieux, et **ralentir les robots destinés à paralyser le site Internet ou à récupérer de l'information pour un concurrent**. Christophe Denoyer indiquait que "ce qui est acceptable pour un humain qui ne consulte qu'une page toutes les dix secondes ou moins ne l'est pas pour un robot programmé pour faire du request flood. **Les attaquants n'ont pas des ressources infinies** : la tactique appliquée (...) consiste à leur demander d'utiliser plus de ressources que ce dont ils disposent." La start-up avait intégré l'incubateur IONIS 361 en 2016.

De son côté, la société Gatewatcher a été créée en 2015. Elle a développé **une solution de détection des cyberattaques** pour les entreprises. Jacques de la Rivière, président-directeur général de l'entreprise, expliquait dans *L'Usine nouvelle* : "si l'on simplifie, une sonde de détection c'est l'équivalent d'un détecteur d'incendie pour une usine. Elle analyse toutes les données qui circulent pour détecter un comportement anormal ou malveillant." La société a **reçu en 2019 la certification "visa de sécurité" de l'Anssi** pour sa sonde TrackWatch Full Edition, ce qui lui a permis de viser les OIV (opérateurs d'importance vitale). Début 2021, **elle contrôlait la quasi-totalité de ce marché** d'après le site *ChannelNews*. La start-up revendiquait avoir installé plus de 300 de ses systèmes, dont une centaine en 2020. La même année, elle a augmenté ses effectifs de 50 %, passant de 40 à 60 salariés. **Elle se rémunère via une formule d'abonnement** dont le montant varie en fonction des quantités de données à analyser. Son chiffre d'affaires s'est lui aussi fortement accru, atteignant **10 millions d'euros en 2019 contre 4 millions l'année précédente**. Pour 2021, l'objectif de l'entreprise consiste à déployer 200 systèmes supplémentaires et à recruter 20 employés de plus. Gatewatcher vise **un chiffre d'affaires réalisé à 80 % à l'étranger à l'horizon 2025**, contre 30 % en 2019. Elle se développe également en collaborant avec des prestataires comme Orange Cyberdefense, Atos et Sopra Steria. Elle a notamment noué un partenariat avec le Crédit Agricole en 2021. Elle travaille par

ailleurs avec l'association Luatix qui promeut les solutions open source en cybersécurité. En 2020, Gatewatcher a procédé en outre à **l'acquisition de la société française LastInfoSec en 2020**, spécialisée dans le renseignement lié aux cybermenaces. Elle a remporté le prix spécial du jury au Forum international de la cybersécurité en 2017, et le challenge cyber du ministère des Armées en 2019.

La start-up Eho.Link s'est positionnée sur le marché en 2016. Elle a développé une solution s'appuyant sur un boîtier, une application et un service SaaS pour **analyser tous les flux entre le réseau de l'entreprise et Internet**. Des alertes sont automatiquement émises pour signaler les anomalies. Ces dernières sont **définies en fonction de critères spécifiques au client**, comme les sites Internet dont l'accès est restreint, la politique interne concernant la navigation privée ou encore la gestion des mots de passe. **La société se focalise sur les petites entreprises** : "nous ciblons les TPE/PME parce qu'elles sont mal équipées et ne mesurent pas précisément leurs besoins de protection et leurs obligations, alors qu'**il est plus grave pour une société de dix personnes de subir une attaque**, de perdre l'accès à tout son système d'information, que pour un groupe de 2 000 personnes qui disposera des ressources internes pour s'en relever", comme le précisait son président, Christophe Mansincal, à *L'Usine digitale*, fin 2021. La start-up les soutient également dans **leur mise en conformité avec la législation**, notamment concernant la confidentialité des données. Elle cherche à s'appuyer sur un réseau de distributeurs (intégrateurs IT, revendeurs…), via notamment des partenariats avec les entreprises Feeder et Bluemega. **Elle a réalisé deux levées de fonds**, l'une en 2019 et l'autre en 2020, pour un montant de 3 millions d'euros. **Une nouvelle opération a été effectuée** en 2021 à hauteur de 2 millions d'euros supplémentaires.

En 2016, un autre acteur a été créé dans le secteur : ContentArmor, **spécialiste du tatouage numérique dit "en filigrane"** (*watermarking*). L'entreprise peut marquer les copies de contenus vidéo afin d'**identifier les sources en cas de piratage ou de diffusion illégale**. Chaque copie s'avère ainsi "tatouée" de façon indétectable par le spectateur, le système se montre complexe à neutraliser par les pirates. Alain Durand, cofondateur, expliquait l'avantage compétitif de ContentArmor fin 2019 au site *Bretagne Économique* : "Contrairement à nos concurrents, nous sommes capables de *watermarquer* sur du contenu compressé, directement en régie juste après l'encodage des vidéos destinées au live. Résultat, **notre technologie utilise moins de puissance de calcul et donc moins de mémoire**." En 2021, la moitié du chiffre d'affaires de la start-up provenait des studios de production audiovisuelle, 30 % des plateformes de vidéo à la demande et 20 % du direct sur Internet et des compagnies aériennes. Son principal client était Mediasilo.com, une plateforme américaine de partage de vidéos entre professionnels. **ContentArmor a opté pour la vente indirecte**, sa solution étant vendue par des agrégateurs de services aux diffuseurs.La société se diversifie, notamment via **des accords de collaboration** : "on développe des partenariats avec des acteurs comme Viaccess Orca, filiale d'Orange, qui fournit des systèmes de contrôle d'accès aux chaînes payantes. Sur ce marché, les Européens et les Asiatiques sont très demandeurs. En 2020, le sport devrait représenter un tiers de notre chiffre d'affaires", expliquait le dirigeant fin 2019. La jeune société a réalisé **une levée de fonds de 1,1 million d'euros en 2017** auprès de Calao Finance, Bpifrance, le Crédit Agricole ou encore le fonds breton Breizh Up. En 2021, **le groupe britannique Synamedia**, spécialisé contre le piratage, **a racheté les parts** de Calao Finance et de Breizh Up, acquérant ainsi le contrôle de l'entreprise.

OneWave a pour sa part développé **des cartes Bluetooth et biométriques permettant de gérer les accès aux systèmes d'information**. Créée en 2016, l'entreprise offre une solution intégrant **un gestionnaire de mots de passe et un dispositif de double authentification**, empêchant les intrusions en cas de tentative de phishing. Équipées d'un écran, voire de boutons tactiles, **les cartes chiffrent les données et les communications** et peuvent afficher les codes-barres et les QR codes professionnels. **La start-up cible en priorité le marché BtoB**, comme l'indiquait à *L'Usine digitale* fin 2021 le fondateur, Thomas Lechevallier : "nous visons en particulier le secteur du nu-

mérique, avec les ESN, les éditeurs de logiciels, les hébergeurs… mais aussi les experts-comptables." OneWave souhaite cependant **étendre son activité en BtoC**. Elle a dans ce but mis en place une expérimentation avec la société Keolis, qui s'est achevée en septembre 2021. Une centaine de particuliers ont ainsi pu utiliser les cartes connectées de OneWave comme titres de transport. Ces dernières sont **commercialisées sous forme d'abonnement**, et s'accompagnent d'un logiciel SaaS de gestion des cartes ainsi que d'options complémentaires (contrôle accès physique, sauvegarde des données…). La jeune pousse a réalisé **plusieurs opérations de financement**. En 2017, elle a récolté près de **300 000 euros** sur la plateforme de crowdfunding Gwenneg. Une levée de fonds de **265 000 euros** a ensuite été effectuée en 2020, complétée par Bpifrance à hauteur de **700 000 euros**. La start-up a rassemblé **600 000 euros** lors d'une autre levée de fonds en 2021.

La société Red Alert Labs, fondée en 2017, s'est quant à elle **spécialisée dans les solutions de sécurité dédiées à l'Internet des objets**. Elle propose différents produits et services, tels que **le logiciel de veille et de détection** des menaces IoT Inspector, des tests de pénétration des systèmes, des analyses de risques, des formations spécifiques ou encore des accompagnements relatifs à des certifications. Elle se positionne **auprès de clients variés** : Thales, CS Group, Sigfox, Legrand, l'Agence du Numérique en Santé…

Yagaan a elle aussi été lancée en 2017. Elle développe **des solutions de détection des vulnérabilités des applications, dédiés aux équipes de développeurs**. Ces derniers peuvent ainsi procédér aux améliorations lors de la phase de création de l'outil (DevSecOps). Le cofondateur Hervé Le Goff expliquait mi-2020 au site *Le Mag IT* : "nous sommes partis du constat que, pour développer des applications sûres, il faut fournir des outils pertinents aux équipes de développement afin qu'elles puissent **intégrer la sécurité dès le début**." La solution se veut apprenante grâce à un système autonome et supervisé permettant "**d'automatiser la classification des alertes**." Une autre fonctionnalité offerte par l'outil de la jeune pousse rend possible l'intégration de descriptions relatives aux finalités de l'application. Les anomalies détectées peuvent être **transmises non seulement aux ingénieurs mais aussi aux autres départements concernés** afin d'établir plus précisément les risques afférents. Yagaan se rémunère via **des formules d'abonnement** (SaaS ou installation des logiciels en interne) **et par des prestations ponctuelles**. La start-up a reçu le prix de l'innovation au salon ViV Healthtech 2020, et annonçait vouloir réaliser une levée de fonds.

Citalid a développé de son côté **un logiciel d'évaluation et de gestion des systèmes de cybersécurité** d'une entreprise. Lancée en 2017, elle propose à ses clients **un panorama des risques spécifiques** auxquels ils sont confrontés ainsi qu'**une simulation des coûts afférents**, tant au niveau des pertes potentielles que des dépenses en cybersécurité. Les utilisateurs peuvent modifier de façon virtuelle leur politique de sécurité afin d'**identifier l'impact des changements opérés et optimiser le budget dédié**. Maxime Cartan, fondateur et CEO, soulignait aux *Échos* fin 2019 : "C'est un sujet fondamental et pourtant encore trop entre les mains des équipes techniques. Avec Citalid, nous voulons **nous adresser directement aux décideurs** pour déclencher des budgets et mettre en place une stratégie de cybersécurité la plus adaptée à chaque entreprise." L'entreprise compte des clients dans l'énergie, la finance ou encore les transports. Mi-2019, elle a réalisé **une levée de fonds de 1,2 million d'euros** auprès d'Axeleo Capital et de BNP Paribas. Cette opération lui permettra de développer une offre de cyberassurance et de poursuivre son développement commercial. Peu après sa création, la start-up avait bénéficié d'un partenariat avec l'École Polytechnique visant à améliorer ses algorithmes en modélisant le risque géopolitique. **Elle a remporté plusieurs prix**, notamment ceux de l'innovation et du public aux Assises de la sécurité de 2018, et le prix du Jury du Forum international de la cybersécurité de 2020. Elle fait également partie des lauréats du Grand Défi Cyber organisé en 2021 par le gouvernement. Citalid a en outre été **soutenue par plusieurs programmes et incubateurs**, à l'instar de Shake'Up de Wavestone, l'accélérateur Allianz ou encore le Scale du cabinet PwC.

Fondée en 2017, Cybelius s'est spécialisée dans **la protection des systèmes numériques industriels**. L'entreprise a développé plusieurs solutions (notamment CyFence et CyPres) afin de cartographier les réseaux, de détecter les vulnérabilités et de faciliter les interventions. **Elle a noué de nombreux partenariats** avec des sociétés comme Network Perception, Inetum ou encore Semeru. En juin 2020, Cybelius s'est associée à Sesame IT pour développer en commun **une sonde destinée aux opérateurs d'importance vitale (OIV)**. Elle a ensuite renforcé sa collaboration avec Inetum qui a rejoint les deux partenaires pour créer une offre globale. La start-up a en outre mis en place **une alliance technique et commerciale** avec le spécialiste en sécurité des infrastructures critiques Selab début 2021.

La société Cyrating s'est positionnée en 2017 dans **la notation des politiques de cybersécurité des organisations**. Elle se revendique comme la première agence européenne du domaine. Sa solution fournit **une note globale de l'exposition au risque** de la structure évaluée, reposant sur des critères quantitatifs et automatisés. Interrogé par le site *Alliancy* mi-2018, François Gratiolet, cofondateur de Cyrating, expliquait l'intérêt de la démarche : "les entreprises cherchent à **se renseigner sur leur propre situation**, à appréhender l'impact de leurs arbitrages en matière de cybersécurité. **Elles se comparent à leur secteur** ou examinent les différences entre entités et filiales. Surtout, **elles évaluent la sensibilité de leur écosystème**. Quand on traite avec des centaines de fournisseurs, on est incapable de les évaluer en continu…" En 2018, **Cyrating a établi des partenariats** avec les entreprises de cybersécurité Excellium (Luxembourg) et UbCom (Suisse) et l'agence de notation digitale française D-Rating.

HarfangLab a pour sa part été lancée en 2018. La société a mis au point un EDR, un système de lutte contre les cybermenaces qui agit au niveau des terminaux. Elle dispose du **seul EDR certifié par l'Anssi et commercialise sa solution en SaaS ou sur site (*on-premise*) de façon indirecte**, par le biais de partenariats avec des acteurs tels que PwC, Wavestone et Intrinsec. Elle compte parmi ses clients Thales, Safran, Sanofi et le ministère des Armées, et cherche à s'adresser aux collectivités territoriales. L'entreprise met en avant **le caractère ouvert, flexible et transparent** de solution, permettant une intégration facilitée dans les systèmes informatiques et de sécurité des clients. HarfangLab a été lauréate du Grand Défi Cyber organisé par l'État en 2021. La même année, elle a effectué **une levée de fonds pour un montant de 5 millions d'euros**, dont 3,5 millions provenant du fonds Elaia et 1,5 million sous forme de prêt. Elle a par ailleurs noué une collaboration avec le cabinet de conseil en cybersécurité EVA Group fin 2021. À la même période, **elle s'est associée avec les entreprises Sekoia et Pradeo**, respectivement spécialistes en renseignements sur les menaces (*threat intelligence*) et en protection des terminaux et applications mobiles. Les trois entités proposent ainsi **un bouquet commun modulable** selon les besoins des clients. Clément Saad, dirigeant de Pradeo, expliquait alors à *L'Informaticien* : "aucune structure française n'a la capacité de traiter tout l'éventail de la sécurité à elle seule. Mais nous avons des champions, chacun dans son domaine." Le partenariat vise également à **simplifier la tâche des ingénieurs en cybersécurité** grâce à une solution unifiée. Après avoir atteint un million d'euros de chiffre d'affaires en 2020, HarfangLab compte **doubler ce montant d'ici fin 2021**. La start-up devrait en outre passer de 30 collaborateurs à une quarantaine sur la période.

Également créée en 2018, la start-up Serenicity a quant à elle développé **un ensemble de six solutions dédiées avant tout aux TPE-PME** et aux collectivités locales. "Ce que l'on veut faire, c'est apporter un niveau de sécurité équivalent aux TPE que celui dont peuvent disposer les grands groupes", indiquait mi-2021 au *Monde Informatique* Cyrille Elsen, directeur des systèmes d'information de l'entreprise. L'offre combine des systèmes de détection et de blocages des éléments suspects ainsi que des dispositifs de supervision. S'appuyant sur **un modèle d'abonnement en vente indirecte**, l'entreprise revendiquait plus de 250 clients en 2021. Elle se montre **également présente dans le domaine de la *safe city*** avec des détecteurs phoniques alertant les autorités en cas de signaux anormaux. L'expérimentation menée à Saint-Étienne a toutefois été annulée par la Cnil fin 2019. Serenicity a réalisé **deux levées**

de fonds de montants non communiqués. Elle a successivement intégré le Village By CA en 2019 et la Manufacture Cyber en 2020.

