To cloud or not to cloud ?

Des dangers de la grêle et de la beauté des nuages

Inti Rossenbach

JSSI – Mardi 11 mars 2025

TLP : GREEN

whoami

Infosec practitioner 25+ years of experience

Group CISO of an international group 7000+ employees

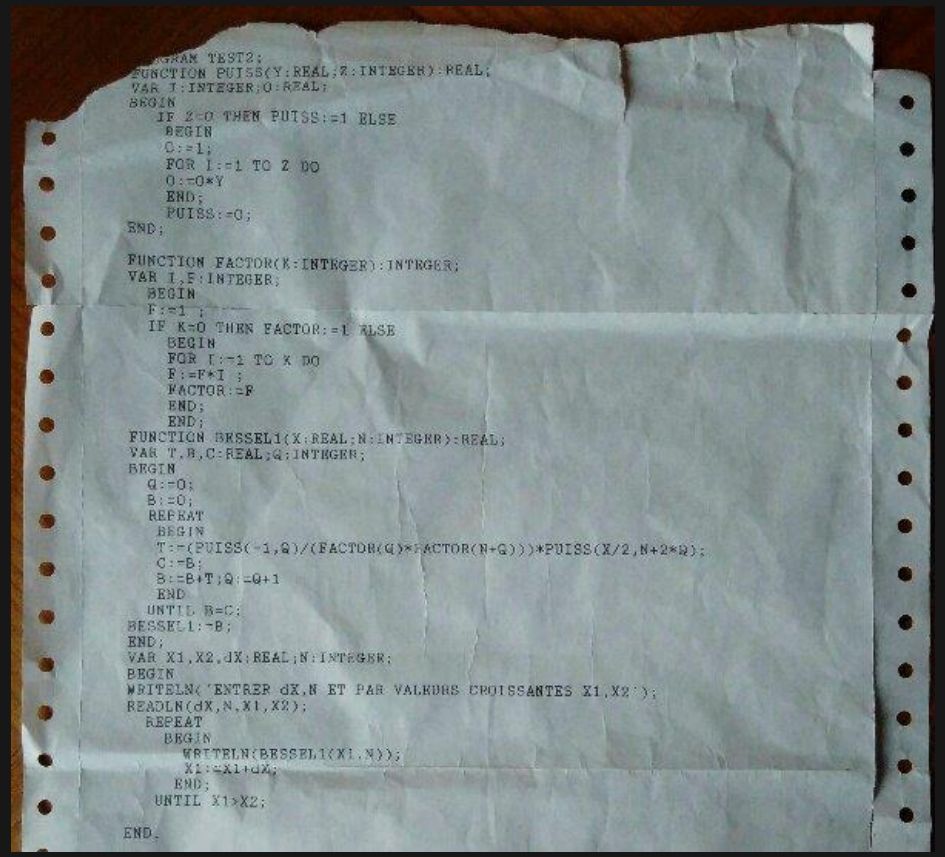
Lecturer at university – Paris Sorbonne Nord & Nanterre

Présentation à la JSSI 2022 – « Cyber code éthique »

www.cryptosec.org

Mastodon infosec.exchange/@cryptosec

Mes propos n'engagent que moi



```
PROGRAM TEST2;
FUNCTION PUISS(Y:REAL;Z:INTEGER):REAL;
VAR I:INTEGER;O:REAL;
BEGIN
   IF Z=0 THEN PUISS:=1 ELSE
    BEGIN
    O:=1;
    FOR I:=1 TO Z DO
    O:=O*Y
    END;
    PUISS:=O;
END;

FUNCTION FACTOR(K:INTEGER):INTEGER;
VAR I,F:INTEGER;
  BEGIN
  F:=1 ;
  IF K=0 THEN FACTOR:=1 ELSE
    BEGIN
    FOR I:=1 TO K DO
    F:=F*I ;
    FACTOR:=F
    END;
    END;
FUNCTION BESSEL1(X:REAL;N:INTEGER):REAL;
VAR T,B,C:REAL;Q:INTEGER;
BEGIN
  Q:=0;
  B:=0;
  REPEAT
   BEGIN
   T:=(PUISS(-1,Q)/(FACTOR(Q)*FACTOR(N+Q)))*PUISS(X/2,N+2*Q);
   C:=B;
   B:=B+T;Q:=Q+1
   END
  UNTIL B=C;
BESSEL1:=B;
END;
VAR X1,X2,dX:REAL;N:INTEGER;
BEGIN
WRITELN('ENTRER dX,N ET PAR VALEURS CROISSANTES X1,X2');
READLN(dX,N,X1,X2);
  REPEAT
    BEGIN
      WRITELN(BESSEL1(X1,N));
      X1:=X1+dX;
    END;
   UNTIL X1>X2;

END.
```

TLP : GREEN

Objectifs

Discuter les raisons d’aller, ou pas, de rester ou de quitter le cloud

Prisme sécurité

Pour ne pas se contenter de contraintes, modes, clichés

Éléments pour construire des méthodes, pas une méthode

Discussion et débat

Cloud ? Clair comme un beau cumulus

IaaS, PaaS, SaaS, cloud public, privé, souverain, *move to cloud*…
Passons sur les définitions, vous savez ce que c’est

L’essence du cloud ?

