

AU SOMMAIRE

5 actus · 1 Skill

- 01 Amazon interdit à l'assistant de Meta d'acheter sur son site
- 02 L'État met 80 millions d'euros pour pousser l'IA dans les entreprises
- 03 Xiaomi publie gratuitement un modèle de 1 020 milliards de paramètres
- 04 3 chercheurs ont pris la main sur des comptes de salariés d'OpenAI
- 05 Les chatbots répondent moins bien quand la demande sonne féminine

LE SKILL

claude-ecom : votre fichier de commandes devient un bilan commercial complet.



01

Amazon interdit à l'assistant de Meta d'acheter sur son site

Depuis dimanche soir, Amazon bloque Muse, l'assistant lancé par Meta le 8 septembre, dès qu'il tente de valider un panier à la place d'un client.

Muse est un assistant qui agit à votre place : il remplit des formulaires, réserve un voyage, envoie des messages, passe des commandes. Lancé le 8 septembre, il est devenu en une semaine l'application gratuite la plus téléchargée des États-Unis sur l'App Store d'Apple, devant ChatGPT. Depuis dimanche soir, quiconque s'en sert pour acheter sur Amazon tombe sur un message : l'accès prolongé par un agent IA non autorisé viole les conditions d'utilisation du site, que les clients ont acceptées en ouvrant leur compte.

Amazon avance 3 griefs. Meta ne l'a jamais prévenu. L'assistant ne dit pas qui il est quand il navigue. Et il semble capturer puis conserver les identifiants des clients, ce qui lui ouvrirait les pages de compte et l'historique des commandes. Meta répond que Muse n'a aucune visibilité sur les mots de passe ni sur les moyens de paiement, et que ce que l'utilisateur lui confie part dans un coffre auquel l'assistant n'accède pas directement. Amazon affirme avoir demandé à Meta de retirer son site du périmètre avant de couper. Le terrain choisi n'est pas anodin : Amazon avait attaqué Perplexity pour son navigateur Comet et obtenu une interdiction provisoire en mars, avant que la cour d'appel ne l'annule le 4 août, au motif que c'est l'utilisateur, et non l'éditeur de l'IA, qui accède au site. Restent les conditions d'utilisation.

Amazon fait tourner ses propres agents acheteurs, qui s'annoncent et laissent les marques se retirer. La bataille ne porte donc pas sur la technologie mais sur la propriété de la relation client au moment où un logiciel achète. Si vous vendez en ligne, la question devient concrète cette semaine : acceptez-vous que des agents commandent chez vous, et à quelles conditions ? Un agent qui ne s'identifie pas ressemble à un robot d'aspiration et finira bloqué. Un agent qui s'annonce peut devenir un canal de vente, à condition que votre site sache le reconnaître. Cela se règle dans les réglages du serveur, pas dans une réunion de stratégie.



02

L'État met 80 millions d'euros pour pousser l'IA dans les entreprises

Présenté hier à Station F, le plan Impulsion IA 2027 réunit 12 mesures et 80 millions d'euros, avec les TPE et les PME comme cible affichée.

3 ministres l'ont présenté hier à Paris : le ministre du Travail Jean-Pierre Farandou, le ministre de l'Économie Roland Lescure et la ministre déléguée chargée de l'IA et du Numérique Anne Le Hénanff. Le plan porte un objectif chiffré, sensibiliser et former près de 30 millions de personnes, et une date d'entrée en vigueur, le 1er janvier 2027. Il ne crée aucune loi nouvelle : il s'appuie sur les organismes existants.

Le contenu tient en quelques dispositifs. Une plateforme publique gratuite, Explore IA, pour tester ses connaissances et suivre des parcours. Une certification d'État sur les compétences en IA, finançable par le compte personnel de formation. Des parcours pour les demandeurs d'emploi, avec un diagnostic de maturité individuel. Un kit baptisé Recrut'IA, distribué par les 408 équipes entreprises de France Travail, qui couvre le recrutement du libellé de l'offre jusqu'à l'accueil du nouveau salarié. Un accompagnement des PME, expérimenté en janvier 2027 puis généralisé en mai. Un guide de conformité écrit avec la Cnil. Un observatoire national sur l'effet réel de l'IA sur les métiers. Et un crédit d'impôt qui accélère l'amortissement des robots, mécanique plus favorable aux petites structures qu'aux grandes.

Le chiffre qui explique la démarche vient d'une étude publiée en avril : 1 emploi sur 6 en France, soit environ 5 millions de postes, serait automatisable d'ici 3 à 4 ans. Les critiques portent sur la taille de l'enveloppe, 80 millions d'euros pour 30 millions d'actifs, à comparer aux 2,5 milliards d'économies demandées au même ministère pour le budget 2027. Reste que 2 dispositifs sont exploitables sans attendre par un dirigeant : la formation financée par le compte personnel de formation, qui ne coûte rien à l'entreprise, et l'accompagnement PME, dont l'expérimentation démarre dans 3 mois. Les textes d'application manquent encore.