Fondée en 2019, Aucae a pour sa part mis au point un système de **prévention, de formation et de gestion de crise** en cas de cyberattaque. Baptisé "Digital Crisis Response", le dispositif propose des entraînements, des fausses attaques, des questionnaires ou encore un suivi des comportements afin d'identifier les risques. La solution offre également des fonctionnalités de **création et de gestion d'une cellule de crise**, avec un plan d'action associé. Aucae commercialise son outil **en mode SaaS** mais il peut aussi **être installé directement sur les terminaux du client**. L'entreprise s'adresse à des secteurs variés, ayant décroché des contrats avec un groupe hôtelier, un acteur industriel ainsi que **la Centrale d'Achat de l'Informatique Hospitalière (CAIH), qui représente 1 300 établissements**. Aucae avait organisé en mai 2021 un exercice de simulation d'une cyberattaque avec les membres du groupement. Elle est soutenue par la société de financement Crealia Occitanie et a **intégré l'incubateur Nubbo en 2020**.

La jeune entreprise TrustHQ (anciennement MyPSSI) s'est lancée sur le marché en 2020. Elle a développé **un logiciel de gestion de la cybersécurité**, offrant un suivi global des politiques mises en œuvre et des missions réalisées par les équipes internes. Il fournit également **un système de reporting permettant d'uniformiser et de centraliser** les informations transmises par les collaborateurs. L'outil cartographie les exigences réglementaires afin d'ajuster les demandes assignées aux équipes. Gilles Favier, le fondateur, expliquait l'un des intérêts de sa solution à *IT for Business* fin 2020 : "un RSSI peut toujours obtenir un point de situation sur un système à un moment donné en réalisant un audit. Mais il lui est très difficile de **savoir si une procédure est appliquée et de disposer de la preuve que les actions de cybersécurité ont bien été réalisées**." L'entreprise souhaitait alors atteindre une cinquantaine de clients en 2021 en commercialisant son service sous la forme d'abonnements SaaS. Elle espérait **réaliser une chiffre d'affaires compris entre 400 000 et 600 000 euros**. Parmis ses projets, TrustHQ prévoyait de mettre au point une version dédiée aux PME et d'utiliser l'intelligence artificielle pour améliorer la cartographie de conformité.

La start-up Mantra, elle aussi créée en 2020, propose **un outil de simulation d'attaque de type phishing**. En échangeant avec l'entreprise cliente, elle personnalise les faux emails envoyés aux collaborateurs. "On commence par scanner le contexte de la société : qui sont les personnes-clés, les outils utilisés, dans quel département travaillent les salariés à former… Cela permet d'**envoyer de faux mails très ciblés**", expliquait le cofondateur Gaspard Droz au site *Maddyness* mi-2021. Les employés peuvent signaler les messages suspects et ainsi gagner des points, **Mantra s'appuyant sur la gamification pour stimuler la formation**. Les personnes piégées par les diverses méthodes utilisées par l'entreprise reçoivent des informations afin d'être plus vigilantes à l'avenir. La jeune société a décroché des contrats avec Aircall, Lifen ou encore Dataiku. Elle souhaite **accélérer son développement auprès des ETI**, souvent plus démunies face à la cybermalveillance. Mantra a réalisé dans ce but **une levée de fonds de 1,6 million d'euros en 2021** auprès de OneRagTime, Bpifrance et Axeleo. Elle devrait également développer de nouvelles solutions de prévention des cybermenaces.

Créée en 2021, la société Astrachain a développé l'Omnicloud, une solution permettant de **relier plusieurs fournisseurs cloud afin de réduire la dépendance** et donc les risques d'interruption de service. Les données sont **chiffrées et réparties simultanément chez les différents prestataires**, ces derniers n'hébergeant ainsi que du contenu parcellaire. Cette méthode **limite les risques en cas d'intrusion** ou d'accès non souhaité d'une puissance étrangère aux informations stockées. Les serveurs utilisés par le service d'Astrachain sont implantés en Europe et conformes au RGPD. La société propose le service SPLIT, **un *safe-as-a-service* ou coffre-fort numérique multicloud**. Il s'appuie sur la technologie Omnicloud et s'adresse à des secteurs ayant des exigences fortes en termes de confidentialité et de sécurité, tels que les domaines juridiques et bancaires ou encore celui de la santé. L'entreprise compte plusieurs clients en 2021, tels que Bpifrance, Wavestone, OVHcloud et le groupe Banijay.

La collaboration entre les acteurs progresse

Rennes, place forte de la cybersécurité française

Début 2021, la Bretagne accueillait 130 entreprises dans la cybersécurité pour un total d'environ 8 000 emplois d'après l'agence Bretagne Développement Innovation. Cette concentration s'explique notamment par **la création en 2014 du Pôle d'Excellence Cyber** à Rennes par le ministère des Armées. Les grands groupes comme Airbus et Thales y côtoient des start-up et des centres de recherche. En 2019, l'État y a ouvert **la Cyberdefense Factory** ainsi que des locaux de 11 000 m² pour **le Commandement de la cyberdéfense (ComCyber)**. Celui-ci accueille 400 experts en cybersécurité. Quant à la Factory, elle est rattachée à la DGA et à l'Agence de l'innovation de défense, et permet de **mettre en commun des données pour le développement d'innovations**. La Direction générale de l'armement (DGA) et l'université de Rennes 1 ont par ailleurs **créé en 2020 la Cyberschool**, afin de promouvoir la formation dans le domaine. Environ 2 000 étudiants suivaient un cursus en cybersécurité à Rennes en 2021 selon *L'Usine digitale*.

Les partenariats se multiplient

De nombreux acteurs initient ou consolident des projets de coopération, tandis que de nouveaux organismes spécialisés favorisent l'essor du secteur.

En 2020, l'opérateur Orange a **créé son Centre de formation d'apprentis (CFA)** dans le but de **former environ 80 élèves aux métiers de la cybersécurité** ainsi que d'autres domaines du digital. Il propose des cours uniquement en distanciel tandis que les apprentis restent en entreprise à temps plein. La formation dure de 12 à 24 mois et s'adresse tant aux jeunes qu'aux personnes en reconversion professionnelle. **Elle est conçue avec des partenaires** comme le Cnam (Conservatoire national des arts et métiers) et l'Afdas. Élisabeth Fonteix, directrice du Learning & Development chez l'opérateur, soulignait début 2021 dans *Entreprise & Carrières* "qu'**il existe des métiers émergents pour lesquels il n'y avait pas d'offre de CFA**, comme les data analystes, les ingénieurs en cybersécurité ou encore les spécialistes du cloud." En 2019, **Capgemini avait lui aussi ouvert sa propre école** afin de former 400 ingénieurs en cybersécurité, au cloud ou encore à l'IA.

Plusieurs acteurs tels que Thales, Naval Group et YesWeHack ont fondé fin 2020 **l'association France Cyber Maritime** afin de développer des projets communs liés à la cybersécurité du secteur maritime et portuaire. "**Les navires et les ports se numérisent rapidement**, entraînant de nouvelles opportunités, mais également de nouveaux risques", notait alors le directeur de l'Anssi, Guillaume Poupard. Soutenue par le Cluster maritime français – organisation regroupant plus de 400 acteurs du domaine – l'association vise également à **favoriser l'émergence de nouvelles solutions de cybersécurité spécifiques**. En lien avec l'État, un centre national de coordination de la cybersécurité pour le monde maritime devrait en outre voir le jour en 2022.

De leur côté, La Poste et l'Institut national de recherche en sciences et technologies du numérique (Inria) ont conclu **un partenariat début 2021 pour une durée de trois ans**. Outre le digital écoresponsable et les données de santé, l'un de leurs axes de travail porte sur la confiance dans le numérique. Ce dernier se décline en **plusieurs programmes de recherche concernant la cybersécurité**, la protection des données personnelles et les questions relatives à l'IA. L'accord prévoit également que le groupe La Poste **favorise la formation et le recrutement** de chercheurs et d'ingénieurs de l'Institut. Il devrait par ailleurs **soutenir la création d'une centaine de projets de start-up par an** au sein de l'Inria Startup Studio.

Mi-2021, Airbus CyberSecurity a **renforcé son partenariat avec l'école d'ingénieurs Institut Mines-Télécom (IMT) Atlantique** afin de promouvoir la formation, le recrutement des diplômés et des programmes de R&D. Cette collaboration avait été lancée en 2017. La filiale du groupe aéronautique avait par ailleurs **noué un partenariat avec le Cnam Grand Est** en 2020. Ce dernier incluait la fourniture de la solution Cyber-

La cyberassurance, un domaine amené à se développer

Fin 2021, l'Association pour le Management des Risques et des Assurances de l'Entreprise (Amrae) indiquait que 87 % des grands groupes en France disposaient d'une cyberassurance, un chiffre tombant à 8 % pour les ETI, 1 % chez les collectivités et à peine 0,01 % pour les PME. Le marché représentait 130 millions d'euros en 2020. La couverture du risque demeure faible, s'élevant en moyenne à 38 millions d'euros pour les grands groupes et 8 millions pour les ETI. Le coût élevé de telles garanties et la frilosité des assurances amènent les entreprises à payer les rançons en cas de cyberattaques, un choix fait par 65 % d'entre elles en France en 2020. Les compagnies d'assurance françaises, moins engagées dans le domaine que leurs homologues anglo-saxonnes, défendent l'idée de partenariats public-privé afin d'assurer une meilleure prise en charge par les acteurs. Le ministère de l'Économie a initié en 2021 une réflexion autour de la création d'une offre d'assurance cyber, les résultats devant être dévoilés en 2022.

Range d'Airbus pour soutenir les exercices pédagogiques. Responsable ingénierie chez Airbus CyberSecurity, Éric Chambareau notait dans *Inffo Formation* fin 2020 : "quand des stagiaires ont déjà utilisé la CyberRange et sont formés sur nos outils, il est plus facile de les intégrer dans nos équipes ensuite".

En 2022, **une nouvelle antenne du Campus Cyber devrait ouvrir dans les locaux d'Euratechnologies**, pôle d'innovation réunissant des centaines d'entreprises, d'écoles, de centres de recherche et d'investisseurs. Le projet est soutenu par des groupes majeurs tels comme Atos, Capgemini, Thales et Orange Cyberdefense. Euratechnologies avait par ailleurs ouvert en 2019 **un incubateur dédié à la cybersécurité** ainsi qu'à d'autres domaines (fintech, legaltech...). Ce dernier visait à connaître trois promotions par an, soit un nombre de projets compris entre 20 et 25.

Des structures pour financer l'innovation

En 2017, le fonds français ACE Capital Partners, filiale de Tikehau Capital, a lancé **Brienne III, un véhicule d'investissement dédié à la cybersécurité**. Il a rassemblé 80 millions d'euros en 2019, dont 40 millions provenant de Tikehau Capital. Le financement restant a été apporté par Bpifrance ainsi que Naval Group, EDF, Sopra Steria et la Région Nouvelle-Aquitaine. Il prévoyait d'**investir entre un et dix millions d'euros dans chaque start-up sélectionnée**. À la même période, un partenariat a été signé avec le ministère des Armées, qui présentera des jeunes pousses pouvant faire l'objet d'une participation. Ce dernier confirmait alors à *L'Usine nouvelle* l'importance d'une telle démarche : "on s'est rendu compte que **le domaine de la cybersécurité est peu attractif pour les investisseurs financiers**. C'est un domaine considéré comme très technique, avec des cycles de développement et d'accès aux marchés qui sont parfois jugés trop longs." En 2021, le fonds a bénéficié de **nouveaux apports de capitaux, atteignant 175 millions d'euros** au total. Outre les soutiens historiques, Brienne III a notamment vu le Crédit Agricole venir renforcer ses capacités de financement. Il avait déjà pris des participations à hauteur de 50 millions d'euros dans neuf entreprises françaises et européennes.

Les fonds Axeleo Capital et Go Capital, associés aux incubateurs Axeleo et Le Poool, ont mis en place en 2021 **une nouvelle structure baptisée French Cyber Booster**. Lauréat du Grand Défi Cyber fin 2019, ce projet visait à créer un "start-up studio" ayant pour vocation à accompagner plusieurs dizaines de jeunes sociétés durant trois ans. Un fonds spécifique prévoit de les financer à hauteur de 150 000 euros minimum et devrait être doté de 10 millions d'euros à terme. Le French Cyber Booster est implanté à Rennes et à Paris.

Les jeunes pousses positionnées dans la cyberdéfense peuvent en outre **bénéficier du fonds Definnov**. Créé en 2020 et soutenu par Bpifrance, il est **doté de 200 millions d'euros** et finance des start-up et des PME. Il vient compléter le fonds Definvest, qui dispose quant à lui de 50 millions d'euros.

LA FILIÈRE FACE À DE MULTIPLES ENJEUX POUR SON AVENIR

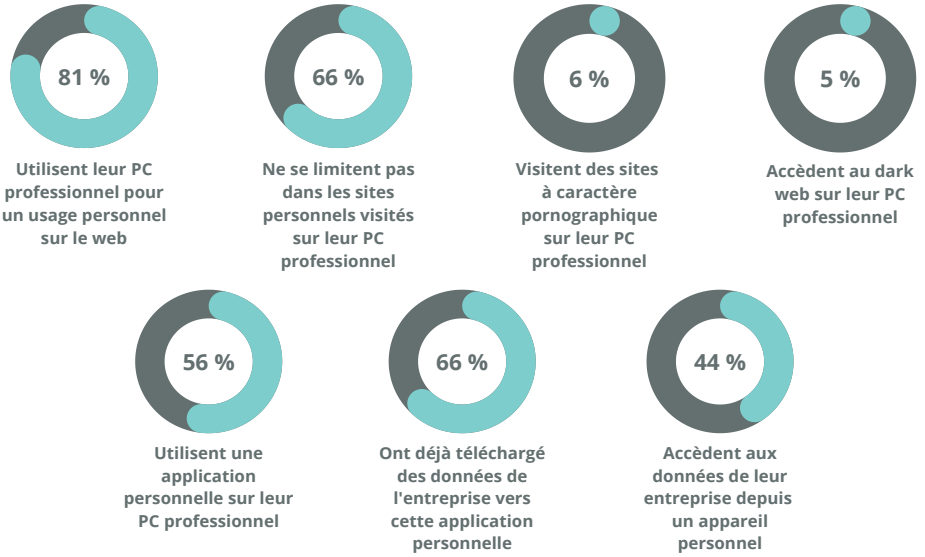
Développer une culture de la cybersécurité

L'humain, une limite à prendre en compte

Si les organisations multiplient leurs équipements et logiciels de sécurité informatique, elles peinent encore à appréhender une faille majeure : l'humain. "Dans de nombreux cas, **l'homme est le maillon faible**, de sorte que tout effort de cyber-résilience doit inclure tous les mécanismes appropriés pour conduire le changement de comportement requis au sein de l'organisation", avertit Synetis, cabinet spécialisé dans la transformation numérique et la cybersécurité. De nombreuses attaques informatiques aboutissent parce qu'**un employé n'a pas respecté les consignes de sécurité ou s'est montré inattentif**. "Les cyberdélinquants ont orchestré leurs campagnes d'emailing à partir de prérepérages de failles techniques ou de comportements à risque de salariés", exposait *Option Finance* en juillet 2020, dans un article évoquant la hausse des cyberattaques durant la crise sanitaire. Les salariés cliquent sur un lien inconnu dans un mail ou téléchargent une pièce jointe non sécurisée, et ouvrent ainsi une porte aux attaquants. De nombreuses autres actions s'avèrent dangereuses pour la sécurité informatique de l'entreprise, depuis l'utilisation d'un appareil ou d'un logiciel non officiel **jusqu'à l'usage d'outils professionnels à des fins personnelles**.