TLP : GREEN

https://www.wired.com/story/china-backed-hackers-steal-microsofts-signing-key-post-mortem/

SECURITY POLITICS GEAR THE BIG STORY BUSINESS SCIENCE CULTURE IDEAS MERCH

LILY HAY NEWMAN SECURITY SEP 6, 2023 8:01 PM

The Comedy of Errors That Let China-Backed Hackers Steal Microsoft's Signing Key

After leaving many questions unanswered, Microsoft explains in a new postmortem the series of slipups that allowed attackers to steal and abuse a valuable cryptographic key.

PHOTOGRAPH: YAROSLAV KRYUCHKA/GETTY IMAGES

If you buy something using links in our stories, we may earn a commission. This helps support our journalism. Learn more. Please also consider subscribing to WIRED

MICROSOFT SAID IN June that a China-backed hacking group had stolen a cryptographic key from the company's systems. This key allowed the attackers to access cloud-based Outlook email systems for 25 organizations, including multiple US government agencies. At the time of the disclosure, however, Microsoft did not explain how the hackers were able to compromise such a sensitive and highly guarded key, or how they were able to use the key to move between consumer- and enterprise-tier systems. But a new postmortem published by the company on Wednesday explains a

MOST POPULAR

POLITICS

A Sensitive Complex Housing a CIA Facility Was on GSA's List of US Properties for Sale

Septembre 2023 | https://www.wired.com/story/china-backed-hackers-steal-microsofts-signing-key-post-mortem/

https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

TLP : GREEN

Don't be like these 900+ websites and expose millions of passwords via Firebase

Warning: Poorly configured Google Cloud databases spill billing info, plaintext credentials

Thomas Claburn

Mon 18 Mar 2024 // 21:29 UTC

At least 900 websites built with Google's Firebase, a cloud database, have been misconfigured, leaving credentials, personal info, and other sensitive data inadvertently exposed to the public internet, according to security researchers.

Among these websites, it's estimated that at least 125 million user records were found to be publicly accessible, including billing information and plaintext passwords. In short: If you're using Google's Firebase, make sure it's securely configured to avoid leaking private info to the rest of the world.

Firebase is a popular backend service that websites and apps use for storing data in the cloud. It provides security rules to keep data safe, in theory anyway.

In practice, we recall an incident where 24,000 Android apps exposed data through ham-handed Firebase implementations. According to one software engineer who used to work at Google and as a Firebase consultant, "the concerns with security rules have always

TLP : GREEN

https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers

PROPUBLICA

Technology

Microsoft Chose Profit Over Security and Left U.S. Government Vulnerable to Russian Hack, Whistleblower Says

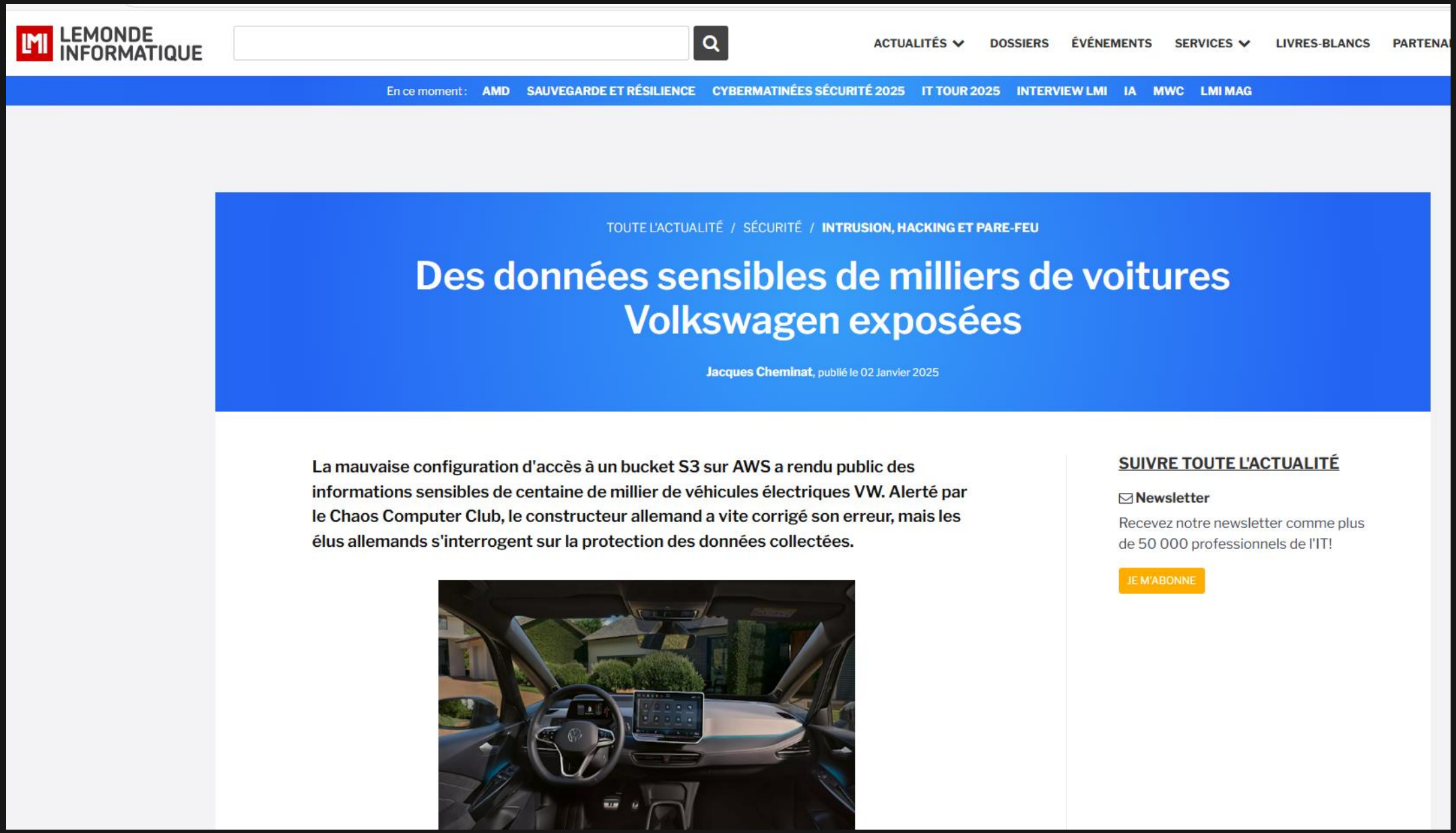
by Renee Dudley, with research by Doris Burke

