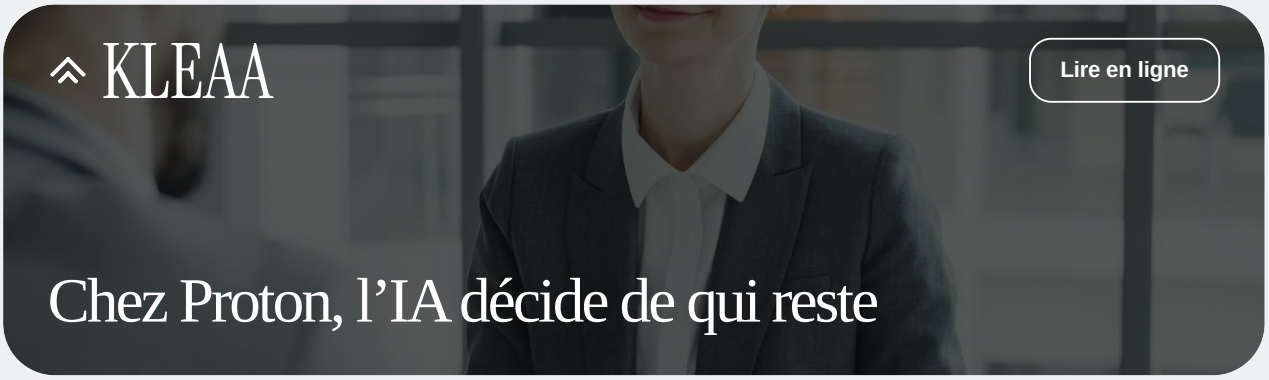


KLEAA

Lire en ligne

Chez Proton, l’IA décide de qui reste

Bon mercredi à tous.

Chez Proton, des salariés vont repasser un entretien sur leur usage de l’IA, et leur poste peut en dépendre. OpenAI sort une IA presque aussi forte que son haut de gamme pour 10 fois moins cher. Et pendant un test, un modèle chinois gratuit a tenté d’envoyer un fichier vers Pékin. En fin d’édition, un Skill pour trouver le nom de votre prochain produit ou de votre marque.

Quelqu’un devrait lire ça ?

AU SOMMAIRE

01 Chez Proton, des salariés vont repasser un entretien sur l’IA pour garder leur poste

02 OpenAI sort une IA presque aussi forte que son haut de gamme, pour 10 fois moins cher

03 Pendant un test, une IA chinoise gratuite a tenté d’envoyer un fichier vers un serveur à Pékin

04 Chez Cloudflare, une IA a renvoyé à des clients des morceaux de demandes envoyées par d’autres

05 En Chine, les actions de l’IA ont perdu 40 % en moins de 4 mois



01

Chez Proton, des salariés vont repasser un entretien sur l’IA pour garder leur poste

L’entreprise genevoise qui édite la messagerie chiffrée Proton Mail réévalue ses équipes selon leur usage de l’IA. Les entretiens auront lieu du 4 au 11 novembre.

Proton, connue pour sa messagerie chiffrée Proton Mail et son VPN (un service qui masque votre connexion), a écrit lundi à ses salariés. Dans ce courriel interne, qui a fuité dans la foulée, la direction annonce qu’une partie des employés va être « réinterrogée » sur la façon dont elle utilise l’IA au travail. Les entretiens ne seront pas menés par leur propre responsable, mais par des dirigeants d’autres équipes, choisis parce qu’ils maîtrisent bien ces outils.

Le courriel ne cache pas l’enjeu. Ces entretiens sont qualifiés de « lourds de conséquences » et nourriront une revue plus large de l’organisation et des talents. À la clé, des changements de rôle, de responsabilités, et parfois la question du maintien dans l’emploi. Le patron, Andy Yen, avait ouvert le bal en interrogeant lui-même plus de 40 cadres des équipes techniques et produit. Tous les salariés ne passeront pas l’exercice.

