

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



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 !

 IDENTITY DAYS

Webinar

S

Face Swap

C'est mignon !

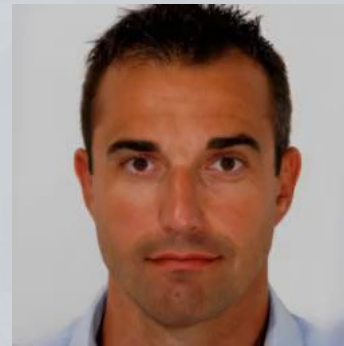


Ou très moche



Deepfake

C'est dangereux !



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

La conférence de trop !



PROLONGEZ L'EXPERIENCE
IDENTITY DAYS

iID IDENTITY DAYS

La conférence de trop !

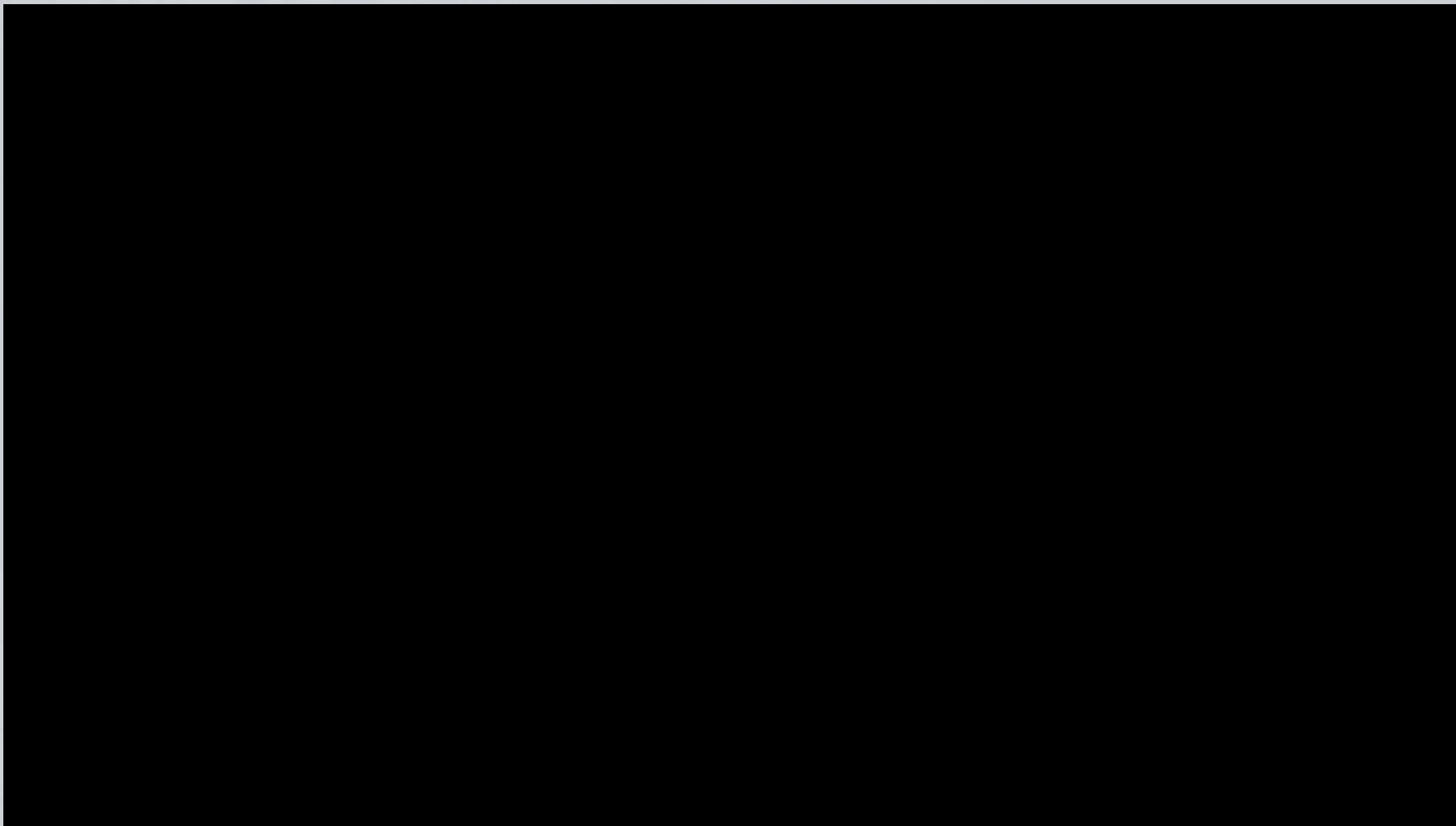


Elevenlabs & Clipchamp

PROLONGEZ L'EXPERIENCE
IDENTITY DAYS

iIDENTITY DAYS

Jordan Peele



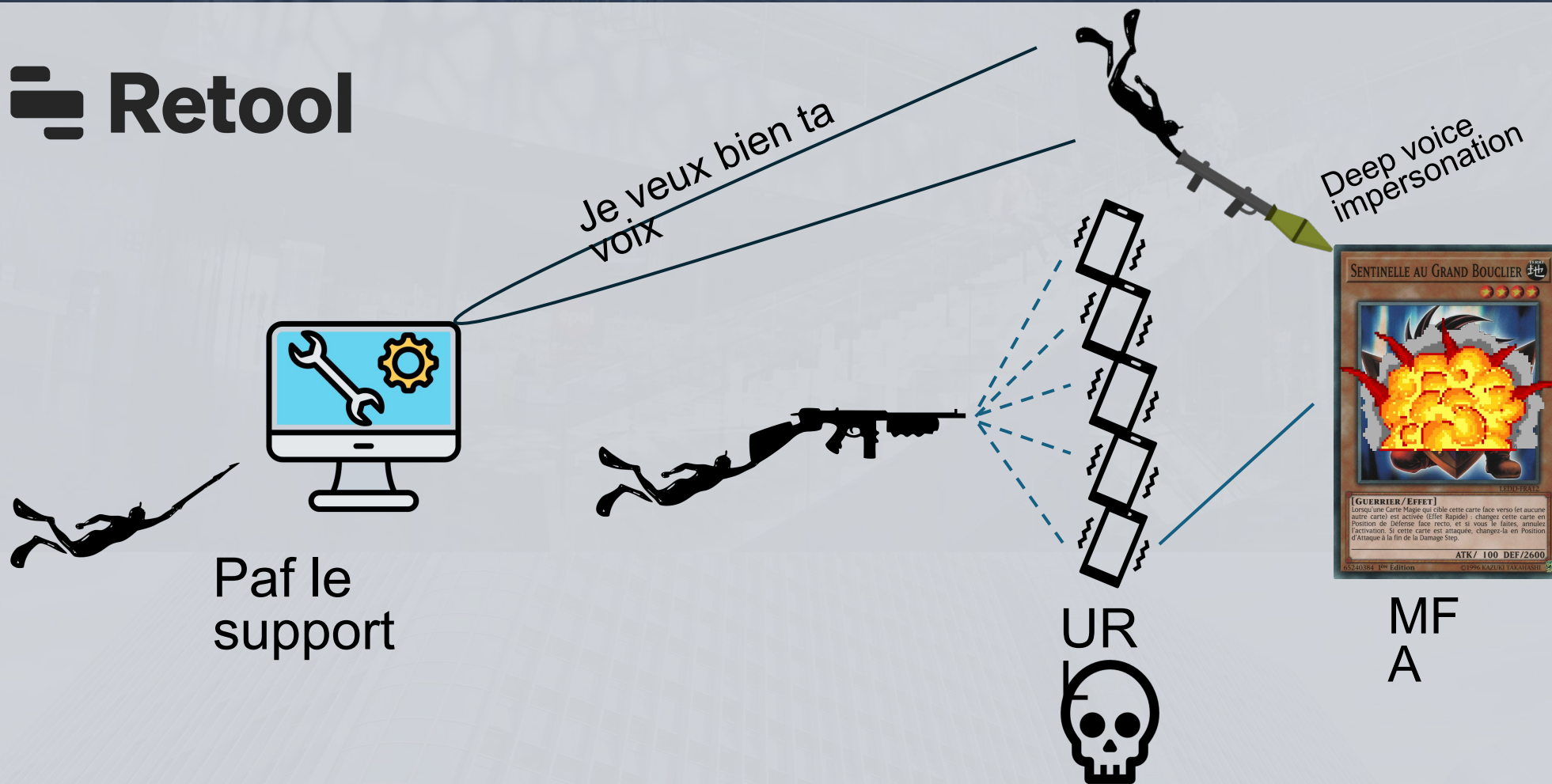
<https://www.youtube.com/watch?v=cQ54GDm1eL0>

