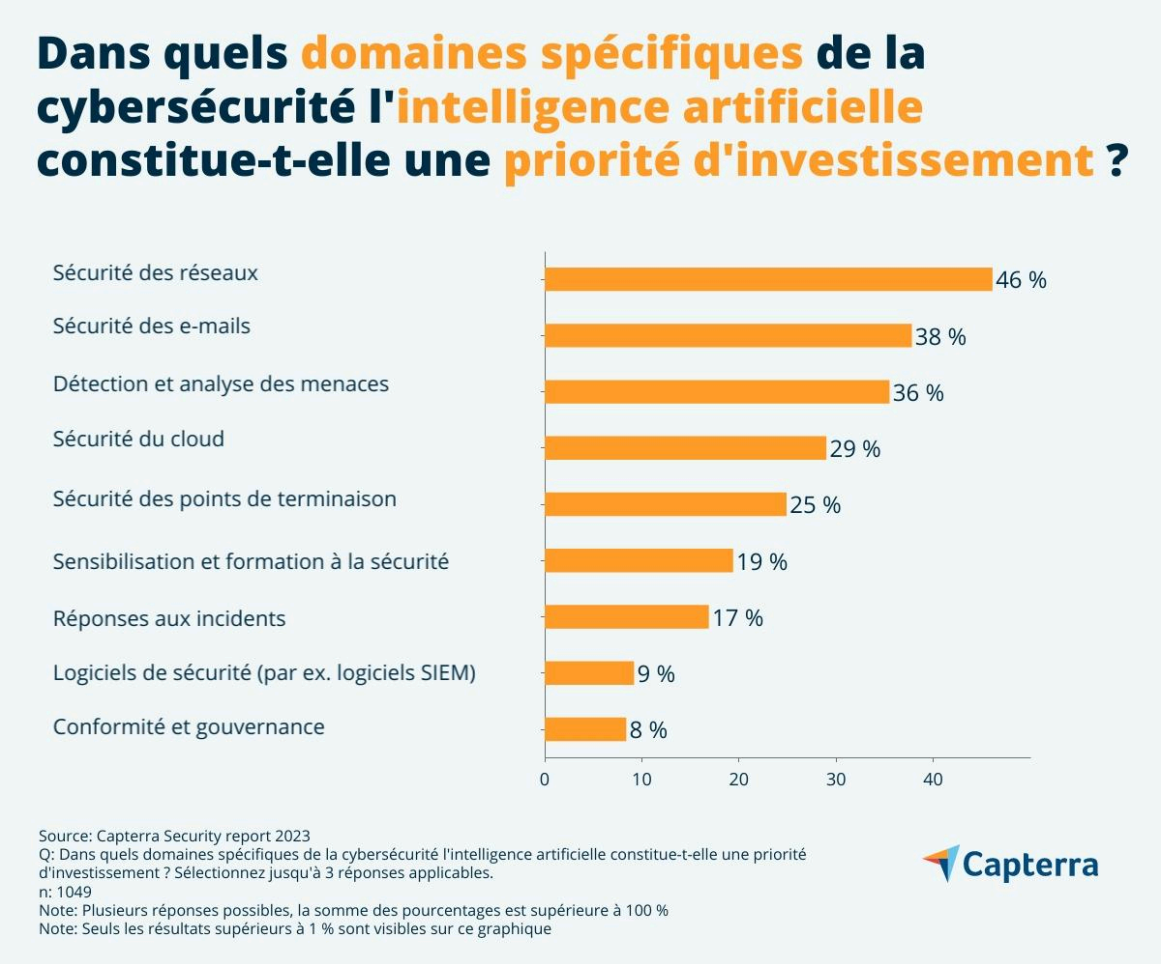
LES ENTREPRISES FRANÇAISES ET LEUR INVESTISSEMENT DANS L'IA POUR LEUR CYBERSÉCURITÉ

Paris, 13 juillet 2024
L'intelligence artificielle se profile comme un moteur de transformation depuis quelques années au sein des entreprises, révolutionnant certains processus opérationnels. Cependant, son évolution se traduit également en matière de cybersécurité. D'une part les cybercriminels l'utilisent pour que leurs attaques soient de plus en plus difficiles à détecter, d'autre part, les entreprises l'emploient afin de renforcer leur défense face à ces dernières. Cette convergence entre IA et cybersécurité redéfinit la manière dont les entreprises abordent la question de la protection des données dans un monde numérique en constante évolution.