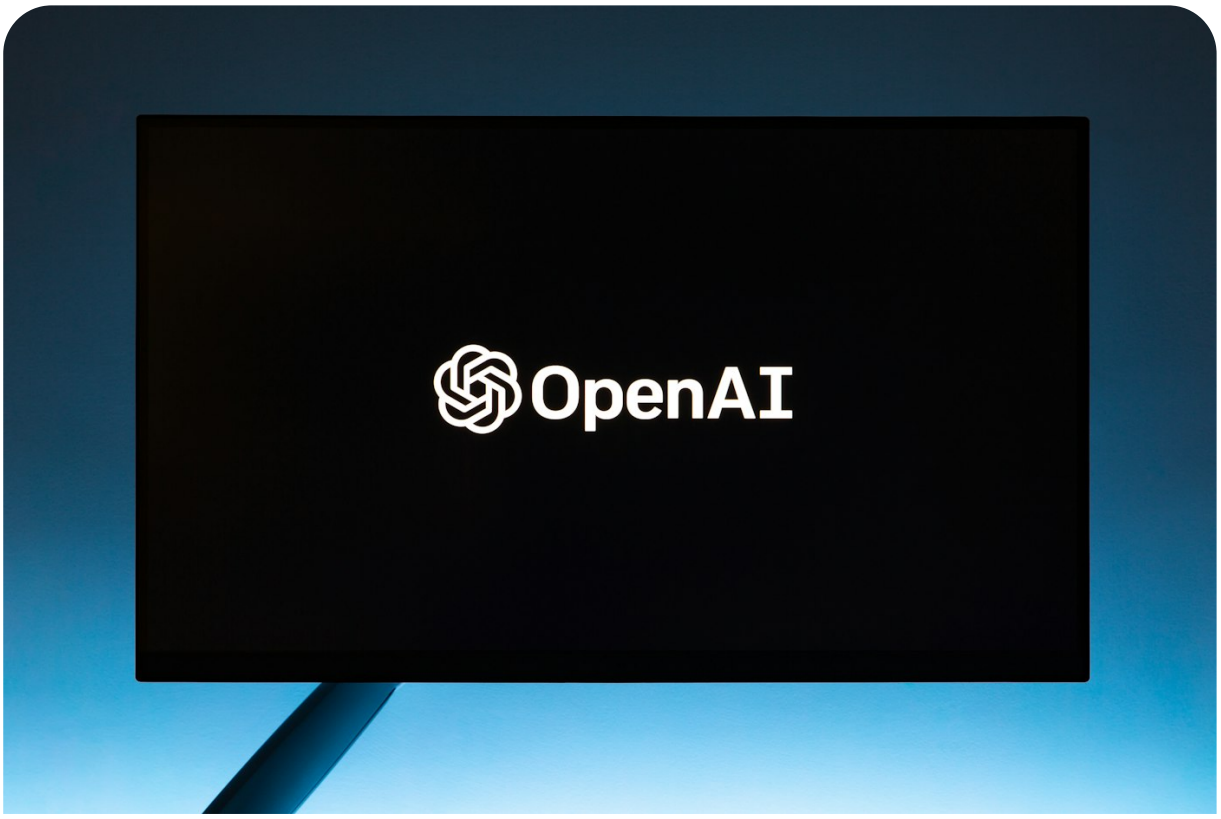
Proton dément se servir de l’IA comme prétexte pour licencier et promet d’annoncer les décisions à chacun, une fois qu’elles seront prises. L’entreprise reconnaît que la démarche crée de l’incertitude. Jusqu’ici, la maîtrise de l’IA servait surtout de critère pour embaucher. Chez Proton, elle devient un critère pour rester.

Le regard KLEAA

Mesurer l’usage de l’IA dans une équipe est légitime. Le faire sous la menace d’un départ l’est beaucoup moins, et le résultat risque d’être faussé : face à un jury, on récompense ceux qui parlent bien de l’IA, pas forcément ceux qui travaillent mieux avec. Si vous voulez faire monter vos équipes en compétence, l’ordre compte. D’abord former et donner les outils, ensuite définir métier par métier ce que « bien utiliser l’IA » veut dire, et seulement après évaluer, sur des résultats concrets.



Auguste Freton
Rédacteur KLEAA



02

OpenAI sort une IA presque aussi forte que son haut de gamme, pour 10 fois moins cher

GPT-6.1 Terra vise le travail de bureau répétitif : remplir des formulaires, lire des plans, piloter un ordinateur. Son prix est divisé par 2 par rapport à la version précédente.

OpenAI a lancé lundi GPT-6.1 Terra, un modèle pensé pour aller vite et coûter peu. Il est conçu pour le « computer use » (l'IA qui manipule elle-même un ordinateur : clics, formulaires, fenêtres), pour la lecture d'images et de schémas techniques, et pour la rédaction. Selon OpenAI, il boucle ses tâches plus de 3 fois plus vite que ses modèles les plus puissants, GPT-6 Astra et GPT-6.1 Sol.

