

69% des entreprises estiment qu'elles ne seront pas en mesure de faire face aux menaces de cybersécurité sans l'aide de l'intelligence artificielle

Deux entreprises sur trois prévoient de déployer des systèmes IA dès 2020 afin renforcer leur défense

Paris, le 11 juillet 2019 – Selon une nouvelle étude du [Capgemini Research Institute](#), les entreprises accélèrent le rythme des investissements dans les systèmes IA en vue de se protéger contre la prochaine génération de cyberattaques. Deux tiers d'entre elles (69%) estiment que, sans l'IA, elles ne seront pas en mesure de réagir en cas de cyberattaque majeure. Avec les avancées technologiques dans les domaines de cloud, de l'IoT¹, de la 5G et des interfaces conversationnelles, le nombre d'appareils connectés, de réseaux et d'interfaces utilisateur ne cesse d'augmenter. Dans ce contexte, les organisations doivent passer à la vitesse supérieure en matière de cybersécurité.

L'étude « [Reinventing Cybersecurity with Artificial Intelligence: the new frontier in digital security](#) », a été menée auprès de 850 cadres dirigeants travaillant dans l'informatique (cybersécurité, sécurité de l'information et des opérations IT), à travers 10 pays et 7 domaines d'activité. En parallèle, le *Capgemini Research Institute* a organisé des entretiens approfondis avec des experts du secteur, des start-up spécialistes de la cybersécurité et des universitaires.

Voici les principales conclusions de l'étude :

Intégrer l'IA aux solutions de cybersécurité est devenu indispensable : pour plus de la moitié (56%) des dirigeants, les analystes cybersécurité sont submergés par la multiplication du nombre de points de données à surveiller afin de détecter et de prévenir toute intrusion. En outre, les cyberattaques qui exigent une intervention immédiate ou qui ne peuvent pas être contournées assez rapidement par les analystes ont considérablement augmenté, notamment :

- Les cyberattaques affectant les applications pour lesquelles la rapidité est essentielle (42% des personnes interrogées déclarent qu'elles ont augmenté, et en moyenne, de 16%)
- Les attaques automatisées, extrêmement rapides, évoluent à un rythme tel que les systèmes d'intervention traditionnels ne parviennent pas à les neutraliser (43% des personnes interrogées déclarent qu'elles ont augmenté, et en moyenne, de 15%)

Face à ces nouvelles menaces, une grande majorité des entreprises (69%) estiment qu'elles ne seront pas en mesure de répondre aux cyberattaques sans l'aide de l'intelligence artificielle. Elles sont 61% à affirmer avoir besoin de l'IA pour identifier les menaces majeures. Un dirigeant sur cinq a d'ailleurs connu une faille de cybersécurité en 2018. Dans 20% des cas, l'incident a coûté plus de 50 millions de dollars à l'entreprise ciblée.

¹ IoT : Internet des objets



Les dirigeants investissent de plus en plus dans l'IA pour renforcer la cybersécurité de leurs organisations : une grande majorité de dirigeants reconnaît que l'IA représente sans aucun doute l'avenir de la cybersécurité :

- 64% estiment que l'IA réduit le coût de la détection et de la correction des incidents, de l'ordre de 12% en moyenne
- 74% considèrent que l'IA permet un délai de réponse plus rapide avec une réduction de 12% en moyenne du temps nécessaire pour la détection des menaces, la correction des failles et le déploiement des correctifs
- 69% déclarent que l'IA améliore la précision de la détection des brèches de sécurité, et 60% d'entre eux estiment qu'elle renforce l'efficacité du travail des analystes cybersécurité, en réduisant le temps qu'ils consacrent à l'analyse des faux positifs et en améliorant la productivité

En conséquence, près de la moitié des dirigeants (48%) indiquent que les budgets consacrés à l'IA pour la cybersécurité augmenteront de près d'un tiers (29%) au cours de l'exercice 2020. En ce qui concerne le déploiement, 73% testent actuellement des cas d'utilisation de l'IA dans le domaine de la cybersécurité. Seule une organisation sur cinq utilisait déjà l'IA avant 2019, mais les taux d'adoption s'apprêtent à grimper en flèche : près de deux entreprises sur trois (63%) prévoient de déployer l'intelligence artificielle d'ici 2020 pour renforcer leur défense.

