

# L'IA

Quels sont les avantages et les risques associés  
à l'utilisation de l'IA dans la sécurité des  
entreprises ?

Présenté par Angelo Macaire



# SOMMAIRE

1 L'IA c'est quoi ?	5 Les avantages de l'ia
.....	.....
2 Aujourd'hui	6 Les risques de l'ia
.....	.....
<u>3 Dans les années à venir</u>	<u>7 Perspectives</u>
.....	.....
<u>4 Études de cas</u>	
.....	

# INTELLIGENCE ARTIFICIELLE, C'EST QUOI

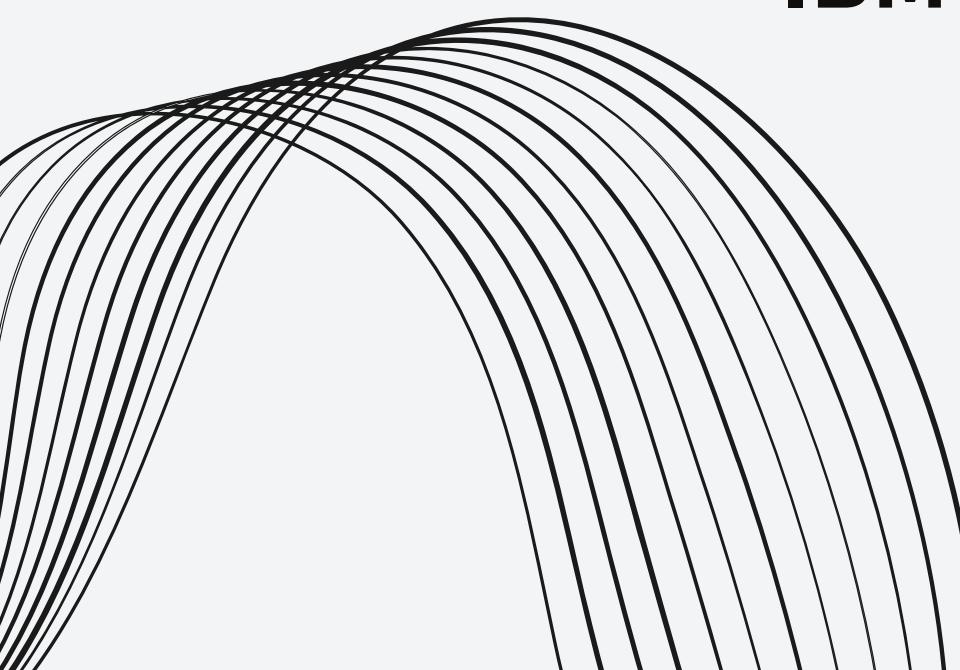
?



## QU'EST-CE QUE L'INTELLIGENCE ARTIFICIELLE

Elle exploite les ordinateurs et les machines pour imiter les fonctions de résolution de problèmes et de prise de décision du cerveau humain

IBM



## IA , DE QUOI PARLE-T-ON ?

L'intelligence artificielle n'est pas une technologie à proprement parler mais plutôt un domaine scientifique dans lequel des outils peuvent être classés lorsqu'ils respectent certains critères.

