Deep impersonation et les risques liés à l'IA

Il ne faut pas croire tous ce que vous voyez ou entendez !

IDENTITY DAYS

Webinar

S

Clément SERAFIN

Clément Serafin

M365 Architect

https://msblog.fr

aMS Community

Ninja Modern Workplace France

IDENTITY DAYS

POWER 365

Power Platform French Summit

Experts Exchange

the original technology community™

Agenda

- Deepfake impersonation, à quel point ?
- L’IA ce n’est pas tout blanc
- Augmenter sa productivité mais à quel prix ?

Deep impersonation

Il ne faut pas croire tous ce que vous voyez ou entendez !

s

Face Swap

C’est mignon !

Ou très moche

Deepfake

C’est dangereux !



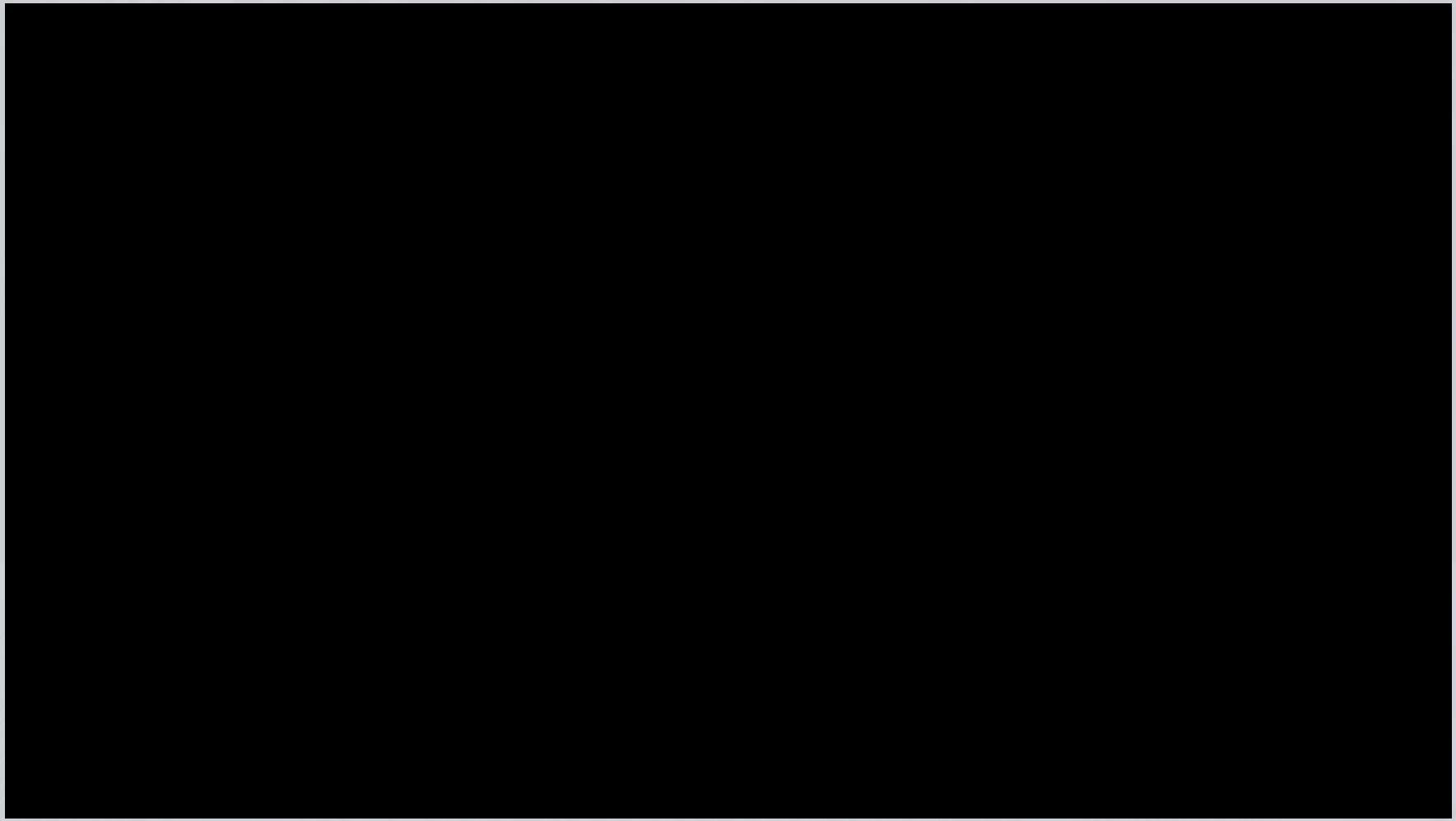

https://replicate.com/yoyo-nb/thin-plate-spline-motion-model

La conférence de trop !

La conférence de trop !

