L’IA alimentée par la cybersécurité

Description: La technologie se développe rapidement et le monde est façonné par de nouvelles tendances et opportunités. Des développements passionnants se produisent dans l’ensemble des technologies telles que l’intelligence artificielle (IA), l’Internet des objets (IOT), le cloud computing, la réalité augmentée, etc. Ces technologies émergentes ont leurs propres avantages et défis. Voyons comment l’IA est alimentée par la cybersécurité.

Cybersécurité (CS)

La cybersécurité est un processus visant à protéger, prévenir et détecter les attaques indésirables ou les accès non autorisés. La cybersécurité est une combinaison de personnes, de politiques, de processus et de technologies utilisés par les organisations pour protéger leurs cyberactifs. La cybersécurité est optimisée à des niveaux définis par l’entreprise, en équilibrant les besoins en ressources avec la facilité d’utilisation/de gestion et le degré de compensation des risques (glossaire Gartner).

À mesure que la dépendance et l’utilisation de la technologie augmentent, l’impact des cybermenaces et des cyberattaques augmente également. Les pratiques de cybersécurité protègent contre les menaces telles que l’hameçonnage, le déni de service (DOS), les attaques de logiciels malveillants, et.al. qui proviennent de l’intérieur ou de l’extérieur de n’importe quel espace professionnel ou même personnel.

De plus, selon le rapport du magazine numérique Atos (2023), il existe différentes catégories de cybermenaces, par exemple:

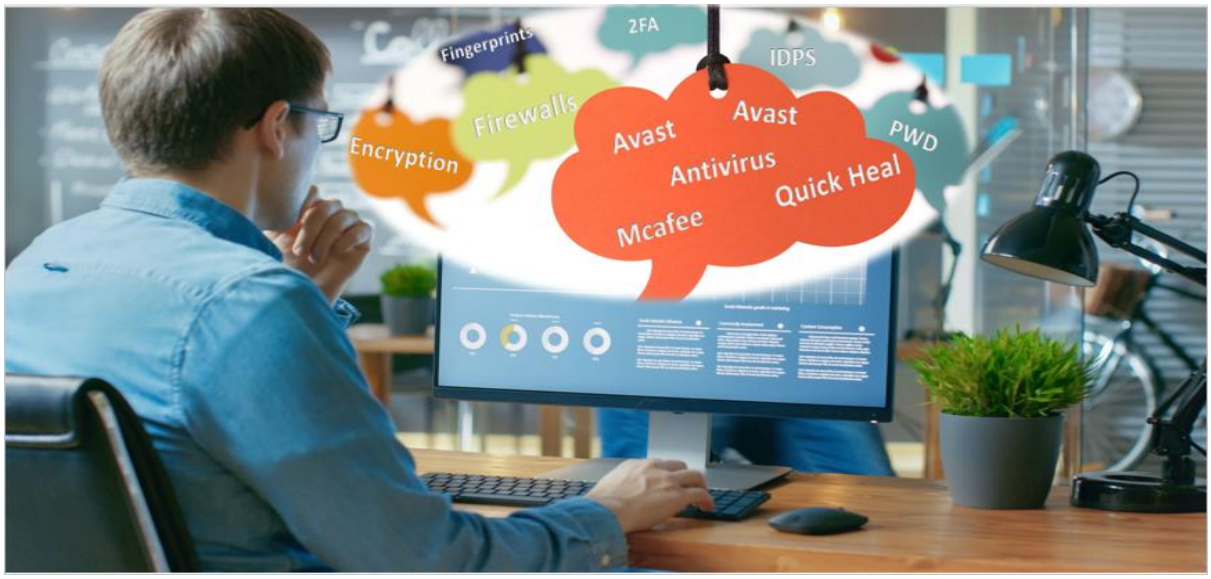
Menaces de ransomware : Il s’agit d’un type de logiciel malveillant conçu pour crypter les fichiers de la victime et exiger le paiement de la clé de déchiffrement.

Menaces de la chaîne d’approvisionnement : ces menaces ciblent les réseaux et les systèmes des fournisseurs et des vendeurs qui ont accès aux systèmes informatiques et aux données d’une organisation. Ces menaces peuvent entraîner des pertes de données, des pertes monétaires et des atteintes à la réputation.

Menaces cloud : Il cible les environnements de cloud computing, qui consistent à stocker, traiter, accéder à des données et à des applications sur des serveurs tiers disposant d’un accès à Internet.

Menaces mobiles : Il cible les appareils mobiles qui stockent des données sensibles et sont utilisés à des fins personnelles et professionnelles.

À mesure que la technologie évolue et devient de plus en plus omniprésente dans notre vie quotidienne, la probabilité de cyberattaques augmente également. Les spécialistes de la technologie ont alors mis au point des moyens de se défendre contre les cyberattaques. Ces solutions de cybersécurité peuvent être classées en fonction de leurs fonctionnalités, telles que la sécurité du réseau, la sécurité des données, la sécurité des applications, la sécurité du cloud, la gestion des accès, etc. Ces solutions protègent les informations sensibles tout en préservant la confidentialité des données.