June 13, 2024, 5 a.m. EDT

Juin 2024 | https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers

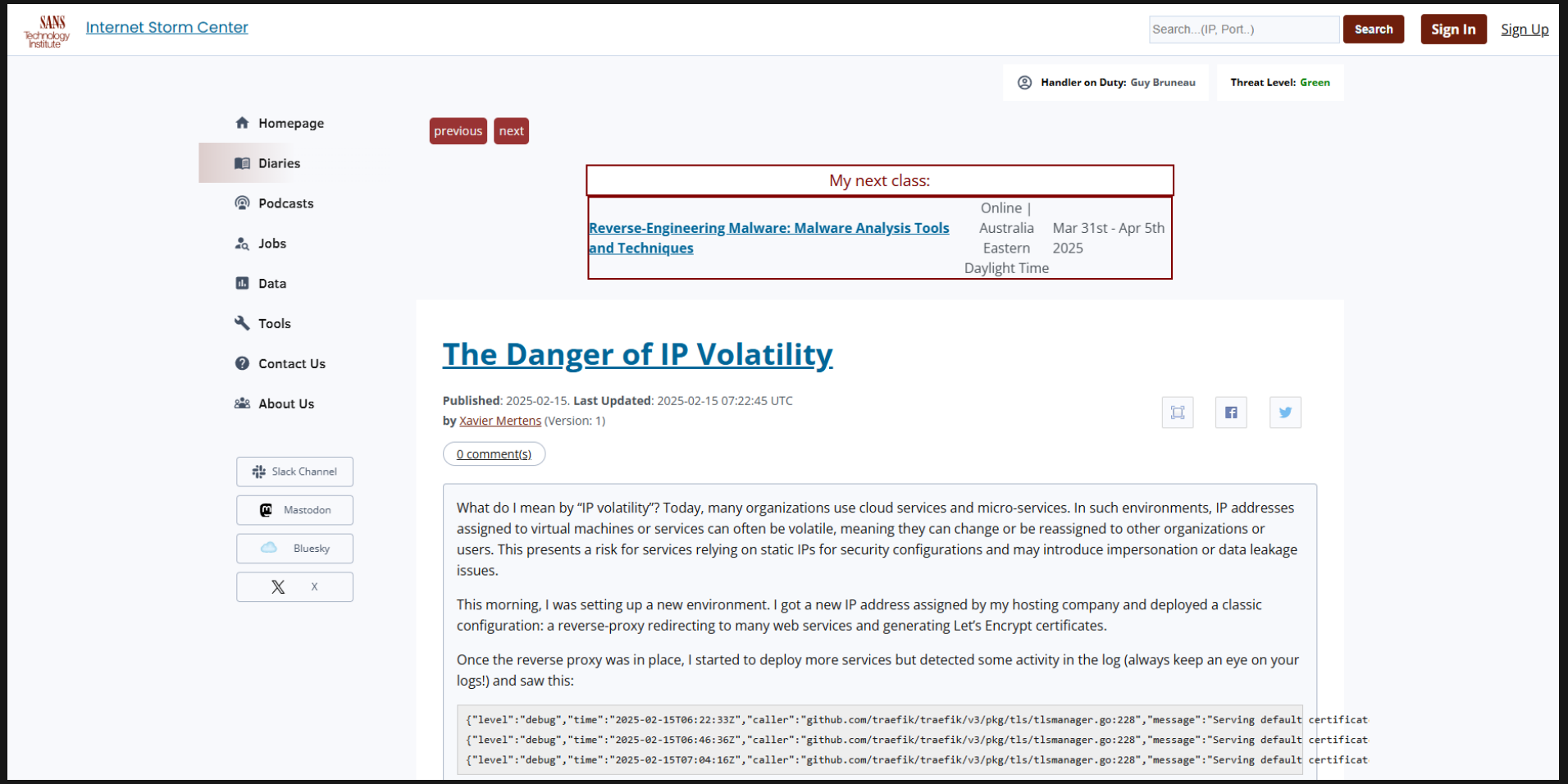
Juin 2024 | https://www.theregister.com/2024/06/10/security_in_brief/

