

GitHub впав на сім годин

Критичний інцидент дав 20% помилок у вебі й 50% на завантаженнях, тривав 7,5 години.

вівторок, 18 серпня 2026

У ЦЬОМУ ВИПУСКУ

1. GitHub лежав 7 годин 35 хвилин, статус «critical» - і це не «трохи повільніше», а 20% помилок на всьому вебі і 50% на завантаженнях
2. Wiz: «автофікс» від GitHub Copilot сам створив дірку, автономний агент знайшов її за 5 днів і виліз у внутрішню Jira Snowflake. Це найважливіший пункт дня для нас
3. Брокман (OpenAI) публікує «Вікно захисника» - і в ньому є замір, який я можу відтворити сьогодні. Але половину поста я даю з протиотрутою
4. Anthropic: \$65 млрд річного run rate, ×7 за рік, IPO у вересні-жовтні. І цього разу цифра підтверджена трьома джерелами, а не твітом
5. AI;DR - «III; не читав». 696 балів, найбільша дискусія доби після GitHub. І це прямо про твої LinkedIn-пости
6. Cursor запускає Origin - конкурента GitHub. Рівно в день, коли GitHub лежав сім годин
7. DuckDB 2.0: клієнт-серверний режим, тригери і рекурсивні запити в 40 разів швидші. 576 балів
8. Qwen 3.8 27B набрав 52 на Artificial Analysis - і в треді знайшлась поправка, яка міняє вчорашній висновок
9. Пам'ять подорожчала на 500% за рік, DDR5 128 ГБ - \$3 399. І в треді пояснили, звідки це
10. Гаррі Тан відкрив gbrain - 70 своїх скілів для агента, MIT, 28,6 тис. зірок. Найближче до нашого репо з усього, що вийшло за добу

ТЕМА 1

GitHub лежав 7 годин 35 хвилин, статус «critical» - і це 20% помилок на всьому вебі і 50% на завантаженнях

Головна подія доби і за масштабом, і за кількістю тредів: на HN інцидент розлетівся на **п'ять окремих гілок** (698, 535, 524, 288, 102 балів). Такого розсипання по темі не траплялось за час ведення дайджесту.

Хронологія з першоджерела - взята з [status API GitHub](#), де лежать усі 34 апдейти інциденту:

- 13:40 UTC - «investigating reports of impacted performance»
- 13:45 - перша чесна цифра: «**приблизно 20% помилок** на численних сценаріях, включно з Pull Requests та Issues»

- **14:04** - картина повнішає: 20% на веб і API, а **завантаження архівів і сирого вмісту репозиторіїв** - близько 50% помилок • **14:24** - додалися SAML і OIDC автентифікація, SCIM і Team Sync. Тобто лягла вхід • **16:36** - «виявили проблемний компонент і вжили заходів»
- **17:34** - і одразу ж: «бачимо залишковий вплив на численних сервісах»
- **19:13** - «частково вимкнули повторні спроби видачі токенів автентифікації» - єдина технічна деталь, яку GitHub видав про причину • **21:15 UTC** - resolved. Разом 7 год 35 хв, офіційний impact - **critical**

Детального RCA ще нема: «буде опубліковано, щойно стане доступним».

Найгостріше в тредах - статус-сторінка. Дослівно з MallocVoidstar: «Все зелене, тобто все працює. Ігноруйте єдинорога на кожній сторінці» - і за 5-10 хвилин GitHub нарешті **вручну** відкрив інцидент. Розвиток від cyphar: «Тішить, що це назвали "деградацією продуктивності". Якщо добряче примружитись, **сервіс, який взагалі не працює, - це просто дуже великі стрибки латентності**». І фінальний удар від malfist: «"Деградація" не рахується в статистику аптайму. Issues позначені як degraded зі 100% аптайму».

jjice описав симптом, який відчув кожен: «Соромно, що довелось іти на HN перевіряти, чи проблема тільки в одного, замість того щоб покластись на статус-сторінку, на яку сам GitHub і посилається».

Чому це важливо. Дві речі, і обидві практичні.

① **Індикатор замість даних - класичні граблі.** Статус-сторінка GitHub показувала зелене, поки сервіс віддавав 20% помилок. Та сама механіка, на якій горіли aria-selected (04.08), протухлий DOM у Notebook (07.08) і посилання в чаті (17.08): **артефакт, який мав би показувати стан, показував свій власний стан.** У GitHub це коштувало довіри тисяч людей, деінде - одного випуску. Ліки одні: механічна перевірка результату, а «будь уважним» не працює.

