Relations media :
Florence Lièvre
Tel.: +33 1 47 54 50 71
Email: florence.lievre@capgemini.com

L'IA et l'IA générative devraient transformer la cybersécurité de la plupart des organisations

L'IA générative multiplie les vulnérabilités, mais plus de la moitié des organisations prévoient également une détection plus rapide et plus précise des menaces grâce à son utilisation

Paris, le 19 novembre 2024 – Le nouveau rapport du Capgemini Research Institute, intitulé 'New defenses, new threats : What AI and Gen AI bring to cybersecurity' *(Nouvelles défenses, nouvelles menaces : ce que l'IA et l'IA générative apportent à la cybersécurité)*, publié aujourd'hui, suggère que, même si de nouveaux risques de cybersécurité liés à la prolifération de l'IA et de l'IA générative (Gen AI) émergent, ces technologies permettent une transformation des stratégies de cyberdéfense à long terme pour prédire, détecter et répondre aux menaces. Deux tiers des organisations privilégient désormais l'IA pour leurs opérations de cybersécurité.

Selon le rapport, alors que l'IA est considérée par les organisations comme une technologie critique pour renforcer leurs stratégies de sécurité, l'adoption croissante de l'IA générative par de nombreux secteurs d'activité[1] entraîne une vulnérabilité accrue. L'IA générative présente trois risques majeurs pour les organisations : des attaques plus sophistiquées impliquant davantage de protagonistes, une extension de la surface de cyber-attaque, et une augmentation des vulnérabilités dans l'ensemble du cycle de vie des solutions d'IA générative. L'utilisation inappropriée de l'IA et de l'IA générative par les employés peut également accroître considérablement le risque de fuite de données.

Deux organisations sur trois se disent préoccupées par l'augmentation de l'exposition aux menaces

Presque toutes les organisations interrogées (97%) déclarent avoir été confrontées à des violations ou à des problèmes de sécurité liés à l'IA générative au cours de l'année écoulée. Par ailleurs, l'IA générative engendre des risques supplémentaires, notamment des hallucinations, la génération de contenus biaisés, nuisibles ou inappropriés, et des attaques par injection rapide[2]. Deux organisations sur trois (67%) s'inquiètent de possibles contaminations de données et de fuite de données sensibles par le biais des données d'entraînement utilisées pour former les modèles d'IA générative.

En outre, la capacité de IA générative à produire des contenus artificiels très réalistes pose des risques supplémentaires : plus de deux organisations sur cinq interrogées (43%) ont déclaré avoir subi des pertes financières à la suite de l'utilisation de *deepfakes*.

Près de 6 organisations sur 10 estiment devoir augmenter leur budget de cybersécurité pour renforcer leurs défenses en conséquence.

L'IA et l'IA générative sont primordiales pour détecter les attaques et y répondre

[1] Près d'un quart des organisations (24%) intègrent l'IA générative pour une partie de leurs implantations ou fonctions - *Capgemini Research Institute, "Harnessing the value of generative AI 2nd edition: Top use cases across sectors," juillet 2024.*

[2] Il s'agit d'utiliser des données malveillantes pour manipuler les modèles d'IA et d'IA générative et en compromettre l'intégrité.

Selon le rapport, la majorité des 1 000 organisations interrogées[3] ayant envisagé de recourir à l'IA pour leur cybersécurité, ou qui l'utilisent déjà, s'appuient sur cette technologie pour renforcer la sécurité de leurs données, de leurs applications et de leur cloud, en raison de la capacité de la technologie à analyser rapidement de grandes quantités de données, à identifier des schémas d'attaque et à prédire les violations potentielles.

Plus de 60% d'entre eux ont signalé une réduction d'au moins 5% de leur temps de détection, et près de 40% ont déclaré que leur temps de remédiation a diminué de 5% ou plus après la mise en œuvre de l'IA dans leurs centres d'opérations de sécurité (SOCs).