CNIL

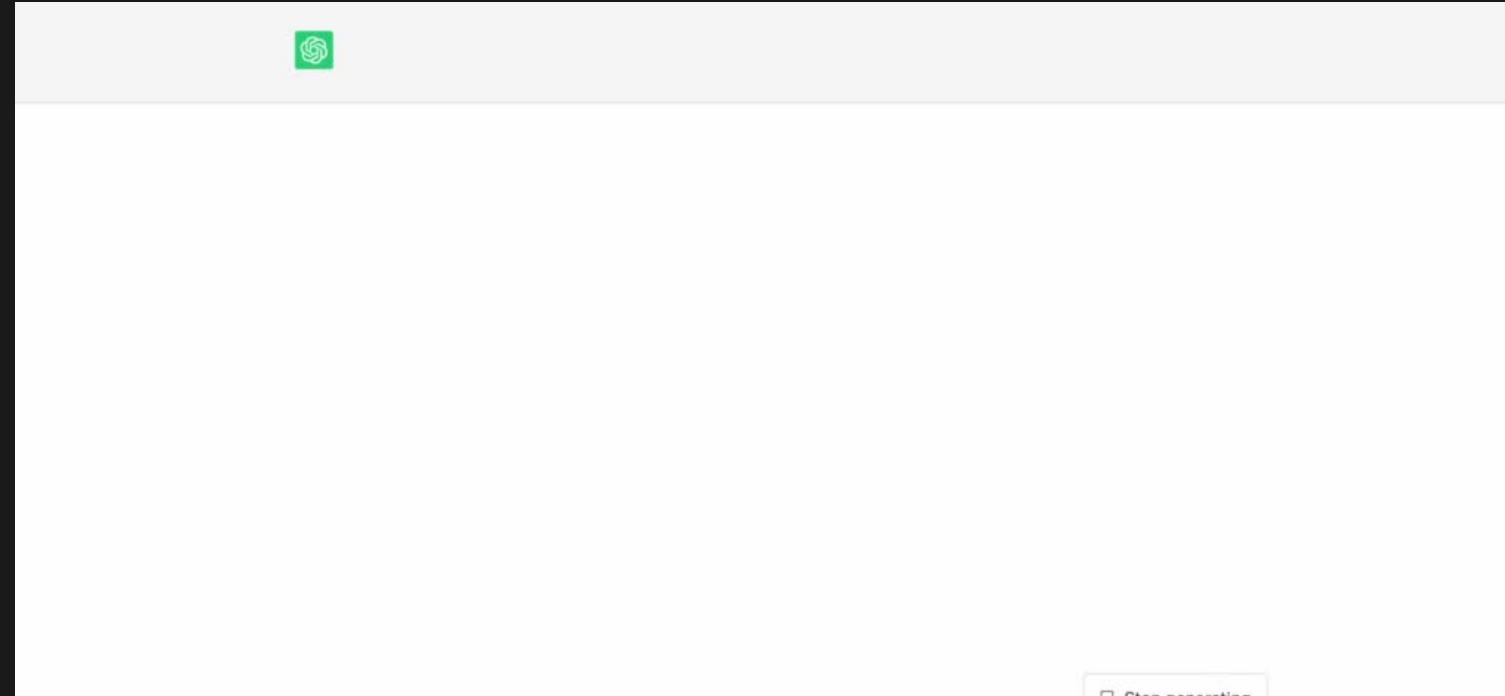


## LES IA NE SONT PAS DES ROBOTS !

De manière très concrète, une IA est un programme informatique codé pour réaliser automatiquement des tâches, à partir de la collecte et du traitement de données. Ce programme doit aboutir à l'accomplissement d'une tâche spécifique : modifier une image, reconnaître un visage, obtenir le résultat d'une équation. Cela se traduit par un apprentissage, un entraînement.

NUMERAMA





**IA FORTE**

Pour me donner toutes les chances de vous répondre au mieux, merci d'écrire des phrases courtes. *exemple: comment créer un compte ?*

Vous pouvez à tout moment revenir à ce message en tapant "accueil".