Intelligence artificielle (IA)

L'intelligence artificielle est un mot à la mode, qui fait beaucoup de bruit, que ce soit dans les affaires, la recherche ou l'éducation. Selon la définition du NIST, l'IA est une branche de l'informatique qui se concentre sur la création de systèmes de traitement de données capables de s'engager dans des activités telles que le raisonnement, l'apprentissage et l'amélioration de soi qui sont généralement associées à l'intelligence humaine. Il peut être résumé comme un système qui effectue des tâches telles que la prise de décision basée sur la perception et le traitement du langage naturel qui nécessiteraient généralement l'intellect humain. Permettez-moi de vous donner un exemple, lorsque vous téléchargez des images sur Facebook, vous pouvez observer que le système détecte les visages et identifie automatiquement les personnes sur l'image. Le système analyse les données disponibles à l'aide d'algorithmes d'apprentissage automatique pour reconnaître les visages et repérer les modèles qui lui permettent de faire correspondre précisément les visages aux personnes. Facebook utilise une technologie de reconnaissance faciale basée sur l'IA qui fonctionne avec des algorithmes d'apprentissage profond pour être en mesure de reconnaître les modèles de visage des personnes.

Comment l'intelligence artificielle contribue-t-elle au domaine de la cybersécurité ?

En bref, nous pouvons dire que l'IA est un catalyseur de la cybersécurité. L'IA a le potentiel de détecter, de prévenir et de répondre aux cyberattaques, améliorant ainsi l'efficacité des solutions de cybersécurité. Par exemple:

- Les algorithmes d'IA aident à analyser les ensembles de données et à trouver des tendances qui indiquent des cyberattaques potentielles ;

- Il analyse également les modèles de comportement d'un virus malveillant et évalue les risques;

- L'IA a le potentiel d'améliorer les procédures d'authentification;

- L'IA peut automatiser les réponses aux attaques probables et réduire le temps de réponse et les dégâts, tout en prédisant les attaques futures.

D'autre part, les pirates ou les cybercriminels utilisent également l'IA pour augmenter l'impact de leurs attaques. Les cybercriminels utilisent des méthodes basées sur l'IA pour créer des techniques complexes afin d'échapper à la détection et d'infiltrer les systèmes et les réseaux informatiques.

Pendant ce temps, la cybercriminalité ne cesse d'augmenter à mesure que nous utilisons de plus en plus de technologies. Les analystes des opérations de sécurité (SOA) se concentrent sur l'IA pour détecter les attaques potentielles. De plus, ils déploient des efforts pour

personnaliser afin d'incorporer des caractéristiques uniques qui minimiseront considérablement le temps de réponse à de telles attaques. À partir de maintenant, nous comprenons que l'IA soutient les solutions de cybersécurité. Voyons si la cybersécurité est meilleure que l'IA.

Cependant, d'une part, la cybersécurité fournit des solutions ou des stratégies pour protéger les systèmes, et l'IA crée des modèles intelligents pour appliquer efficacement ces solutions pour de meilleurs résultats. CSET (Centre pour la Sécurité et les Technologies Émergentes) travaille sur un projet appelé cyber IA. Le but du projet est d'automatiser les cyberopérations et la prévention à l'aide de l'IA. Selon un article de Deloitte Insights (Tendances technologiques, 2022), les organisations peuvent être en mesure de répondre plus rapidement qu'un attaquant ne peut le faire en utilisant cyber IA. Cela peut également les aider à prédire le prochain mouvement d'un attaquant et à préparer une réponse immédiate. Les outils et la technologie de cyber IA en sont encore aux premières phases d'adoption. De plus, indique également le post, l'IA peut agir comme un multiplicateur de force, aidant les professionnels de la technologie à automatiser les tâches chronophages et à accélérer le confinement et la réponse.

L'objectif principal de la cybersécurité est de protéger les systèmes, les réseaux, les données,etc., et l'IA peut être utilisée pour renforcer les défenses de cybersécurité. Par conséquent, la cybersécurité et l'IA sont toutes deux importantes pour gérer l'évolution des cybermenaces.

Références

Entreprise CNBC. (2022, 13 septembre). L'intelligence artificielle joue un rôle plus important dans la cybersécurité, mais les méchants pourraient en bénéficier le plus. AI has bigger role in cybersecurity, but hackers may benefit the most (cnbc.com)

Perspectives de Deloitte. (2022). CyberAI: Une Vraie Défense. The future of cybersecurity and AI | Deloitte Insights

Glossaire Gartner, Definition of Cybersecurity - Gartner Information Technology Glossary

Glossaire de Définitions NIST, Laboratoire des Technologies de l'Information, Centre de Ressources sur la Sécurité Informatique, CSRC Topics - artificial intelligence | CSRC (nist.gov)

Publication de PWC. (2021). Équilibrer puissance et protection: l'IA dans la cybersécurité et la cybersécurité dans l'IA. pwc-balancing-power-protection-ai-cybersecurity.pdf

Prévisions des menaces pour -2023. (2023). The top 10 cybersecurity threats for 2023 - Atos