PROLONGEZ L'EXPERIENCE
IDENTITY DAYS

 IDENTITY DAYS

En quoi ça me concerne ?

Retool



<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



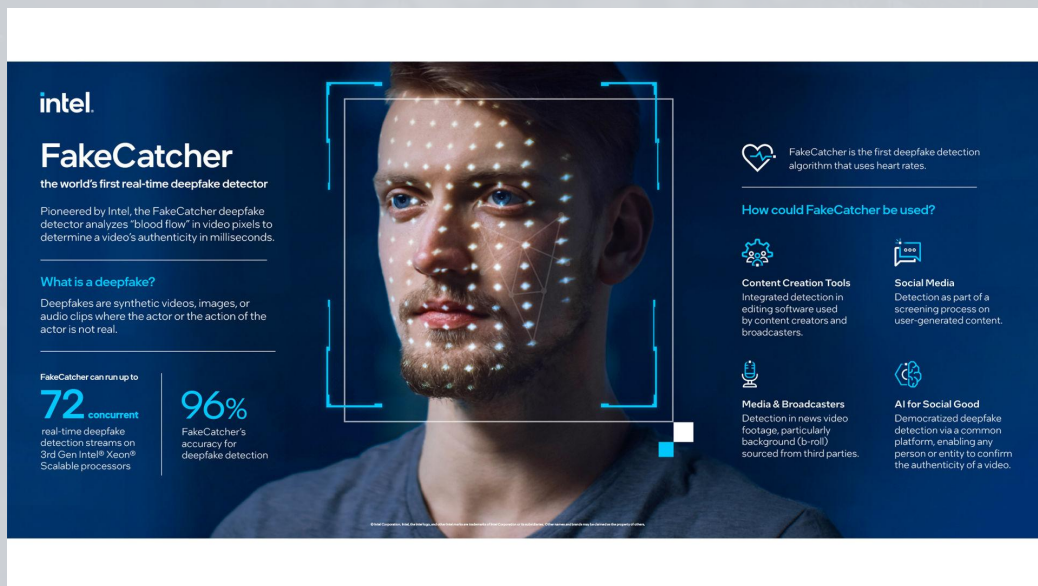
PROLONGEZ L'EXPERIENCE
IDENTITY DAYS

Generative AI



Le pentagon, vraiment
?!

I need somebody help !



intel.
FakeCatcher
the world's first real-time deepfake detector

Pioneered by Intel, the FakeCatcher deepfake detector analyzes "blood flow" in video pixels to determine a video's authenticity in milliseconds.

What is a deepfake?
Deepfakes are synthetic videos, images, or audio clips where the actor or the action of the actor is not real.