09h37

Un envoi ou réception de courrier / colis avec numéro de suivi

**IA FAIBLE**



**QUAND ?**

1950

Creation de la premiere  
IA

L'objectif est de creer un  
ordinateur qui pense  
comme nous

**QUI ?**

John  
McCarthy  
chercheur chez IBM

**OÙ ?**

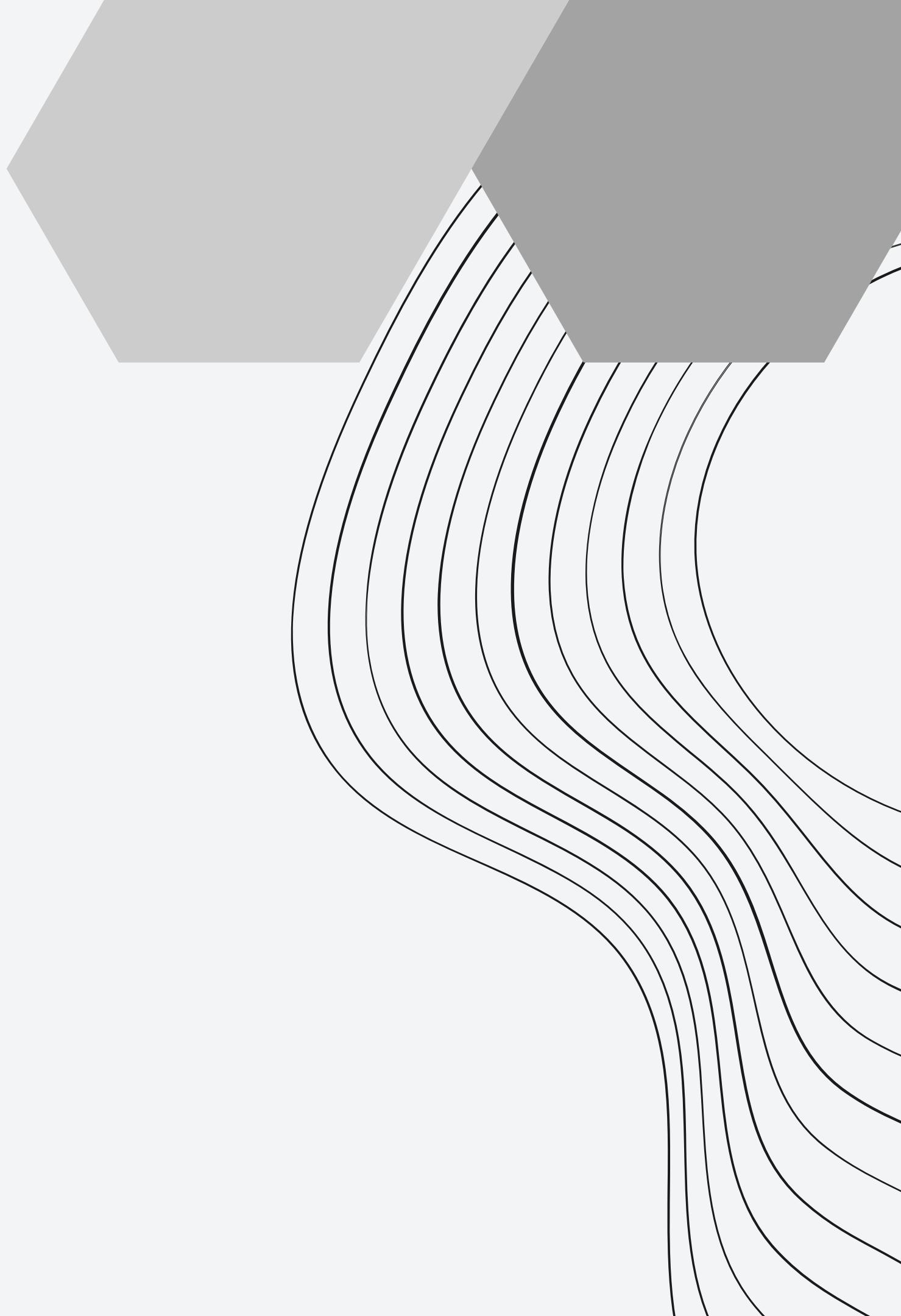
Californie

**POURQUOI ?**

Rendre la machine intelligente pour  
aider l'humain dans son évolution

# LA SÉCURITÉ EN ENTREPRISE

- 1 PROTECTION DES DONNÉES (RGPD)**
- 2 SURVEILLANCE DES ACTIVITÉS**
- 3 CREATION DE POLITIQUE DE SÉCURITÉ**