TLP : GREEN



Janvier 2025 | https://www.lemondeinformatique.fr/actualites/lire-des-donnees-sensibles-de-milliers-de-voitures-volkswagen-exposees-95651.html

TLP : GREEN


SANS Technology Institute
Internet Storm Center
Search...(IP, Port..)
Search
Sign In
Sign Up
Handler on Duty: Guy Bruneau
Threat Level: Green
Homepage
Diaries
Podcasts
Jobs
Data
Tools
Contact Us
About Us
Slack Channel
Mastodon
Bluesky
X
previous
next
My next class:
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Online | Australia Eastern Daylight Time
Mar 31st - Apr 5th 2025
The Danger of IP Volatility
Published: 2025-02-15. Last Updated: 2025-02-15 07:22:45 UTC
by Xavier Mertens (Version: 1)
0 comment(s)
What do I mean by "IP volatility"? Today, many organizations use cloud services and micro-services. In such environments, IP addresses assigned to virtual machines or services can often be volatile, meaning they can change or be reassigned to other organizations or users. This presents a risk for services relying on static IPs for security configurations and may introduce impersonation or data leakage issues.
This morning, I was setting up a new environment. I got a new IP address assigned by my hosting company and deployed a classic configuration: a reverse-proxy redirecting to many web services and generating Let's Encrypt certificates.
Once the reverse proxy was in place, I started to deploy more services but detected some activity in the log (always keep an eye on your logs!) and saw this:
{"level":"debug","time":"2025-02-15T06:22:33Z","caller":"github.com/traefik/traefik/v3/pkg/tls/tlsmanager.go:228","message":"Serving default certificat
{"level":"debug","time":"2025-02-15T06:46:36Z","caller":"github.com/traefik/traefik/v3/pkg/tls/tlsmanager.go:228","message":"Serving default certificat
{"level":"debug","time":"2025-02-15T07:04:16Z","caller":"github.com/traefik/traefik/v3/pkg/tls/tlsmanager.go:228","message":"Serving default certificat

The Register

Check out this free automated tool that hunts for exposed AWS secrets in public repos

You can find out if your GitHub codebase is leaking keys ... but so can miscreants