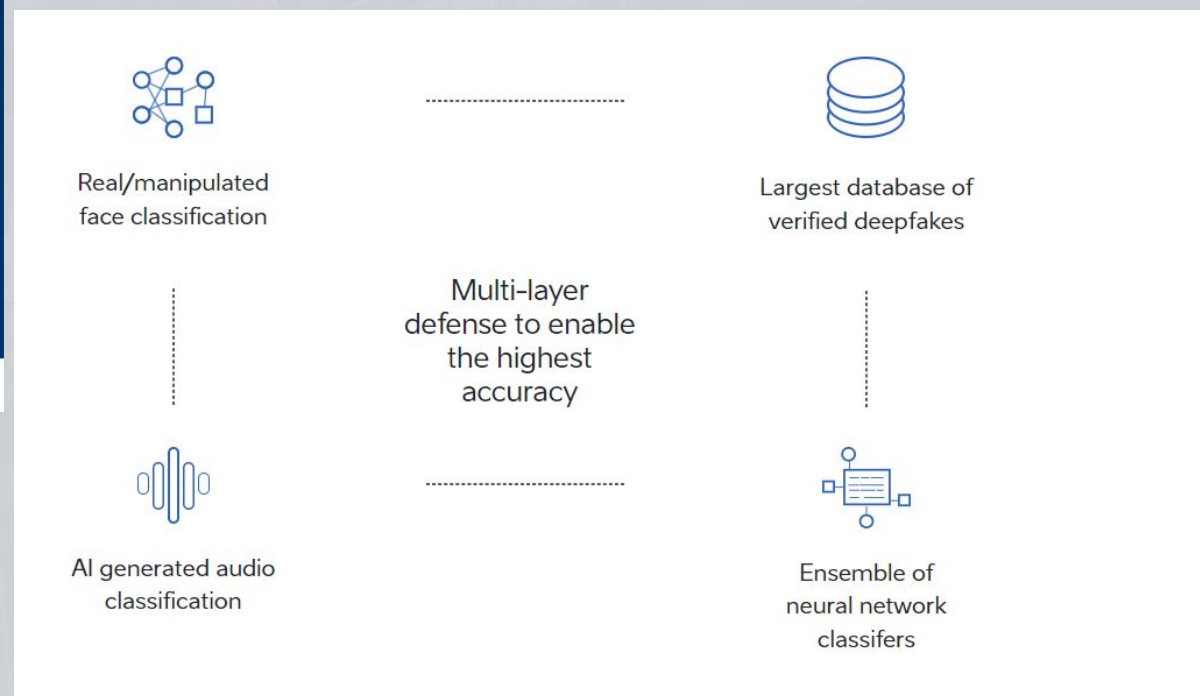
FakeCatcher can run up to **72** concurrent real-time deepfake detection streams on 3rd Gen Intel® Xeon® Scalable processors

96%
FakeCatcher's accuracy for deepfake detection

FakeCatcher is the first deepfake detection algorithm that uses heart rates.

How could FakeCatcher be used?

- Content Creation Tools**
Integrated detection in editing software used by content creators and broadcasters.
- Social Media**
Detection as part of a screening process on user-generated content.
- Media & Broadcasters**
Detection in news video footage, particularly background (b-roll) sourced from third parties.
- AI for Social Good**
Democratized deepfake detection via a common platform, enabling any person or entity to confirm the authenticity of a video.



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

<https://thesentinel.ai/>

PROLONGEZ L'EXPERIENCE
IDENTITY DAYS

ii IDENTITY DAYS

Méchant Chat !

AI-POWERED CYBERCRIME —

ChatGPT is enabling script kiddies to write functional malware



Abusing ChatGPT to create Dark Web Marketplace scripts

by [redacted] Saturday December 31, 2022 at 11:54 AM

December 31, 2022, 11:54 AM (This post was last modified: December 31, 2022, 12:34 PM by [redacted]) #1

Now let me begin with this is not going to be used by myself but rather is funny since to be fair any normal site could be created through [redacted] that accepts cryptocurrencies, Hell you could simply ask it to "Accept" other non-crypto payment methods just so it would look less obvious to be a DNM or something.

Since they essentially blacklisted malware creation there's still work around however I ain't here to discuss that because let's be honest, We seen cheating software make more money than the botnet attached to it which it's sole purpose was to steal money and information coming up short. However this article is more or less to discuss abuse and being a lazy ass skid who doesn't wanna be bothered to learn languages like python, Javascript or how to create a basic web page all together but rather would have something that generates around 95% of the webpage only leaving CSS & Basic cosmetics to essentially do the remainder of things.

What if you wanted to make something like a dark web marketplace? Have no knowledge no fucking problem here I'll share some snippets of just how easy it was to code something that doesn't rely on JS and is written in PHP, Although Python maybe easier since there's tons of tutorials and less room for error when modifying or fixing the code. Although it doesn't use bootstrap or Django it'll do perfectly for newbies who aren't really expecting to make large scale marketplaces but would rather make something similar to a vendors shop.

Now since [redacted] knows very limited info post-2021, it is recommended that you do host a local copy of the site and scan your code for potential vulds as it may not be fully up to date.