03

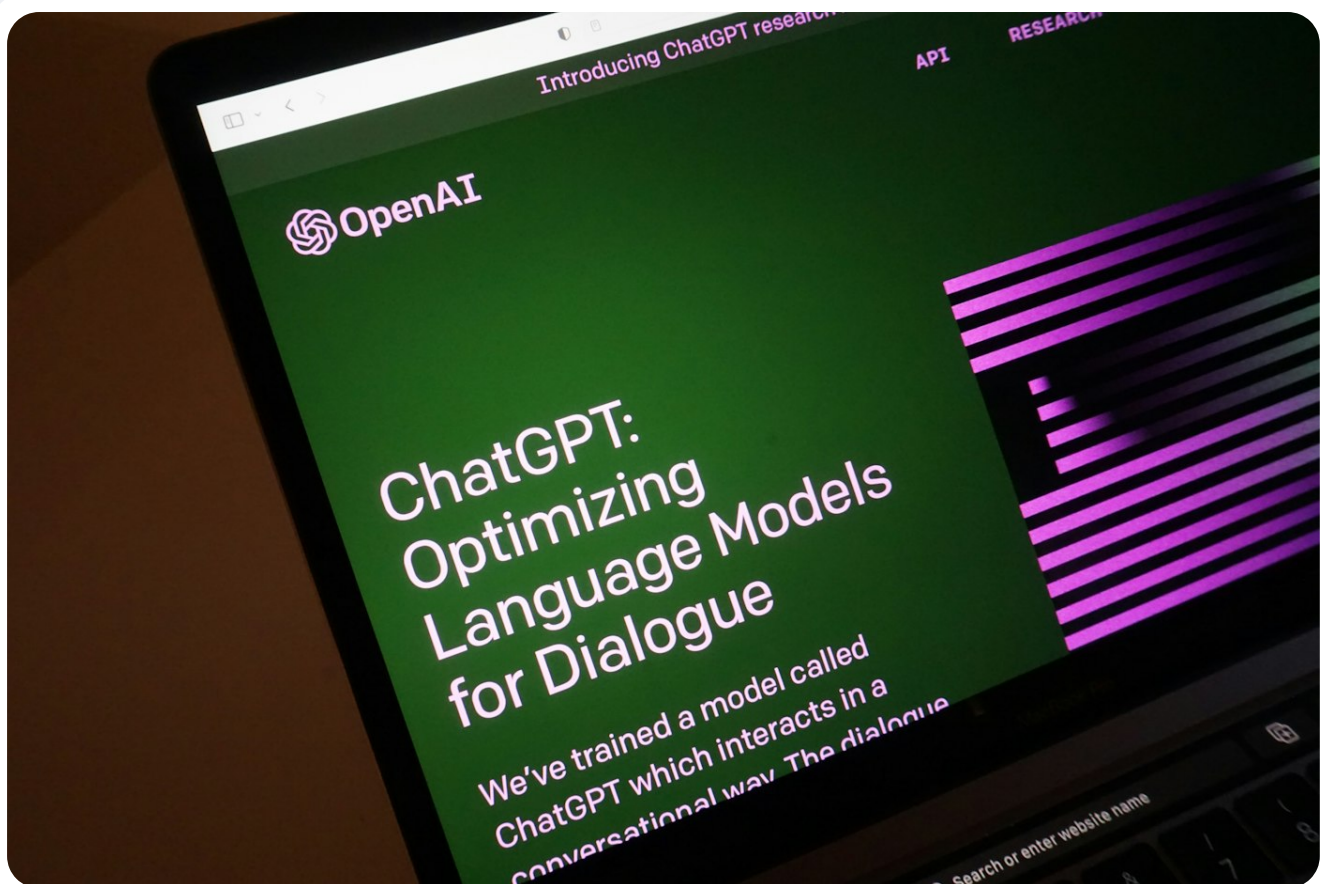
Xiaomi publie gratuitement un modèle de 1 020 milliards de paramètres

Le fabricant de téléphones a mis en ligne hier MiMo-V2.6-Pro et, avec lui, la recette complète de sa fabrication, sous la licence la plus permissive qui existe.

Un modèle de langage, c'est un très gros fichier de réglages internes, les paramètres, qui lui tiennent lieu de connaissance. MiMo-V2.6-Pro en compte 1 020 milliards, mais n'en allume que 42 milliards par question, une construction dite en mélange d'experts qui divise la facture de calcul. Il lit le texte, les images, la vidéo et le son, retient jusqu'à un million de jetons, c'est-à-dire l'équivalent de plusieurs livres dans une même conversation, et il est publié sous licence MIT : usage commercial autorisé, modification autorisée, hébergement chez soi autorisé, sans contrepartie.