« L'IA offre énormément d'opportunités en matière de cybersécurité », explique Oliver Scherer, responsable de la sécurité des systèmes d'information (RSSI) chez MediaMarktSaturn Retail Group, leader européen de l'électronique grand public. « Aujourd'hui, le processus de détection, d'intervention et de correction est principalement manuel. Grâce à l'IA, nous allons pouvoir automatiser la correction. C'est l'objectif que toute organisation souhaite atteindre au cours des trois à cinq prochaines années. »

Il existe des freins au déploiement de l'IA à grande échelle : 69% des dirigeants interrogés déclarent de pas savoir comment déployer les cas d'utilisation, en phase test (*Proof Of Concept*), à grande échelle.

Selon Geert van der Linden, responsable de l'offre cybersécurité au sein du groupe Capgemini, *« Les entreprises doivent faire face à un volume sans précédent de cybermenaces de grande complexité et ont pris conscience de l'importance de l'IA comme première ligne de défense. Les analystes cybersécurité sont débordés, et près d'un quart d'entre eux ne sont pas en mesure de résoudre tous les incidents identifiés. Il est donc essentiel pour les organisations d'intensifier les investissements et de se concentrer sur les avantages métier que l'IA peut apporter pour améliorer la cybersécurité. »*

De plus, la moitié des organisations interrogées a indiqué être confrontée à des défis d'intégration avec leurs infrastructures, systèmes de données et environnements applicatifs actuels. Bien que la majorité des dirigeants aient des objectifs précis concernant l'utilisation de l'IA dans le domaine de la cybersécurité, seulement la moitié (54%) a identifié les ensembles de données nécessaires pour rendre les algorithmes IA opérationnels.

Anne-Laure Thieullent, responsable de l'offre *AI and Analytics* du groupe Capgemini, conclut : *« Les entreprises doivent d'abord s'attaquer aux défis sous-jacents d'implémentation qui empêchent de maximiser le potentiel de l'IA dans le domaine de la cybersécurité. Pour cela, il faut établir une feuille de route pour surmonter ces principaux obstacles et se focaliser sur les cas d'utilisation qui peuvent être mis à l'échelle le plus facilement et offrir le meilleur retour sur investissement. Ce n'est qu'en adoptant ces mesures que les organisations pourront*



s'armer correctement pour s'adapter à l'évolution rapide des cybermenaces. Ce faisant, elles économiseront de l'argent et réduiront la probabilité d'être la cible de violations de données majeures. »

Vous pouvez télécharger une copie du rapport en cliquant [ici](#).

Méthodologie

L'étude a été menée auprès de 850 dirigeants, occupant un poste de directeur ou de niveau supérieur, dans sept secteurs : biens de consommation, vente au détail, banque, assurance, automobile, énergie et télécommunications. Un cinquième des dirigeants occupaient un poste de DSI et un dixième un poste de RSSI. Ils travaillaient pour des entreprises dont le siège se trouve en France, en Allemagne, au Royaume-Uni, aux Etats-Unis, en Australie, aux Pays-Bas, en Inde, en Italie, en Espagne et en Suède. Capgemini a également réalisé des entretiens avec des leaders du secteur, en se penchant sur l'état actuel et sur l'impact de l'IA en matière de cybersécurité.

À propos du Capgemini Research Institute

Le « Capgemini Research Institute » est le centre de recherche de Capgemini. Il 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 de plusieurs centres de recherche dédiés en Inde, au Royaume-Uni et aux Etats-Unis. Il a été récemment classé **N°1 mondial** pour la qualité de ses recherches par des analystes indépendants.

Plus d'informations sur <https://www.capgemini.com/researchinstitute/>

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 plus de 200 000 collaborateurs présents dans plus de 40 pays. Il a réalisé un chiffre d'affaires de 13,2 milliards d'euros en 2018. Plus d'informations sur www.capgemini.com. *People matter, results count.*