Anyway here's snippet number 1 which uses CoinGecko's API to get up to date prices every 30-60 minutes this way looks normal and not unusual.

```
$xmr_price_gbp = $response["monero"]["gbp"];
$xmr_price_cny = $response["monero"]["cny"];
$xmr_price_eur = $response["monero"]["eur"];
echo * <p>XMR prices:</p>*;
echo * <ul>*;
echo * <li>RUB: * . $xmr_price_rub . *</li>*;
echo * <li>GBP: * . $xmr_price_gbp . *</li>*;
echo * <li>CNY: * . $xmr_price_cny . *</li>*;
echo * <li>EUR: * . $xmr_price_eur . *</li>*;
echo * </ul>*;
```

<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

Technical preview

Your AI pair programmer

```
fetch_pic.js  push_to_git.py  JS_d3_scale.js  JS_fetch_stock.js  JS_material_ui.js

1  const fetchNASAPictureOfTheDay = () => {
2    return fetch('https://api.nasa.gov/planetary/apod?api_key=DEMO_KEY', {
3      method: 'GET',
4      headers: {
5        'Content-Type': 'application/json',
6      },
7    })
8    .then(response => response.json())
9    .then(json => {
10     return json;
11   });
12 }
```

 **GitHub Copilot**

The numbers speak for themselves.