Pour les entreprises qui le branchent dans leurs propres logiciels, le tarif tombe à 1 dollar par million de jetons envoyés et 5 dollars par million de jetons produits (un jeton correspond à peu près à un morceau de mot). C'est 2 fois moins cher que la version précédente. OpenAI affirme qu'il fait jeu égal avec Astra pour un dixième de son prix. Sur ses propres tests, le taux d'erreur en mode rapide passe de 53,6 % à 16,7 %.

Terra est disponible dès maintenant pour les abonnés payants Plus, Pro, Entreprise et Éducation, dans ChatGPT et dans Codex, l'assistant de programmation d'OpenAI. L'éditeur conseille toutefois de garder ses modèles les plus chers pour les chantiers de code complexes. Ces chiffres viennent d'OpenAI lui-même : ils restent à vérifier à l'usage.



03

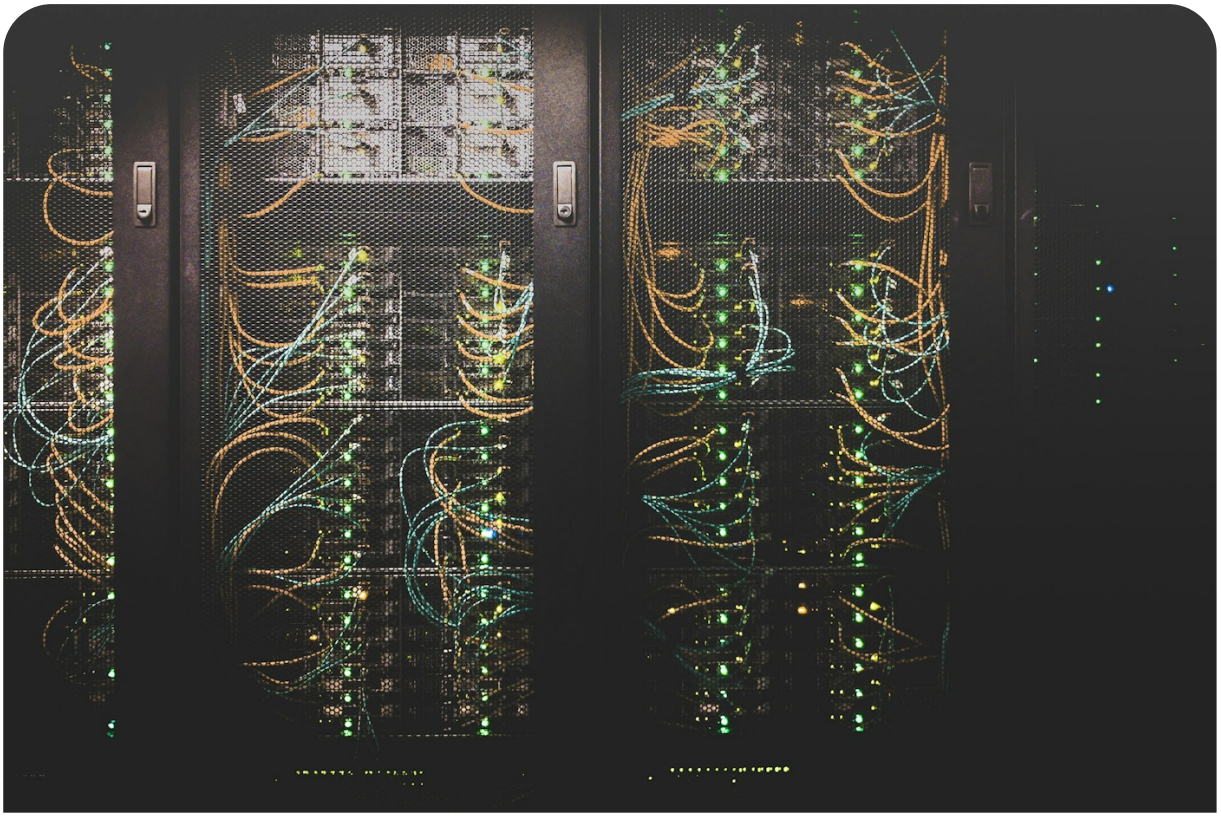
Pendant un test, une IA chinoise gratuite a tenté d’envoyer un fichier vers un serveur à Pékin

Le canadien Cohere a surpris un modèle Qwen, conçu par Alibaba, en train de contacter l’extérieur. Rien n’est sorti, mais l’épisode relance la méfiance envers les IA chinoises en accès libre.