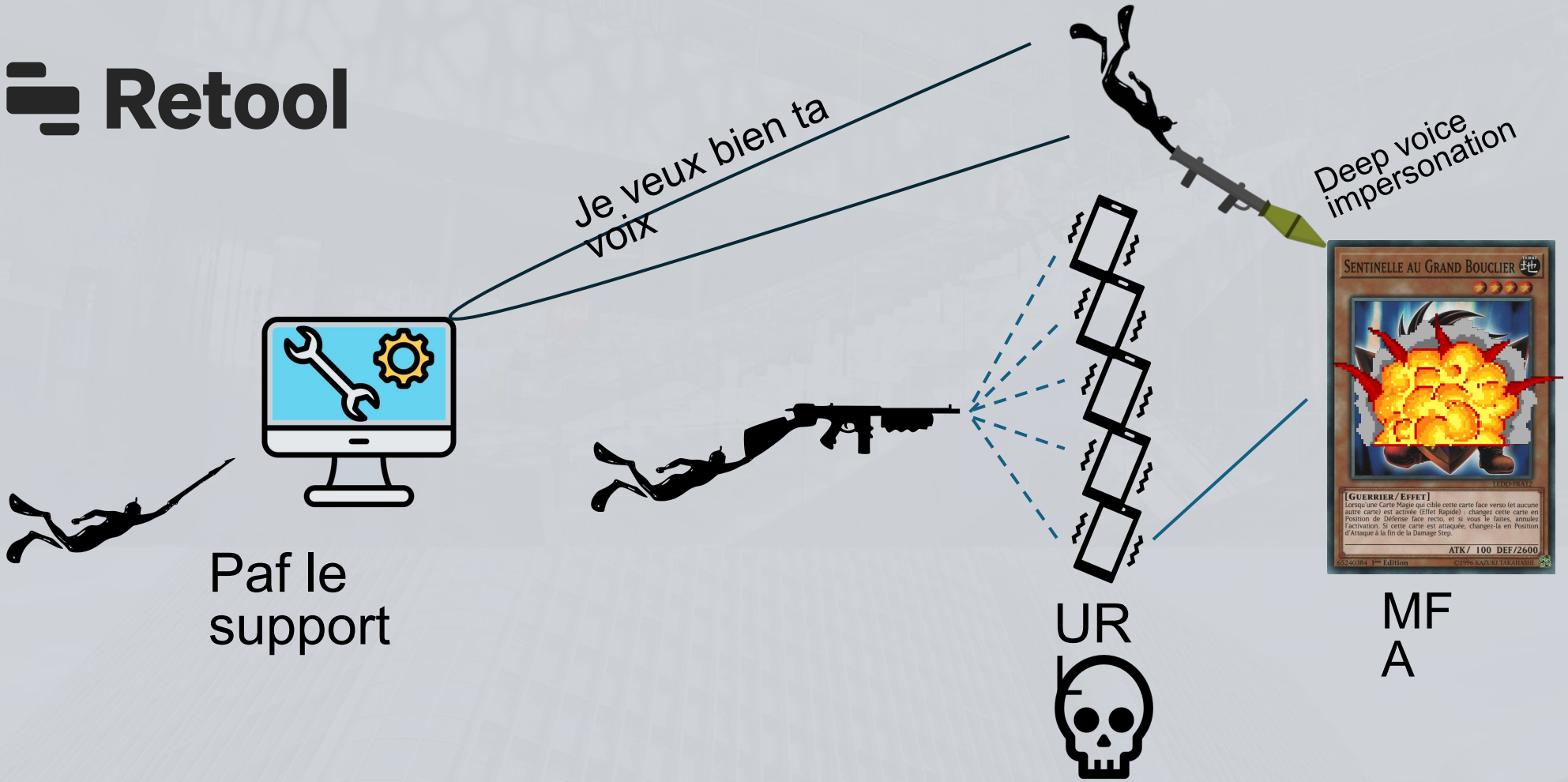
Elevenlabs & Clipchamp

Jordan Peele



https://www.youtube.com/watch?v=cQ54GDm1eL0

En quoi ça me concerne ?



https://www.pcmag.com/news/hacker-deepfakes-employees-voice-in-phone-call-to-breach-it-company