55%
faster coding

75%
more fulfilled

46%
code written

PROLONGEZ L'EXPERIENCE
IDENTITY DAYS

 **IDENTITY DAYS**

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>

PROLONGEZ L'EXPERIENCE
IDENTITY DAYS

 IDENTITY DAYS

Les premières recommandations



Code Scanning
and CodeQL

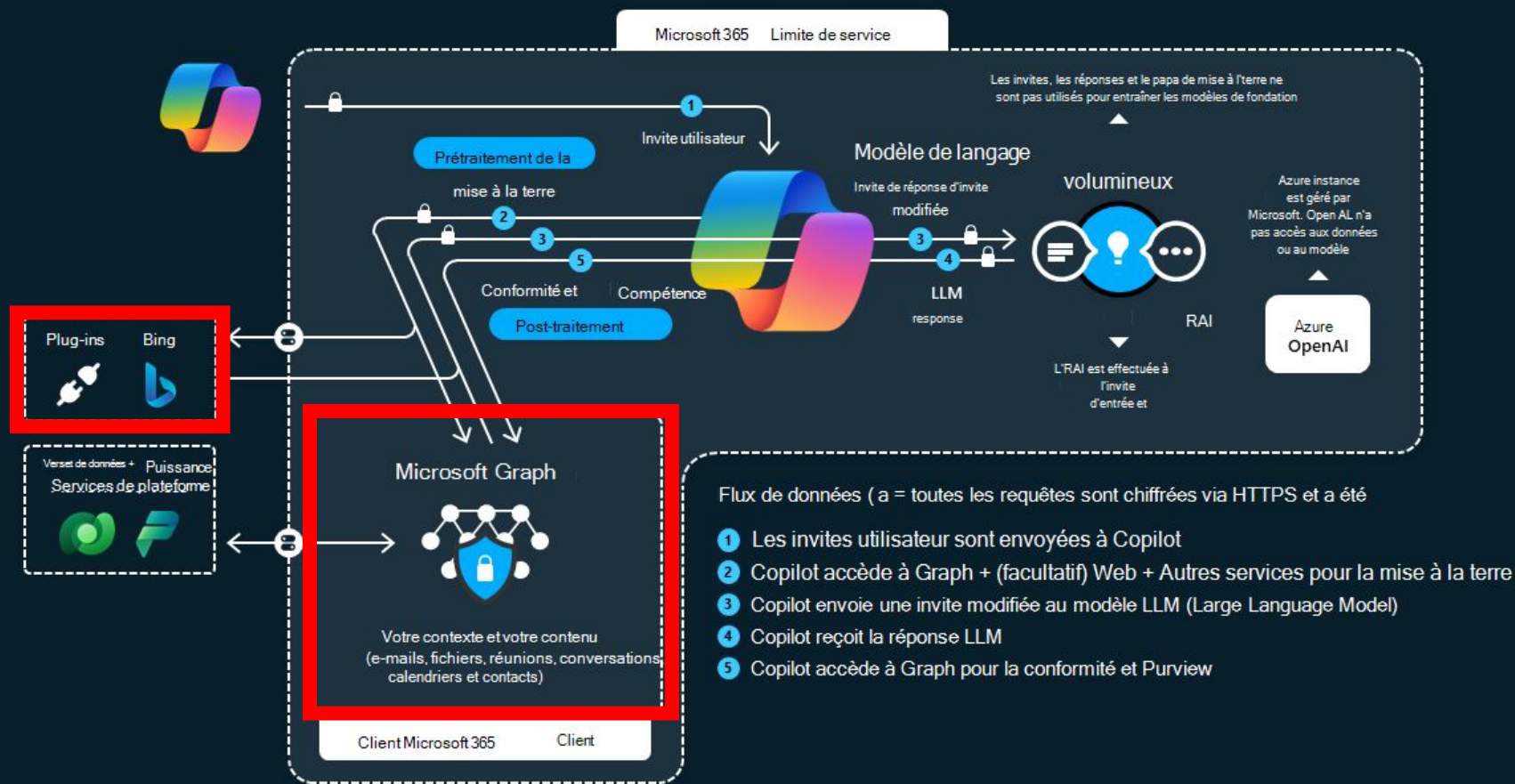
Filter Public Code



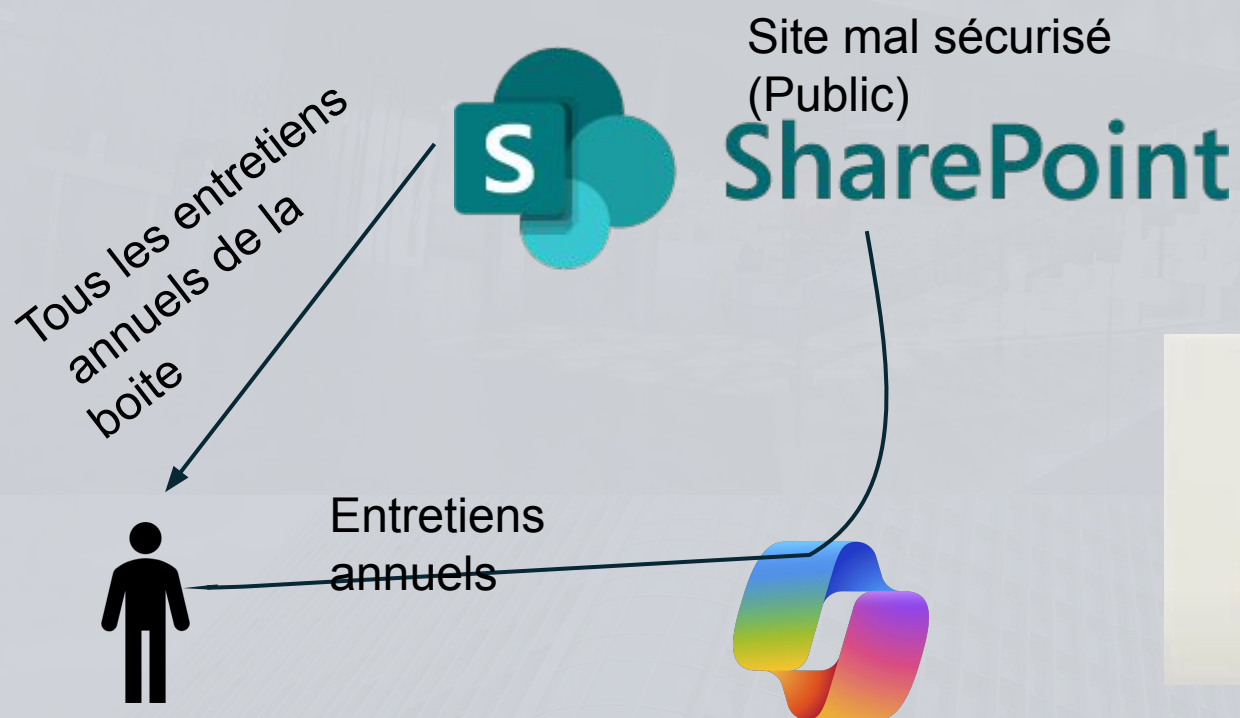
GitHub Enterprise Server