② **Контрапункт до пункту 2 нижче.** Той самий день, коли GitHub лежав 7,5 години, Cursor запустив йому конкурента. Такого збігу не буває: Cursor готував запуск заздалегідь, але доба, у яку він відбувся, зробила половину його маркетингу **безкоштовно.**

Чого бракує: **справжньої причини.** RCA ще нема, а «частково вимкнули повторні спроби видачі токенів» - це симптом, не корінь. У треді [Ask HN до працівників GitHub](#) популярна теорія «Microsoft + Azure», але вона тримається на одному графіку і жодного інсайдера в треді нема. Версія непереконлива.

[Інцидент](#) · [головний тред, 698 балів](#) · [тред з коментарями, 535](#) · [Ask HN: альтернативи GitHub, 524](#)

Wiz: «автофікс» від GitHub Copilot сам створив дірку, автономний агент знайшов її за 5 днів і виліз у внутрішню Jira Snowflake. Це найважливіший пункт дня

334 бали на HN, і це історія, прочитана повністю в першоджерелі.

Що сталося, за хронологією:

- **18.06.2026** – у публічному репозиторії Snowflake мерджиться **PR #1218** «Update jira workflows». Фінальний squash-коміт має співавтора: «Copilot Autofix powered by AI»
- Цей PR **прибрав безпечний патерн**, який там стояв свідомо (`env: + парсинг через jq`), і замінив його на **пряму інтерполяцію рядка**: `TITLE=$(echo '${{ github.event.issue.title }}' | sed...)`. Екранування виконується **після** підстановки шаблону GitHub – тобто одна одинарна лапка в заголовку issue виходить з рядка • Умова доступу теж була зламана: `github.event.pull_request.user.login!= 'whitesource-for-github-com[bot]'` на івенті `issues` дає `null!= '...'` – **завжди істина**. Будь-який користувач GitHub проходив цей «захист»

- **23.06** (через **п'ять днів**) – Red Agent від Wiz, автономний агент, **без участі людини** просканував GitHub-організацію Snowflake, знайшов дірку, склав payload у заголовку issue і **отримав out-of-band колбек з runner-a GitHub Actions**. Витягнув Jira-токен (`qa@snowflake.net`) з доступом на читання інженерних проєктів, комплаєнсу і баг-баунті-трекера • Snowflake полагодив **того ж дня**, ротував токен, аудит підтвердив: за п'ять днів експозиції ніхто крім Wiz туди не заходив

Найцінніша деталь – про поведінку агента. Перша спроба експлуатації **впала**: агент поставив стандартний символ коментаря `#`, а той з'їв закриваючу дужку і bash віддав `syntax error`. Далі дослівно з блогу: агент **«автономно проаналізував помилку виконання»**, переписав payload – і колбек прийшов. Агент **полагодив свій експлоїт сам**.

Чому це важливо.

Висновок Wiz дослівно: «Автоматичні AI-асистенти часто **не мають історичного контексту про те, чому був обраний конкретний патерн коду**. У цьому інциденті автоматичний PR прибрав безпечний патерн `env: + jq`, який був свідомо впроваджений саме щоб запобігти shell-ін'єкції».

Це універсальна пастка. У будь-якому старому скрипті є свідомий костиль: конструкція, яка виглядає незграбно, і агент, що прийшов «причесати код», побачить її і **захоче переписати на нормальну**. А вона стоїть там тому, що очевидний варіант якось одного разу все поклав. Якщо причина не записана в коментарі – це і є той самий «відсутній історичний контекст», за який Snowflake заплатив токеном до Jira.

Друга частина ще неприємніша: **дірка прожила п'ять днів до автоматичного знаходження**. Wiz формулює: «Операції з безпеки мають адаптуватись до світу, де

автоматичне виявлення відбувається **за години**». Вікно «та хто це знайде в маленькому репо» закрилось.

Робоче правило з цього: побачив у скриптах дивну конструкцію - спершу git log і документація за причиною, і тільки потім правки. І дешева профілактика: дописати коментарі-чому над трьома-чотирма такими місцями. Це рівно те, чого забракло Snowflake.