En septembre 2020, la société informatique Trend Micro a mené une enquête sur l'attitude

Comportements des télétravailleurs français durant le confinement du printemps 2020



Traitement IndexPresse. Source : Trend Micro / *L'Informaticien*

des télétravailleurs vis-à-vis de la politique informatique de leur entreprise lors de la période de confinement. Les résultats se révèlent alarmants et démontrent **une prise de conscience insuffisante par rapport à la problématique sécuritaire**, alors que le risque de cyberattaque n'a jamais été aussi fort. 81 % des Français interrogés admettent par exemple utiliser leur ordinateur professionnel pour un usage personnel, tandis que 44 % accèdent aux données de leur société via un appareil personnel, "allant très certainement à l'encontre de la politique de sécurité de leur entreprise", note la revue spécialisée *L'Informaticien*. Dans le même temps, 79 % des sondés estiment pourtant prendre au sérieux les directives de leur service informatique, signe d'**un décalage entre l'intention présumée des employés et leurs actions concrètes**.

Pour les organisations, il devient primordial d'**élaborer une culture de la cybersécurité en interne**, en avertissant les employés sur les risques induits par leurs comportements afin qu'ils les améliorent d'eux-mêmes. La **rédaction de chartes informatiques et de guides de bonnes pratiques**, ensuite diffusés auprès des collaborateurs, constitue un premier pas. "Elles sensibilisent leurs employés sur les comportements à risques comme ouvrir la pièce jointe d'un email suspect, surfer sur des sites illicites ou utiliser une clé USB", précise *L'Usine Digitale*. Des documents déjà rédigés existent et peuvent être relayés. L'Agence nationale de la sécurité des systèmes d'information a déployé un Mooc, *massive open online course*, accessible à tous après inscription sur son site, qui offre une initiation à la cybersécurité et à la protection des outils numériques. Pour accompagner les banques, la Fédération bancaire française a de son côté édité le guide *Cyber-sécurité au quotidien : 9 réflexes clés*, reprenant les principes basiques à respecter afin de limiter les risques d'intrusion.

Afin d'accélérer la formation des employés, il est également possible de **procéder à des fausses attaques ou à des campagnes ciblées**. "Plus engageantes que les formations classiques, les mises en situation permettent aux collaborateurs de se confronter directement à la menace. Une simulation de cyberattaque évaluera le pourcentage d'utilisateurs qui se sont laissés piéger par de faux courriels infectés", explique *L'Usine Digitale*. Partenaire chez Magellan Consulting, un cabinet de conseil en stratégie et systèmes d'information, Arnaud Deschavanne évoque également des "campagnes de sensibilisation avec des démonstrations (ciblées pour les administrateurs, les développeurs), des "campagnes de phishing pour l'ensemble des collaborateurs" afin de les confronter à la réalité du danger, et **des "sessions de sensibilisation personnalisées" pour répondre spécifiquement aux besoins de chaque société**.

La start-up française Mailinblack se positionne sur ce créneau avec sa formule Phishing Coach, qui envoie de faux mails de phishing aux salariés. Le spécialiste des cours en ligne OpenClassrooms s'est associé avec la société pour former ses équipes. "On a eu 35 personnes sur 270 employés qui ont cliqué sans se méfier. Ce qui est intéressant, c'est que plusieurs salariés se sont douté de quelque chose et ont pris sur eux d'avertir au plus vite le reste de leurs collègues", observe Jonathan Lefebre, directeur technique chez OpenClassrooms. Quality Assistance, un spécialiste des sciences analytiques, a également eu recours aux services de Mailinblack et remarque une plus grande méfiance vis-à-vis des mails étrangers depuis l'opération. "Les collaborateurs sont vraiment sensibilisés au problème. Ils sont maintenant plus vigilants face à ce type de pratiques. C'est constructif parce qu'**ils se sentent concernés par le problème désormais**", indique Jean-Pol Dolata, directeur informatique du groupe.

Ces simulations permettent également de **prendre conscience de thématiques annexes, comme le management adéquat à adopter en cas de cyberattaque**. "Il faut aussi entraîner le Comex sur la communication de crise, qui reste mauvaise la plupart du temps", confirme Alain Bouillé, délégué général du Club des experts de la sécurité de l'information et du numérique. Selon une enquête effectuée en février 2021 par ce dernier auprès de responsables de la sécurité des systèmes d'information d'entreprises françaises, seules 33 % des sociétés interrogées possédaient un programme d'entraînement à la cyber-crise.

Les activités de conseil et de formation constituent un élément clé dans la maîtrise des risques cyber

Afin de les aider à bâtir cette culture de la cybersécurité, les entreprises peuvent se tourner vers des cabinets de conseil et de formation positionnés sur cette thématique. À l'image de l'ensemble de la filière cybersécurité, ce segment se développe en France. Entre 2019 et 2020, **le chiffre d'affaires de l'audit, du planning et du conseil cyber a augmenté de 13,6 %, à 1,74 milliards d'euros**. Dans le même temps, la formation à la cybersécurité connaissait une croissance de 5,6 %, à 118 millions d'euros, selon l'Observatoire de la filière de la confiance numérique qui relaie les chiffres du cabinet DECISION. Dans ce contexte de demande en hausse, **les prestataires spécialisés apparaissent donc comme des acteurs clés pour déployer une culture de la cybersécurité efficace**. Sur ce marché en plein essor, ils tentent d'accroître leur pouvoir de marché par divers moyens.

Linkbynet a opté pour **la consolidation en rachetant deux de ses concurrents français** : Securiview, spécialiste de la sécurité des systèmes d'information, en 2018, et Wise Partners, cabinet de conseil en cybersécurité et confiance numérique, l'année suivante. "Nous sommes fiers de cette acquisition qui confirme l'attractivité du groupe Linkbynet en matière de sécurité informatique. Cette ambition de devenir l'un des leaders en France et en Europe se concrétise avec nos 130 collaborateurs dédiés au pôle cybersécurité. Nous avons désormais la force de frappe stratégique, humaine et technologique pour accompagner nos grands comptes dans leur transformation et gestion des risques", indiquait Julien Trassard, membre de la direction générale du groupe, en 2019. Deux ans après cette acquisition, Linkbynet réorganisait son offre autour d'une marque unique, Linkbynet CyberSecurity, concentrant l'ensemble de son expertise autour de la thématique sécuritaire et actant définitivement l'intégration des entreprises rachetées. "Nous assistons à **un phénomène de concentration en quelques acteurs à la taille critique**, dont Linkbynet entend bien faire partie", notait alors *ITRNews*, média spécialiste des marchés numériques. À l'été 2021, Linkbynet était finalement racheté à son tour par le cabinet international Accenture.

En 2018, Hub One, filiale du gestionnaire d'aéroports ADP, avait de son côté pris le contrôle de Sysdream, un spécialiste français des audits et formations en sécurité informatique. En 2020, il finalisait les acquisitions de deux autres sociétés tricolores, Oveliane et OïkiaLog, développeuses de solutions de sécurisation des systèmes d'information. Grâce à ces opérations de croissance externe, Hub One ambitionne de devenir un acteur majeur des services de cybersécurité en France. Ce secteur représente l'un de ses principaux leviers de croissance **pour dépasser les 200 millions d'euros de chiffre d'affaires à l'horizon 2025**, contre 155 millions en 2018.

A contrario de ces entités cherchant à regrouper un maximum de compétences variées, **certains acteurs misent sur une approche très spécifique**. Créé en 2018, RGPD Chatain & Associés accompagne ses clients dans la mise en application du RGPD (Règlement général sur la protection des données) et la sécurisation de leurs données. Le cabinet se charge de la mise en conformité, élabore des modules complémentaires de cybersécurité et propose un volet de formation pour que les outils déployés soient correctement utilisés.

Dans le cadre de la montée en puissance du télétravail, **la formation à distance peut représenter un atout précieux**. Le cabinet Almond se déploie sur ce segment avec son offre BYCE, Boost your cyber experience. Cette plateforme d'e-learning met à disposition des clients huit modules de formation et de sensibilisation sur les virus, les rançongiciels, la gestion des mots de passe, le RGPD, etc. Akerva, un autre cabinet de cybersécurité et

de gestion des risques informatiques, s'était positionné sur l'e-learning dès 2017. En mars 2021, il s'est lancé dans **le micro-learning sur la plateforme spécialisée 2Spark, avec son programme "1 minute for cybersecurity"**. Chaque jour, les clients ont accès à une formation d'une minute qui met en exergue deux questions contextualisées et leurs solutions. Des challenges sont régulièrement proposés pour vérifier que les participants ont retenu les conseils prodigués. Les managers ont accès aux résultats afin de vérifier l'implication des collaborateurs et d'identifier de potentielles lacunes chez certains.

TerraNova Security et Microsoft, un partenariat à l'échelle mondiale

Considéré comme l'un des leaders mondiaux de la sensibilisation à la cybersécurité, avec 1 000 programmes de simulation et plus de 10 millions de personnes formées, le groupe canadian TerraNova Security s'est associé à Microsoft début 2020. Son catalogue de formation a été ajouté à la suite Office 365 Advanced Threat Protection de l'éditeur américain. Microsoft enrichit ainsi sa solution, alors que TerraNova Security peut toucher plus de personnes via ses programmes.

Pallier la pénurie de main d'œuvre

Des experts toujours trop peu nombreux

Malgré l'essor du marché, le soutien public et la multiplication des formations, la cybersécurité reste confrontée à un problème majeur : **un déficit de personnel qualifié**. Dans les entreprises, les experts en sécurité informatique s'avèrent très recherchés, mais les candidats demeurent peu nombreux. Selon PwC, **plus de 5 000 postes seraient à pourvoir en France en 2021**. Ce déséquilibre freine la croissance de la filière ainsi que le développement d'une culture de la cybersécurité dans la sphère professionnelle.

Pour attirer les spécialistes, les entreprises n'hésitent pas à augmenter les salaires, ce qui entraîne un fort turnover parmi les experts, rapidement débauchés. "On assiste à une guerre des talents. Cela déstabilise le marché. [...] Certains jeunes ingénieurs, qui reçoivent des propositions d'emploi par dizaines une fois leur CV en ligne, prennent la grosse tête. Ils changent de poste au bout de six ou neuf mois", constate Jacques de La Rivière, président de la start-up de détection des cyberattaques Gatewatcher. D'après PwC, le salaire moyen d'un spécialiste en cybersécurité avoisine les 80 000 euros par an en France, un chiffre 2,6 fois plus élevé que la moyenne du reste des pays de l'OCDE.

Ces difficultés de recrutement **touchent encore plus le secteur public, moins attractif que le privé en termes de revenus**. "Dans la cyber, et dans l'IT en général, les talents sont assez chers et, de facto, le milieu hospitalier ayant peu de moyens pour les fonctions support, il n'est pas en mesure d'embaucher des ressources plus expertes", poursuit Jacques de La Rivière, interviewé par *L'Informaticien* dans le cadre d'un article sur la sécurité informatique des hôpitaux. *La Gazette des communes, des départements et des régions* note également que "toutes les collectivités ne partent pas avec la même chance pour dénicher la perle rare". Les plus grandes, disposant de moyens plus importants, présentent un argumentaire financier plus convaincant. **Les plus petites essaient de faire la différence sur des critères annexes** : service d'un territoire et de l'intérêt général, expérience plus variée que dans le privé, etc.

Des revenus imposants ne suffisent toutefois pas

pour résoudre le problème. Selon PwC, d'autres leviers doivent être activés, tant du côté des experts en cybersécurité que des entreprises, afin que cette pénurie de talents ne freine pas la croissance du secteur et que l'emploi retrouve un équilibre plus sain sur ce marché. La sécurité informatique doit par exemple **améliorer son attractivité**. En effet, elle souffre encore d'une image "poussiéreuse" en raison des préjugés qui entourent encore l'informatique et ses spécialistes. En simplifiant ses messages, en intervenant davantage dans les médias et sur les réseaux,

Les freins à lever pour lutter contre la pénurie de compétences en cybersécurité

Freins	Symptômes	Solutions
Une image sectorielle poussiéreuse, en décalage avec la réalité.	• Domaine obscur, au langage spécifique, mal compris par beaucoup. • Secteur encore marqué par la caricature de l'informaticien solitaire devant son écran.	• Travailler l'attractivité du secteur en simplifiant les messages et en dynamisant les prises de parole. • Accroître les interventions dans les médias et sur les réseaux pour illustrer la réalité du métier, sa modernité, ses défis et ses enjeux clés.
Des cursus d'apprentissage trop longs, réservés à une élite scientifique.	• Processus de formation long et complexe. • Difficulté à trouver des professeurs expérimentés et compétents.	• Accepter la longueur des études, indispensable pour former des experts de qualité. • Se tourner vers des spécialistes moins diplômés, mais dont les compétences suffisent pour protéger l'organisation.
Des recruteurs non spécialisés aux commandes.	• Difficultés pour les recruteurs et chefs d'entreprise, peu familiers de la cybersécurité, d'évaluer les compétences techniques des spécialistes.	• Privilégier les profils polyvalents et armés techniquement pour limiter les erreurs. • Prendre en compte les *soft skills* et compétences humaines : capacité à travailler en équipe, à faire face à la pression, éthique, etc.
Une mixité inexistante.	• Seulement 11 % de femmes dans le secteur. • Image du métier encore très masculine, accentuée par les stéréotypes portés par les films ou séries télévisées.	• Combattre les clichés en relayant les parcours et témoignages de femmes exerçant dans le secteur. • Valoriser les qualités et l'approche féminines dans cette profession : forte capacité d'innovation, meilleures relations sociales, etc.
Un manque de reconnaissance de la profession.	• Profession encore peu reconnue, malgré une image qui change peu à peu. • Population pas assez sensibilisée à l'importance de la cybersécurité.	• Développer la culture de la cybersécurité afin de la légitimer dans les entreprises. • Réinventer la relation avec les spécialistes pour valoriser leur travail : prises d'initiatives individuelles, management horizontal, éthique, etc. • Accélérer les efforts des écoles et centres de formation pour attirer plus de talents.

Traitement IndexPresse. Source : PwC

la cybersécurité pourrait **se bâtir une nouvelle réputation**. Cette évolution pourrait également permettre de **mobiliser plus de femmes dans ce domaine**. Elles ne représentent que 11 % des effectifs, alors qu'elles possèdent de véritables atouts différenciants pour s'imposer dans le secteur. "Les femmes qui exercent ces métiers y obtiennent des résultats souvent meilleurs. Elles sont plus innovantes et possèdent très tôt des compétences verbales et relationnelles plus aiguisées qui leur permettent de mener des audits avec d'excellents résultats", souligne PwC. Enfin, **la cybersécurité gagnerait en notoriété grâce à une communication plus dynamique**. Si cette thématique devient centrale dans les entreprises, elle demeure peu connue du grand public et de la population d'étudiants non spécialisés. Une reconnaissance accrue augmenterait le nombre de candidats intéressés par ce domaine d'activité.

