L'utilisation de l'IA dans le domaine de la sécurité

Dans la sécurité les IA sont utilisées pour:

La détection de la fraude :

les acteurs:

- Les entreprises (de nombreuses entreprises utilisent l'IA pour détecter la fraude interne et externe. Elles peuvent utiliser des algorithmes d'apprentissage automatique pour analyser les données de transaction et détecter les comportements suspects qui pourraient indiquer une fraude).

- Les gouvernements et les organismes de réglementation (les gouvernements et les organismes de réglementation peuvent utiliser l'IA pour détecter la fraude fiscale, la fraude à l'assurance et d'autres formes de fraude).

- Les fournisseurs de logiciels de sécurité (il existe de nombreux fournisseurs de logiciels de sécurité qui proposent des solutions basées sur l'IA pour la détection de la fraude. Ces solutions peuvent être utilisées par les entreprises et les gouvernements pour protéger leurs activités contre la fraude).

- Les experts en intelligence artificielle (pour mettre en œuvre une solution de détection de la fraude basée sur l'IA, les entreprises et les gouvernements peuvent faire appel à des experts en intelligence artificielle pour développer et entraîner les algorithmes d'apprentissage automatique qui seront utilisés).

Les utilisateurs finaux sont les individus et les entreprises.

les apports métiers:

- Amélioration de l'efficacité

- Réductions des coûts

- Prise de décision améliorée

- Meilleur conformité réglementaire

Analyse de la menace :

les acteurs:

- Les entreprises (de nombreuses entreprises utilisent l'IA pour analyser les menaces qui pèsent sur leur réseau et leurs activités. Elles peuvent utiliser des algorithmes d'apprentissage automatique pour analyser en temps réel les données de réseau et détecter les comportements suspects ou les menaces potentielles).

- Les gouvernements et les organismes de sécurité (protéger leurs pays et leurs citoyens contre les menaces en ligne. Utiliser des algorithmes d'apprentissage automatique pour analyser les données et détecter les menaces potentielles, comme les attaques informatiques, les cybermenaces et les campagnes de désinformation).

- Les fournisseurs de logiciels de sécurité (il existe de nombreux fournisseurs de logiciels de sécurité qui proposent des solutions basées sur l'IA pour l'analyse de la menace. Ces solutions peuvent être utilisées par les entreprises et les gouvernements pour protéger leurs activités contre les menaces en ligne).

les apports métiers:

- Aider à identifier et à analyser les menaces de manière plus rapide et plus précise.

- Prédire les futures menaces et à déterminer comment elles pourraient être abordées.

- Pour surveiller en temps réel les réseaux et les systèmes.

- Automatiser certaines tâches de l'analyse de la menace.

Gestion des accès:

les acteurs:

- Les entreprises (de nombreuses entreprises utilisent l'IA pour gérer les accès aux données et aux ressources de leur réseau. Elles peuvent utiliser des algorithmes d'apprentissage automatique pour analyser les données de réseau et contrôler l'accès des utilisateurs aux différentes ressources en fonction de leurs rôles et de leurs autorisations).

- Les gouvernements et les organismes de sécurité (les gouvernements et les organismes de sécurité peuvent utiliser l'IA pour gérer les accès aux données sensibles et protéger leur pays contre les menaces en ligne. Ils peuvent utiliser des algorithmes d'apprentissage automatique pour contrôler l'accès aux données et aux ressources en fonction des autorisations de chaque utilisateur).

- Les fournisseurs de logiciels de sécurité : il existe de nombreux fournisseurs de logiciels de sécurité qui proposent des solutions basées sur l'IA pour la gestion des accès. Ces solutions peuvent être utilisées par les entreprises et les gouvernement

les apports métiers:

- Facilite la collaboration et la communication entre les membres de l'entreprise en leur donnant accès aux ressources et aux données dont ils ont besoin pour travailler.

- Contrôler les accès + renforcer la sécurité.

- Protéger l’entreprise contre les fuites de données, les attaques informatiques etc..

Prévention de la cybercriminalité:

les acteurs:

- Les entreprises (de nombreuses entreprises utilisent l'IA pour protéger leurs réseaux et leurs activités contre les menaces en ligne. Elles peuvent utiliser des algorithmes d'apprentissage automatique pour analyser les données de réseau et détecter les comportements suspects ou les menaces potentielles).

- Les gouvernements et les organismes de sécurité (les gouvernements et les organismes de sécurité peuvent utiliser l'IA pour protéger leur pays contre les menaces en ligne. Ils peuvent utiliser des algorithmes d'apprentissage automatique pour analyser les données et détecter les menaces potentielles, comme les attaques informatiques, les cybermenaces et les campagnes de désinformation).

- Les fournisseurs de logiciels de sécurité (il existe de nombreux fournisseurs de logiciels de sécurité qui proposent des solutions basées sur l'IA pour la prévention de la cybercriminalité. Ces solutions peuvent être utilisées par les entreprises et les gouvernements pour protéger leurs activités contre les menaces en ligne).

- Les experts en intelligence artificielle (pour mettre en œuvre une solution de prévention de la cybercriminalité basée sur l'IA, les entreprises et les gouvernements peuvent faire appel à des experts en intelligence artificielle pour développer et entraîner les algorithmes d'apprentissage automatique qui seront utilisés).

- Les utilisateurs finaux (enfin, les utilisateurs finaux, c'est-à-dire les individus et les entreprises qui utilisent les services de l'entreprise).

les apports métiers:

- Détection de menaces (les IA peuvent être utilisées pour détecter des comportements suspects ou des patterns inhabituels qui peuvent indiquer une activité malveillante).

- Analyse de données (les IA peuvent analyser de grandes quantités de données de différentes sources, ce qui peut aider à identifier des modèles et des tendances qui peuvent être utilisés pour prévenir les cyberattaques).

- Prédiction des futurs risques (les IA peuvent être utilisées pour prédire les futurs risques de cybercriminalité en se basant sur les données passées et en utilisant des algorithmes de prédiction).

- Mise en œuvre de mesures de sécurité (les IA peuvent être utilisées pour mettre en œuvre des mesures de sécurité automatisées, telles que la mise à jour des logiciels de sécurité ou la désactivation des comptes utilisateur compromis).

- Prise de décision (les IA peuvent aider à prendre des décisions rapides et éclairées en matière de

sécurité, en fournissant des informations en temps réel et en proposant des solutions adaptées).

From:
https://wiki.sio.bts/ - **WIKI SIO : DEPUIS 2017**

Permanent link:
https://wiki.sio.bts/doku.php?id=ia23-securite&rev=1672748614

Last update: **2023/01/03 12:23**