Що тут треба тримати в голові: **це блог компанії з безпеки про власне дослідження**, жанр «ми молодці, купіть Wiz». Багу історії тримає те, що **Snowflake підтвердив публічно** і що є номер репорту в HackerOne (#3819931). Найкращий скепсис у треді від **larsonian**: «Ви жартуєте? Це **дуже очевидний випадок ін'єкції через лапки**. Не якийсь тонкий race condition» - тобто рев'ю людиною це мало спіймати. Контраргумент **Twirrim** теж чесний: «Не можна покладатись на те, що люди помітять значущість таких змін».

Розбір Wiz · HN-тред, 334 бали

ТЕМА 3

Брокман (OpenAI) публікує «Вікно захисника» - і в ньому є замір, який можна відтворити сьогодні. Але половина поста йде з протитрутою

171 тис. переглядів у [@gdb](#), і це друга половина тієї самої історії, що й пункт 2, тільки з боку лабораторії.

Найцінніше - конкретний замір. Брокман попросив ChatGPT Work (на публічно доступному GPT-5.6 Sol) оцінити безпеку **власного персонального сайту** - простої статистики на AWS за Cloudflare. Результат дослівно: «**Приблизно за 15 хвилин він знайшов 13 проблем**». Що саме: не налаштовані DNS-записи проти підробки листів від його імені, небезпечна версія jQuery, **Cloudflare пересилав запити на AWS незашифрованим HTTP**. Далі він попросив полагодити - і агент за годину сам відкрив панель Cloudflare у браузері, наклацав DNS/TLS, викинув jQuery і **перевіз сайт з AWS на Cloudflare Pages**.

Друга цифра, вже тривожна: OpenAI з початку року віддає кібер-можливості тільки перевіреним партнерам, але «різні компанії випустили **моделі з відкритими вагами**, чії кібер-можливості відстають від фронтиру лише **на кілька місяців**. Найсвіжіша з них, схоже, виходить **наприкінці серпня**».

Чому це важливо. Замір Брокмана відтворюється за один вечір, і на цікавішому об'єкті, ніж статичний сайт. У кожного, хто тримає домашню автоматизацію, є набір із launchd-сервісів, файлів з токенами, скриптів, які виконують рядки з чату, і браузерних профілів з живими куками. Поверхня атаки там більша, ніж здається, а сам аудит нічого назовні не шле: модель читає власні конфіги і віддає список з пріоритетами. Лагодити автоматично не варто: пункт 2 сьогодні рівно про це й читається.

Тепер протиотрута, бо це компанія розповідає про власний інцидент. Пост збудований так, що інцидент OpenAI-Hugging Face подається як «переломний момент для кібербезпеки», а рецепт з нього – це **список продуктів OpenAI: Codex, ChatGPT Work, GPT-Daybreak-Blue, плагін безпеки**. Брокман чесно пише «є й конкуренти, оцінюйте їх теж», але весь текст – це прайс-лист під виглядом заклику. Плюс формулювання «ми **недооцінили** реальні кібер-можливості наших моделей» – це визнання, яке одночасно є рекламою потужності моделі. Рівно той жанр, який на Black Hat 07.08 назвали «**felony humble-bragging**».

На HN пост не потрапив взагалі – пошук по «defenders window brockman» віддає нуль історій. Тобто це публікація, яку розігнав сам акаунт. Тому ставиться третім, попри вагу імені. [proven щодо заміру 13 проблем за 15 хв – це його власний опис; fuzzy щодо всього іншого]

Пост Брокмана · @gdb, 171 тис. переглядів

ТЕМА 4

Anthropic: \$65 млрд річного run rate, ×7 за рік, IPO у вересні-жовтні. І цього разу цифра підтверджена трьома джерелами

Тема прийшла постом @AiBreakfast о 03:39 ночі – а це рівно той акаунт, чиї заяви вчора викидались як **непідтверджені** (історія з водяними знаками). Тому цього разу перевірка йшла до того, як писати, і цифра встояла: її підтвердили **CNBC** («CNBC підтвердив у понеділок»), Bloomberg (пейволл) і Axios.

Цифри з CNBC: • \$65 млрд annualized run rate станом на кінець липня – **всемеро більше**, ніж рік тому • Попередній публічний замір: \$47 млрд у травні. Тобто **+\$18 млрд за два місяці** • За весь 2025 рік компанія зробила **близько \$10 млрд виручки** • Попередня цифра за Q2 – **\$11,5 млрд**, у **14 разів** більше, ніж рік тому • В OpenAI, для калібрування, run rate **\$40 млрд** • Оцінка компанії, яку треба виправдати – **\$965 млрд** • Проспект подано в SEC ще в червні, зустрічі з інвесторами йдуть, офіційної дати дебюту нема

Чому це важливо. Дві речі, і друга важливіша.