L'externalisation, une piste à étudier

Face aux difficultés de recrutement et de fidélisation des experts, les entreprises peuvent décider d'externaliser leur SOC (*security operation center*) et compétences de cybersécurité. "Mettre en place un SOC interne, c'est recruter une dizaine de personnes pour animer ce SOC. Or un responsable de la sécurité des systèmes d'information n'est pas souvent en mesure de recruter autant de personnes, notamment lorsque l'IT n'est pas l'activité principale de l'entreprise. L'externalisation permet de **pallier cette problématique de ressources humaines**, notamment dans un contexte où il est très difficile de trouver les bonnes compétences sur le marché" explique Martine Guignard, membre du Club de la sécurité de l'information français.

Le nombre de prestataires et indépendants proposant leurs services augmente. Selon Xerfi, le marché du SOC externalisé, aussi appelé cyberSOC ou MSSP (*managed security service provider*), a connu **une croissance annuelle de 10 % en France sur la période 2017-2020**. Plusieurs acteurs de poids se positionnent sur ce segment, notamment Atos, Capgemini ou Thales, en plus de nombreuses entreprises de services numériques. L'Agence nationale de la sécurité des systèmes d'information (Anssi) a même mis en place **une qualification pour certifier ces prestataires**.

Cette solution affiche aussi des arguments économiques. Elle **réduit en effet les coûts de mise en place et d'exploitation d'infrastructures informatiques**, en les faisant reposer en partie sur son partenaire. L'investissement de départ s'avère donc moins conséquent, alors que ce type d'infrastructures peut rapidement dépasser le million d'euros.

"Une limite forte de cette externalisation réside dans le manque de connaissances, côté prestataire, du contexte de l'entreprise. Dans un SOC interne, les analystes seront plus facilement capables de distinguer les événements qui sont normaux dans le contexte de l'entreprise (ses horaires de fonctionnement, son activité, ses connexions, ses flux de données) de ceux qui ne le sont pas", alerte cependant la revue *IT for Business*. D'un autre côté, "**les analystes d'un SOC interne ne seront jamais aussi pointus que ceux d'un SOC externe**

Prestataires de SOC qualifiés par l'Anssi à mars 2021 :

Qualification valable jusqu'en 2022 :
- Airbus Cybersecurity
- Capgemini Technology Services
- Orange Cyberdefense
- Sopra Steria Infrastructures and Security Services
- Thales SIX GTS France

Qualification en cours d'obtention :
- Atos/Bull
- BT Services

qui travaillent pour plusieurs clients et qui ont une vue très large sur les menaces", estime Abdou Berghani, consultant expert en cybersécurité. Alors que l'externalisation complète pose donc encore question, **un modèle tend à s'affirmer comme un entre-deux pertinent, le SOC hybride**.

Il consiste à combiner une activité de sécurité interne avec un apport externe. Le prestataire prend en charge uniquement certaines fonctionnalités avancées, gère la protection de paramètres précis, lors d'horaires spécifiques, etc. "L'hybridation gagne de plus en plus les entreprises qui arrivent aux limites de leur SOC interne. Et au-delà d'une segmentation basée sur des périmètres, on voit aussi des entreprises basculer leur SOC interne vers celui d'un prestataire en dehors des heures ouvrées", détaille Benjamin Leroux, directeur marketing d'Advens, spécialiste du management de la sécurité de l'information. Le SOC hybride nécessite toutefois une gestion des données adéquate pour que les services de sécurité internes et externes collaborent efficacement, ainsi qu'une circulation de l'information optimale. "**Ce mode de fonctionnement hybride sera certainement un modèle dominant dans les années à venir** car les ressources humaines cyber sont difficiles à embaucher et fidéliser. Il est difficile de pouvoir compter sur des équipes stables et l'externalisation partielle pallie ce problème", prédit Xavier Leschaeve, administrateur du Club des experts de la sécurité de l'information et du numérique, au printemps 2021.

L'avenir des SOC externalisés passe également par **une meilleure prise en charge des problématiques métiers de chaque client**. Une banque souhaitera par exemple insister davantage sur l'analyse anti-fraude qu'une société d'un autre secteur, peu concernée par cet enjeu. "Les entreprises vont vouloir **casser les silos entre applications métiers et données de cybersécurité, et les SOC vont devoir se mettre au diapason pour parler le même langage que les métiers** afin de renforcer la collaboration avec les entreprises", analyse *L'Informaticien*.

La mutualisation, une solution pour les collectivités

Si l'externalisation peut toujours apparaître comme trop coûteuse pour une petite collectivité, la mutualisation s'avère plus intéressante. Il s'agit de partager les savoirs et les expériences en matière de sécurité informatique, tout en pouvant compter sur des agents capables d'intervenir à plusieurs endroits et niveaux (communes, intercommunalités, départements, etc.) en cas de besoin. "On est en train de créer un réseau de responsables de la sécurité des systèmes d'information pour s'aider et partager entre les collectivités rapidement", expliquait ainsi en décembre 2020 Cyril Bras, responsable pour la métropole Grenoble - Alpes.

Tirer profit des nouvelles technologies

L'intelligence artificielle amenée à devenir essentielle

Les progrès de l'intelligence artificielle, que ce soit en matière de traitement massif des données, d'anticipation des menaces ou de repérage de comportements inhabituels, présentent un intérêt certain pour la cybersécurité. "Les cybercriminels étant passés maîtres dans l'art de faire évoluer leurs virus et malwares, les systèmes de protection traditionnels qui consistent, une fois une menace détectée, à créer son vaccin et sa signature, montrent leurs limites. L'IA change radicalement l'approche. Les dispositifs faisant appel aux technologies du *machine learning* et du *deep learning* vont, cette fois, **de façon préventive, détecter les caractéristiques d'un email suspect**", indique *L'Usine Digitale*.

Déjà déployée dans les logiciels depuis de nombreuses années, l'IA est vouée à se développer dans le secteur de la cybersécurité grâce à ses atouts. Elle **valorise un modèle où les attaques sont anticipées et détectées avant même qu'elles n'aient lieu**, même si le virus ou la manière de l'introduire dans le système se révèlent inédits. De plus, l'intelligence artificielle **pallie le manque de personnel dans le secteur de la sécurité informatique**, en prenant en charge plus de tâches que les outils précédemment développés et en optimisant le quotidien des experts. Elle constitue également un outil majeur pour **faire face aux attaques de masse automatisées, très complexes à gérer pour les humains**. "L'IA permet de combler le manque de personnel, de renforcer les moteurs de détection ainsi que les outils de réponse et de remédiation des éditeurs", énumère *L'Informaticien*.

Depuis 2020, les entreprises françaises du secteur s'activent sur la thématique de l'IA. En janvier 2020, Thales lançait Cybels Analytics, une nouvelle plateforme apprenante reposant sur des technologies d'intelligence artificielle et de *big analytics*. Elle permet de chercher et de détecter des menaces en temps réel. Cet outil découle notamment de l'approche TrUE AI du groupe, amorcée en 2019, qui vise à **utiliser l'intelligence artificielle de manière transparente et éthique auprès de ses clients**. En mai 2021, Thales poursuivait ses avancées en s'associant avec Atos pour donner naissance à Athea, une société commune centrée sur l'IA et le traitement de données massives au service de la défense et de la sécurité. "Athea permettra de créer une solution capable d'exploiter les données sensibles de façon sécurisée, à l'échelle d'un pays, et facilitera son implémentation au sein des programmes gouvernementaux concernés. La structure fournira également des services d'expertise, de conseil et de formation", précisent les deux partenaires.

De son côté, **Capgemini a officialisé en juin 2021 son partenariat avec Tehtris**, un éditeur français de solutions de cybersécurité, pour mettre au point une nouvelle offre à destination des entreprises et services publics. Elle inclut entre autres la détection et la neutralisation automatique des menaces grâce à l'IA.

De nombreuses start-up tricolores accélèrent également autour de cette thématique. En février 2020, CybelAngel, qui sonde le net grâce à ses algorithmes basés sur l'IA pour repérer les fuites de données de ses clients, a levé 36 millions d'euros. Un an plus tard, elle intégrait le Next 40, l'indice regroupant les 40 start-up technologiques françaises les plus prometteuses. Son objectif est de **devenir une licorne, c'est-à-dire d'être valorisée à plus d'un milliard de dollars**.

Dathena, une jeune pousse basée à Singapour mais créée par un Français et possédant aussi des bureaux à Paris, a renforcé son capital de 12 millions de dollars au printemps 2021. Elle se sert de l'intelligence artificielle pour identifier les données sensibles de ses clients et leur octroyer davantage de protection. Cette levée de fonds va lui permettre de **se déployer sur le marché américain**, après avoir ouvert des locaux à New York.

Ubble vise également un développement à l'échelle mondiale. Née en 2018, cette start-up a levé 8 millions d'euros en 2020 pour poursuivre son ambition. Sa solution lutte contre la fraude d'identité et les documents falsifiés en combinant intelligence artificielle et flux vidéo. Elle collabore déjà avec l'organisme de crédit Sofinco ou la fintech Treezor, filiale de Société Générale. L'entreprise souhaite atteindre 10 millions d'euros de chiffre d'affaires en 2020, "**en décrochant de nouveaux projets auprès de grands groupes et à l'international**", précise Juliette Delanoë, cofondatrice d'Ubble.

Malgré les promesses de cette technologie, **la consolidation sur le segment mêlant cybersécurité et intelligence artificielle n'a pas encore réellement débuté**. Quelques opérations peuvent toutefois être signalées. En 2018, le géant américain Oracle avait racheté la start-up de la même nationalité Zenedge, qui élabore notamment des pare-feux améliorés par l'IA. L'année suivante, un autre poids lourd américain de l'informatique, Cisco, mettait la main sur Sentryo, une jeune société française centrée sur l'IA appliquée à la protection des équipements industriels connectés. Si les acquisitions deviennent de plus en plus courantes sur le marché en construction de la cybersécurité, la présence de technologies d'intelligence artificielle ne semble pas revêtir une importance spécifique pour les acheteurs.

Exemples de start-up françaises associant cybersécurité et intelligence artificielle :

- **Cryptosense :** simulation d'actions malveillantes et recherche de failles de sécurité.
- **DataDome** : lutte contre les attaques de bots malveillants.
- **Glimps** : automatisation des processus de sécurité informatique des entreprises.
- **Parcoor :** développement d'algorithmes de détection de malwares ciblant les objets connectés.

La blockchain sécurise les échanges et garantit l'authenticité de l'information

Derrière ses aspects économiques liés aux cryptomonnaies et autres *tokens* (en français jetons), la blockchain possède un indéniable caractère sécuritaire. "Les propriétés de la blockchain – la décentralisation, le consensus et le secret de l'information échangée – permettent de **garantir une confiance qui était dure à défendre**, même avec une base de données décentralisée", explique Lucas Comparini, responsable blockchain d'IBM France. La blockchain redéfinit ainsi la sécurisation des relations numériques.

Georges Gonthier, chercheur à l'Institut national de recherche en sciences et technologiques du numérique, évoque une "machine à confiance", qui permet d'**établir "des accords vérifiables par des parties qui a priori ne se font pas confiance"**.

L'inviolabilité de la blockchain apparaît également comme une solution majeure pour **assurer la fiabilité et la protection de datas**. "Son essor répond à un besoin de traçabilité, de chiffrement de données et d'identification de plus en plus

pressant face à la sophistication des attaques. Les opportunités d'applications, elles, sont infinies, de la garantie des objets de luxe à la traçabilité de l'alimentation, et pourraient bien révolutionner la sécurisation des données telle qu'on l'intègre aujourd'hui", affirmait en avril 2021 Julien Piperault, ingénieur au sein du cabinet Exclusive Networks, spécialiste en cybersécurité.

Les spécialistes français se sont déjà emparés de cette thématique, à l'image d'Atos qui possède une offre "Trusted blockchain". Le groupe collabore avec plusieurs entreprises, principalement dans les secteurs de l'assurance, de l'automobile et de l'énergie, **pour mettre au point des blockchains privés sécurisés** ou innover sur la sécurité des objets connectés. De son côté, Thales travaille depuis 2019 avec MGI, éditeur français de solutions pour la logistique portuaire et de *cargo community systems*, afin d'intégrer la blockchain à ses outils et ainsi sécuriser les échanges entre les bateaux, les ports, les douanes, les transporteurs, etc.

Si les projets et consortiums régis par de grands groupes de la cybersécurité se multiplient, des entreprises de taille plus modeste engagent elles aussi des initiatives. Initiée en 2019, Archipels a ensuite été déployée début 2021. Cette blockchain émane de la société du même nom, créée par La Poste, EDF, Engie et la Caisse des dépôts. Elle vise à certifier les documents numériques et à garantir leur authenticité pour lutter contre la fraude. Archipels propose sa solution aux éditeurs B2B pour qu'ils l'intègrent dans leurs logiciels, ou directement aux entreprises confrontées à une gestion de documents massive : banques, fournisseurs d'énergie, opérateurs téléphoniques, etc. "Nous souhaitons **prendre une position de leader sur la certification de données d'identité sur blockchain à l'échelle européenne**", assure Hervé Bonazzi, PDG d'Archipels, en mai 2021 dans *Revue Banque*.

Des start-up tricolores se positionnent également sur ce segment. Primée dans la catégorie cybersécurité au Consumer Electronics Show 2020, ByStamp a mis au point un tampon électronique reposant sur la blockchain afin d'assurer la traçabilité d'une signature ou d'une transaction. Les utilisateurs sont ainsi **assurés de l'authenticité du document final grâce à un certificat hébergé sur la blockchain**. En septembre 2020, *L'Usine Nouvelle* révélait les projets de ByStamp : lever 1,5 million d'euros pour renforcer son niveau de certification, puis industrialiser la fabrication de son tampon grâce à un potentiel partenariat avec le géant finlandais de l'électronique Nokia.

Fondée en 2014, Keeex a levé 100 000 euros en 2016 pour booster son développement suite à sa création deux ans plus tôt. En 2021, la jeune entreprise marsellaise collabore avec la SNCF, EDF, Orange ou encore Thales. Sa solution de protection des données, basée sur la blockchain, permet de certifier et de tracer des documents et informations numériques. Laurent Henocque, fondateur et PDG de Keeex, constatait en 2020 dans la revue *Archimag* une diminution des délais de vente, **les professionnels s'avérant de plus en plus intéressés et familiers d'une telle technologie**. La société souhaite étoffer ses équipes pour élargir son offre et investir d'autres secteurs clients.

Autres exemples de start-up françaises qui associent cybersécurité et blockchain :

- **Tanker** : protection et chiffrement des données.
- **Trustpair** : lutte contre la fraude bancaire et contrôle de documents.
- **Wiztopic** : certification de documents et d'informations.

Le quantique, un défi futur et une opportunité à saisir

L'ordinateur quantique n'est pas encore une réalité en 2021, mais l'engouement qui entoure cette technologie pourrait la rendre opérationnelle entre 2025 et 2050, selon différentes estimations. Le quantique aura un impact majeur sur les systèmes de cybersécurité puisque **des ordinateurs adaptés pourront aisément craquer les chiffrements actuels**. "Faute d'évolution du cryptage, ce sera un jeu d'enfant de déchiffrer ces données grâce aux capacités des ordinateurs quantiques. [...] Quand un ordinateur classique mettait des dizaines, voire des centaines d'années à faire cette décomposition, son équivalent quantique le ferait en quelques minutes ou secondes !", résume *L'Usine Nouvelle*. À court terme, le quantique semble donc **représenter un danger pour la cybersécurité, qui va devoir adapter ses défenses au plus tôt**. Mais il constitue aussi **une opportunité pour les acteurs qui réussiront les premiers à développer des solutions adaptées**.