L’IA ce n’est pas tout blanc

IDENTITY DAYS

Webinar

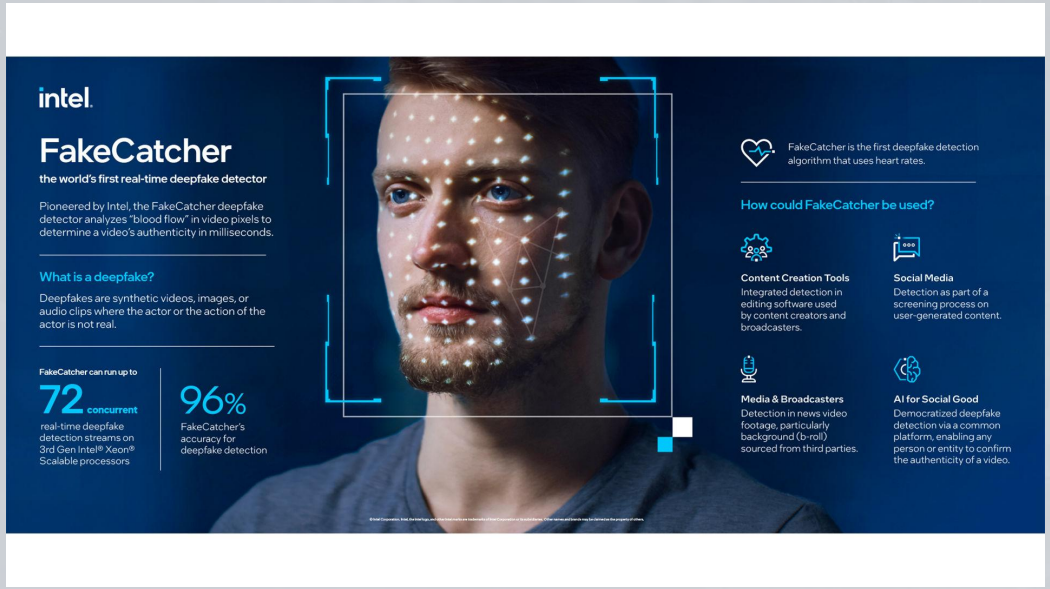
S

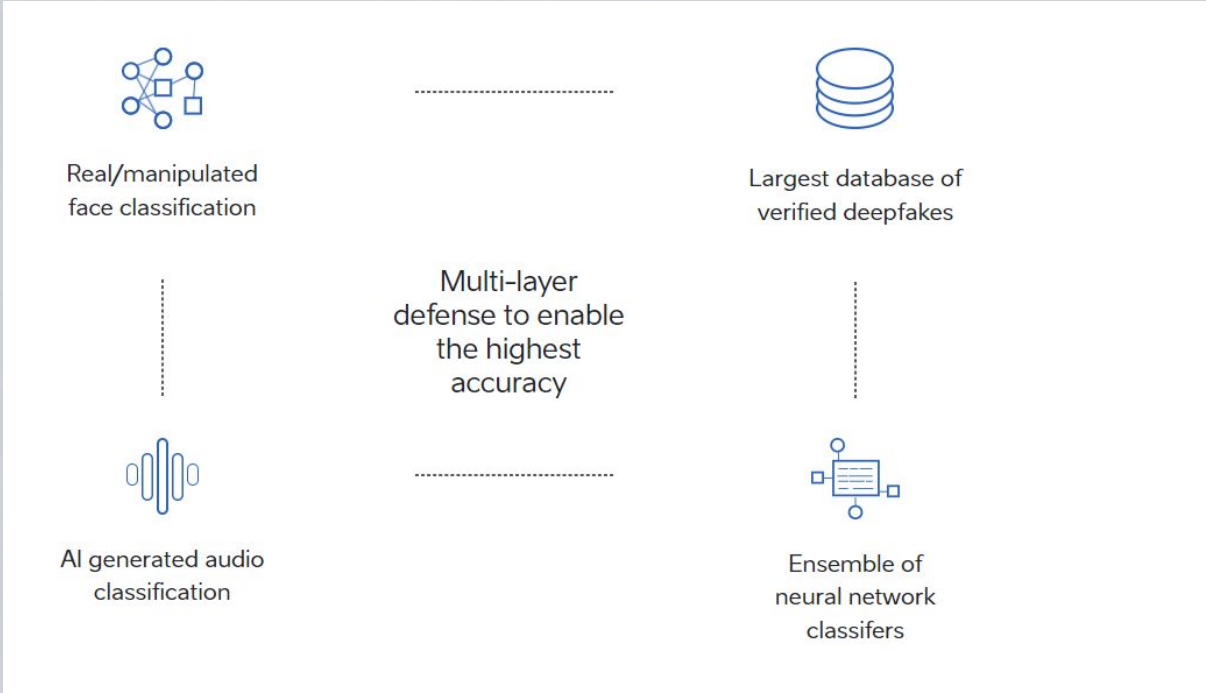
Generative AI

Generative AI

Le pentagon, vraiment ?!

I need somebody help !



