Quel est l'impact de l'IA sur la cybersécurité ?

Luciano. C

L'IA est-elle un allié ou un ennemi en cybersécurité ?

L'intelligence artificielle (IA) peut être à la fois un allié et un ennemi en matière de cybersécurité. Son impact dépend largement de la manière dont elle est utilisée .

Quelques exemples :

Allié en cybersécurité :

Détection des menaces : L'IA peut analyser de grandes quantités de données en temps réel pour détecter les modèles et les comportements suspects, facilitant ainsi la détection précoce des attaq ues.

Analyse comportementale : En utilisant l'apprentissage machine, l'IA peut apprendre le comportement normal des systèmes et des utilisateurs, facilitant l'identification des anomalies qui pourraient indiquer une cyberattaque.

Exemple pour des personne malveillante :

Attaques par ingénierie sociale améliorées : Les cybercriminels peuvent utiliser des modèles d'IA pour personnaliser et optimiser leurs attaques d'ingénierie sociale, en adaptant le contenu des messages, courriels ou appels pour augmenter leur crédibilité et tromper les victimes.

Attaques de phishing automatisées : L'IA peut être utilisée pour automatiser la création et l'envoi de campagnes de phishing plus sophistiquées. Les attaques peuvent être mieux ciblées en

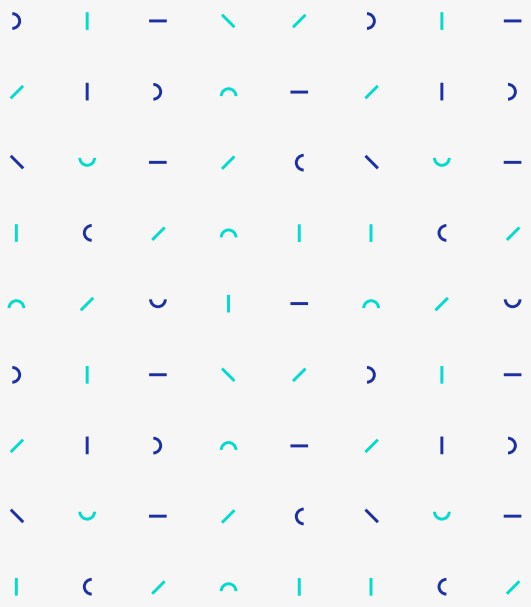
analysant le comportement en ligne des individus et en adaptant les messages en conséquence.

L'utilisation croissante de l'intelligence artificielle (IA) a profondément impacté le monde de la cybersécurité c'est dernières années , tant du côté des entreprises cherchant à renforcer leurs défenses que des cybercriminels qui cherchent à exploiter les opportunités offertes par l'IA.

L'année 2023 semble marquer un record en termes d'incidents de cybersécurité, avec une augmentation notable des exfiltrations de données et des attaques par ransomware.

UTILISATION DE L'IA DANS LA CYBERSÉCURITÉ

Les entreprises ont adopté massivement l'IA pour détecter les cyberattaques. Les solutions d'analyse des risques alimentées par l'IA offrent une détection précoce en produisant des récapitulatifs d'incidents pour des alertes fiables. Cela accélère les enquêtes et le tri des alertes de 55%, en moyenne, selon une étude IBM de mars 2023. De plus, ces solutions s'adaptent continuellement aux nouvelles menaces grâce à l'exploitation de nouvelles données.



Activités de l'IA en Cybersécurité

L'IA est devenue une force dans la cybersécurité. Elle analyse chaque tentative de connexion, vérifie les intentions des utilisateurs et identifie les comportements anormaux susceptibles de signaler une cyberattaque naissante.

Les algorithmes d'apprentissage automatique peuvent alerter le personnel de sécurité et prendre des mesures automatisées pour atténuer les menaces. Cela inclut la surveillance des réseaux à la recherche d'activités suspectes, la détection d'appareils non autorisés et la réponse automatisée à ces incidents.

Lutte contre les menaces

Les algorithmes d'apprentissage automatique sont utilisés pour détecter les malwares en analysant leur comportement, repérant ainsi des variantes qui échappent aux antivirus classiques.

Pour contrer le phishing, les solutions basées sur l'IA examinent le contenu et la structure des e-mails, ainsi que le comportement des utilisateurs, signalant toute activité suspecte aux équipes de sécurité. En ce qui concerne les ransomwares, l'IA identifie des schémas de chiffrement inhabituels ou des comportements suspects, permettant une réaction rapide de la part des équipes de cybersécurité.

Détournement de l'IA par les Cybercriminels

Les cybercriminels exploitent également l'IA pour repérer, identifier et exploiter les vulnérabilités des entreprises. L'utilisation de l'IA permet aux cybercriminels de s'adapter rapidement aux environnements de cybersécurité, en identifiant et contournant plus facilement les mécanismes de détection des entreprises. L'IA générative, une branche de l'IA axée sur la création autonome de contenus, est utilisée pour mener des attaques plus rapides et sophistiquées, optimisant ainsi les cyberattaques à une échelle automatisée.

Bonus :
L'IA générative est notamment utilisée pour créer du contenu réaliste de manière automatisée, tels que des images, des sons ou des textes. Cela signifie que cette technologie peut générer des éléments originaux sans être programmée pour chacun d'eux.
En d'autre mots, cela signifie que les technologies d'intelligence artificielle générative peuvent créer des éléments originaux sans qu'on leur dise exactement quoi produire à chaque fois. Elles apprennent à partir de données existantes et peuvent ensuite générer de nouveaux éléments qui ressemblent à ceux qu'elles ont déjà vus.

Elle peut aussi être détournée à des fins malveillantes, comme la création de logiciels malveillants sophistiqués.

Préoccupations et Réactions

Des études montrent une préoccupation croissante parmi les responsables de la cybersécurité et les dirigeants d'entreprise. La montée en puissance de l'IA générative suscite des inquiétudes quant à ses impacts potentiels sur la sécurité des données. Les dirigeants reconnaissent la nécessité de renforcer les défenses et les budgets de cybersécurité associés à l'IA ont augmenté en moyenne de 51% au cours des deux dernières années. Cependant, la menace persistante de l'utilisation malveillante de l'IA souligne la nécessité d'une vigilance continue et d'une adaptation constante des stratégies de cybersécurité.

Merci pour votre attention.