Contact presse :
Florence Lièvre
Tél. : +33 (0) 1 47 54 50 71
E-mail : florence.lievre@capgemini.com

Les entreprises alertent sur le besoin urgent de compétences en cybersécurité

Des stratégies innovantes d'acquisition et de rétention des talents digitaux doivent être mises en place

Paris, le 21 février 2018 – Une nouvelle étude du Digital Transformation Institute de Capgemini met en exergue une pénurie croissante de talents en cybersécurité. Les entreprises doivent adopter de nouvelles stratégies de recrutement et de fidélisation des collaborateurs pour lutter contre les cybermenaces et en tirer un avantage concurrentiel. Le rapport intitulé Cybersecurity Talent : The Big Gap in Cyber Protection révèle que sur l'ensemble des compétences nécessaires aux entreprises leaders dans le digital, celles en cybersécurité sont les plus convoitées.

L'étude a été menée auprès de plus de 1 200 dirigeants et employés et analyse les avis exprimés sur les réseaux sociaux par plus de 8 000 spécialistes en cybersécurité. Parmi les entreprises interrogées, 68% ont exprimé un besoin de compétences en cybersécurité, contre 61% pour des capacités d'innovation et 64% pour des qualités analytiques. Ces besoins ont ensuite été comparés aux compétences déjà disponibles au sein de l'entreprise. L'écart mesuré entre la demande et l'offre disponible est ainsi de 25 points pour les compétences en cybersécurité (43% des entreprises les possèdent déjà en interne), contre 13 points pour les qualités analytiques (51% en interne) et 21 points pour l'innovation (40% en interne).

« Le manque de compétences en cybersécurité a un impact sur les entreprises quel que soit leur secteur d'activité », affirme Mike Turner, en charge des opérations pour la ligne de services cybersécurité du groupe Capgemini. *« Les entreprises qui mettent plusieurs mois à trouver des candidats compétents buttent non seulement sur un problème d'efficacité, mais s'exposent aussi à des risques accrus de cybercriminalité. Les dirigeants doivent revoir rapidement leur stratégie de recrutement et de rétention des talents, afin de tirer le meilleur parti de leur investissement dans la transformation digitale. »*

La demande de talents en cybersécurité devrait continuer de croître au cours des 2 à 3 prochaines années : 72% des personnes interrogées estiment qu'elle sera élevée en 2020, contre 68% aujourd'hui. Les entreprises doivent non seulement se protéger contre un nombre croissant de cyberattaques, mais aussi mieux prendre en compte la sécurité afin de transformer la digitalisation en avantage concurrentiel. Le rapport présente une liste de priorités stratégiques pour aider les dirigeants à atteindre ces objectifs.

Priorité n° 1 – Intégrer la sécurité à tous les niveaux de l'entreprise
La priorité consiste à évaluer le niveau d'intégration de la sécurité à l'échelle de l'entreprise. Existe-t-il une culture de cybersécurité en dehors de l'équipe responsable de la protection des données ? Quelle importance les développeurs d'applications et les administrateurs de réseaux accordent-ils à la sécurité ?

« Il est essentiel d'améliorer la cybersécurité à l'échelle de l'entreprise et de faire adopter à toutes les équipes des principes de sécurité et des processus entièrement sécurisés », explique Mike Turner. *« Doivent être mieux sécurisés : le développement des applications, le codage et le Cloud sur lequel travaillent les architectes et les ingénieurs réseau. Intégrer la sécurité dès la conception permet de remédier efficacement à la pénurie de compétences. »*

Priorité n° 2 – Maximiser les compétences existantes

« Les entreprises doivent également apprendre à identifier les compétences en cybersécurité non visibles. La moitié des employés montrent une appétence pour les compétences digitales et commencent à les développer par leurs propres moyens[1]. Les sociétés qui ont du mal à recruter en externe peuvent ainsi rechercher ces profils parmi leurs collaborateurs et les former. Les fonctions qui impliquent des compétences en cybersécurité, transférables après formation complémentaire, sont notamment la gestion de réseaux, l'administration de bases de données et le développement d'applications. »

Les entreprises doivent également intégrer la sécurité dans chacun de leurs services et applications, et faire appel à des formateurs afin de compléter les compétences techniques de leurs équipes. Certains analystes et marketers peuvent évoluer vers des fonctions de cybersécurité afin de favoriser l'adoption de bonnes pratiques à l'échelle de l'entreprise.