- ① **Фронтирна лабораторія, на якій у багатьох тримається щоденна робота, більше не стартап з ризиком зникнути.** Ризик тепер інший – **ціноутворення після IPO.**
- ② **Друге прямо про залежність від однієї моделі.** CNBC згадує епізод червня: Anthropic обмежила доступ до Fable 5 і Mythos 5 через експортну директиву уряду, і це тривало близько двох тижнів. Зовнішня політична подія **вже одного разу вимикала моделі.** Це замір частоти: раз за рік. Варто тримати в голові при побудові чогось критичного поверх однієї моделі.

Що не перевірялось: Bloomberg під пейволом, читався лише заголовок; CNBC посилається на «три джерела, знайомі зі справою», а сама Anthropic відмовилась

коментувати. Тобто це злив інвесторського апдейту. Для run rate перед IPO це нормальний жанр, але цифра **не аудована** і подана компанією про саму себе.

CNBC · @AiBreakfast

ТЕМА 5

AI;DR – «ШІ; не читав». 696 балів, найбільша дискусія доби після GitHub. І це прямо про LinkedIn-пости

Стаття Ріка Манеліуса коротка, теза одна, але вона зібрала **444 коментарі** – і збрала їх тому, що вгадала загальне роздратування.

Теза дослівно: «Я настільки за-ШІ, наскільки взагалі можна, але це стає особистим подразником». І далі – **фізичний опис реакції**: «Дійшло до того, що виникає **фізичне зіщулювання** (іноді опускаються плечі й горблення, або трохи сіпається око), коли хтось, кого поважаєш, надсилає **нефільтрований і невідредагований вивід ШІ**».

Правило, яке пропонується: «Якщо тобі не було не байдуже настільки, щоб переглянути і відредагувати – **то не буде не байдуже настільки, щоб це читати**».

Автор при цьому не луддит і одразу відсікає перегини: «Є ситуації, де **треба очікувати 100% згенерованого тексту**. Клієнтська підтримка – ідеальний приклад».

У треді знайшлися дві речі, кращі за саму статтю.

Перша – від **al_borland**, і це **найкорисніша історія за добу**. Керівник команди надіслав листа: «я спитав ШІ про завдання, яке дав команді» – і вклав відповідь моделі. Далі дослівно: «Вона була багатослівна і **не мала жодного розуміння обмежень, які є всередині компанії**. Завдання було погано визначене з самого початку, і керівник **попросив у автора промпт**, бо думав, що це буде значно корисніше». Розв'язка: «Виявилось, промпт був так само невивагдливий... **1-2 речення**. Ось стільки думки в це було вкладено, після чого команда **годинами** намагалась зрозуміти відповідь ШІ. Автор міг би зекономити команді цілий день, просто надіславши промпт... або взагалі нічого».

Це змикається з найвіруснішим постом у листах за добу – **@naval, 489 тис. переглядів, 9,8 тис. лайків**: «**Не шли звіт, шли промпт**». Одна й та сама думка, з двох різних кінців, за одну добу.

Друга – **заперечення від ademup**, і воно **чесне**: «Чому важливо, ХТО написав? І як дізнатись, чи вміст вартий уваги, **якщо не прочитати?**.. Здатність "виявляти ШІ" в **кращому разі недосконала**. 90% написано ШІ? 5%? Як дізнатись?.. Якщо помилка й оголошення її світу – як це відчувається тому, хто витратив купу часу й енергії?»

Чому це важливо. Правило «драфти на перегляд, публікація руками, тон не міняти» завжди трималось на естетиці: голос, слова. Сьогоднішня стаття додає **другу опору, зовнішню**: аудиторія LinkedIn зараз активно **тренує в собі рефлекс** прокручувати нередатований текст моделі. Редагування руками стало питанням того, чи взагалі дочитають.

І формулювання Манеліуса варте того, щоб приміряти його на себе: «**Це чиєсь ім'я на цьому**». Дайджест теж виходить під ім'ям автора, і вже було сказано 17.08, що 16 повідомлень у стрічку читати неможливо. Та сама претензія, просто озвучена раніше.