Jessica Lyons

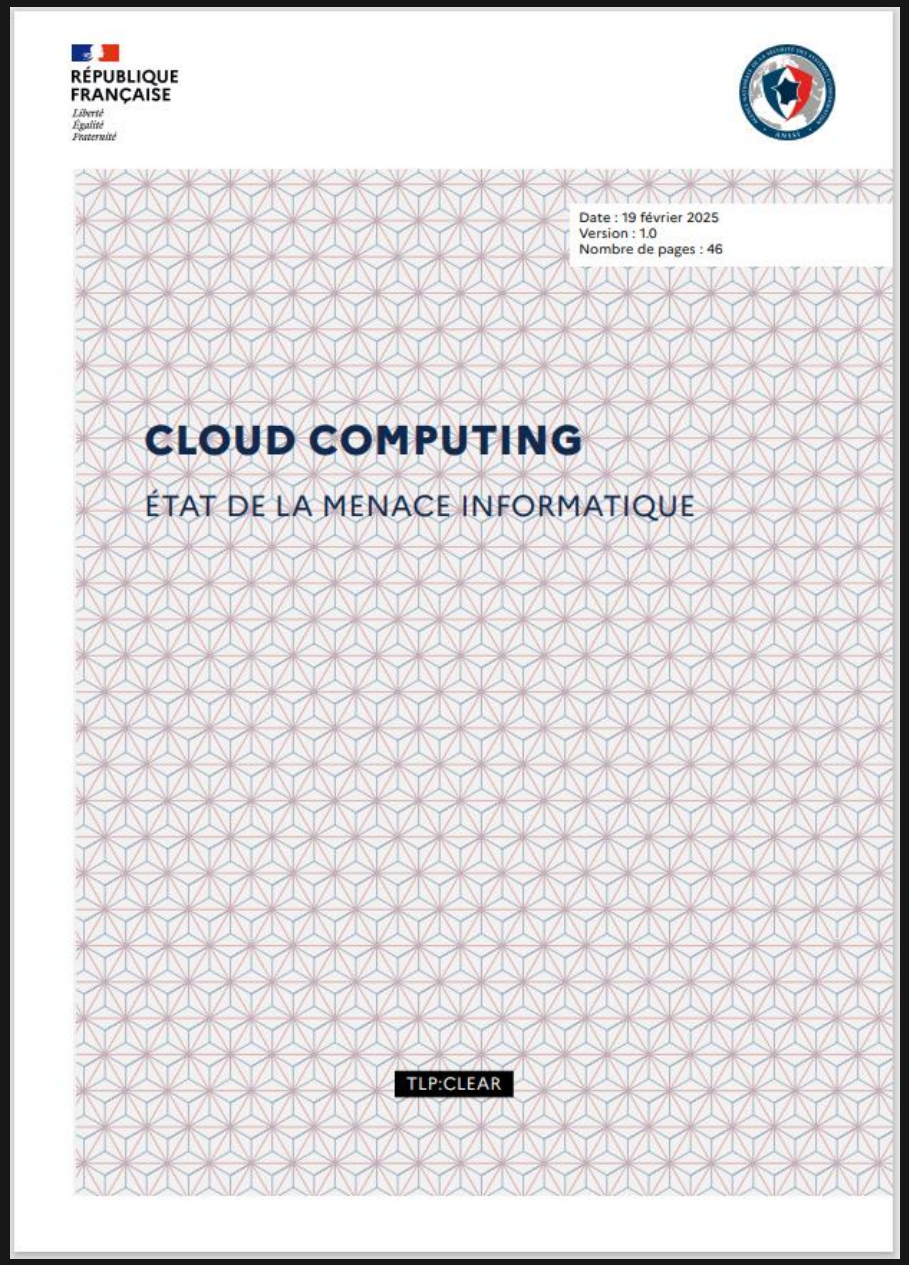
Wed 19 Feb 2025 // 20:45 UTC

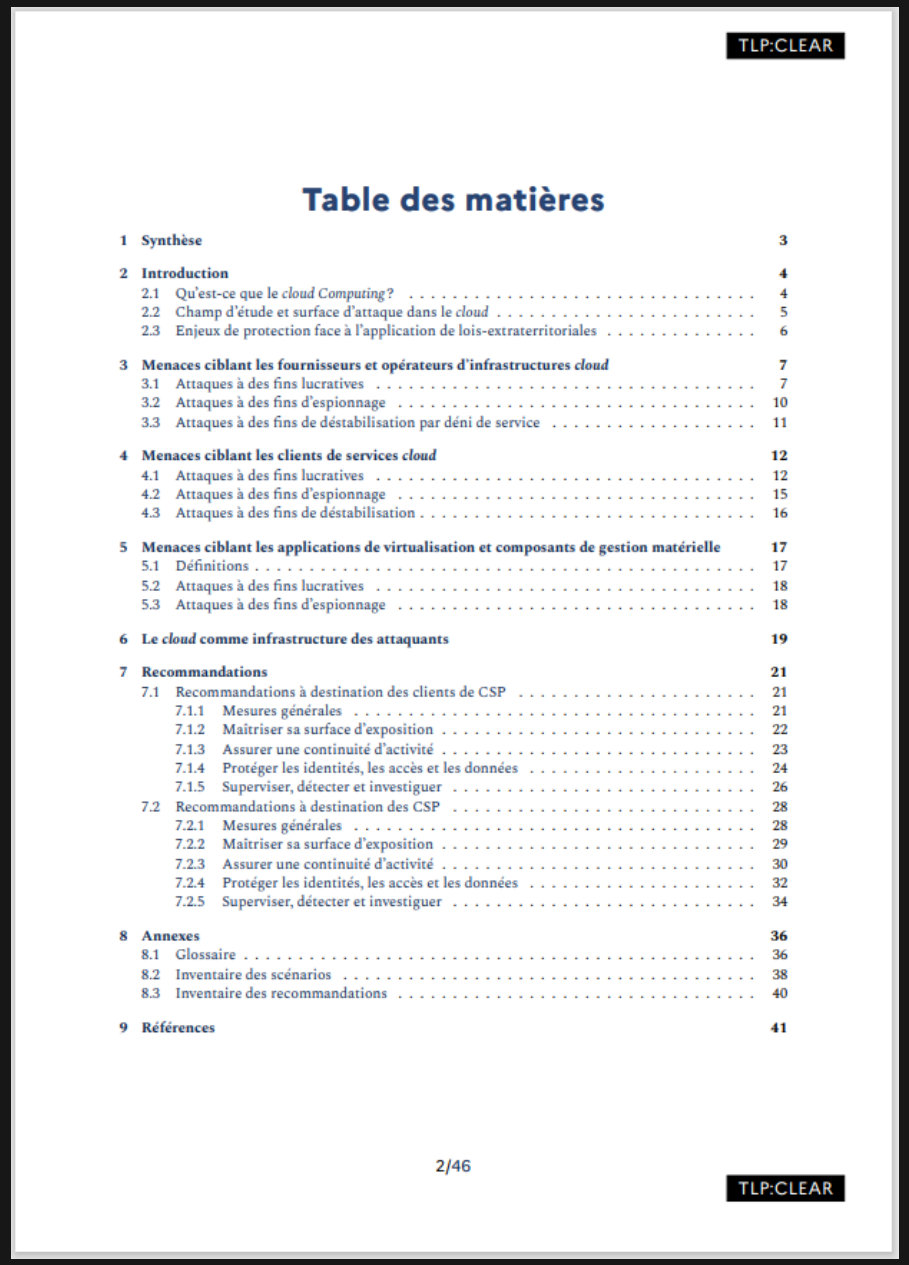
A free automated tool that lets anyone scan public GitHub repositories for exposed AWS credentials has been released.