# AUJOURD'HUI

**RESPONSABLE DE LA  
SÉCURITÉ DE  
L'INFORMATION**

1

2

3

Équipe de sécurité  
informatique

**ÉQUIPE DE GESTION DES  
RISQUES**

# DANS LES ANNÉES À VENIR

**RESPONSABLE DE LA  
SÉCURITÉ DE  
L'INFORMATION**

1

2

3

Équipe de sécurité  
informatique

Intelligence Artificielle

# ÉTUDES DE CAS



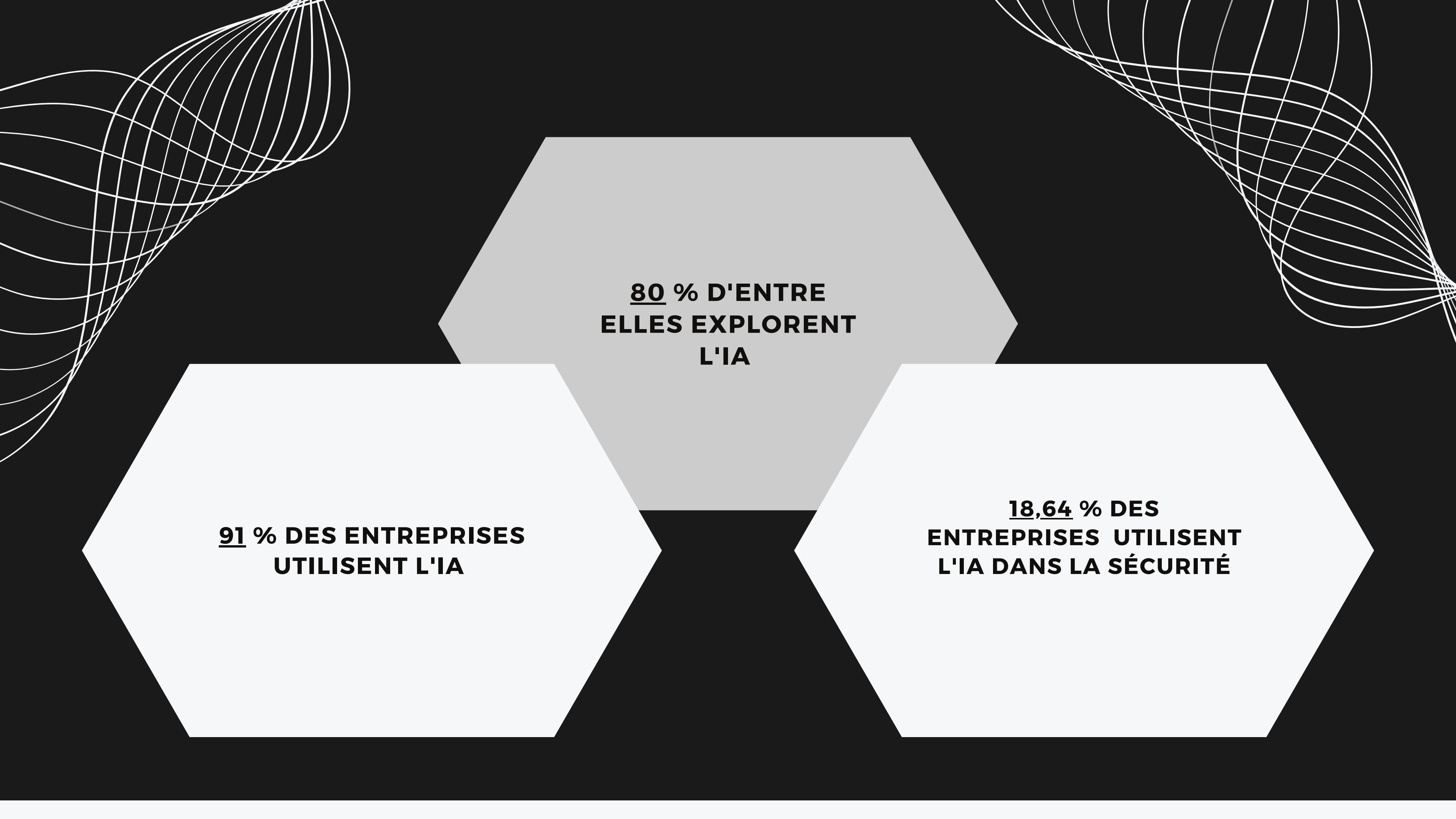
## CYLANCE

Cylance fait partie des tout premiers fournisseurs de protection en cybersécurité à appliquer l'IA à son système. L'entreprise fournit notamment des solutions anti-malware basées sur l'IA.