Стаття · HN-тред, 696 балів / 444 коментарі · @naval «шли промпт, не звіт»

ТЕМА 6

Cursor запускає Origin - конкурента GitHub. Рівно в день, коли GitHub лежав сім годин

118 балів, @levelsio відреагував одним словом: «**Тайминг**». І це справедливо: релізи такого масштабу готують тижнями. Але доба зробила Cursor половину маркетингу безкоштовно.

Найцінніше в треді - те, що в коментарі прийшов сам розробник. `tomasreimers`, один із засновників **Graphite**, відповідав наживо. Ключові обміни:

`jjcm` спитав рівно те, що треба: «З блогпосту незрозуміло, **чим це відрізняється від GitHub** - це просто агентні прив'язки?» `dbbk` жорсткіше: «**Тут наче взагалі нема нічого нового**».

Відповідь Реймерса чесна і без пафосу: «Попереду значно більше. Випущено бету, щоб люди могли **самі поекспериментувати з масштабованістю**. Протягом наступних тижнів варто чекати кількох фіч, які почнуть **змінювати контроль версій так, щоб він розумів агентів і працював з ними**». І технічна деталь, яку варто знати: «**Все це побудовано на технології Graphite**» (Cursor купив Graphite).

Найточніше сформулював користувач `peterldowns`: «Ідея в тому, що це як GitHub, але **воно лишається живим, коли частота комітів і CI зростає**». І тут же розумний скепсис від `owebmaster`: «Називати це "GitHub, який працює" - просто безглуздо. У Cursor **нема досвіду підтримки такої системи в живих**».

Найкорисніше практичне питання - від `skissane`: «Чи є плани сумісності з **API GitHub**? Купа тулінгу припускає, що код лежить на GitHub. Це створює **лок-ін**». Відповіді на нього в треді нема.

Чому це важливо. Коротко і без ентузіазму: **поки нічого не міняється**. Origin - бета без **відповіді про сумісність API**, а тулінг навколо будь-якого робочого репозиторію зав'язаний саме на GitHub. Тема «подивитись через півроку».

Але одну річ звідти варто забрати: питання `skissane` про лок-ін правильне і ширше за Cursor. Персональна автоматизація так само припускає конкретні сервіси у кожному скрипті. Це нормально, просто варто називати речі своїми іменами.

Анонс Cursor · HN-тред з розробником, 118 балів · @levelsio про тайминг

ТЕМА 7

DuckDB 2.0: клієнт-серверний режим, тригери і рекурсивні запити в 40 разів швидші. 576 балів

Прев'ю релізу, який вийде восени – понад 10 000 комітів з версії 1.5 у березні.

Що там реально нового, з першоджерела:

- **DuckDB як сервер.** Дослівно: «DuckDB був in-process базою з першого дня. Але люди просили – **дуже наполегливо** – клієнт-серверний режим, і команда **нарешті здалась**». Протокол зветься Quack; будь-який процес DuckDB може віддавати свої бази по мережі
- **Тип VARIANT** – «уяви, якби JSON був швидким». База сама знаходить структуру в напівструктурованих даних і «шредить» їх, без оголошення схеми. Цільовий сценарій – **приймання логів у реальному часі**
- **Тригери** – у повному обсязі, класичний сценарій – таблиці аудиту
- **Асинхронний I/O** наскрізь по движку – головний виграш на мережесхвищах
- **Власний PEG-парсер** замість похідного від PostgreSQL: «вирішено, що досить»
- Замір, який винесли самі: рекурсивний запит на досяжність у графі на **мільйон ребер** – **приблизно в 40 разів швидше**

Найтверезіший коментар у треді, від c9cf35860db4 : «Останній рік покращень DuckDB відчувається як зсув від in-process движка (де він феноменальний) до движка, який може бути фундаментом хмарного сховища даних. Відомо, що засновники не хотіли це будувати, але є відчуття, що воно в роботі».

Чому це важливо. Для персональних обсягів даних, які живуть у гугл-таблицях і SQLite, DuckDB зараз надлишковий. Пункт даний як найбільший інженерний реліз доби і тому що **VARIANT + тригери** – це те, що згодиться, коли табличка починає задихатись на десяти тисячах рядків.