En France, Thales fait figure de pionnier. Le groupe travaille sur les algorithmes de cryptologie post-quantique depuis 2013 et emploie douze chercheurs dans son laboratoire de cryptographie industrielle basée à Gennevilliers (Hauts-de-Seine). L'un de ses algorithmes, le Falcon, a même été présélectionné par le National institute of standards and technology, l'organisme américain de standardisation des technologies. À l'été 2021, Thales a également annoncé la commercialisation à venir d'un boîtier de chiffrement capable de résister aux attaques d'ordinateurs quantiques. Il a été mis au point en partenariat avec le groupe australien Senetas, spécialiste de la cybersécurité.

La thématique intéresse également de jeunes start-up. En novembre 2020, le cabinet Wavestone recensait **13 jeunes pousses tricolores positionnées sur les technologies quantiques, dont trois dans la cryptographie quantique et post-quantique**. Sur ce segment, VeriQloud ne cache pas ses ambitions : "devenir leader du monde quantique, et ce, à l'échelle de la planète", déclarait en juillet 2020 Marc Kaplan, cofondateur de la société. Celle-ci développe "des applications pour de nouveaux usages des réseaux de communication quantique, notamment dans la cybersécurité", explique *La Tribune*. VeriQloud a rejoint la Quantum Internet Alliance, un collectif européen qui se concentre sur le futur d'Internet à l'heure du quantique. L'entreprise travaille aussi depuis 2019 avec Airbus afin d'étudier la faisabilité d'un réseau de communication quantique européen.

CryptoNext Security compte de son côté sur le soutien de Thales, qui l'a incubée au sein de l'organisme parisien Station F. La start-up élabore des logiciels renforçant les outils informatiques pour qu'ils ne cèdent pas face aux ordinateurs quantiques. "Puisqu'il faut, dès maintenant, protéger les données de cette menace, **nous sommes en face d'une opportunité qui ne se reproduira pas**", assure Ludovic Perret, PDG de CryptoNext Security. En 2020, la société a reçu le Grand Prix du concours i-Lab, qui lui a permis de gagner en légitimité en tant que *deeptech* (start-up développant des technologies de rupture). Une première levée de fonds avait été réalisée peu de temps avant l'obtention de cette récompense, et une seconde pourrait suivre en 2021.

Fondée en 2008, CryptoExperts reste toutefois très discrète. Son site mentionne onze employés. L'entreprise entend vouloir "combler le fossé qui existe entre l'état de l'art scientifique et le niveau technologique des produits de sécurité actuels". Elle aide ses clients et associés à "bénéficier des dernières avancées disponibles

Atos ouvre un laboratoire

Atos a inauguré un nouveau laboratoire de recherche-développement dans les Yvelines en avril 2021. Il regroupe 350 ingénieurs qui travaillent sur des domaines variés dans lesquels le groupe est actif : cybersécurité, intelligence artificielle, informatique quantique, calcul haute performance, edge computing... La lutte contre le réchauffement climatique se place également au cœur des recherches.

en cryptographie pour améliorer leurs produits et services". CryptoExperts mentionne dans sa liste de partenaires plusieurs acteurs du secteur de la recherche, comme le Centre national de la recherche scientifique (CNRS), ou l'Institut national de recherche en sciences et technologies du numérique (Inria). Sur une technologie du quantique encore très jeune, **la collaboration avec le monde scientifique et universitaire s'avère cruciale**. "C'est un impératif pour garder à jour sa technologie", explique ainsi *Les Échos* en évoquant CryptoNext Security et ses travaux académiques. L'Inria a par exemple développé Saturnin, un algorithme qui protège les smartphones et les objets connectés des attaques quantiques.

Soutenir l'écosystème français pour limiter la fuite des talents

Une forte emprise des acteurs étrangers

Malgré l'accélération du soutien public et le dynamisme national, l'influence des grands groupes étrangers reste forte. Ces derniers parviennent notamment à **attirer les experts de l'Hexagone grâce à leurs moyens financiers conséquents**. "La fourchette des salaires déroulée par les entreprises américaines pour débaucher les seniors serait comprise entre 150 000 et 200 000 euros bruts par an… contre 60 000 à 120 000 en France", constatait *L'Express* à l'été 2021. Les entreprises françaises les plus prestigieuses parviennent à limiter le turnover, mais **les sociétés moins réputées peinent à rivaliser avec leurs concurrents internationaux**. "En temps de pénurie, si vous êtes petit, vous allez recruter les quinzièmes couteaux, parce que les talents auront déjà été absorbés", explique Thierry Berthier, chercheur en cybersécurité.

Des start-up peuvent également **passer sous contrôle étranger lorsque les ressources françaises ne suffisent plus à combler leurs besoins de financement**. "De nombreuses 'pépites' françaises de la French Tech sont rachetées par les géants du numérique, lors des levées de fonds, faute de la disponibilité d'un financement français", indique ainsi un rapport sénatorial portant sur la cybersécurité des entreprises, déposé en juin 2021. Cette même année, Alsid, qui emploie 104 salariés et se concentre sur la sécurité entourant le répertoire informatique Active Directory, a été acquise par l'entreprise américaine Tenable pour 98 millions de dollars. Quelques jours avant cette opération, le marché français avait déjà été impacté par le rachat de Sqreen, qui repère les failles de sécurité dans les applications de développeurs et a été reprise par le groupe américain Datadog. Ce dernier avait concrétisé les acquisitions de deux autres start-up françaises de cybersécurité par le passé, Logmatic.io en 2017 et Madumbo en 2019. "Les industriels et les fonds américains se sont rendu compte que **les start-up françaises de la cyber avaient de très bonnes compétences, et étaient souvent sous-capitalisées**. Avec un tel rapport qualité-prix, il ne faut pas s'étonner qu'ils fassent leur marché", résume Jacques de La Rivière, fondateur de la société Gatewatcher.

Le secteur national se heurte encore à **certaines limites lorsqu'il faut soutenir financièrement ses start-up dans leur progression**. "Il nous manque des fonds capables d'investir 100, 200, 300 millions de dollars pour faire émerger des licornes en France et en Europe. Une start-up cyber peut lever 10 ou 20 millions d'euros en France, mais elle ne pourra pas y passer le cap des

Acquisitions de start-up françaises de cybersécurité par des acteurs étrangers depuis 2017

Start-up	Acquéreur (pays d'origine)	Secteur d'activité de l'acquéreur	Année
Logmatic.io	Datadog (États-Unis)	Cybersécurité	2017
Smart Me Up	Magneti Marelli (Italie)	Automobile	2018
Acorus Networks	Volterra (États-Unis)	Services cloud	2019
Madumbo	Datadog (États-Unis)	Cybersécurité	2019
Sentryo	Cisco (États-Unis)	Services informatiques	2019
Alsid	Tenable (États-Unis)	Cybersécurité	2021
Sqreen	Datadog (États-Unis)	Cybersécurité	2021

Traitement IndexPresse. Sources : Radars 2017-2021 Wavestone / Bpifrance des start-up de la cybersécurité française

séries C à plus de 100 millions", détaille Bernard Barbier, fondateur du cabinet BBCyber. Les fonds privés doivent se mobiliser pour accompagner davantage les entreprises, mais **la puissance publique peut aussi agir davantage**. En parallèle de ses investissements, de la création de pôles et de centres de recherches dédiés ou du lancement de plans nationaux, il s'agit de donner plus d'opportunités aux sociétés hexagonales afin qu'elles puissent déployer leurs solutions et prouver leur valeur.

Bâtir une souveraineté française via les achats publics

Intégrer l'offre française de cybersécurité dans l'écosystème national et public apparaît comme une solution pour permettre aux jeunes acteurs de passer à l'étape supérieure. "Il n'est pas acceptable que Microsoft fasse à la fois les systèmes d'exploitation (Windows), les logiciels (Office 365, Outlook), les outils de visioconférence (Teams), et toute la cybersécurité du système. Il faut **un tiers de confiance souverain, une couche de cybersécurité française que nos start-up ont tout à fait la compétence de réaliser**", estime Bernard Barbier, fondateur du cabinet BBCyber, début 2021. L'Agence nationale de la sécurité des systèmes d'information a déjà déployé cette approche pour les sondes de détection de cyberattaques équipant 250 institutions et entreprises jugées vitales pour le pays. Ces sondes doivent **provenir d'un acteur national ayant obtenu la qualification requise**. Depuis 2019, deux entreprises bénéficient de cette certification : le géant Thales et la start-up Gatewatcher. "Gatewatcher est, de fait, une des plus belles success stories du secteur cyber français", se réjouissait *Challenges* lors de cette annonce.

La commande publique doit suivre la même voie en **priorisant le recours à des outils locaux**. "Le développement de l'excellence de la filière française de cybersécurité doit se traduire par **une politique publique d'achat de solutions de cybersécurité françaises**", conseille le rapport sénatorial de juin 2021 sur la cybersécurité. Jusqu'alors, le choix des solutions adoptées était uniquement basé sur le prix, un critère où les entreprises américaines et chinoises, déjà en capacité de réaliser des économies d'échelle, étaient avantagées. "En plus de pénaliser les acteurs français de la filière, l'achat de solutions étrangères non maîtrisées est susceptible de menacer la souveraineté de la France lorsque les acheteurs sont des organismes publics, des OIV (opérateur d'importance vitale), et/ou des OSE (opérateur de service essentiel)" alerte le rapport. En privilégiant les outils provenant d'entreprises tricolores, **la commande publique légitime l'écosystème national, offre de nouvelles opportunités aux start-up, et développe le marché**. "Je ne veux ni subvention publique ni aide de l'État mais des contrats avec les institutions publiques", assène Erwann Keraudy, dirigeant de la jeune pousse CybelAngel.

LES FORCES EN PRÉSENCE

Les spécialistes historiques de la cybersécurité en France

IndexPresse a réalisé un panel de **27 entreprises françaises historiquement implantées sur le marché de la cybersécurité**. 82 % ont vu le jour entre 2000 et 2010 et 14 % avant 2000. Une seule société est née après 2010 (Akerva, en 2012). Ce panel se concentre sur les entités exclusivement positionnées sur la cybersécurité (cabinets, éditeurs, prestataires, etc.), ce qui exclut des groupes majeurs du secteur tels qu'Atos, Capgemini, Thales ou Sopra Steria. Ils ne possèdent pas de filiales officielles dédiées à la sécurité informatique et incluent souvent cette activité dans un ensemble plus large de services numériques destinés aux entreprises.

Pionnières du marché lors de leur création, les sociétés du panel se sont largement développées depuis, profitant de l'essor croissant du numérique. Aucun acteur recensé – parmi ceux dont les résultats financiers ont été communiqués pour l'année 2020 – ne réalise moins de 3 millions d'euros de chiffre d'affaires. **66 % dépassent la barre des 10 millions d'euros et 38 % s'affichent au-dessus de 20 millions d'euros**. Cette évolution s'observe également au sein des effectifs. À l'exception de TheGreenBow, seule très petite entreprise du panel avec moins de 10 salariés, **toutes comptent au moins 20 employés et ont atteint le statut de PME**. 77 % possèdent un effectif supérieur à 50 personnes, 42 % à 100 personnes, et 17 % à 200 personnes.

L'évolution du marché se reflète aussi dans les dynamiques actionnariales. De nombreuses entreprises du panel ont été **rachetées par des géants du marché depuis leur création** : Novidy's est passée dans le giron de CS Group, Openminded a été reprise par Accenture, IDNomic a été acquise par Atos, etc. Plusieurs créations de holdings sont aussi à signaler. Elles témoignent généralement d'**une volonté d'élargissement de l'activité**, la société initiale devenant une filiale au sein d'un plus grand groupe à la suite d'opérations de fusion-acquisition.

Malgré la globalisation de la demande, **l'implantation des spécialistes reste centrée sur la capitale**. 74 % sont installés à Paris ou dans les départements limitrophes. Le reste du panel a opté pour la région toulousaine (deux entreprises), l'Ouest et la ville de Rennes (deux entreprises), le Nord (deux entreprises) et le Bas-Rhin à l'Est (une entreprise).

Concurrencées par les nombreuses start-up qui bousculent le marché français, les spécialistes historiques de la cybersécurité présentent donc des atouts pour ne pas se laisser distancer, notamment **un développement commercial amorcé depuis plusieurs années et des effectifs nombreux**. Le mouvement de consolidation du secteur a même déjà commencé parmi eux, et pourrait se répandre auprès des jeunes pousses à l'avenir.

Nom de l'entreprise	Maison-mère	Activité / Offre	Année de création	Ville d'implantation	Chiffre d'affaires	Tranche d'effectif
Orange Cyberdefense	Orange	Prestations de services en cybersécurité.	2009	92000 Nanterre	768 millions d'euros (2020)	2 000 à 4 999
Airbus CyberSecurity	Airbus	Solutions de cybersécurité.	2010	78990 Elancourt	74,8 millions d'euros (2020)	200 à 249
I-TRACING	I-TRACING HOLDING	Conseil et prestations de services en cybersécurité.	2005	92400 Courbevoie	45,2 millions d'euros (2020)	100 à 199
CS Novidy's	CS Group	Services et solutions de cybersécurité.	2009	78941 Vélizy-Villacoublay	36,6 millions d'euros (2020)	200 à 249

Nom de l'entreprise	Maison-mère	Activité / Offre	Année de création	Ville d'implantation	Chiffre d'affaires	Tranche d'effectif
Advens	Holding Advens II	Services en cybersécurité et management de la sécurité de l'information.	2000	59800 Lille	23 millions d'euros (2020)	250 à 499
Synetis	-	Conseil, audit et formation en cybersécurité.	2010	75008 Paris	21,5 millions d'euros (2020)	100 à 199
Intrinsec Sécurité	Dragonfly	Prestations de services en cybersécurité.	1995	92400 Courbevoie	20,8 millions d'euros (2020)	100 à 199
Openminded	Accenture	Conseil et prestations de services en cybersécurité.	2009	75009 Paris	20,7 millions d'euros (2020)	100 à 199
Wallix	Wallix Group	Édition de logiciels de cybersécurité.	2003	75008 Paris	19,8 millions d'euros (2020)	100 à 199
IDnomic	Atos	Édition de solutions de gestion des identités numériques.	2004	92130 Issy-les-Moulineaux	14,8 millions d'euros (2019)	100 à 199
Harmonie Technologie	Harmonie Management	Conseil, audit, intégration et prestations de services en cybersécurité.	2005	75008 Paris	14,4 millions d'euros (2020)	100 à 199
Formind	-	Conseil et intégration en cybersécurité.	2010	92130 Issy-les-Moulineaux	13,2 millions d'euros (2019)	200 à 249
Vade Secure	LTGR	Édition d'outils de protection des données et de détection des menaces.	2008	59510 Hem	12,4 millions d'euros (2019)	50 à 99
Systemis IT	-	Conseil en cybersécurité.	2009	94270 Le Kremlin-Bicêtre	10 millions d'euros (2021)	50 à 99
Systancia	-	Édition de logiciels de cybersécurité.	1998	68390 Sausheim	9,4 millions d'euros (2020)	50 à 99
Ilex International	Inetum	Édition de logiciels de gestion des identités et des accès.	1989	92600 Asnières-sur-Seine	8,9 millions d'euros (2020)	50 à 99
Arcatem	Artemys	Prestations de services en sécurité des réseaux et environnements de travail.	2008	75010 Paris	8 millions d'euros (2020)	50 à 99
inWebo Technologies	inWebo Group	Édition d'outils d'authentification.	2008	75008 Paris	3,6 millions d'euros (2019)	20 à 49
SCASSI Conseil	SCASSI HLD	Prestations de services et éditions de logiciels pour la cybersécurité.	2009	31670 Labège	3,3 millions d'euros (2020)	20 à 49
iTrust	-	Édition d'outils et de technologies de rupture pour la cybersécurité.	2007	31100 Toulouse	3 millions d'euros (2019)	20 à 49
AISI	MDO Holding	Prestations de services en cybersécurité.	2010	94160 Saint-Mandé	n.c.	20 à 49
Akerva	Orians	Conseil en cybersécurité et gestion des risques liés aux systèmes d'information.	2012	35000 Rennes	n.c.	20 à 49
Amossys	-	Conseil, audit, formation et prestations de sevices en cybersécurité.	2006	35000 Rennes	n.c.	50 à 99
Brainwave	-	Édition d'outils de gestion d'accès numériques et de contrôle des utilisateurs.	2010	92600 Asnières-sur-Seine	n.c.	20 à 49
Olfeo	Oscar	Édition d'outils de sécurisation des données web.	2003	75001 Paris	n.c.	50 à 99
TheGreenBow	-	Édition de VPN et de logiciels de sécurisation de connexion.	1998	75009 Paris	n.c.	6 à 9
XMCO	XMCO Holding	Prestations de services en cybersécurité.	2000	75008 Paris	n.c.	50 à 99

Les start-up de la cybersécurité en France

Le nombre de start-up françaises présentes dans le secteur de la cybersécurité augmente depuis 2015. Sur le panel de 38 sociétés recensées par IndexPresse, **67,5 % ont cinq ans d'existence ou moins**.