Trois organisations interrogées sur cinq (61%) considèrent l'IA comme critique pour répondre efficacement aux menaces, et permettre la mise en œuvre de stratégies de sécurité proactives contre des attaques de plus en plus sophistiquées. La même proportion de répondants estime que l'IA générative renforcera les stratégies de défense proactives à long terme, car elle permet une détection plus rapide des menaces. Plus de la moitié d'entre eux pensent également que la technologie permettra aux analystes en cybersécurité de se concentrer davantage sur la stratégie de lutte contre les menaces complexes.

« L'utilisation des technologies d'IA et d'IA générative s'est jusqu'à présent révélée être à double tranchant. D'un côté, la prolifération de l'IA introduit des risques sans précédent ; de l'autre, les organisations s'appuient de plus en plus sur la technologie pour une détection plus rapide et plus précise des cyber incidents. L'IA et l'IA générative fournissent aux équipes de sécurité de nouveaux outils puissants pour limiter ces incidents et transformer leurs stratégies de cyberdéfense. Pour s'assurer qu'elles représentent un avantage significatif face à des menaces de plus en plus sophistiquées, les organisations doivent maintenir et prioriser une surveillance continue de l'évolution des menaces et de la cybersécurité, construire une infrastructure de gestion des données appropriée, mettre en place des cadres et lignes directrices éthiques pour l'adoption de l'IA, ainsi que des programmes robustes de formation et de sensibilisation de leurs employés, » déclare Marco Pereira, à la tête de la Cybersécurité des services *Cloud Infrastructure* du groupe Capgemini.

Méthodologie

L'institut de recherche Capgemini a interrogé 1 000 organisations qui ont envisagé l'IA pour la cybersécurité ou qui l'utilisent déjà, dans 12 secteurs et 13 pays d'Asie-Pacifique, d'Europe et d'Amérique du Nord, et ayant un chiffre d'affaires annuel d'au moins 1 milliard de dollars. L'enquête mondiale s'est déroulée en mai 2024. Les organisations interrogées représentent un large éventail de secteurs, notamment l'automobile, les produits de consommation, la vente au détail, la banque, l'assurance, les télécommunications, l'énergie et les services publics, l'aérospatiale et la défense, la haute technologie, la fabrication d'équipements industriels, l'industrie pharmaceutique et les soins de santé, ainsi que le secteur public.

À propos de Capgemini

Capgemini, partenaire de la transformation business et technologique de ses clients, les accompagne dans leur transition vers un monde plus digital et durable, tout en créant un impact positif pour la société. Le Groupe, responsable et multiculturel, rassemble 340 000 collaborateurs dans plus de 50 pays. Depuis plus de 55 ans, ses clients lui font confiance pour répondre à l'ensemble de leurs besoins grâce à la technologie. Capgemini propose des services et solutions de bout en bout, allant de la stratégie et du design jusqu'à l'ingénierie, en tirant parti de ses compétences de pointe en intelligence artificielle, en cloud, et en data, ainsi que de son expertise sectorielle et de son écosystème de partenaires. Le Groupe a réalisé un chiffre d'affaires de 22,5 milliards d'euros en 2023.
*Get The Future You Want** | www.capgemini.com

**Capgemini, le futur que vous voulez*

[3] 1 000 organisations dans 12 secteurs et 13 pays d'Asie-Pacifique, d'Europe et d'Amérique du Nord, et ayant un chiffre d'affaires annuel d'au moins 1 milliard de dollars.

À propos du Capgemini Research Institute
Le Capgemini Research Institute est le groupe de réflexion interne de Capgemini sur tout ce qui touche au numérique. L'Institut publie des recherches sur l'impact des technologies numériques sur les grandes entreprises traditionnelles. L'équipe s'appuie sur le réseau mondial d'experts de Capgemini et travaille en étroite collaboration avec des partenaires universitaires et technologiques. L'Institut dispose de centres de recherche dédiés à Paris, en Inde, au Royaume-Uni, à Singapour et aux États-Unis. Il a récemment été classé n°1 au monde pour la qualité de ses recherches par des analystes indépendants.
Pour plus d'informations : https://www.capgemini.com/researchinstitute/