Jusqu'où l'IA peut-elle réduire le déficit d'experts en cybersécurité ?

Grégory Cardiet, Directeur Security Engineering Vectra pour la zone EMEA, tire le signal d'alarme : 350 000 postes en cybersécurité ne seront pas pourvus en Europe sur les 3 prochaines années, du fait du manque de professionnels formés et qualifiés. L'intelligence artificielle permettrait à la fois de gagner en productivité et de réduire les obstacles techniques à l'accès aux postes d'experts cyber.

Au-delà des gains de productivité évidents qu'elle apporte, l'intelligence artificielle aide aussi à résoudre le déficit d'experts en cybersécurité sur le marché du travail. L'IA réduit en effet les obstacles techniques que doivent gérer de tels professionnels dans l'exercice de leur fonction et, de fait, permet même aux profils moins qualifiés d'être efficaces dans la lutte contre la cybercriminalité.

Selon un rapport récent de l'ISC2, plusieurs entreprises ont déjà déployé des plates-formes d'intelligence artificielle pour aider le personnel moins qualifié à jouer un rôle de première ligne dans les opérations de cybersécurité. Et dans certains cas, nous avons même observé que des stagiaires en études supérieures, qui traditionnellement - sans une formation continue et un perfectionnement professionnel - seraient cantonnés à des postes d'analyste de premier niveau, devenaient rapidement des membres productifs de l'équipe. En d'autres mots, l'IA leur permettait d'être efficace plus rapidement.

Une pénurie de professionnels qui devient dangereuse

La demande d'experts en sécurité est importante dans tous les secteurs. Néanmoins, l'offre des profils aptes à remplir ces missions est dramatiquement restreinte par diverses qualifications en informatique jugées essentielles pour travailler dans ce domaine. Hélas, la promotion de ces matières au sein des établissements scolaires a été inversement proportionnelle aux besoins. Si bien que l'écart se creuse entre la quantité d'offres d'emplois et le bassin de talents disponibles.

Plusieurs études fournissent des prédictions légèrement différentes mais avec un constat toutefois clair, le secteur de la cybersécurité fait face à une pénurie extraordinaire de profils ! D'après Cybersecurity Ventures, l'une des sources de données et analyses reconnue sur le secteur, il y aurait plus de 350 000 offres de postes en cybersécurité non pourvus par des candidats en Europe d'ici à 2022, et ce nombre atteindrait 3,5 millions à l'échelle mondiale à l'échéance 2022.

Il est pourtant urgent de combler le déficit de compétences en cybersécurité car, au cours des cinq dernières années, le nombre et la diversité des cyberattaques a grimpé en flèche, tandis que la surface d'attaque des entreprises, du fait de leur transformation numérique, n'a cessé de croître. La situation a pris de telles proportions que la cybersécurité n'est plus seulement une préoccupation des commerciaux sur le terrain, elle est devenue prioritaire jusqu'aux actionnaires.

Soulager le besoin en ressources humaines avec l'automatisation des analyses

Sans les compétences nécessaires dans leurs rangs, les entreprises sont limitées dans leur capacité à réagir rapidement et efficacement face aux cyberattaques. Les responsables doivent donc évaluer de nouvelles stratégies pour résoudre la situation. Parmi celles-ci, l'intelligence artificielle et le machine learning présentent l'intérêt d'augmenter les capacités humaines à travailler et

d'automatiser autant que possible la collecte des données, la validation des menaces et les tâches opérationnelles. Si bien que la quantité d'individus habituellement nécessaires à l'exploitation des systèmes de détection diminue. En déployant de telles solutions, les personnels en place peuvent se concentrer sur des tâches plus prioritaires.

On comprend dès lors que la pertinence de certaines qualifications demandées est discutable, d'autant plus quand elles freinent les embauches. Les compétences techniques sont l'une des composantes du profil idéal. Apprendre et s'adapter rapidement, acquérir une compréhension contextuelle de l'entreprise qu'on protège et dans laquelle on travaille est tout aussi important. L'IA peut combler une insuffisance technique en augmentant les capacités humaines au-delà des quantités ou des vitesses atteignables par des approches manuelles traditionnelles.

Selon le rapport de l'ISC2, un grand nombre d'analyses dans la surveillance des réseaux, dans la détection des intrusions ou encore dans l'investigation post-intrusion pénalisent le temps qu'il faudrait accorder aux tâches opérationnelles. Or, dès lors qu'une plateforme d'intelligence artificielle divise par 36 la durée de ces analyses, l'accomplissement des autres travaux de sécurité, qui ne nécessitent pas d'expertise de haut niveau, ne pose plus aucun problème.

Aider les humains à gérer l'inattendu

Soyons honnêtes : le système éducatif devrait consacrer plus de temps à l'enseignement des méthodes de développement collaboratif. Elles correspondent en effet plus au travail qui sera demandé aux prochains diplômés en cybersécurité que les procédures de support technique qu'ils apprennent aujourd'hui.

En attendant, l'augmentation des capacités humaines par des technologies capables d'assister la gestion des « inconnues inattendues » devient incontournable.