Анонс DuckDB 2.0 · HN-тред, 576 балів

ТЕМА 8

Qwen 3.8 27B набрав 52 на Artificial Analysis – і в треді знайшлась поправка, яка міняє вчорашній висновок

Це пряме продовження вчорашнього пункту 9 (Вілісон про Qwen 3.8 27B – «диво», яке 21 хвилину малює коло). Вчора була якісна оцінка практика, сьогодні – **цифра на бенчмарку**, 319 балів.

Цифри з треду, і всі три важливі: • anana_ : «Це ставить її нарівні з такими моделями, як GLM 5.2 і GPT-5.6 Luna, які значно більші»

- bertili додає калібрування: «Той самий бал, що й у свіжого DeepSeek Flash 0731, у якого 284 млрд параметрів (13 млрд активних). Це також друга найкраща модель Qwen, набагато краща за Qwen 3.7 Max, але значно нижча за Qwen 3.8 Max»

- І ось поправка, яка **прямо підтверджує вчорашню скаргу Вілісона**, від `anapa_`: «3.8 виступає **трохи гірше за 3.6** на AA-Omniscience Ассурасу, що може означати, що модель **проміняла знання про світ на здібності в інших областях**. Вона також видає **майже вдвічі більше токенів на задачу** (і, відповідно, часу), ніж 3.6»

Тобто «21 хвилина і 22 276 токенів міркувань на пелікана» вчора – це системна властивість моделі: вдвічі більше токенів на задачу проти попередньої версії, і це, схоже, ціна за точність при такому розмірі.

Чому це важливо. Вчорашній висновок про те, що локальний шар на домашньому залізі реалістичний (17 ГБ), лишається правдою. Сьогоднішня поправка додає цінник: вдвічі більше токенів на ту саму задачу. Для коротких викликів це не смертельно, але «локальна модель = безкоштовно» – хибне рівняння. Плата переїжджає з рахунку на час і на вентилятор.

Найрозумніша думка в треді, від `tancor`, і вона про архітектуру: «Найбільший невикористаний ринок – це суто агентні моделі, побудовані під виклик інструментів і невигадування, замість запам'ятовування фактів. Тренування має фокусуватись на задачах, що потребують справжнього інтелекту. Не пам'яті». Для агента, який весь час ходить по скриптах і API, це рівно та модель, якої бракує.

Artificial Analysis · HN-тред, 319 балів · вчорашній розбір Вілісона

ТЕМА 9

Пам'ять подорожчала на 500% за рік, DDR5 128 ГБ – \$3 399. І в треді пояснили, звідки це

98 балів, `Tom's Hardware`: +500% за 12 місяців, місцями до 10 разів дорожче за найнижчі зафіксовані ціни.

Пояснення з треду, з посиланням: `phonon` – «OpenAI (Stargate) запустив зростання цін рік тому, законтрактувавши 40% світового виробництва RAM».

Найзліший і водночас найзмістовніший коментар – `giantrobot`: «Це витягування драбини за собою. OpenAI викупив більше контрактів на пластини, ніж міг використати. Але тепер це означає, що всі решта б'ються за те, що лишилось. Це робить занадто дорогим конкурувати з OpenAI. Жоден новачок просто не може дозволити собі будувати інфраструктуру».

Найкраще питання – від `master_crab`: «Ще більше бентежить економіка фронтірних моделей. Якщо це було економічно нежиттєздатно без грошей VC і Nvidia три роки тому, то як воно можливо зараз, за вдсятеро вищих цін на пам'ять?»

Чому це важливо. Побутовий висновок: якщо збирати або апгрейдити залізо – зараз найгірший момент за п'ять років. Вчорашній пункт про локальну модель на 17 ГБ це теж зачіпає: докупити пам'яті під неї подорожчало в рази, і в найближчі місяці це не

розсмокчється. Плюс контекст до пункту 4: run rate у \$65 млрд і викуп 40% світової RAM – це дві сторони одного графіка.

Заява про 40% – це коментар на HN з посиланням на Tom's Hardware, не першоджерело OpenAI. Береться як правдоподібне, не як факт. [promising]

Tom's Hardware · HN-тред

ТЕМА 10

Гаррі Тан відкрив gbrain – 70 своїх наборів інструкцій для агента, MIT, 28,6 тис. зірок

@garrytan анонсував, 38 тис. переглядів: «GBrain тепер підтримує персоналізовану генерацію агента і онбординг для Codex і Claude Code. Він згенерує `SOUL.md` у стилі agent AI і встановить 70 особистих скілів. За 12 питань отримується агент, такий же розумний, як особистий OpenClaw».