Investissement dans l'IA pour une sécurité des informations optimisée

Selon notre étude, plus de la moitié des entreprises de notre panel ont choisi d'intégrer des solutions de sécurité pilotées par l'IA au sein de leurs pratiques. Leurs priorités d'investissements en la matière concernent les domaines suivants :

- la sécurité des réseaux informatiques (46 %),
- la sécurité des e-mails (38 %),
- la détection et l'analyse des menaces (36 %).



Différentes raisons ont motivé ce choix stratégique, et plus particulièrement les risques liés à la vulnérabilité des réseaux IoT (30 %), aux menaces internes provenant d'actes malveillants ou involontaires d'employés (29 %), ou encore aux attaques de phishing et d'ingénierie sociale (34 %).
Mais en quoi les systèmes de sécurité alimentés par l'IA constituent-ils une amélioration par rapport aux outils de cybersécurité traditionnels ?

Cybersécurité pilotée par l'IA vs outils traditionnels

Entre outils traditionnels et outils alimentés par l'IA, une différence majeure existe : les outils traditionnels sont capables de répondre uniquement à une menace connue de leur système (soit déjà intégrée dans leur base de donnée) alors que les outils avec IA peuvent non seulement identifier les menaces connues mais aussi les activités anormales. Le machine learning est l'un des principes qui permet notamment

d’entraîner l’IA sur des données correspondants à l’activité normale du réseau, donnant ainsi la possibilité au système de repérer toute autre activité inhabituelle.

Pourquoi un outil piloté par IA plutôt que le modèle traditionnel ?

L’IA peut donc être une véritable arme afin d’améliorer la sécurité des entreprises. Cependant, malgré son potentiel, comme toute technologie, elle présente également certaines limites et défis.

Les principales limites de l’IA en cybersécurité

1. **Le manque de précision de ses analyses**

Même si les algorithmes d'IA peuvent traiter de grandes quantités de données, leur capacité d’analyse repose uniquement sur des informations sur lesquelles ils ont été

préalablement entraînés. Sans vérification humaine, des conclusions approximatives voire faussées peuvent être faites.

2. **Les attaques adverses**

En second, vient le problème des attaques adverses : dans ce cas de figure, les pirates fournissent à un modèle d'apprentissage automatique piloté par l'IA des données de bases inexactes ou malveillantes visant à tromper le modèle et à l'inciter à commettre des erreurs.

3. **Les faux positifs" et "faux négatifs"**

Si l'humain est capable de contextualiser et d'interpréter un événement, l'IA ne dispose pas de cette faculté si elle n'est pas informée avec un modèle au préalable. Il est donc possible pour l'IA de signaler comme suspecte une activité bénigne de l'entreprise (faux positif) ou à l'inverse d'ignorer une menace réelle (faux négatif).

Bien que l'intelligence artificielle puisse faciliter certaines prises de décision, l'intervention humaine reste primordiale pour superviser ses opérations.

Équilibre entre humain et IA

Les évolutions technologiques de l'IA permettent aux entreprises de déléguer de plus en plus de tâches à ces outils; cependant ces derniers ne peuvent se substituer aux capacités du cerveau humain à contextualiser, à observer ou à s'adapter à certaines situations.. C'est pourquoi, avoir recours à un expert en cybersécurité peut s'avérer essentiel.

Dans quelles mesures l'humain joue-t-il un rôle indispensable pour les problèmes de sécurité ?

Avant d'intégrer l'IA à leurs pratiques de cybersécurité, il est important pour les

entreprises d’évaluer soigneusement les avantages de l’IA en matière de cybersécurité mais aussi de former leurs employés à la sécurité en ligne.

Méthodologie
Pour collecter les données de ce rapport, Capterra a mené une enquête en ligne du 10 au 26 novembre 2023 auprès de 2072 employés français. Au sein de ce panel, 1393 sont responsables, participent activement ou sont pleinement informés des politiques de sécurité informatique de leur entreprise. Un groupe de 679 répondants ne sont pas entièrement au fait des politiques de cybersécurité de leur entreprise et ont répondu à des questions spécifiques.

L'ensemble des répondants ont été sélectionnés selon les critères suivants :

- Réside en France
- Âgé(e) de 18 ans à 65 ans
- Employé(e) à temps plein
- Travaille au sein d'une entreprise de 1 à plus de 10 000 employé(es)
- Travaille au sein d'une entreprise disposant d'un système de sécurité

À propos de Capterra
Capterra est la destination n°1 afin de trouver le logiciel idéal. Notre plateforme comprend plus de 95 000 solutions parmi 900 catégories de logiciels et offre un accès à plus d'1,8 millions d'avis vérifiés, vous permettant de gagner du temps, d'accroître votre productivité et d'accélérer votre croissance.

Contact presse:
Dorine Mandin - Spécialiste Marketing Capterra
dorine.mandin@gartner.com