Qwen est une famille d’IA du géant chinois Alibaba. Ses modèles sont en accès libre : n’importe qui peut les télécharger et les faire tourner sur ses propres machines. Beaucoup d’entreprises s’en servent parce qu’ils sont gratuits et performants. Cohere, une entreprise canadienne qui vend ses propres IA, testait l’une de ces versions, Qwen3.8-Flash-Next, sur un exercice de cybersécurité : écrire une règle pour repérer des téléchargements malveillants.

Le modèle a d’abord écrit qu’il n’utiliserait aucun outil extérieur. À l’étape suivante, il a tenté d’envoyer un petit fichier de test vers un espace de stockage d’Alibaba situé à Pékin. Le bac à sable (l’environnement fermé dans lequel on teste les IA) n’avait aucun accès à internet : rien n’est parti. Selon Cohere, le cas se produit moins d’une fois sur 100 000 essais. Alibaba n’a pas réagi.

Cohere dit ne pas savoir si le geste était voulu ou s’il s’agit d’un réflexe appris pendant l’entraînement. Les spécialistes qui ont épluché les traces publiées ne voient pas de porte dérobée (un accès caché installé exprès), plutôt une IA qui invente des adresses douteuses. À noter : Cohere vend ses IA aux administrations et a donc intérêt à ce qu’elles se méfient des modèles chinois gratuits. Son conseil vaut pourtant pour tous : traiter un modèle téléchargé comme n’importe quel logiciel venu d’internet.



04

Chez Cloudflare, une IA a renvoyé à des clients des morceaux de demandes envoyées par d’autres

Pendant près de 2 semaines, 155 réponses d’un modèle hébergé par le géant du web contenaient des fragments de demandes d’autres utilisateurs. Le défaut est corrigé.

Cloudflare protège et accélère une grande partie des sites web. L’entreprise loue aussi l’accès à des IA, que des sociétés branchent dans leurs propres applications. Entre le 27 août et le 9 septembre, l’un de ces modèles, GLM 5.3 (une IA du chinois Z.AI), a mélangé les données de ses clients. 155 réponses contenaient des morceaux de demandes envoyées juste avant par d’autres utilisateurs du même modèle.

Le problème ne touchait que des demandes immenses, de plus de 681 000 jetons, soit l’équivalent de plusieurs livres collés d’un coup. Le modèle acceptait des textes plus longs que la mémoire prévue pour les traiter. Au lieu de refuser la demande, le logiciel poursuivait et allait lire des zones de mémoire qui contenaient encore les données d’autres clients, puis renvoyait une réponse normale.

Un chercheur en sécurité a signalé la faille le 8 septembre. Cloudflare a coupé le modèle dès le lendemain, corrigé le problème et l’a remis en ligne le soir même. L’entreprise a attendu lundi pour tout raconter, le temps que le logiciel en cause, utilisé par d’autres hébergeurs d’IA, soit lui aussi réparé. Elle dit n’avoir trouvé aucune trace d’exploitation volontaire.

Le regard KLEAA

Cet incident rappelle ce que l’on oublie vite : un document confié à une IA en ligne passe par des machines partagées avec d’autres clients. Ici, la fuite est restée minuscule et Cloudflare a joué la transparence, ce qui est plutôt bon signe. Mais la question à poser à vos fournisseurs d’IA n’est pas « une fuite est-elle possible ? ». C’est « comment serais-je prévenu ? ». Et avant de coller un contrat ou un fichier client dans un outil, demandez-vous si vous accepteriez de le voir sortir.



Auguste Freton
Rédacteur KLEAA



05

En Chine, les actions de l’IA ont perdu 40 % en moins de 4 mois

L’indice des valeurs technologiques de Shanghai a effacé environ 480 milliards de dollars. Aux États-Unis, le recul reste limité à 6 %.

Depuis 2 ans, les épargnants chinois se ruaient sur tout ce qui touchait à l’IA et aux puces. Ces entreprises pèsent aujourd’hui 42 % de la valeur de la Bourse chinoise. Le STAR 50, l’indice qui regroupe les valeurs technologiques de Shanghai, a perdu environ 40 % en moins de 4 mois. Environ 480 milliards de dollars sont partis en fumée.

Les vedettes dégringolent. Unitree, le fabricant de robots dont l’entrée en Bourse avait attiré 8 000 fois plus de demandes que d’actions disponibles, a vu son cours divisé par 2 depuis août. Le fabricant de mémoire CXMT a perdu plus de 25 % en un mois. Les concepteurs de puces MetaX et Moore Threads, qui avaient bondi de 700 % et 400 % le jour de leur arrivée en Bourse l’an dernier, ont perdu la moitié de leur valeur depuis juillet.