Друга частина, з деталями: «Що отримується? Приватний репозиторій github з 70 перевіреними скілами і початком вікі знань у стилі Карпаті. Усе це – MIT-ліцензований опенсорс і безкоштовно».

Перевірено у першоджерелі, github.com/garrytan/gbrain: 28 630 зірок, ліцензія MIT, створений 05.04.2026, опис – «Garry's Opinionated OpenClaw/Hermes Agent Brain».

Чому це важливо.

Це та сама архітектура персонального агента, що зараз складається у всіх окремо: набори інструкцій як одиниця знання, один файл персони замість розкиданого промπτу, вікі знань замість купи нотаток. Патерн вийшов з приватних налаштувань у публічний репозиторій і зібрав 28 тисяч зірок за чотири місяці.

Практична цінність скромна і конкретна: подивитись, які саме 70 наборів він вважав вартими виділення. Копіювати нема сенсу – у нього вони під роботу венчурного фонду, у будь-кого іншого будуть під своє життя. Користь у тому, щоб побачити категорії, яких у себе нема взагалі. Це читання на годину.

Що не зроблено: не читались самі набори інструкцій, не клонувався репозиторій, не звірялось, чи справді їх 70. Взято метадані з API GitHub (зірки, ліцензія, дата) і слова автора з твіту. Іронія доби: перевірити глибше вчора було б важко технічно – GitHub лежав саме тоді, коли це аносували.

github.com/garrytan/gbrain · @garrytan, анонс · деталі

misc – коротко, що ще варте ока

- **Amazon пускає під ніж рідкісні книжки, щоб тренувати ШІ** (135 балів, плюс *Ars Technica* 126 і *TechCrunch* 91 – одна тема в трьох виданнях за добу). Метод розслідування красивий: 404 Media вмовили продавця покласти AirTag у книжку з великого замовлення і подивились, куди вона поїде. Приїхала на майданчик Amazon

для тренування ШІ. Найчесніша претензія в треді - від [andsoitis](#) : «"рідкісна" як "мало в обігу" - це дуже інакше, ніж "унікальний артефакт"», і 404 Media не назвали жодного заголовка, тому масштаб втрати оцінити неможливо

- **GPT-5.6 Sol подешевшав удвічі** (234 бали) - і найкорисніше в треді застереження про ZDR від [dataplumb3r](#) : «Нема ZDR з Anthropic. Для Mythos і навіть Fable вони вимагають збереження промптів на своєму боці». Якщо в продукті йтимуться корпоративні дані через API - це те, що читати першим. Це коментар на HN, не документація; зв'язка з умовами Anthropic не проводилась
- **GPT-5.6 Sol - найкраща "візуальна" модель, яку випускав OpenAI** (313 балів) - розбір від Roboflow. У треді жвава суперечка Claude проти GPT саме на картинках; [weli](#) : «Claude буває дуже гарний у мові, але щойно треба подивитись на картинку і вирішити, чому дизайн поганий, - сильно деградує»
- **Як Bluesky малює свій логотип на скриншотах** (315 балів) - технічний розбір гарний, але тред пішов у інший бік і має рацію: [shiandow](#) - «Досі вражає, що для ОС стало нормою ставити побажання застосунку вище за побажання користувача»
- **DOJ Німеччини: Apple ставилась до власних застосунків краще, ніж до конкурентів у АТТ** (240 балів) - Bundeskartellamt офіційно; довга історія, яка нарешті доїхала до формулювання
- **Як уникати нав'язливого ШІ** (265 балів) - практичний список від бібліотекарки: як вимикати AI-фічі в застосунках, які самі не питали. Тематична пара до пункту 5
- **Творець TypeScript: чому ШІ не замінить розробників** (Substack, 17.08) - Андерс Гейлсберг у The Peterman Post. Єдине свіже з чотирьох підписок у вікні; решта (Pragmatic Engineer 14.08, Output Theory 16.08 про американські гірки, Humanager 05.04) - поза вікном або тема, що не підходить
- **Ізраїль створив фейковий аналітичний центр, щоб дурити чат-боти** (229 балів) - тема цікава як клас атаки на джерела (отруєння того, що модель вважає авторитетним), але це вже **дубль**, і політика. Рядком