Intelligence Artificielle & cybersÃ©curitÃ© : avantages et limites
Internet
PostÃ© par : JerryG
PubliÃ©e le : 15/5/2023 13:00:00

En matiÃ¨re de cybersÃ©curitÃ©, les techniques dâattaque et de dÃ©fense adoptent rapidement toute innovation technologique, et lâIntelligence Artificielle (IA) ne fait pas exception, notamment pour Ã©crire du code.

Selon GitHub, 46 % du code produit dans les langages oÃ¹ Copilot est activÃ© proviennent ainsi dÃ©sormais de son assistant. Cependant, si lâIA est utilisÃ©e pour amÃ©liorer la cybersÃ©curitÃ© et soutenir les Ã©quipes IT, quelles sont ses limites ?

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

Â« Automatiser les actions Ã faible valeur ajoutÃ©e est une stratÃ©gie courante et trÃ¨s pratiquÃ©e dans la cybersÃ©curitÃ© depuis plusieurs annÃ©es. Lâ IA, et plus particuliÃ¨rement le Machine Learning, joue ainsi un rÃ´le important lorsque des quantitÃ©s massives de donnÃ©es sont Ã analyser afin de pouvoir en tirer un Ã©clairage pertinent et exploitable.

En effet, la numÃ©risation gÃ©nÃ¨re des quantitÃ©s massives de donnÃ©es et de logs. En parallÃ¨le, le nombre d'appareils (mobiles) connectÃ©s augmente Ã un rythme que la plupart des experts dans les annÃ©es 90 et au dÃ©but des annÃ©es 2000 n'avaient pas prÃ©vu.

Cette situation nÃ©cessite donc des outils dotÃ©s de capacitÃ©s intÃ©grÃ©es Ã mÃªme d'apprendre et de raisonner Ã partir de ces donnÃ©es. 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 rÃ©seau - pour dÃ©busquer un cybercriminel en pleine action, de surveiller le comportement des utilisateurs, pour dÃ©tecter l'anomalie indiquant un compte compromis, ou de dÃ©terminer si les donnÃ©es doivent Ãªtre traitÃ©es comme sensibles en fonction des diffÃ©rentes juridictions dans le monde, l'IA peut apporter un avantage significatif.

Seulement, cela ne peut sâeffectuer quâÃ condition que les organisations gardent Ã l'esprit qu'elle est rapide et prÃ©cise uniquement dans les domaines pour lesquels elle a Ã©tÃ© spÃ©cifiquement formÃ©e. Mais confrontÃ©e Ã quelque chose dâinÃ©dit, elle Ã©chouera (du moins pour l'instant) dans ce qui demeure la prÃ©rogative de l'intelligence humaine : l'imagination.

L'IA et les algorithmes de Machine Learning peuvent donc amÃ©liorer considÃ©rablement les opÃ©rations de sÃ©curitÃ© en aidant Ã assimiler encore plus d'informations qu'auparavant. Mais l'inconvÃ©nient de l'IA est que les entreprises tendent Ã en attendre plus que ce dont elle est rÃ©ellement capable pour faire face aux cybermenaces.

L'ingÃ©niositÃ© 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 Ã©lÃ©ments, mais la maniÃ¨re dont nous assemblons ces derniers ne dÃ©pend toujours que de nous. Â»