Before you say anything, yes, we're pretty sure similar programs and services are out there – including GitHub's own built-in secrets scanner – but hey, where's the harm in highlighting today the fact that this sort of software is easily available?

Security engineer Anmol Singh Yadav built AWS-Key-Hunter after he found more than 100 exposed AWS access keys, some with high privileges, in public repositories, "just waiting to be exploited," as he wrote in a blog about the discovery and the custom-built tool.

Leaked security keys can be abused by criminals to hijack people's cloud accounts and access their AWS resources. This leads to all manner of evil deeds: Stealing compute





TLP:CLEAR

Table des matières

TLP:CLEAR

Février 2025 | https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-001.pdf

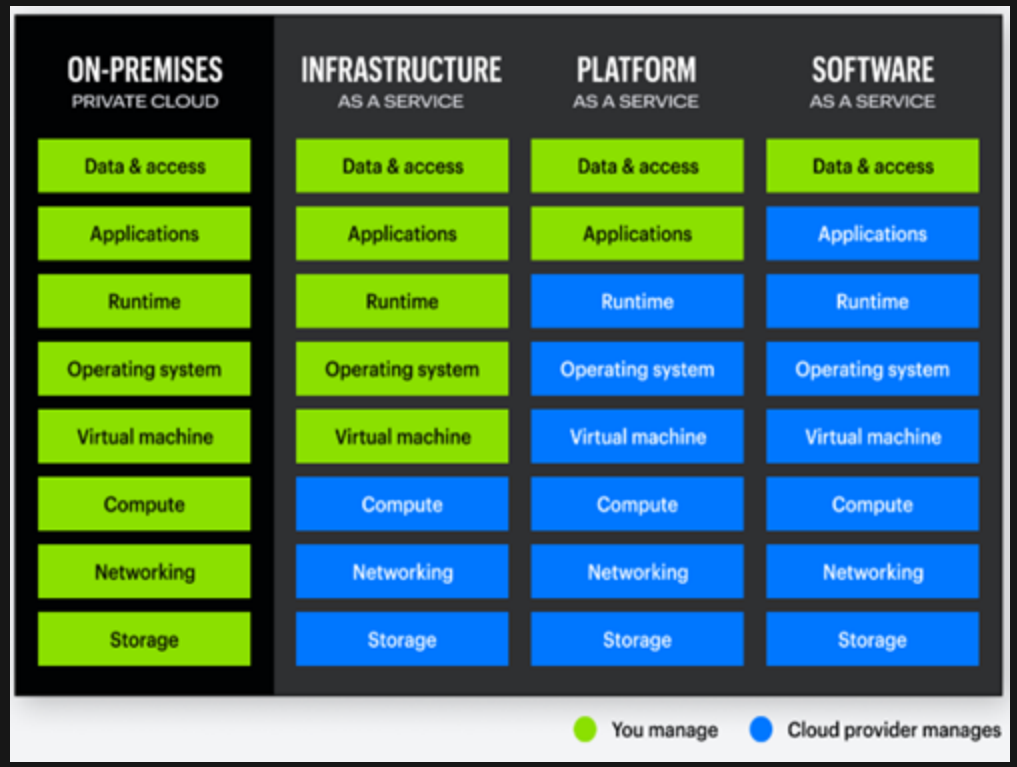
TLP : GREEN

Pourquoi nous devrions éviter les nuages

- **Fonctionnel** : avons-nous toujours besoin de la disponibilité, de l'ubiquité ou de la flexibilité que permet le cloud ?
- Difficulté de la **réversibilité** – le voyage aller est souvent simple, le chemin de sortie, moins – *vraiment ?*
- Encore plus « **boîte noire** » que la plupart des logiciels *on-prem*

Pourquoi nous devrions éviter les nuages

- Le ***shared responsability model*** est souvent mal compris
- La sécurité n’est pas toujours activée **par défaut**
- Problème de la **souveraineté** | Cloud Act | FISA | Localisation des données, accès aux données | Garanties juridiques ? Dans la plupart des cas, n’imaginez pas négocier des contrats



TLP : GREEN

Pourquoi nous devrions éviter les nuages

- Problème de la **dépendance** – en particulier vu la faiblesse des restrictions anti-concentration (*anti-trust*) et les politiques / l'éthique des offreurs
- Impact des attaques ***supply chain*** (e.g. Okta 2022)
- Sommes-nous toujours certains de l'**équation économique** ? – et augmentation des prix sur clients captifs / coûts cachés

Pourquoi nous devrions éviter les nuages

- Perte de **maîtrise** (sysadmin vs. FinOps…)
- *Shadow IT*
- C’est « **industrialisé** » : bon pour le fournisseur, pas toujours pour le client

TLP : GREEN

Pourquoi monter dans les nuages

- **Flexibilité** – en particulier en cas de variation rapide du chiffre d’affaires / de l’activité
- **Maintenance** facilitée
- Les éditeurs nous y obligent – en ne montant les **évolutions** que sur les versions cloud, négligeant les versions *on-prem*