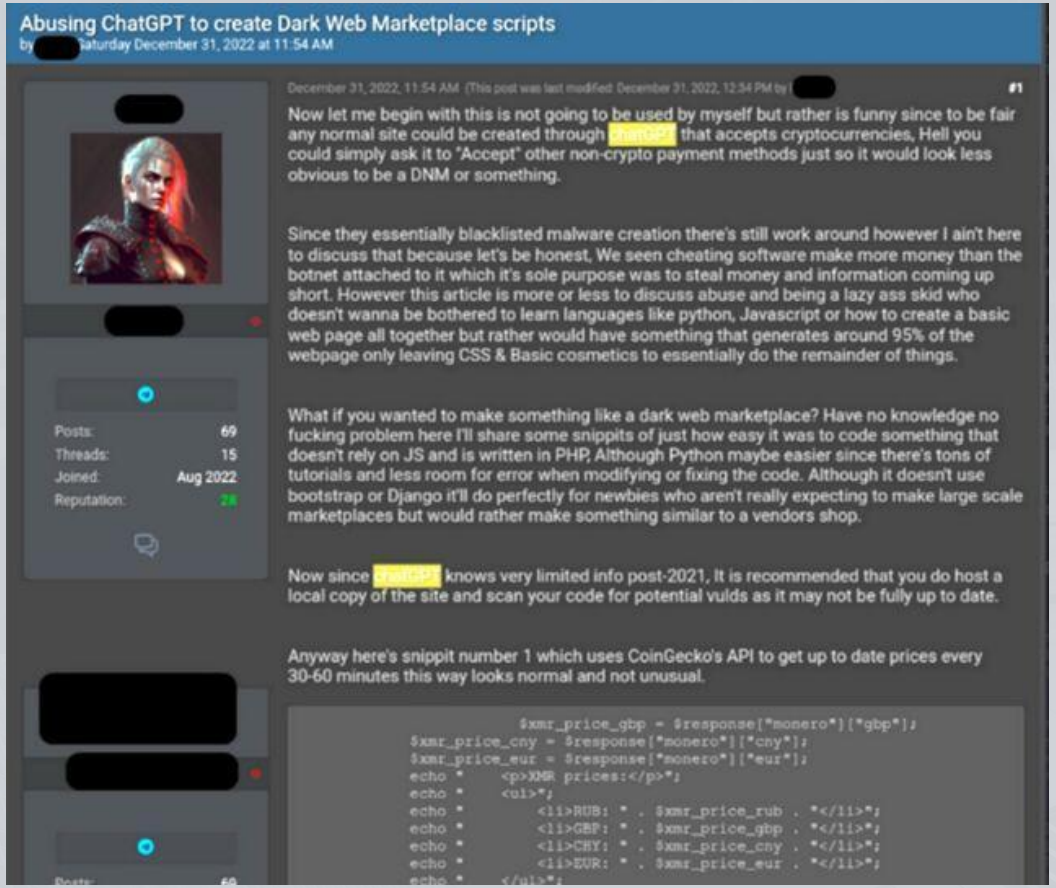


https://www.intel.com/content/www/us/en/newsroom/news/intel-introduces-real-time-deepfake-detector.html#gs.2i4bt3
https://thesentinel.ai/

Méchant Chat !

AI-POWERED CYBERCRIME —