L'inhabituel n'est pas le modèle, c'est ce qui l'accompagne. Xiaomi a publié le rapport technique, le cadre logiciel d'entraînement, plus de 7 000 environnements d'exercice et une version réduite à 9 milliards de paramètres. Il a aussi donné la facture : environ 2,62 millions de dollars pour la phase d'apprentissage par renforcement du grand modèle, 850 000 dollars pour la version Flash, en 30 étapes et quelque 750 000 essais étalés sur 6 jours. Sur l'indice indépendant d'Artificial Analysis, le modèle obtient 46,3 et prend la tête des modèles à poids ouverts. Par son interface de programmation, il est facturé 0,435 dollar le million de jetons en entrée et 0,87 en sortie.

L'information utile n'est pas le classement, elle est dans les 2,62 millions de dollars. Une capacité que les laboratoires américains facturaient comme un exploit est désormais reproduite pour le prix d'un appartement parisien, par un fabricant de téléphones, et la méthode est offerte à qui veut la refaire. Pour une entreprise, cela déplace la négociation : aucun fournisseur ne peut plus justifier un tarif par la rareté de la technologie. Attention toutefois à ne pas confondre gratuit et sans effort. Faire tourner 1 020 milliards de paramètres chez soi réclame du matériel sérieux. La voie réaliste reste de louer l'accès, en vérifiant où sont hébergées les données.



04

3 chercheurs ont pris la main sur des comptes de salariés d'OpenAI

Une équipe de 3 personnes a enchaîné 2 failles, en partant d'une simple image envoyée sur un forum, jusqu'à ouvrir les comptes ChatGPT et Codex de salariés d'OpenAI.

Les 3 chercheurs travaillent chez Hacktron AI, une jeune pousse de sécurité. Leur point de départ n'était pas ChatGPT mais le forum communautaire d'OpenAI, un outil annexe qui tourne sur un logiciel de discussion du commerce. Une image au format HEIF, fabriquée pour l'occasion, a provoqué un débordement de mémoire dans la brique qui decode ce format. De là, une seconde faille, cette fois du côté de la page de connexion d'OpenAI, a permis de récupérer des sessions déjà ouvertes de salariés. La chaîne complète a tenu en moins de 72 heures.

Le détail qui a fait parler : le programme d'attaque a été écrit par une IA. Les chercheurs racontent avoir échoué pendant plusieurs sessions avec la version précédente de Claude, puis avoir réussi avec la suivante dans les heures qui ont suivi sa sortie. Pour prouver l'accès sans lire le moindre document confidentiel, ils ont utilisé l'outil de code d'un employé pour ouvrir une demande de modification inoffensive dans le dépôt interne d'OpenAI. L'entreprise a confirmé son correctif environ 14 heures après le signalement et versé une prime de 6 500 dollars, en précisant qu'elle récompensait la faille de son côté, pas les actions menées contre le forum.

2 leçons, et aucune ne concerne l'intelligence artificielle. La première : la porte d'entrée était un forum, c'est-à-dire l'outil que personne ne surveille. Faites la liste des services branchés à votre système de connexion, le support, le blog, l'outil de sondage, l'espace client ; chacun est une porte, et la plus faible décide du niveau de sécurité de l'ensemble. La seconde : le coût d'une attaque s'effondre. Ce qui exigeait un spécialiste rare et plusieurs semaines tient désormais en 3 jours avec un outil vendu quelques dizaines d'euros par mois. La bonne nouvelle est que la défense dispose exactement des mêmes outils.



05

Les chatbots répondent moins bien quand la demande sonne féminine

Des chercheurs de Johns Hopkins montrent que 4 assistants parmi les plus utilisés renvoient des textes plus courts et moins soignés quand la consigne contient des tournures statistiquement plus fréquentes chez les femmes.

L'équipe est partie de vraies demandes de bureau : rédiger un message professionnel, une candidature, une lettre de démission. Elle y a ensuite glissé des marqueurs de langage documentés comme plus fréquents chez les femmes, sans changer le fond : les précautions, du type « peut-être » ou « je pense », le collectif, du type « nous » ou « notre équipe », et les adjectifs expressifs, du type « formidable ». 4 modèles ont été testés, dont ceux qui font tourner ChatGPT et l'assistant de Mistral.

