Intelligence Artificielle & cybersécurité : avantages et limites

Internet

Posté par : JerryG

Publié le : 15/5/2023 13:00:00

En matière de cybersécurité, les techniques d'attaque et de défense adoptent rapidement toute innovation technologique, et l'Intelligence Artificielle (IA) ne fait pas exception, notamment pour écrire du code.

Selon GitHub, 46 % du code produit dans les langages ¹ Copilot est activé provient ainsi désormais de son assistant. Cependant, si l'IA est utilisée pour améliorer la cybersécurité et soutenir les équipes IT, quelles sont ses limites ?

Dirk Schrader, Resident CISO (EMEA) and VP of Security Research chez Netwrix, nous en dit plus

« Automatiser les actions à faible valeur ajoutée est une stratégie courante et très pratiquée dans la cybersécurité depuis plusieurs années. L'IA, et plus particulièrement le Machine Learning, joue ainsi un rôle important lorsque des quantités massives de données sont à analyser afin de pouvoir en tirer un éclairage pertinent et exploitable.

En effet, la numérisation génère des quantités massives de données et de logs. En parallèle, le nombre d'appareils (mobiles) connectés augmente à un rythme que la plupart des experts dans les années 90 et au début des années 2000 n'avaient pas prévu.

Cette situation nécessite donc des outils dotés de capacités intégrées à même d'apprendre et de raisonner à partir de ces données. Qu'il s'agisse d'analyser les logs des actifs de l'infrastructure - tels que les ordinateurs de bureau, les serveurs et les dispositifs de mise en réseau - pour détecter un cybercriminel en pleine action, de surveiller le comportement des utilisateurs, pour détecter l'anomalie indiquant un compte compromis, ou de déterminer si les données doivent être traitées comme sensibles en fonction des différentes juridictions dans le monde, l'IA peut apporter un avantage significatif.

Seulement, cela ne peut s'effectuer qu'à condition que les organisations gardent l'esprit qu'elle est rapide et précise uniquement dans les domaines pour lesquels elle a été spécialement formée. Mais confrontée à quelque chose d'inédit, elle chouera (du moins pour l'instant) dans ce qui demeure la prérogative de l'intelligence humaine : l'imagination.

L'IA et les algorithmes de Machine Learning peuvent donc améliorer considérablement les opérations de sécurité en aidant à assimiler encore plus d'informations qu'auparavant. Mais l'inconvénient de l'IA est que les entreprises tendent à en attendre plus que ce dont elle est réellement capable pour faire face aux cybermenaces.

L'ingéniosité humaine, l'imagination d'une nouvelle forme d'attaque, tout cela n'est pas possible avec l'IA. En d'autres termes, cette technologie nous aide partiellement avec des éléments, mais la manière dont nous assemblons ces derniers ne dépend toujours que de nous. »