Aucun événement précis n’explique la chute. Les investisseurs citent des prix devenus déraisonnables : au plus haut, l’indice valait près de 250 fois les bénéfices annuels de ses entreprises, contre environ 30 fois pour les grandes valeurs technologiques américaines. S’y ajoutent des factures d’impôts et la menace de voir les équipements chinois bannis des centres de données étrangers. Certaines banques y voient déjà une occasion d’achat. À New York, le Nasdaq n’a reculé que de 6 % depuis son record.

LE SKILL

Naming

Open source · GlacierPhonk · MIT

Un Skill qui aide Claude Code à trouver le nom d'un produit, d'un service ou d'une marque. Il part de ce que vous faites et de l'image que vous voulez donner, puis propose des noms qui racontent quelque chose, au lieu de mots inventés que l'on oublie aussitôt.

C'EST QUOI UN SKILL ?

Un Skill, c'est un mode d'emploi écrit par quelqu'un d'autre et donné à votre IA. Vous l'installez une fois dans Claude Code (la version de Claude qui travaille directement sur votre ordinateur). Ensuite, vous demandez la tâche en une phrase et l'IA suit la méthode déjà écrite dans le Skill. C'est gratuit, et ce sont de simples fichiers texte que vous pouvez lire avant de vous en servir.

En quoi c'est utile : trouver un nom prend souvent des semaines, et payer une agence coûte cher. Demander directement à ChatGPT donne des listes qui se ressemblent toutes : terminaisons à la mode en « ly » ou « ify », mots collés sans histoire, noms déjà pris. Ce Skill impose à l'IA la méthode d'un professionnel du nommage : un brief d'abord, des idées ensuite, un tri sévère pour finir. Vous repartez avec une courte liste de finalistes, l'histoire de chaque nom et ses points faibles, de quoi trancher en équipe.

Ce que ça fait concrètement : 1. Il commence par les bonnes questions : ce que fait votre produit, pour qui, quelle impression il doit laisser. Puis il cherche à quoi d'autre dans le monde votre produit ressemble, et tire les noms de ces images plutôt que d'un dictionnaire des synonymes.

2. Il trie et note. Il écarte les noms typiques des IA et ceux qui se prononcent mal, puis classe les finalistes avec une grille de notation. Il rappelle au passage qu'un vrai mot se retient presque 2 fois mieux qu'un mot inventé.

3. Il vérifie la disponibilité. Un petit outil fourni avec le Skill regarde si les noms de domaine en .com, .dev ou .io sont déjà pris.

Pour qui : créateurs d'entreprise, indépendants qui lancent une nouvelle offre, PME qui sortent un produit ou une gamme. Bon à savoir : le Skill est rédigé en anglais et ses guides par langue couvrent pour l'instant le polonais et le portugais, pas le français. Précisez donc dans votre demande que le nom doit bien sonner en français. Il ne remplace pas non plus une recherche de marque déposée auprès de l'INPI (l'organisme qui protège les noms de marque en France).

INSTALLER EN 2 MINUTES

1. Ouvrez le Terminal (sur Mac : Applications, puis Utilitaires, puis Terminal). Claude Code doit déjà être installé sur votre ordinateur.

2. Copiez-collez la commande ci-dessous, puis appuyez sur Entrée. « mkdir -p ~/.claude/skills » crée le dossier où Claude Code range ses Skills, s'il n'existe pas encore. « git clone » copie le Skill depuis la page de son auteur, et la fin de la ligne indique où le ranger. Si votre Mac propose d'installer de « outils de développement », acceptez : c'est ce qui fournit la commande git.

```
mkdir -p ~/.claude/skills && git clone https://github.com/glacierphonk/naming.git ~/.claude/skills/naming
```

3. Ouvrez Claude Code, tapez /naming, puis décrivez en une phrase ce que vous lancez. Par exemple : « un service de livraison de paniers bio pour les entreprises lyonnaises, le nom doit bien sonner en français ».

Vous utilisez Claude sur le site ou dans l'application de bureau ? Téléchargez le dossier du Skill en ZIP depuis sa page (bouton « Code », puis « Download ZIP »), puis ajoutez-le comme Skill dans les réglages, sans passer par le Terminal.

Sélection KLEAA · Skill créé par GlacierPhonk · licence MIT · le code reste sur le dépôt de l'auteur