ChatGPT is enabling script kiddies to write functional malware



https://arstechnica.com/information-technology/2023/01/chatgpt-is-enabling-script-kiddies-to-write-functional-malware/

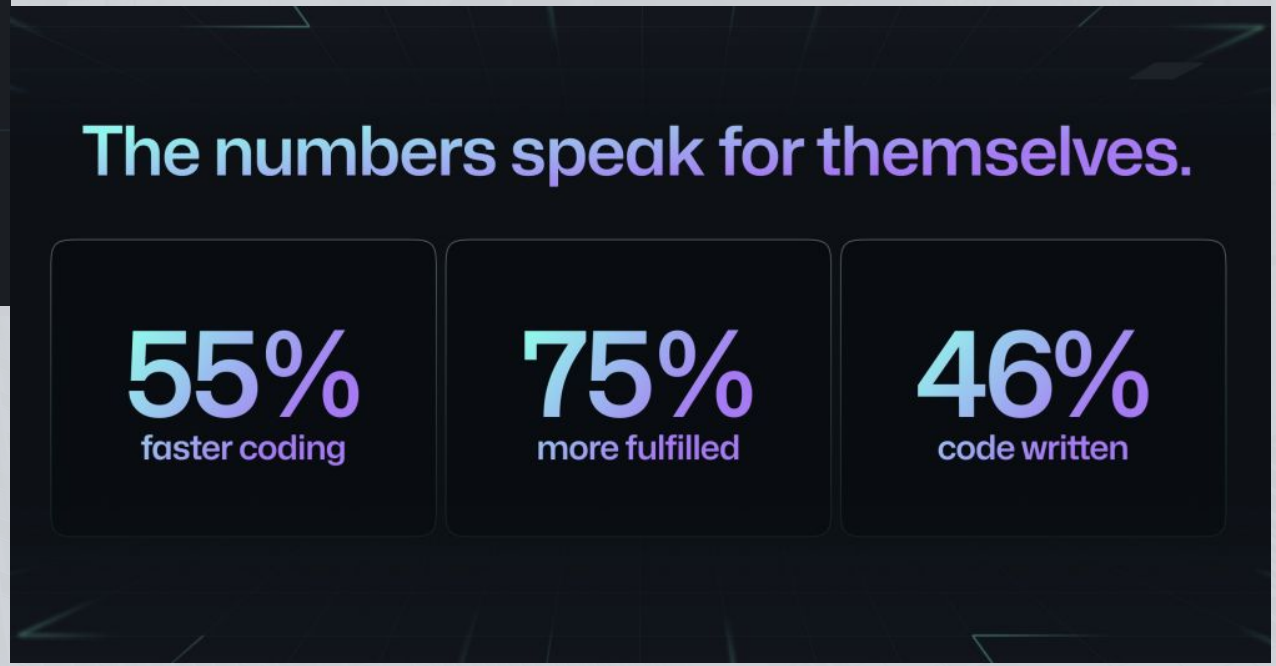
Augmenter sa productivité mais à quel prix ?