Cette longévité leur permet d'afficher une plus grande maturité économique. Seules 11 entreprises publient leur chiffre d'affaires, dont près de la moitié ayant été fondées en 2010 ou plus tôt. Sur ces 11 start-up, **deux réalisent un chiffre d'affaires supérieur à 10 millions d'euros et s'imposent parmi les champions nationaux du marché hexagonal**, DataDome et Gatewatcher. Derrière, quatre ont terminé leur dernier exercice connu avec un chiffre d'affaires compris entre 5 et 10 millions d'euros : Mailinblack, Dashlane, Sekoia et Pradeo Security Systems. Les cinq autres restent sous la barre des 5 millions, trois ne dépassant pas le million.

La jeunesse des start-up s'observe également dans l'analyse de leurs effectifs. Deux seulement emploient plus de 100 personnes (Dashlane et CybelAngel), et cinq autres entre 50 et 99 salariés (DataDome, GateWatcher, Pradeo Security Systems, Tehtris et YesWeHack). Dans le même temps, **62,1 % des sociétés listées possèdent 19 salariés ou moins**. Leur ancienneté, inférieure à cinq ans pour une majorité d'entre elles, justifie ces effectifs encore peu élevés.

Concernant l'implantation de ces start-up, la majorité, **59,4 %, optent pour Paris**. 10,8 % se trouvent également dans les départements adjacents. **D'autres pôles tendent toutefois à émerger** : la Bretagne regroupe quatre sociétés du panel (YAGAAN et Glimps à Cesson-Sévigné, OneWave à Rennes et ByStamp à Vannes), la ville de Marseille en accueille trois (Mailinblack, Eho.link, Keeex). La région Auvergne-Rhône-Alpes se repose sur Lyon (Parcoor) et Saint-Étienne (Serenicity), alors que l'Occitanie compte également deux grandes villes accueillant chacune une société du panel : Toulouse (Aucae) et Montpellier (Pradeo Security Systems).

Encore très jeunes, les start-up françaises intéressent encore peu les plus grands groupes. **81,1 % des sociétés recensées restent indépendantes et ne font partie ni d'un holding**, ni d'une plus grande entreprise. Les mouvements de fusion-acquisition ne sont pas inexistants pour autant. Le statut de leader de certaines jeunes pousses, plus développées que leurs concurrentes, peut les inciter à se lancer elles-mêmes dans des opérations de rachat, à l'image de Gatewatcher, propriétaire de LastInfoSec depuis 2020. La diversité de ces nouveaux acteurs – que ce soit par leur nombre ou leur positionnement –, leur montée en puissance et l'essor du marché de la cybersécurité devraient toutefois provoquer **un mouvement de consolidation à moyen terme** afin de faire émerger de véritables champions français.

Nom de l'entreprise	Maison-mère	Activité / Offre	Année de création	Ville d'implantation	Chiffre d'affaires	Tranche d'effectif
DataDome	-	Lutte contre les attaques de bots malveillants.	2015	75008 Paris	12,9 millions d'euros (2020)	50 à 99
Gatewatcher	Kerizon	Détection des intrusions et protection des réseaux.	2015	75008 Paris	10 millions d'euros (2019)	50 à 99
Mailinblack	District MIB	Protection des messageries électroniques.	2003	13002 Marseille	6,5 millions d'euros (2020)	20 à 49
Dashlane	-	Solutions de gestion et de protection des mots de passe informatiques.	2009	75018 Paris	6,07 millions d'euros (2020)	100 à 199

Nom de l'entreprise	Maison-mère	Activité / Offre	Année de création	Ville d'implantation	Chiffre d'affaires	Tranche d'effectif
Sekoia	-	Audit, évaluation, conseil et gestion des crises en cybersécurité.	2008	75008 Paris	6 millions d'euros (2019)	20 à 49
Pradeo Security Systems	-	Solutions de cybersécurité mobiles (terminaux, applications, objets connectés, etc.)	2010	34000 Montpellier	5 millions d'euros (2020)	50 à 99
Tehtris (Tehtri-Security)	Poincet-Oudot	Produits et services pour lutter contre les cyberattaques et le cyberespionnage.	2010	75009 Paris	3,5 millions d'euros (2019)	50 à 99
Harfang Lab	-	Détection des menaces et protection des données.	2018	75008 Paris	1 million d'euros (2020)	20 à 49
YAGAAN	-	Outils de détection des vulnérabilités dans le code source des applications logicielles.	2017	35510 Cesson-Sévigné	380 000 euros (2019)	3 à 5
Tanker	-	Protection et chiffrement des données.	2015	75003 Paris	297 900 euros (2020)	20 à 49
Serenicity	-	Logiciels de détection, d'analyse et de blocage des cyberattaques.	2018	42000 Saint-Étienne	68 200 euros (2020)	6 à 9
Astrachain	-	Solution de sécurisation du stockage dans le cloud.	2021	75017 Paris	n.c.	10 à 19
Aucae	-	Formation à la cybersécurité et simulations de cyberattaques.	2019	31100 Toulouse	n.c.	6 à 9
ByStamp	-	Solution de traçabilité et de certification de documents via un tampon électronique.	2016	56000 Vannes	n.c.	10 à 19
Citalid Cybersécurité	-	Développement d'algorithmes évaluant le risque cyber et conseils stratégiques.	2017	92300 Levallois-Perret	n.c.	10 à 19
CryptoExperts	-	Développement d'outils de cryptographie et de cybersécurité post-quantique.	2008	75002 Paris	n.c.	10 à 19
CryptoNext Security	-	Développement d'outils et de logiciels de cybersécurité post-quantique.	2019	75005 Paris	n.c.	6 à 9
Cryptosense	-	Gestion du cycle de vie de la cryptographie utilisée dans la protection de données.	2013	75001 Paris	n.c.	10 à 19
Culmineo Technologies	-	Plateforme d'intelligence artificielle d'identification des visiteurs et d'optimisation de l'expérience client.	2014	75015 Paris	n.c.	1 à 2
CybelAngel	-	Lutte contre les fuites de données sur le net et services de cybersécurité.	2013	75008 Paris	n.c.	100 à 199
Cyrating	-	Mesures et notation des systèmes de cybersécurité.	2017	75015 Paris	n.c.	3 à 5
Eho.Link	MAN 5 ALL	Solutions dédiées à la cybersécurité et accompagnement des entreprises.	2016	13011 Marseille	n.c.	10 à 19
Glimps	-	Automatisation des processus de sécurité informatique des entreprises.	2019	35510 Cesson-Sévigné	n.c.	10 à 19
i-Guard	GS2i	Logiciel de cybersécurité basé sur l'intelligence artificielle.	2014	75010 Paris	n.c.	n.c.
Keeex	-	Certification et traçabilité de documents numériques via la blockchain.	2014	13013 Marseille	n.c.	10 à 19
LastInfoSec	Gatewatcher	Collecte et évaluation de données grâce à l'intelligence artificielle pour évaluer le risque cyber et mieux gérer les attaques.	2019	75020 Paris	n.c.	3 à 5
Mantra	-	Plateforme de sensibilisation et d'entraînement pour lutter contre le phishing.	2020	92000 Nanterre	n.c.	6 à 9

Nom de l'entreprise	Maison-mère	Activité / Offre	Année de création	Ville d'implantation	Chiffre d'affaires	Tranche d'effectif
OneWave	-	Outils de renforcement de l'authentification numérique.	2016	35000 Rennes	n.c.	10 à 19
Parcoor	-	Développement d'algorithmes de détection des malwares ciblant les objets connectés.	2019	69001 Lyon	n.c.	6 à 9
Red Alert Labs	-	Solutions et accompagnement dédiés à la cybersécurité des objets connectés.	2017	94140 Alfortville	n.c.	10 à 19
Sesame IT	-	Solutions de lutte contre les attaques réseau.	2017	75002 Paris	n.c.	10 à 19
TrustHQ	-	Solutions de pilotage de la cybersécurité et de la gestion des risques informatiques.	2020	75018 Paris	n.c.	6 à 9
Trustpair	-	Contrôle des documents numériques et lutte contre la fraude bancaire.	2017	75010 Paris	n.c.	10 à 19
Ubble (NJFVision)	-	Lutte contre la fraude d'identité à distance et les documents numériques falsifiés.	2018	75019 Paris	n.c.	20 à 49
VeriQloud	-	Développement de solutions adaptées aux réseaux de communication quantique.	2017	92120 Montrouge	n.c.	6 à 9
Wiztopic	Lascorp	Certification de documents et d'informations via la blockchain.	2014	75009 Paris	n.c.	20 à 49
YesWeHack	-	Plateforme de mise en contact entre les entreprises et des hackers éthiques.	2015	75004 Paris	n.c.	50 à 99

Traitement IndexPresse. Sources : societe.com, presse et sites web des entreprises concernées. Classement par ordre décroissant de chiffre d'affaires

LISTE DES ENTREPRISES CITÉES DANS L'ÉTUDE

Société	Nature de l'entreprise	Pays d'origine
Accenture	Cabinet de conseil	Irlande
ACE Capital Partners	Fonds d'investissement	France
Acorus Networks	Start-up spécialisée dans la lutte contre les attaques par surchage des serveurs	France
Advens	Entreprise spécialisée dans les services de cybersécurité	France
Airbus	Constructeur aéronautique	Europe
Airbus Cybersecurity	Entreprise spécialisée dans les services de cybersécurité	France
AISI	Entreprise spécialisée dans les services de cybersécurité	France
Akerva	Groupe de conseil et de gestion des risques en cybersécurité	France
Almond	Cabinet spécialisé dans le numérique et la cybersécurité	France
Alsid	Start-up spécialisée dans la surveillance du répertoire informatique Active Directory	France
Alven	Fonds d'investissement	France
Amossys	Groupe de conseil, audit et prestations de cybersécurité	France
Apsys	Intégrateur de logiciels de gestion	France
Arcatem	Entreprise spécialisée dans les services de cybersécurité	France
Archipels	Entreprise spécialisée dans la certification de documents via une blockchain	France
Astrachain	Start-up spécialisée dans la sécurisation du stockage dans le cloud	France
Athea	Entreprise spécialisée dans l'intelligence artificielle, le big data et la sécurité	France
Atos	Entreprise spécialisée dans les services numériques	France
Aucae	Start-up spécialisée dans la formation à la cybersécurité	France
Axeleo	Fonds d'investissement	France
Banijay	Groupe de production audiovisuelle	France
Bank of Valletta	Banque	Malte
Bluemega	Distributeur de solutions informatiques	France
BNP Paribas	Banque	France
Brainwave	Éditeur d'outils de gestion des accès numériques	France
Breizh Up	Fonds d'investissement	France
BT Services	Entreprise spécialisée dans les services numériques	Royaume-Uni
Bull	Entreprise spécialisée dans l'informatique professionnelle	France
ByStamp	Start-up spécialisée dans les tampons électroniques certifiant des documents	France
Calao Finance	Fonds d'investissement	France
Capgemini	Entreprise spécialisée dans les services numériques	France
CheckPoint	Éditeur de solutions de cybersécurité	Israël
Cisco	Groupe de services et d'infrastructures numériques	États-Unis
Citalid Cybersécurité	Start-up spécialisée dans l'évaluation du risque cyber et le conseil	France
Crealia Occitanie	Fonds d'investissement	France
Crédit agricole	Banque	France
CryptoExperts	Start-up spécialisée dans la cryptographie et la cybersécurité post-quantique	France
CryptoNext Security	Start-up spécialisée dans la cybersécurité post-quantique	France
Cryptosense	Start-up spécialisée dans la gestion du cycle de vie de la cryptographie	France
CS Group	Groupe spécialisé dans la cybersécurité et l'informatique critique	France
CS Novidy's	Entreprise spécialisée dans les services et solutions de cybersécurité	France
Culmineo Technologies	Start-up spécialisée dans l'identification des visiteurs web par intelligence artificielle	France
CybelAngel	Start-up spécialisée dans la lutte contre les fuites de données	France
Cyrating	Start-up spécialisée dans la notation des systèmes de cybersécurité	France
Dashlane	Start-up spécialisée dans la gestion des mots de passe informatiques	France
Datadog	Entreprise spécialisée dans les services et outils de cybersécurité	États-Unis
DataDome	Start-up spécialisée dans la lutte contre les attaques de bots malveillants	France
Dathena	Start-up spécialisée dans la protection des données sensibles	Singapour
Definnov	Fonds d'investissement	France
Definvest	Fonds d'investissement	France
Digital.Security	Entreprise spécialisée dans les services de cybersécurité	France
D-Rating	Agence de notation des performances digitales	France