## FIREEYE

L'entreprise fait partie de celles qui proposent des solutions avancées basées sur l'IA au niveau sécurité



**91 % DES ENTREPRISES  
UTILISENT L'IA**

**80 % D'ENTRE  
ELLES EXPLORENT  
L'IA**

**18,64 % DES  
ENTREPRISES UTILISENT  
L'IA DANS LA SÉCURITÉ**



## LES AVANTAGES DE L'IA

Présentation de l'IA dans les entreprises, et les bénéfices de l'ia dans une entreprises

## LES RISQUES DE L'IA

Présentation des risques de l'ia dans les entreprises

# LES AVANTAGES DE L'IA



## L'INTELLIGENCE ARTIFICIELLE SAUVE DES VIES

Dans le domaine médical, l'IA est de plus en plus utilisée à des fins d'analyse. Son taux de détection est proche de celui des médecins et surtout, elle travaille en continu, 24 heures par jour

**DEVINCI**



## L'IA DÉTECTE DE NOUVEAUX RISQUES DE SÉCURITÉ

Les solutions de cybersécurité basées sur l'IA peuvent détecter de nouvelles menaces inconnues ainsi que des menaces qui se sont produites au sein du réseau et des menaces connues qui ne se sont pas produites

**ISSQUAREDINC**



## L'INTELLIGENCE ARTIFICIELLE ET LE SECTEUR DE LA LOGISTIQUE

l'IA permet d'éviter les sources d'erreurs et d'obtenir un gain de temps et d'argent. Cette technologie leur a permis de réduire de 10 % l'utilisation des véhicules et de 30 % les distances à parcourir.

**ECN**

**ELLE PERMET AU DEVELOPPEMENT DE L'ENTREPRISE**

# LES RISQUES DE L'IA



## IA GÉNÉRATIVE ET HAMEÇONNAGE

L'intelligence artificielle générative suggère également des risques liés à la confidentialité des données provenant de l'extérieur, l'hameçonnage (ou phishing) en fait partie. Il s'agit d'une technique de fraude sur Internet qui consiste à leurrer un utilisateur, en se faisant passer pour un organisme de confiance, pour qu'il transmette des informations personnelles.

**GETAPP**



## COMMENT L'IA VA BOULEVERSER LA CYBERSÉCURITÉ ?

Les cybercriminels peuvent étudier et comprendre les fonctionnalités des modèles utilisés dans les systèmes de défense. Ainsi, ils cherchent continuellement des moyens de les contourner. À force, ils peuvent trouver des vulnérabilités dans les algorithmes ou exploiter les faiblesses des outils pour élaborer des attaques spécifiques.

**LEBIGDATA**



## INTELLIGENCE ARTIFICIELLE : LES MENACES GRAVES

Usurper l'identité d'une personne en lui faisant dire ou faire des choses qu'elle n'a jamais dite ou faites, dans le but de demander un accès à des données sécurisées, de manipuler l'opinion ou de nuire à la réputation de quelqu'un... Ces vidéos truquées sont quasi indétectables.

**FUTURA-SCIENCE**

# CONCLUSION

C'est pourquoi l'IA est une opportunité pour améliorer la sécurité des données aux seins des entreprises. En effet, elle offre une surveillance continue avec un temps de réaction inférieur à celui d'un humain.

L'entreprise peut donc passer moins de temps sur la sécurité des données.

Néanmoins, il est important de maintenir une surveillance sur les données traitées par l'IA, pour s'assurer que celles-ci soient elles-mêmes protégées. C'est pourquoi l'IA est un bon outil si elle est supervisée par un humain. Ainsi cette association est essentielle pour la sécurité et la confidentialité des informations de l'entreprise.

# PERSPECTIVES



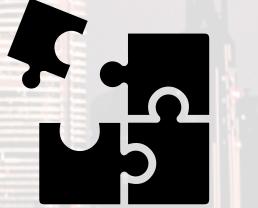
## Automatisation

L'IA sera de plus en plus utilisée pour automatiser les réponses aux menaces en temps réel, limitant les dégâts potentiels.



## Prédiction

L'IA analysera les tendances historiques et actuelles des cyberattaques pour prédire les futures menaces potentielles.



## Menaces Internes

L'IA pourra être déployée pour identifier les comportements suspects des employés et des utilisateurs internes.

**PLACE AU  
QUESTION !**