IDENTITY DAYS

Webinar

s

Github Copilot



Github Copilot

Home › AI/ML › GitHub Copilot under fire as dev claims it emits 'large chunks of my copyrighted code'

AI/ML Development

GitHub Copilot under fire as dev claims it emits 'large chunks of my copyrighted code'

By **Tim Anderson** - October 17, 2022

GitHub mounts second attempt to toss anonymous code writers' claims of software piracy

A group of anonymous code writers are attempting to advance their remaining open source license breach claims against companies connected to GitHub's CoPilot, trained on public repositories of code scraped from the web.

NATALIE HANSON / November 9, 2023

GitHub struggles to keep up with automated malicious forks

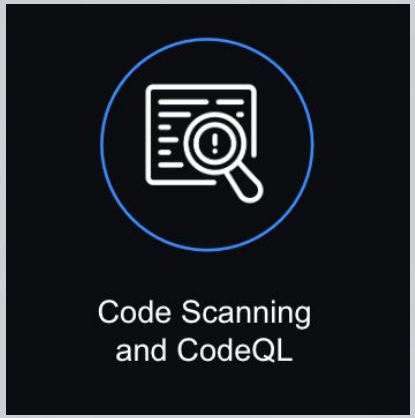
Cloned then compromised, bad repos are forked faster than they can be removed

Thomas Claburn Fri 1 Mar 2024 // 00:45 UTC

A malware distribution campaign that began last May with a handful of malicious software packages uploaded to the Python Package Index (PyPI) has spread to GitHub and expanded to reach at least 100,000 compromised repositories.

https://devclass.com/2022/10/17/github-copilot-under-fire-as-dev-claims-it-emits-large-chunks-of-my-copyrighted-code/#:~:text=Developer%20Tim%20Davis%2C%20a%20professor,attribution%2C%20no%20LGPC%20license.%E2%80%9D