Liste des entreprises citées dans l'étude

Société	Nature de l'entreprise	Pays d'origine
EDF	Producteur d'électricité	France
Eho.Link	Start-up spécialisée dans les solutions dédiées à la cybersécurité	France
Engie	Énergéticien	France
EVA Group	Cabinet de conseil en cybersécurité	France
Excellium Services	Entreprise spécialisée dans les services de cybersécurité	Luxembourg
Feeder	Distributeur de solutions informatiques	France
Formind	Groupe de conseil et prestations de cybersécurité	France
French Cyber Booster	Incubateur	France
F-Secure	Éditeur de solutions de cybersécurité	Finlande
Gatewatcher	Start-up spécialisée dans la protection des réseaux et la détection des intrusions	France
General Catalyst	Fonds d'investissement	États-Unis
Glimps	Start-up spécialisée dans l'automatisation des processus de cybersécurité	France
Go Capital	Fonds d'investissement	France
Greylock Partners	Fonds d'investissement	États-Unis
Harfang Lab	Start-up spécialisée dans la détection des cybermenaces et la protection des datas	France
Harmonie Technologie	Groupe de conseil, audit et prestations de cybersécurité	France
House of Beer	Entreprise de commercialisation de bières	France
Hub One	Opérateur de télécommunications	France
IBM Security	Éditeur de solutions de cybersécurité	États-Unis
Idemia	Entreprise spécialisée dans les services de cybersécurité	France
IDnomic	Éditeur de solutions de gestion d'identité numérique	France
i-Guard	Start-up spécialisée dans l'intelligence artificielle appliquée à la cybersécurité	France
Ilex International	Éditeur de solutions de gestion d'identité numérique	France
Inetum	Entreprise de services du numérique	France
Infoblox	Éditeur de solutions de cybersécurité	États-Unis
Intrinsec Sécurité	Entreprise spécialisée dans les services de cybersécurité	France
inWebo Technologies	Éditeur d'outils d'authentification informatique	France
I-TRACING	Groupe de conseil et de prestations en cybersécurité	France
iTrust	Éditeur d'outils et de technologies de rupture en cybersécurité	France
Kaspersky	Éditeur de logiciels de sécurité	États-Unis
Keeex	Start-up spécialisée dans la certification et la traçabilité de documents	France
Keolis	Société de transport de voyageurs	France
La Poste	Opérateur postal et groupes de services numériques	France
LastInfoSec	Start-up spécialisée dans l'évaluation du risque cyber et la gestion d'attaques	France
Le Poool	Incubateur	France
Legrand	Groupe spécialisé dans les infrastructures électriques et réseaux d'information	France
Linkbynet	Entreprise spécialisée dans les services informatiques et numériques	France
Logmatic.io	Start-up spécialisée dans la gestion et la récupération des logs informatiques	France
Madumbo	Start-up spécialisée dans l'automatisation des tests d'applications web	France
Magneti Marelli	Équipementier automobile	Italie
Mailinblack	Start-up spécialisée dans la protection des messageries électroniques	France
Mantra	Start-up spécialisée dans la formation à la lutte contre le phishing	France
McAfee	Éditeur de solutions de cybersécurité	États-Unis
MGI	Éditeur de solutions pour la logistique portuaire	France
Microsoft	Groupe d'informatique et de services numériques	États-Unis
Moody's	Agence de notation financière	États-Unis
Naval Group	Constructeur naval de défense	France
Network Perception	Éditeur de solutions de cybersécurité	États-Unis
Nokia	Groupe d'électronique et de télécommunications	Finlande
Nubbo	Incubateur	France
Oïkialog	Entreprise spécialisée dans les services de cybersécurité	France
Olfeo	Éditeur d'outils de sécurisation des données web	France
OneRagTime	Fonds d'investissement	France
OneWave	Start-up spécialisée dans l'authentification numérique	France
Open Classrooms	Plateforme de cours en ligne	France
Openminded	Entreprise spécialisée dans les services de cybersécurité	France
Oracle	Groupe de services numériques	États-Unis
Orange	Opérateur de télécommunications	France
Orange Cyberdefense	Entreprise spécialisée dans les services de cybersécurité	France
Oveliane	Entreprise spécialisée dans les services de cybersécurité	France

Liste des entreprises citées dans l'étude

Société	Nature de l'entreprise	Pays d'origine
OVHcloud	Hébergeur de serveurs et de données	France
Palo Alto Networks	Éditeur de solutions de cybersécurité	États-Unis
Parcoor	Start-up spécialisée dans la cybersécurité des objets connectés	France
Pradeo Security Systems	Start-up spécialisée dans les solutions de cybersécurité mobiles	France
PSA	Constructeur automobile	France
Quality Assistance	Entreprise spécialisée dans les sciences analytiques	France
Red Alert Labs	Start-up spécialisée dans la cybersécurité des objets connectés	France
RGPD Chatain & Associés	Cabinet spécialisé dans la mise en application du RGPD	France
Safran	Groupe d'électronique et de défense	France
Sagemcom	Entreprises spécialisée dans les terminaux communicants	France
Sanofi	Laboratoire pharmaceutique	France
SCASSI Conseil	Entreprise spécialisée dans les services de cybersécurité	France
SecureData	Entreprise spécialisée dans les services de cybersécurité	Royaume-Uni
SecureLink	Entreprise spécialisée dans les services de cybersécurité	Pays-Bas
Securiview	Entreprise spécialisée dans la sécurité des systèmes d'information	France
Sekoia	Start-up de conseil, audit et prestations de cybersécurité	France
Semeru	Entreprises spécialisée dans le bâtiment connecté	France
Senetas	Groupe spécialisé dans la cybersécurité	Australie
SentinelOne	Start-up spécialisée dans l'intelligence artificielle appliquée à la cybersécurité	États-Unis
Sentryo	Start-up spécialisée dans la cybersécurité des équipements industriels connectés	France
Sequoia Capital	Fonds d'investissement	France
Serenicity	Start-up spécialisée dans la détection et le blocage de cyberattaques	France
Sesame IT	Start-up spécialisée dans la lutte contre les attaques réseau	France
Sigfox	Entreprise spécialisée dans la communication de l'Internet des objets	France
Smart Me Up	Start-up spécialisée dans la reconnaissance faciale embarquée	France
Sofinco	Organisme de crédit	France
Sopra Steria	Entreprise spécialisée dans les services numériques	France
Sqreen	Start-up spécialisée dans la détection de failles de sécurité informatiques	France
Synamedia	Fournisseur de technologies vidéo	Royaume-Uni
Synetis	Groupe de conseil, audit et formation en cybersécurité	France
Sysdream	Entreprise spécialisée dans les audits et formations en sécurité informatique	France
Systancia	Éditeur de logiciels de sécurité	France
Systemis IT	Groupe de conseil en cybersécurité	France
Tanker	Start-up spécialisée dans le chiffrement et la protection des données	France
Tehtris (Tehtris-Security)	Start-up spécialisée dans la cybersécurité et la cyberdéfense	France
Tenable	Entreprise spécialisée dans les services et outils de cybersécurité	États-Unis
TerraNova Security	Cabinet spécialisé dans les services et la formation à la cybersécurité	Canada
Thales	Groupe spécialisé dans la sécurité, la défense et l'aéronautique	France
TheGreenBow	Éditeur de VPN et d'outils de sécurisation de connexion	France
Tikehau Capital	Fonds d'investissement	France
Travelex	Société financière	Royaume-Uni
Treezor	Start-up spécialisée dans le banking as a service	France
TrustHQ	Start-up spécialisée dans le pilotage de la cybersécurité et la gestion des risques	France
Trustpair	Start-up spécialisée dans le contrôle de documents et la lutte contre la fraude bancaire	France
Ubble (NJFVision)	Start-up spécialisée dans la lutte contre la fraude d'identité et les faux documents	France
UbCom	Entreprise spécialisée dans les services de cybersécurité	Suisse
Utac	Groupe spécialisé dans la mobilité terrestre	France
Vade Secure	Édition d'outils de protection des données et de détection des menaces	France
VeriQloud	Start-up spécialisée dans les réseaux de communication quantique	France
Viaccess Orca	Entreprise spécialisée dans la protection de la diffusion de contenu	France
VMWare Carbon Black	Éditeur de logiciels de sécurité	États-Unis
Volterra	Start-up spécialisée dans l'edge computing et le cloud computing	États-Unis
Wallix	Éditeur de logiciels de sécurité	France
Wise Partners	Cabinet spécialisé dans la cybersécurité et la confiance numérique	France
Wiztopic	Start-up spécialisée dans la certification de documents et d'informations	France
XMCO	Entreprise spécialisée dans les services de cybersécurité	France
Y Combinator	Fonds d'investissement	États-Unis
YAGAAN	Start-up spécialisée dans la détection de vulnérabilités dans le code source	France
YesWeHack	Start-up spécialisée dans la mise en relation entre entreprises et hackers éthiques	France
Zenedge	Start-up spécialisée dans les pare-feux et les solutions de défense informatique	États-Unis

Traitement IndexPresse.

Lexique

- **Blockchain**

Technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle.

- **CERT**

Computer emergency response team. Équipe dédiée à la coordination de la défense de l'organisation en cas de cyberattaque.

- **EDR**

Endpoint detection and response. Système de sécurisation de terminaux associant prévention et intervention face à une cybermenace.

- **Informatique quantique**

Informatique utilisant des ordinateurs et calculateurs dont le fonctionnement repose sur les lois de la physique quantique, ouvrant la voie à de nouveaux champs d'application.

- **IoT**

Internet of Things, ou Internet des objets en français. Fait référence au domaine des objets connectés.

- **Machine learning**

Apprentissage par la machine. Technologie permettant à une intelligence artificielle d'améliorer ses algorithmes de façon continue et autonome grâce à un traitement massif de données.

- **Phishing**

Pratique malveillante où l'attaquant cherche à tromper la victime pour accéder à ses données personnelles.

- **SaaS**

Software as a Service. Mode de commercialisation d'un logiciel sous la forme d'un abonnement donnant accès à diverses fonctionnalités en fonction de la formule choisie.

- **SOC**

Security operation center. Division de l'entreprise dédiée à la sécurité des systèmes d'information. Cet organisme peut aussi être externalisé en totalité ou en partie.

Sources utilisées

Armand Johann, “Qui est Gatewatcher, présentée par Macron comme l’une des futures licornes françaises de la cybersécurité ? “, *channelnews.fr*, 19 février 2021

Armand Johann, “HarfangLab, l’EDR souverain certifié par l’Anssi qui mise sur l’indirect”, *channelnews.fr*, 31 mars 2021

Armandon Laurène, “Capgemini ouvre une école pour les métiers du futur”, *usine-digitale.fr*, 12 juin 2019

Barla Jean-Christophe, “Eho.Link lève 2 millions d’euros pour renforcer la cybersécurité des TPE/PME”, *usine-digitale.fr*, 27 septembre 2021

Biseul Xavier, “Transchain, blockchain publique dédiée à la confiance numérique”, *IT for business*, mai 2020, p.46

Biseul Xavier, “Gatewatcher se veut porte-étendard de la cybersécurité hexagonale”, *IT for business*, juillet-août 2021, p.49

Brébion Patrick, “Les entreprises consolident leur cybersécurité”, *IT for business*, mars 2021, p.14

Cappelle Antoine, “Finance, assurances, légal et cybersécurité : le nouvel incubateur d’Euratechnologies”, *usine-digitale.fr*, 6 février 2019

Cardon Rémi, Meurant Sébastien, “Rapport d’information du Sénat relatif à la cybersécurité aux entreprises”, *senat.fr*, 10 juin 2021

Cartegini Jérôme, “Pourquoi l’IA est devenue incontournable”, *L’Informaticien*, décembre 2020 - janvier 2021, p.48-49

Chaptal Stéphanie, “Hervé Bonazzi, PDG d’Archipels : ‘La certification d’un document faite sur Archipels est ancrée de manière définitive sur l’infrastructure blockchain’”, *RB Banque*, mai 2021, p.42-44

Chéreau Thibaut, “ContentArmor, entreprise de tatouage numérique de Rennes, rachetée par un groupe britannique”, *ouest-france.fr*, 16 août 2021

Clapaud Alain, “Faut-il encore se doter d’un SOC interne en 2021 ?”, *IT for business*, mars 2021, p.34-36

Clapaud Alain, “Faut-il externaliser son ‘SOC’ ?”, *L’Informaticien*, octobre 2019, p.30-36

Clapaud Alain, “HarfangLab défie les grands éditeurs américains d’EDR”, *IT for business*, mars 2021, p.43

Clapaud Alain, “Orange Cyberdefense dépasse les 200 clients pour son offre MicroSOC”, *solutions-numeriques.com*, 15 septembre 2021

Corot Léna, “Atos inaugure un centre de R&D sur l’informatique quantique, l’IA et la cybersécurité”, *usine-digitale.fr*, 22 avril 2021

Corot Léna, “Le gouvernement débloque 250 millions d’euros pour la cybersécurité”, *usine-digitale.fr*, 9 septembre 2021

Corot Léna, “L’Union européenne veut renforcer sa cybersécurité avec une démarche plus proactive”, *usine-digitale.fr*, 18 décembre 2020

De Meyer Bertrand, “Les banques françaises s’organisent face au risque cyber”, *agefi.fr*, 19 juillet 2021

Debes Florian, “CryptoNext Security, déjà en prise avec la cybersécurité du futur”, *lesechos.fr*, 10 mars 2020

Deblock Fabrice, “Le bâtiment connecté, talon d’Achille de la ville intelligente”,*Le Moniteur des travaux publics et du bâtiment*, 23 octobre 2020, p.12-14

Donas Coralie, “Cybersécurité : des salaires élevés pour des profils recherchés”, *emploi-pro.fr*, 2 décembre 2020

Falvy Florence, “Un boulevard pour les hackeurs”, *L’Officiel des transporteurs*, 22 janvier 2021, p.20-26

Feat Thomas, “La crise sanitaire accentue la menace”, *Option finance*, 27 juillet 2020, p.13-15

Feat Thomas, “Cybersécurité. Des services innovants chez les start-up”, *Option finance*, 2 juin 2020, p.23-24

Guillemin Christophe, “Pour effacer la crise sanitaire, on recrute dans l’IT !”, *L’Informaticien*, juin 2021, p.60-65

Guillemin Christophe, “L’IoT : maillon faible naissant de la cybersécurité ?”, *L’Informaticien*, avril 2021, p.27-29

Habchi Vincent, “Culmineo. Cybersécurité et disponibilité”, *L’Informaticien*, mars 2020, p.38-39

Hoze David, “Linkbynet et WISE Partners s’associent”, *wise-partners.fr*, 8 octobre 2019

James Olivier, “Pourquoi Airbus et Thales s’associent dans la cybersécurité”, *usinenouvelle.com*, 9 octobre 2019

Karayan Raphaële, “Cyberassurance : des pistes pour améliorer la protection des entreprises”, *usine-digitale.fr*, 14 octobre 2021

Lamigeon Vincent, “Cyber : l’incroyable razzia américaine sur les pépites françaises”, *challenges.fr*, 15 février 2021

Lamigeon Vincent, “La France dévoile ses boucliers contre les cyberattaques”, *challenges.fr*, 4 avril 2019

Lamigeon Vincent, “CybelAngel, la pépite cyber française, entre au Next40”, *challenges.fr*, 8 février 2021

Le Mao Maureen, “Avec sa carte à puce, OneWave veut démocratiser les bonnes pratiques de cybersécurité en entreprise”, *usine-digitale.fr*, 13 septembre 2021

Lopez Irène, “Orange crée son centre de formation d’apprentis”, *Entreprise & Carrières*, 11 janvier 2021, p.14

Loubière Paul, “Thales se rêve en cyber-champion”, *Challenges*, 3 décembre 2020, p.78

Maignant Véronique, “Watermarking : la société rennaise ContentArmor au palmarès des inventeurs de la French Tech”, *bretagne-economique.com*, 18 octobre 2019

Marcellin Dorian, “F. Gratiolet (Cyrating) : ‘avec la cyber-notation, la cybersécurité devient une discipline de gestion comme les autres’”, *alliancy.fr*, 31 juillet 2018

Matas Jennifer, “Citalid aide les entreprises à évaluer les risques financiers”, *lesechos.fr*, 9 décembre 2019

Meddah Hassan, “Cybersécurité recherche experts désespérément”, *usinenouvelle.com*, 15 janvier 2020

Meddah Hassan, “La cryptographie déjà à l’ère post quantique”, *L’Usine Nouvelle*, juillet-août 2021, p.12-13

Meddah Hassan, “La cyberdéfense française renforce son ancrage rennais”, *usinenouvelle.com*, 3 octobre 2019

