

Veille technologique

L'intelligence artificielle au service de la cybersécurité

Table des matières

1. Introduction	2
2. L'intelligence artificielle, c'est quoi ?	2
3. La cybersécurité, c'est quoi ?	2
4. Comment l'IA peut-elle servir dans la cybersécurité ?	2
5. Événements récents et tendances	3
6. Conclusion	4
7. Outils	4

1. Introduction

L'intelligence artificielle (IA) continue de transformer le domaine de la cybersécurité. Grâce à ses capacités d'analyse avancées, l'IA permet de détecter et de contrer efficacement les cybermenaces en constante évolution. Cette veille technologique explore l'impact de l'IA sur la cybersécurité, en mettant l'accent sur les événements récents et les tendances actuelles.

2. L'intelligence artificielle, c'est quoi ?

L'IA regroupe les technologies et méthodes permettant à une machine d'exécuter des tâches nécessitant une forme d'intelligence humaine, telles que l'apprentissage, la perception ou le raisonnement. Elle repose sur des techniques variées comme le machine learning, le deep learning et les réseaux de neurones.

3. La cybersécurité, c'est quoi ?

La cybersécurité englobe l'ensemble des mesures visant à protéger les systèmes informatiques, les réseaux et les données contre les attaques malveillantes. Elle comprend plusieurs domaines, notamment la protection des infrastructures, la gestion des identités et l'analyse des menaces.

4. Comment l'IA peut-elle servir dans la cybersécurité ?

- Détection proactive des cybermenaces : En analysant de grandes quantités de données en temps réel, l'IA permet d'identifier les comportements suspects et d'anticiper les attaques avant qu'elles ne surviennent.
- Automatisation des réponses aux incidents : Les systèmes basés sur l'IA peuvent réagir instantanément aux menaces détectées, minimisant ainsi les dommages potentiels.
- Amélioration de la gestion des vulnérabilités : L'IA aide à identifier et à corriger les failles de sécurité plus rapidement qu'avec des méthodes traditionnelles.

5. Événements récents et tendances

- [ReliaQuest atteint une valorisation de 3.4 milliards de dollars \(mars 2025\)](#) :

La société ReliaQuest, spécialisée en cybersécurité basée sur l'IA, a levé plus de 500 millions de dollars pour innover et étendre sa portée internationale.

- [Sommet SANS sur l'IA et la cybersécurité 2025](#) :

Organisé les 31 mars et 1er avril 2025 à Denver, l'événement a offert des démonstrations et ateliers pour améliorer la cybersécurité grâce à l'IA.

- **Rapport de Darktrace sur l'IA en cybersécurité (Mars 2025) :**
 - [Impact croissant des menaces alimentées par l'IA](#) : 78 % des responsables de la sécurité de l'information signalent que les cybermenaces basées sur l'IA ont un impact significatif sur leur organisation, soit une augmentation de 5 % par rapport à l'année précédente.
 - **Utilisation de l'IA dans la cybersécurité** : 95 % des professionnels de la cybersécurité pensent que l'IA peut améliorer la rapidité et l'efficacité des processus de prévention, de détection, de réponse et de récupération face aux menaces.
 - [Préparation à la défense contre ces menaces](#) : Plus de 60 % des responsables de la sécurité de l'information estiment être désormais suffisamment préparés pour contrer ces menaces, marquant une amélioration de près de 15 % par rapport à l'année précédente.

- [L'essor des agents IA dans les cyberattaques](#)

Les agents intelligents, capables de planifier et d'exécuter des tâches complexes, pourraient être utilisés pour mener des cyberattaques automatisées à grande échelle. Bien que ces attaques ne soient pas encore répandues, elles représentent une menace émergente.

- [Utilisation croissante de l'IA dans les réponses aux incidents](#) :

Microsoft a récemment introduit de nouveaux agents dans son écosystème Security Copilot pour automatiser des tâches comme la gestion des accès conditionnels et la remédiation des vulnérabilités. Ces outils permettent une réponse plus rapide et adaptative aux menaces.

6. Conclusion

L'intelligence artificielle révolutionne le paysage de la cybersécurité. Elle permet une détection plus rapide, une réponse plus efficace et une anticipation des attaques. Toutefois, elle peut aussi être détournée à des fins malveillantes. L'enjeu est donc double : exploiter l'IA pour mieux se protéger, tout en la régulant pour éviter qu'elle ne devienne une arme entre de mauvaises mains.

7. Outils

Outils utilisés :

Flipboard, Feedly.

Outils bureautiques :

Microsoft Word pour la mise en forme et la structuration du document.