Priorité n° 3 – Recruter différemment

Une autre priorité consiste à adopter une stratégie de recrutement innovante et à comprendre les compétences fondamentales requises en cybersécurité. Il est important de s'intéresser à des qualités et à des capacités généralement associées à des postes complètement différents et de rencontrer des candidats que l'entreprise ne prend pas habituellement en considération. Par exemple, ceux qui travaillent dans les mathématiques possèdent souvent une très bonne capacité à identifier les séquences logiques. *« Recruter différemment, c'est savoir reconnaître les compétences transférables »,* ajoute Mike Turner*. « Par exemple, les personnes autistes sont très douées en reconnaissance de schémas et possèdent souvent des aptitudes exceptionnelles dans tout ce qui a trait au numérique et à la résolution de problèmes ; de plus, elles bénéficient d'un excellent sens du détail ainsi que d'une approche méthodique du travail. Toutes ces qualités sont utiles à la mise en place de bonnes pratiques en cybersécurité. »*

Priorité n° 4 – Fidéliser les talents

La dernière recommandation du rapport concerne la rétention des talents. Sur un marché du recrutement extrêmement concurrentiel, les entreprises doivent accorder de l'importance à l'engagement des collaborateurs pour éviter la fuite des talents.

Selon l'étude, les employés spécialisés en cybersécurité préfèrent les entreprises qui offrent des conditions de travail flexibles, encouragent la formation et proposent des perspectives d'évolution professionnelle claires et accessibles. En revanche, un équilibre difficile entre vie professionnelle et vie privée fait partie des cinq aspects négatifs du métier cités par les professionnels de la cybersécurité sur les réseaux sociaux et constitue un des motifs principaux d'insatisfaction au travail et de départ de l'entreprise. La grande majorité (81%) des professionnels de la cybersécurité déclare être d'accord avec l'affirmation *« Je préfère travailler dans une entreprise qui m'offre un plan de carrière bien défini »*, contre 62% pour l'ensemble des répondants de l'enquête.

Ce nombre est encore plus élevé (84%) pour les employés des générations Y et Z[2], qui considèrent le manque de possibilités d'évolution comme leur principale préoccupation. Ces aspects plus personnels mais tout aussi importants de la fidélisation des collaborateurs doivent impérativement être pris en compte pour développer une compétence de cybersécurité viable et durable.

Méthodologie

Le Digital Transformation Institute de Capgemini a rassemblé les témoignages de 753 employés et 501

[1] Rapport publié par Capgemini en collaboration avec LinkedIn : *« The Digital Talent Gap—Are Companies Doing Enough? »*

[2] Les générations Y et Z désignent les personnes âgées de 18 à 36 ans.

dirigeants qui exercent leurs fonctions dans de grandes entreprises de plus de 1 000 employés ayant un chiffre d'affaires supérieur à 500 millions de dollars en 2016. L'enquête a été menée de juin à juillet 2017 à travers neuf pays - France, Allemagne, Inde, Italie, Pays-Bas, Suède, Espagne, Royaume-Uni et Etats-Unis, et sept secteurs d'activité - l'automobile, la banque, les biens de consommation, les assurances, la vente au détail, les télécommunications et les Utilities.

Capgemini a également réalisé une série d'entretiens avec des recruteurs travaillant pour des firmes internationales, des associations de cybersécurité et des universités afin de déterminer les bonnes pratiques qui permettent de pallier la pénurie de talents digitaux. Enfin, Capgemini a analysé les avis exprimés sur les réseaux sociaux par près de 8 400 employés et anciens employés de 53 entreprises de cybersécurité qui plus de 100 salariés inscrits sur des réseaux sociaux. Les sociétés sélectionnées interviennent principalement dans le secteur de la cybersécurité, notamment dans les domaines de la sécurité des données, du Cloud, des appareils mobiles, des entreprises, des e-mails et des applications.

Vous pouvez télécharger une copie du rapport en cliquant ici.

À propos de Capgemini
Capgemini est un leader mondial du conseil, des services informatiques et de la transformation numérique. A la pointe de l'innovation, le Groupe aide ses clients à saisir l'ensemble des opportunités que présentent le cloud, le digital et les plateformes. Fort de 50 ans d'expérience et d'une grande expertise des différents secteurs d'activité, il accompagne les entreprises et organisations dans la réalisation de leurs ambitions, de la définition de leur stratégie à la mise en œuvre de leurs opérations. Pour Capgemini, ce sont les hommes et les femmes qui donnent toute sa valeur à la technologie. Résolument multiculturel, le Groupe compte 200 000 collaborateurs présents dans plus de 40 pays. Il a réalisé un chiffre d'affaires de 12,8 milliards d'euros en 2017.
Plus d'informations sur www.capgemini.com. People matter, results count.

À propos du Digital Transformation Institute
Le Digital Transformation Institute est le centre de recherche de Capgemini sur les technologies numériques. L'institut publie régulièrement des études sur l'impact des technologies numériques au sein des organisations et des grands secteurs économiques. L'équipe de l'Institut s'appuie sur le réseau international d'experts de Capgemini et travaille en étroite collaboration avec les partenaires académiques et technologiques du Groupe. Il dispose également de plusieurs centres de recherche dédiés en Inde, au Royaume-Uni et aux Etats-Unis.