Meddah Hassan, “Qui est Gatewatcher, la start-up de la cybersécurité qui monte ? “, *usinenouvelle.com*, 4 avril 2019

Neu Mathieu, “Écosystème IT. La sécurité, à la hauteur des enjeux ?”, *Décisions Achats*, décembre 2020, p.60-62

Paoli Lebailly Pascale, “Airbus CyberSecurity consolide son implantation à Rennes”, *latribune.fr*, 15 juillet 2021

Parisot Thierry, “Ubble lutte contre la fraude d’identité”, *IT for business*, avril 2021, p.51

Parisot Thierry, “MyPSSI simplifie le pilotage de la cybersécurité”, *IT for business*, novembre 2020, p.49

Périssat Guillaume, “L’hôpital face au manque de ressources”, *L’Informaticien*, mars 2021, p.30-32

Périssat Guillaume, “HarfangLab, Sekoia et Pradeo unissent leurs forces”, *linformaticien.com*, 7 septembre 2021

Piperault Julien, “Blockchain : vers une révolution de la cybersécurité”, *alliancy.fr*, 26 avril 2021

Poullennec Solenn, “AXA appelle l’État à la rescousse pour assurer le risque cyber”, *lesechos.fr*, 28 septembre 2021

Rieß-Marchive Valéry, “Sécurité applicative : Yagaan veut fluidifier la détection de vulnérabilités dans le code”, *lemagit.fr*, 27 avril 2020

Russell Géraldine, “Mantra teste la vigilance des salariés et les forme à repérer les tentatives de phishing”, *maddyness.com*, 5 juillet 2021

Saviana Alexandra, “Quand les Gafa font des ponts d’or aux experts de la cybersécurité française”, *L’Express*, 26 août 2021, p.19-20

Sources utilisées

Sequeira Martins Gilmar, “Les métiers les plus recherchés selon LinkedIn”, *Stratégies*, 13 février 2020, p.36-37

Shu Catherine, “Singapore-based data protection startup raises $12 millions Series A”, *techcrunch.com*, 14 mai 2020

Talbi Timothée, “Les cyberattaques contre les banques ont triplé pendant le confinement”, *lesechos.fr*, 15 juillet 2020

Thierry Gabriel, “Ces spécialistes de la cybersécurité que l’on s’arrache”, *La Gazette des communes, des départements et des régions*, 17 février 2020, p.22-23

Vestieu Paco, “Mailinblack lance officiellement son nouveau produit Phishing Coach”, *mailinblack.com*, 3 février 2021

Villedieu Anne-Laure, “Cybersécurité. Des règles européennes renforcées pour les entreprises”, *Option finance*, 31 mai 2021, p.21-22

Virol Gautier, “ByStamp, tampon numérique”, *L’Usine Nouvelle*, 3 septembre 2020, p.20

Vitard Alice, “Régulièrement touché par des cyberattaques, le secteur maritime se muscle avec ‘France Cyber Maritime’”, *usine-digitale.fr*, 25 novembre 2020

Vitard Alice, “Atos s’offre Digital.Security pour muscler ses capacités dans la sécurité de l’IoT”, *usine-digitale.fr*, 3 novembre 2020

Vitard Alice, “Face à la recrudescence des cyberattaques, l’État gonfle ses effectifs”, *usine-digitale.fr*, 9 septembre 2021

Vitard Alice, “Le gouvernement dévoile un plan d’un milliard d’euros pour faire émerger des pépites de la cybersécurité”, *usine-digitale.fr*, 18 février 2021

Vitard Alice, “Rennes Métropole au cœur de la stratégie de cyberdéfense française”, *usine-digitale.fr*, 22 janvier 2021

Vitard Alice, “Avec la Joint Cyber Unit, Bruxelles veut lutter plus efficacement contre les cyberattaques”, *usine-digitale.fr*, 28 juin 2021

Vitard Alice, “Après Wavestone, Orange Cyberdefense obtient la certification PRIS de l’Anssi”, *usine-digitale.fr*, 8 septembre 2021

Vitard Alice, “La Poste et l’Inria s’allient pour travailler sur la cybersécurité, les données et l’intelligence artificielle”, *usine-digitale.fr*, 26 mars 2021

Vitard Alice, “L’Anssi présente son plan pour renforcer la souveraineté européenne en matière de cybersécurité”, *usine-digitale.fr*, 8 septembre 2021

Vitard Alice, “Bruxelles souhaite se doter d’une législation pour protéger les objets connectés des cyberattaques”, *usine-digitale.fr*, 17 septembre 2021

Vitard Alice, “Cybersécurité : pour la première fois, l’UE sanctionne des entités russes, chinoises et nord-coréennes”, *usine-digitale.fr*, 31 juillet 2020

Vitard Alice, “Bruxelles enquête sur une fuite de son Atlas européen de la cybersécurité”, *usine-digitale.fr*, 9 août 2021

Weiss Bénédicte, “Airbus CyberSecurity mise sur les partenariats pour recruter”, *Inffo formation*, 1er octobre 2020, p.28-29

“Former les collaborateurs aux bonnes pratiques de cybersécurité, une mesure vitale pour les entreprises dans le contexte actuel”, *2spark.com*, 4 mars 2021

“Accompagnement & formation au RGPD. Le RGPD : le réflexe gagnant des PME qui se développent”, *Informations Entreprise*, juin 2020, p.79

“Cyber-résilience : entre mythe et pragmatisme”, *synetis.com*, 13 janvier 2020

“Anticiper les cyberattaques”, *Archimag*, juillet-août 2021, p.14-21

"Hub One acquiert Sysdream et devient un acteur majeur de la cybersécurité", *hubone.fr*, 22 juin 2018

"Hub One annonce les acquisitions des sociétés Oveliane et Oïkialog pour renforcer son positionnement d'acteur majeur de la cybersécurité et d'opérateur SOC", *hubone.fr*, 14 janvier 2020

"Linkbynet CyberSecurity se met en ordre de bataille pour devenir un acteur majeur de la sécurité dans le cloud", *itrnews.com*, 22 avril 2021

"Grand Défi Sécurité : Mailinblack soutenu par l'État dans la lutte contre la cybercriminalité", *usine-digitale.fr*, 30 avril 2021

"Cybersécurité et télétravail font bon ménage", *L'Informaticien*, septembre 2020, p.13

"Terranova Security a conclu un partenariat avec Microsoft pour fournir du contenu en sensibilisation à la sécurité inclusif et centré sur les personnes", *prnewswire.com*, 21 février 2020

"Dossier cybersécurité", *La Gazette des communes, des départements et des régions*, décembre 2020 - HS, p.46-52

"La cybersécurité fait face à une pénurie de talents constante", *pwc.fr*, 2021

"Blockchain. L'industrie gagne en confiance", *Industrie & Technologies*, mai 2021, p.20-31

"La blockchain au service de la gestion collaborative des marchandises portuaires", *thalesgroup.com*, 20 juin 2019

"Capgemini et Tehtris collaborent pour renforcer la cybersécurité des entreprises et des organisations publiques françaises", *capgemini.com*, 17 juin 2021

"CybelAngel, le scanner du web, lève 36 millions de dollars", *Industrie & Technologies*, avril 2020, p.16

"Pourquoi Oracle a racheté Zenedge ?", *oracle.com*, février 2018

"Thales et Atos créent le champion européen du big data et de l'intelligence artificielle pour la défense et la sécurité", *atos.net*, 27 mai 2021

"Thales lance Cybels Analytics pour détecter les cyberattaques les plus complexes grâce à l'IA", *thalesgroup.com*, 23 janvier 2020

"La *deeptech* française à la conquête de l'Amérique (2/3)", *latribune.fr*, 24 juillet 2020

"Ludovic Perret cofondateur de CryptoNext Security : 'Déjouer dès aujourd'hui les dangers du quantique de demain'", *latribune.fr*, 3 novembre 2020

"Informatique, quantique et cybersécurité, garants de l'autonomie technologique européenne", *Wavestone*, novembre 2020

"Observatoire de la filière de la confiance numérique", *Alliance pour la confiance numérique*, 2021

"ACE CP récolte 175 millions d'euros pour son fonds 'cyber'", *lesechos.fr*, 11 octobre 2021

"L'État rassemble l'élite de la cybersécurité", *Challenges*, 18 février 2021, p.12

"La crise sanitaire a renforcé la pression sur les systèmes informatiques des banques", *Investir, le Journal des Finances*, 7 mai 2021, p.23

"Cybersecurity Act : une étoile européenne dans le ciel de la cybersécurité", *usine-digitale.fr*, 21 mars 2019

"Durant la crise sanitaire, les entreprises ont fait des concessions en matière de cybersécurité", *usine-digitale.fr*, 8 octobre 2020

"Cybersécurité : des signalements plus nombreux en 2020", *vie-publique.fr*, 26 avril 2021

"Plan de relance : le numérique bien servi", *L'Informaticien*, octobre 2020, p.12

"Tests Covid : les données de santé de 1,4 million de personnes volées à l'AP-HP", *lesechos.fr*, 15 septembre 2021

Comment accéder à des données fiables, pertinentes et surtout synthétisées, alors que l'information n'a jamais été aussi accessible en apparence ?
Voilà une question à laquelle sont confrontés quotidiennement les décideurs dans les entreprises lorsqu'il s'agit de prendre les bonnes décisions.
C'est pourquoi nous avons créé la collection **IndexPresse Business Etude**, des études sectorielles complètes, réalisées à partir des plus grands titres de la presse économique et professionnelle. En s'appuyant sur des informations fiables et de qualité, les études d'IndexPresse offrent des synthèses analytiques et éclairées sur les secteurs d'activité émergents ou en mutation.
Vous aurez ainsi toutes les clés en main pour accompagner votre réflexion stratégique, en vous appuyant sur l'examen des enjeux de votre marché, afin d'anticiper ses évolutions et valider, ou modifier, votre positionnement dans le jeu concurrentiel.

IndexPresse *Business Etude*
Date de parution - octobre 2021.

Renaud HAMMAMY
renaud.hammamy@indexpresse.fr
Auteur

Étude rédigée en collaboration avec **Samuel ARNAUD**

IndexPresse *Business Etude*

Secteurs & marchés
Cybersécurité
édition 2021

La crise sanitaire a provoqué une explosion des cybermenaces, déjà en forte augmentation du fait d'une numérisation croissante. Le dynamisme du marché de la cybersécurité s'accompagne du volontarisme de l'État en la matière, qui multiplie les investissements. Les entreprises du secteur font toutefois face à l'insuffisance des budgets dédiés et de la formation du personnel au sein des organisations. Elles doivent par ailleurs trouver des solutions à la pénurie de talents qui pénalise leur développement. Certaines start-up prometteuses se voient en outre rachetées par des firmes étrangères à cause d'une trop grande frilosité de la sphère financière et des investisseurs français.

Comment la pandémie de Covid-19 a-t-elle accru les besoins en cybersécurité ? Dans quelle mesure les aides publiques favorisent-elles le secteur ? En quoi l'IA, la blockchain et le calcul quantique constituent-ils des innovations porteuses ? Comment les nouveaux incubateurs et partenariats au sein de l'écosystème encouragent-ils l'innovation ? Le développement de la formation est-il suffisant pour pallier aux difficultés de recrutement ? Dans quelle mesure le manque de financement national entraîne-t-il le rachat de start-up par des entreprises étrangères ?

Cette étude apporte des éléments de réponse et de réflexion pour comprendre les enjeux et les perspectives de la cybersécurité, décrypter les modèles de développement à potentiel et identifier les orientations stratégiques pour se positionner dans le jeu concurrentiel.

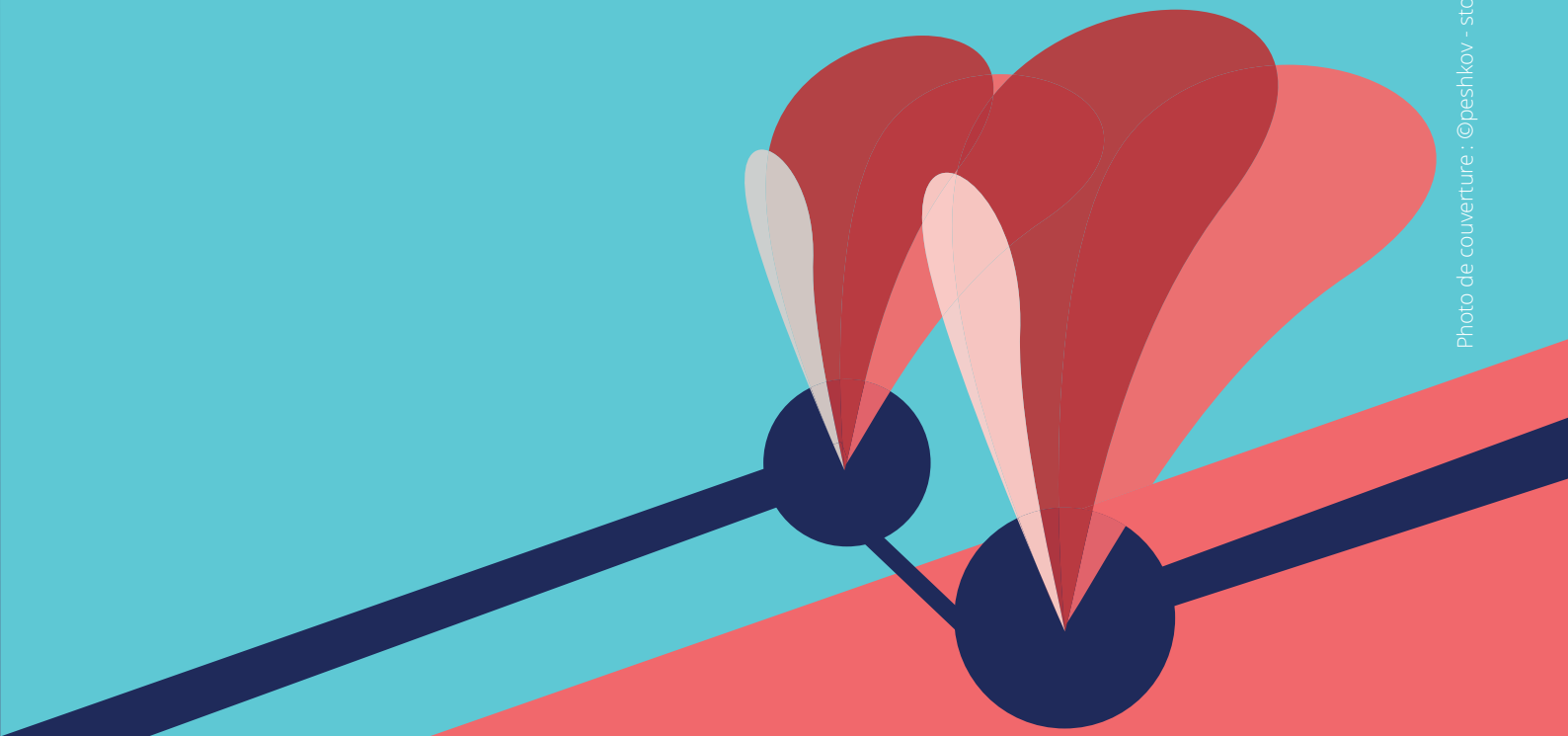


Photo de couverture : ©peshkov - stock.adobe.com

IndexPresse
IndexPresse
19 rue René Thomas
38000 Grenoble
Tél. 04 76 92 05 25
indexpresse@indexpresse.fr