Pourquoi monter dans les nuages

- **Ubiquité** & **collaboration** – adaptation aux nouveaux usages, où « le bureau » perd de sa superbe
- **Moins** de **pertes** de données (?)
- **Disponibilité**
- Services managés – permet de se **concentrer** sur les cœurs de **métier**

Pourquoi monter dans les nuages

- C’est « industrialisé » - **moins de cas particuliers** / standardisation: nouvelles façons de faire (e.g. VPM via *reconstruction*)
- **Sécurité**… | Compétences sécurité des acteurs du cloud
- Et puis… c’est à la **mode** – *Si t’es pas dans le cloud à 50 ans, c’est que t’as raté ta vie…*

Pourquoi? Un curieux marché

From Freddy Dezeure – Jack Cable – CERT-EU Conference – Octobre 24

Éditeurs

- Cherchent gains court-terme
- Souvent organisés par lignes produit
- Se préoccupent des risques légaux
- Font du lobbying contre les régulations

Clients

- Manque de ressources
- Manque de compétences
- Contraintes du *legacy*
- Eparpillés

Régulateurs

- Souvent organisés par pays / secteurs
- Lents et statiques
- Manque de ressources / compétences
- Influencés par les lobbies

Communauté

- Surtout représentée par les organisations les plus matures
- Manque de ressources

Et puis, ces dernières semaines…

Elon Musk sur scène lundi 20 janvier au Capitole, à Washington, pour l'investiture de Donald Trump. (Mike Segar/Reuters)

Le Monde

Consulter le journal

Actualités · Économie · Vidéos · Débats · Culture · Le Goût du Monde

ÉCONOMIE • DONALD TRUMP

Numérique : le feu roulant des Etats-Unis contre la régulation européenne

L'administration de Donald Trump défend les géants de la tech américains contre les textes de l'UE. Bruxelles se dit « totalement déterminé à les appliquer ».

Par Alexandre Piquard

Publié le 05 mars 2025 à 19h00, modifié le 05 mars 2025 à 19h08 · Lecture 5 min.

Offrir l'article

Article réservé aux abonnés

Édition du jour

Daté du lundi 10 mars

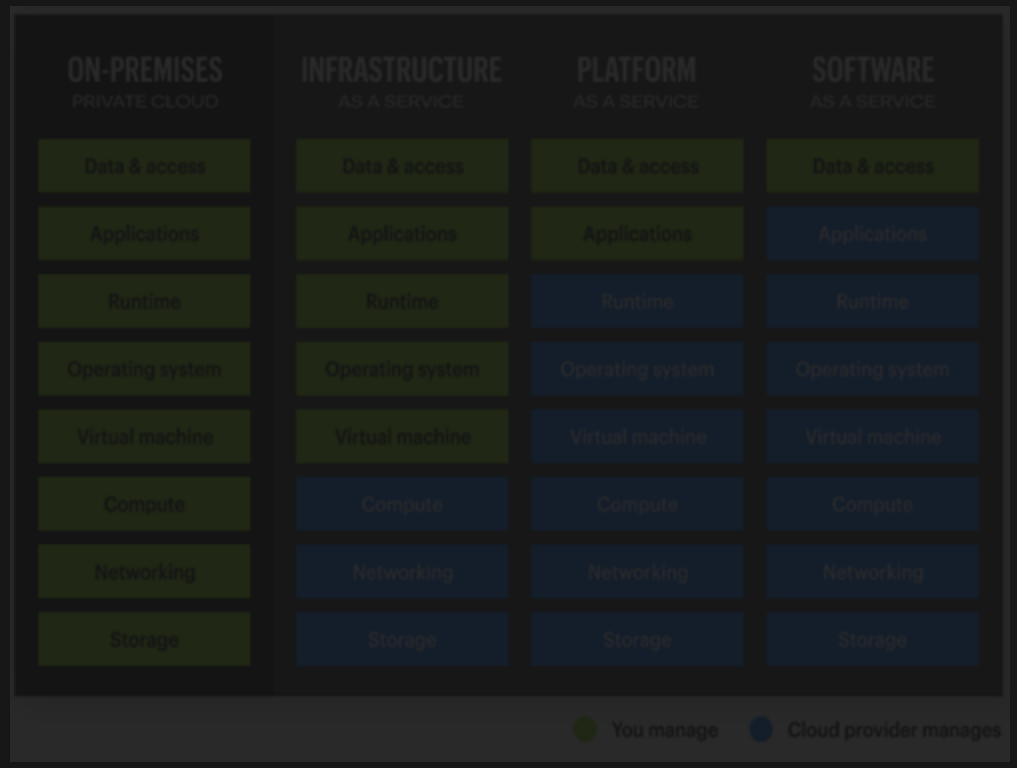
Une décision historique et lourde de conséquences vient bouleverser les relations entre les États-Unis et l'Union européenne. Dans un contexte de tension croissante depuis six mois, le Président Trump a annoncé hier soir, à la veille des célébrations de l'Independence Day, qu'il avait signé un *Executive Order* avec effet immédiat, interdisant aux entreprises technologiques américaines de délivrer des produits et

Ce que ça change ?