Le résultat est constant : les réponses reviennent plus courtes, moins formelles et d'un niveau de langue plus bas. L'écart subsiste après avoir neutralisé le ton de la demande. Un détail contredit l'intuition : mettre un prénom masculin ou féminin ne change presque rien. Ce n'est donc pas l'identité affichée qui compte, mais la façon d'écrire la consigne. Le travail a été mis en ligne en archive ouverte et sera présenté début octobre à une conférence sur les modèles de langage, à San Francisco.

Pour une entreprise, le sujet n'est pas une question de principe, c'est une question de qualité. 2 collaborateurs qui demandent la même chose n'obtiennent pas le même texte, et ni l'un ni l'autre ne peut le savoir. Or le document part ensuite chez un client, un candidat ou un banquier. 2 réflexes suffisent à réduire l'écart. Écrire des consignes directes plutôt que prudentes : dire le format attendu, la longueur, le registre, le destinataire, au lieu d'envelopper la demande. Et fixer un modèle de consigne commun à l'équipe, pour que la qualité du rendu cesse de dépendre de la manière de parler de chacun.

claude-ecom

Open source · Hajime Takeda · MIT

Vous déposez l'export de vos commandes et vous récupérez le bilan commercial qu'un consultant aurait écrit : ce qui monte, ce qui baisse, pourquoi, et quoi corriger en premier.

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 sur votre ordinateur, dans Claude Code, la version de Claude qui tourne chez vous. Ensuite, au lieu de réexpliquer chaque fois ce que vous attendez, vous demandez la tâche en une phrase et l'IA suit la méthode déjà écrite dans le Skill. Ce sont de simples fichiers texte, gratuits, que vous pouvez lire avant de vous en servir.

En quoi c'est utile : la plupart des dirigeants savent que le chiffre d'affaires a monté ou baissé. Presque aucun ne sait dire pourquoi, parce qu'il faudrait découper les ventes par période, par client, par produit, et recommencer chaque mois. C'est exactement le travail que l'on confie à un analyste, quand on a les moyens d'en payer un. Ici, vous partez du fichier que votre boutique en ligne, votre caisse ou votre outil de facturation sait déjà exporter, et vous obtenez en quelques minutes un document lisible : le résumé pour le dirigeant, les écarts sur 30, 90 et 365 jours, et la liste des actions à mener dans l'ordre. Comptez une matinée de travail économisée chaque mois, et surtout une explication là où vous n'aviez qu'un total.

Ce que ça fait concrètement : 3 choses. Il compare la même activité sur 3 durées, le dernier mois, le dernier trimestre et l'année, pour distinguer un coup de chaleur saisonnier d'une vraie tendance. Il décompose le chiffre d'affaires en ses causes, nouveaux clients contre clients qui reviennent, nombre de commandes contre panier moyen, et signale en rouge la branche qui tire les résultats vers le bas. Il termine par un plan d'action classé par priorité, avec pour chaque point ce qu'il faut faire, à quelle échéance et à quoi on verra que ça marche. Vous pouvez aussi poser une seule question, par exemple sur la fidélité de vos clients, au lieu de demander le rapport complet.

Pour qui : toute personne qui vend et qui n'a pas d'analyste sous la main. Commerçant en ligne, marque en vente directe, responsable de boutique, indépendant qui facture à la mission. Il suffit d'un export de commandes. Licence MIT, usage commercial autorisé. 2 précautions : les rapports sortent en anglais si vous ne demandez rien, alors demandez le français ; et le fichier reste sur votre ordinateur, ce qui est précisément l'intérêt quand il contient vos clients.

INSTALLER EN 2 MINUTES

1. Ouvrez le Terminal, la fenêtre où l'on tape des commandes (Mac : Applications → Utilitaires → Terminal. Windows : menu Démarrer, tapez « Terminal »), puis lancez Claude Code en tapant claude et Entrée.

2. Copiez ces 2 lignes, collez-les l'une après l'autre, appuyez sur Entrée :

```
/plugin marketplace add takechanman1228/claude-ecom
/plugin install claude-ecom@claude-ecom
```

Mot à mot : la première ligne indique à Claude Code où trouver le dépôt de l'auteur sur GitHub, la seconde y prend le Skill. La partie calcul, écrite en Python, s'installe toute seule au premier lancement. Fermez puis relancez Claude Code pour qu'il en tienne compte. Rien ne passe par KLEAA.

3. Exportez vos commandes depuis votre boutique ou votre outil de facturation, déposez le fichier dans le dossier ouvert, puis tapez /claude-ecom:ecom review. 4 colonnes suffisent : numéro de commande, date, client (identifiant ou adresse e-mail) et montant encaissé, remises déduites, avant taxes et livraison. La quantité, la référence produit et la remise affinent l'analyse sans être obligatoires. Les intitulés n'ont pas besoin d'être exacts.

Skill publié par Hajime Takeda sous licence MIT. KLEAA sélectionne et explique : le code et la licence restent chez l'auteur.