Microsoft Copilot 365

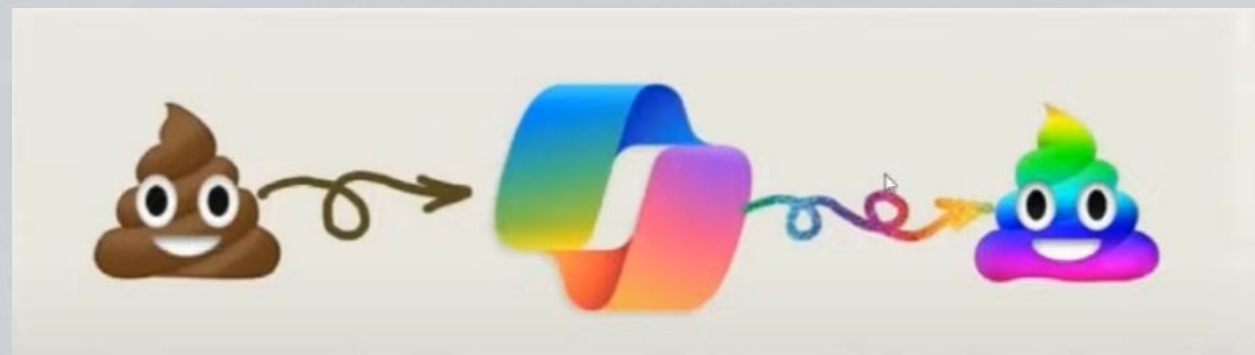
architecture Microsoft Copilot pour Microsoft 365



Microsoft Copilot 365



Préparez vos données avant de la rendre accessible



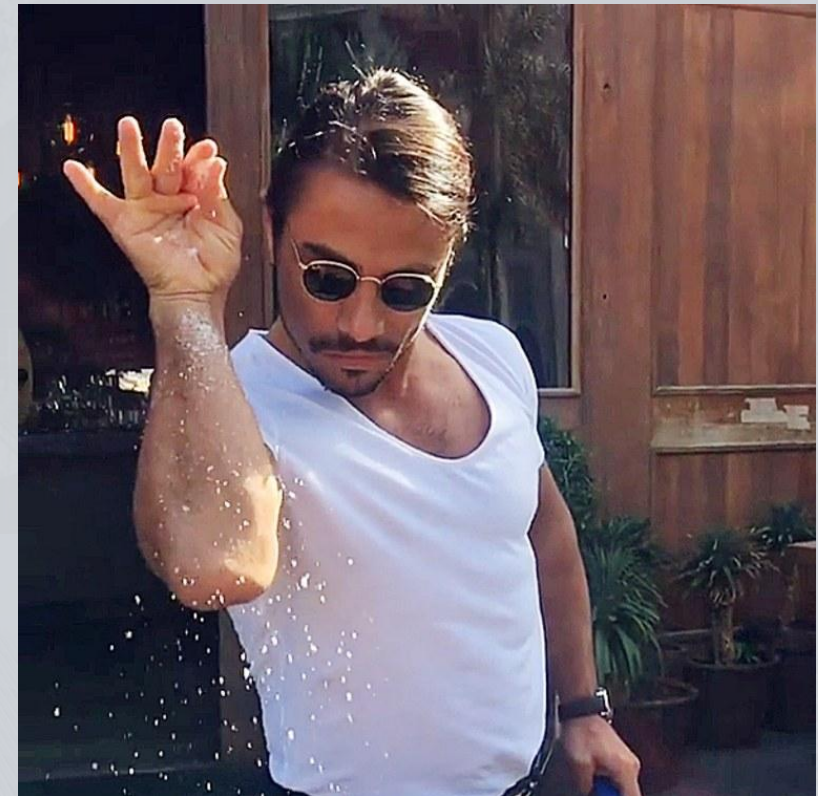
Conclusion

 IDENTITY DAYS

Webinar

S

Conclusion



PROLONGEZ L'EXPERIENCE
IDENTITY DAYS

 IDENTITY DAYS



Merci pour votre écoute !

 IDENTITY DAYS

Webinar

S