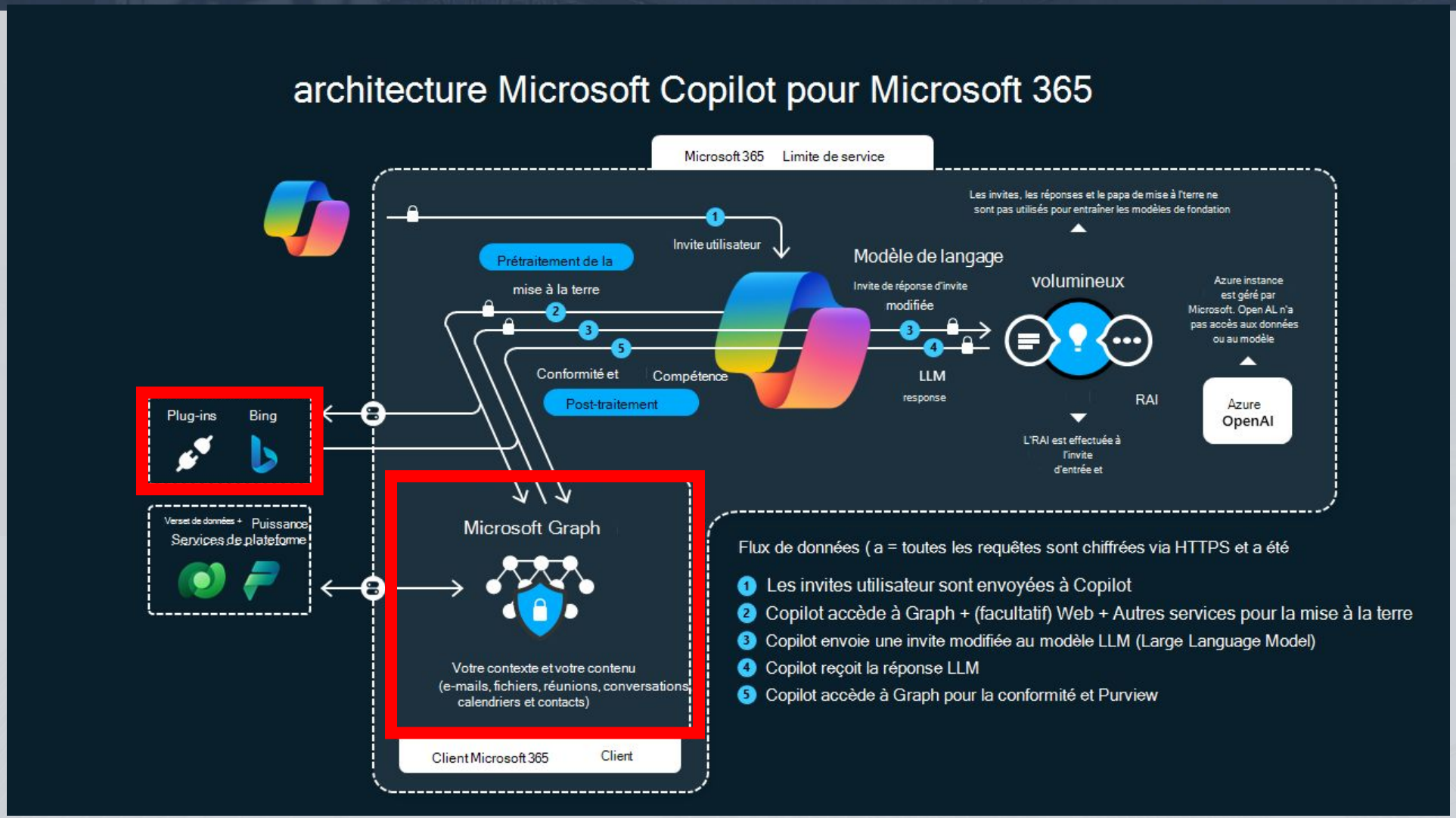
Les premières recommandations



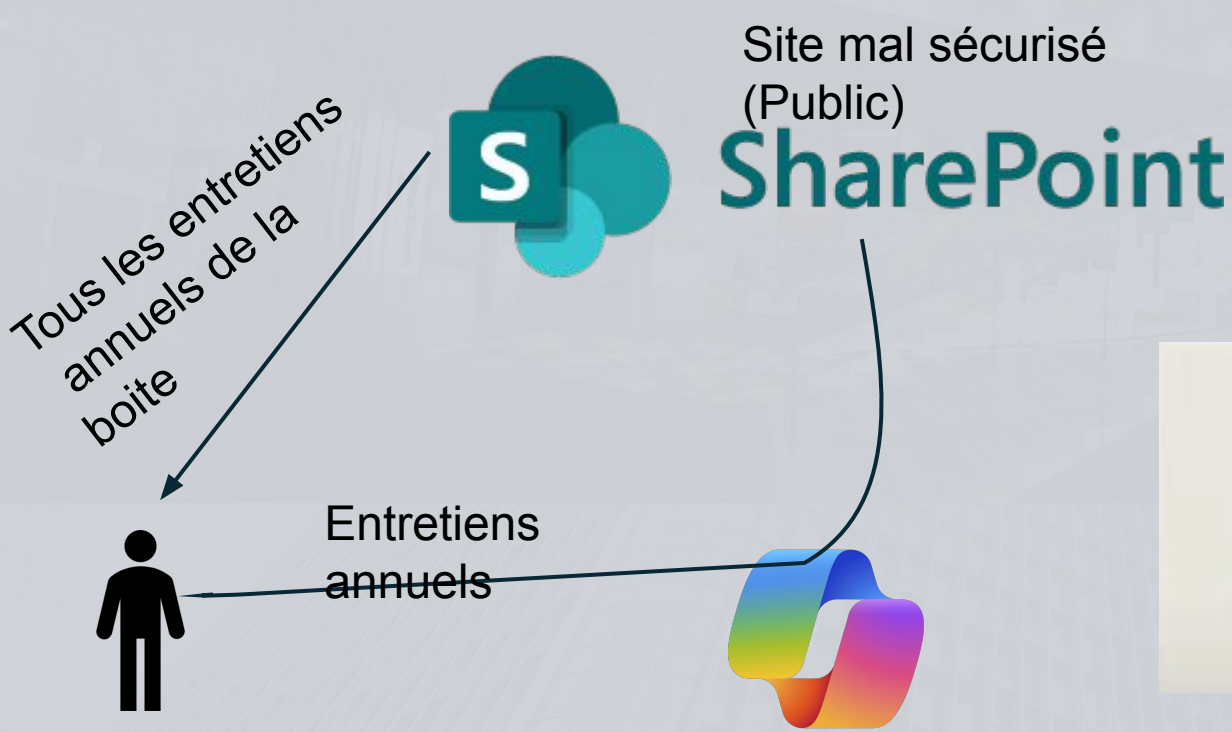
Filter Public Code

GitHub Enterprise Server

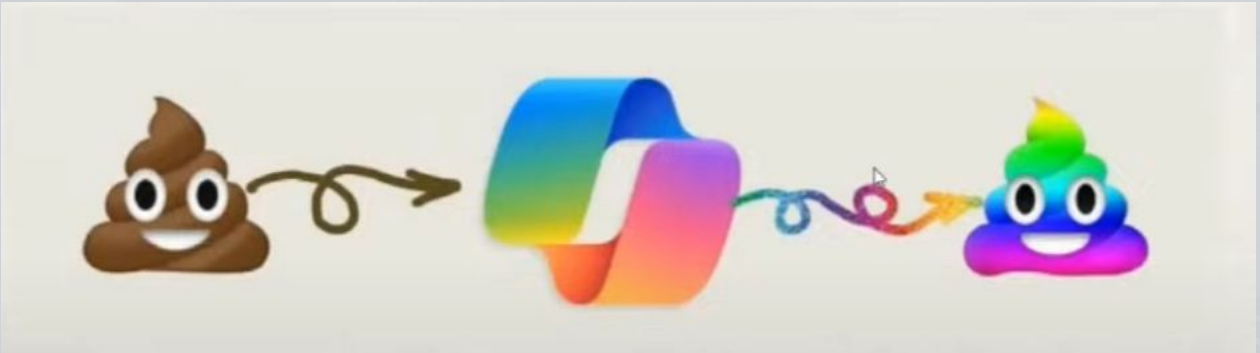
Microsoft Copilot 365



Microsoft Copilot 365



Préparez vos données avant de la rendre accessible



Conclusion

S

Conclusion

Merci pour votre écoute !

IDENTITY DAYS

Webinar

s