TLP : GREEN

Pourquoi nous devrions éviter les nuages

- Ils vous laissent faire la majorité de la sécurité / *Shared responsability model*
- La sécurité n'est pas toujours activée par défaut
- Problème de la souveraineté | Cloud Act | FISA | Localisation des données, accès aux données | Garanties juridiques ? Dans la plupart des cas, n'imaginez pas négocier des contrats | Confiance | Ethique



TLP : GREEN

Transfert de données hors zone RGPD ?

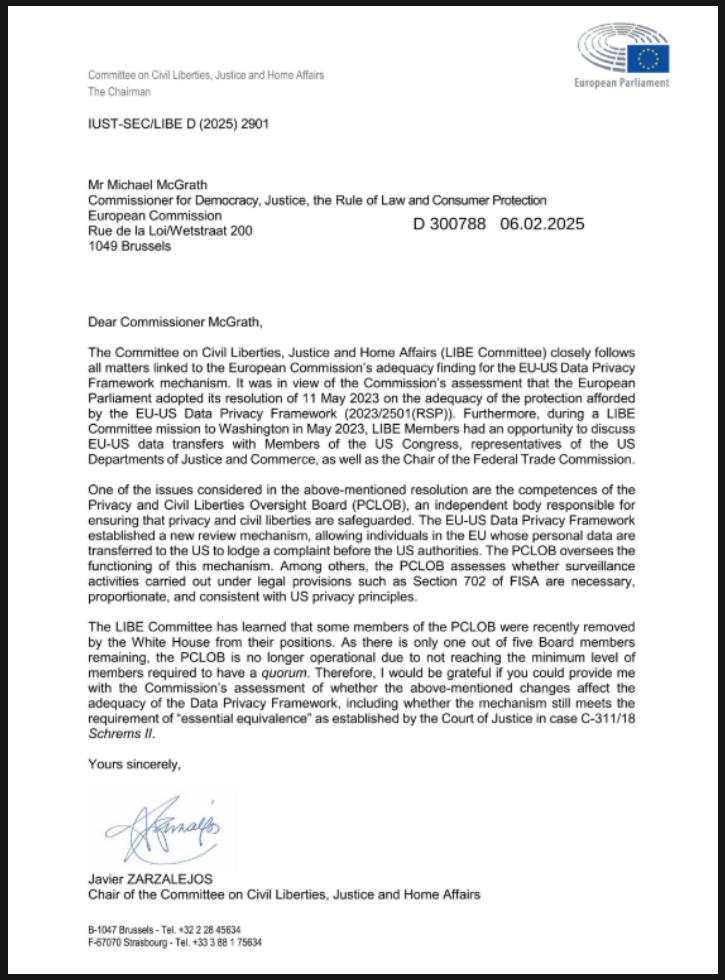
~~Safe Herbor~~ (Schrems 2015)

~~Privacy Shield~~ (2020)

Data Privacy Framework…

Il semble que les recours FISA section 702 (demandes d'accès aux données par les autorités US) soient nombreux, peut-être sans contrôle

Enfin, il ne s'agit bien sûr pas que des US: Russie, Chine…



Committee on Civil Liberties, Justice and Home Affairs
The Chairman

European Parliament

IUST-SEC/LIBE D (2025) 2901

Mr Michael McGrath
Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection
European Commission
Rue de la Loi/Wetstraat 200
1049 Brussels

D 300788 06.02.2025

Dear Commissioner McGrath,

The Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) closely follows all matters linked to the European Commission's adequacy finding for the EU-US Data Privacy Framework mechanism. It was in view of the Commission's assessment that the European Parliament adopted its resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)). Furthermore, during a LIBE Committee mission to Washington in May 2023, LIBE Members had an opportunity to discuss EU-US data transfers with Members of the US Congress, representatives of the US Departments of Justice and Commerce, as well as the Chair of the Federal Trade Commission.

One of the issues considered in the above-mentioned resolution are the competences of the Privacy and Civil Liberties Oversight Board (PCLOB), an independent body responsible for ensuring that privacy and civil liberties are safeguarded. The EU-US Data Privacy Framework established a new review mechanism, allowing individuals in the EU whose personal data are transferred to the US to lodge a complaint before the US authorities. The PCLOB oversees the functioning of this mechanism. Among others, the PCLOB assesses whether surveillance activities carried out under legal provisions such as Section 702 of FISA are necessary, proportionate, and consistent with US privacy principles.

The LIBE Committee has learned that some members of the PCLOB were recently removed by the White House from their positions. As there is only one out of five Board members remaining, the PCLOB is no longer operational due to not reaching the minimum level of members required to have a *quorum*. Therefore, I would be grateful if you could provide me with the Commission's assessment of whether the above-mentioned changes affect the adequacy of the Data Privacy Framework, including whether the mechanism still meets the requirement of "essential equivalence" as established by the Court of Justice in case C-311/18 *Schrems II*.

Yours sincerely,

Javier ZARZALEJOS
Chair of the Committee on Civil Liberties, Justice and Home Affairs

B-1047 Brussels - Tel. +32 2 28 45634
F-67070 Strasbourg - Tel. +33 3 88 1 75634

TLP : GREEN

Finalement, *to cloud or not to cloud?*

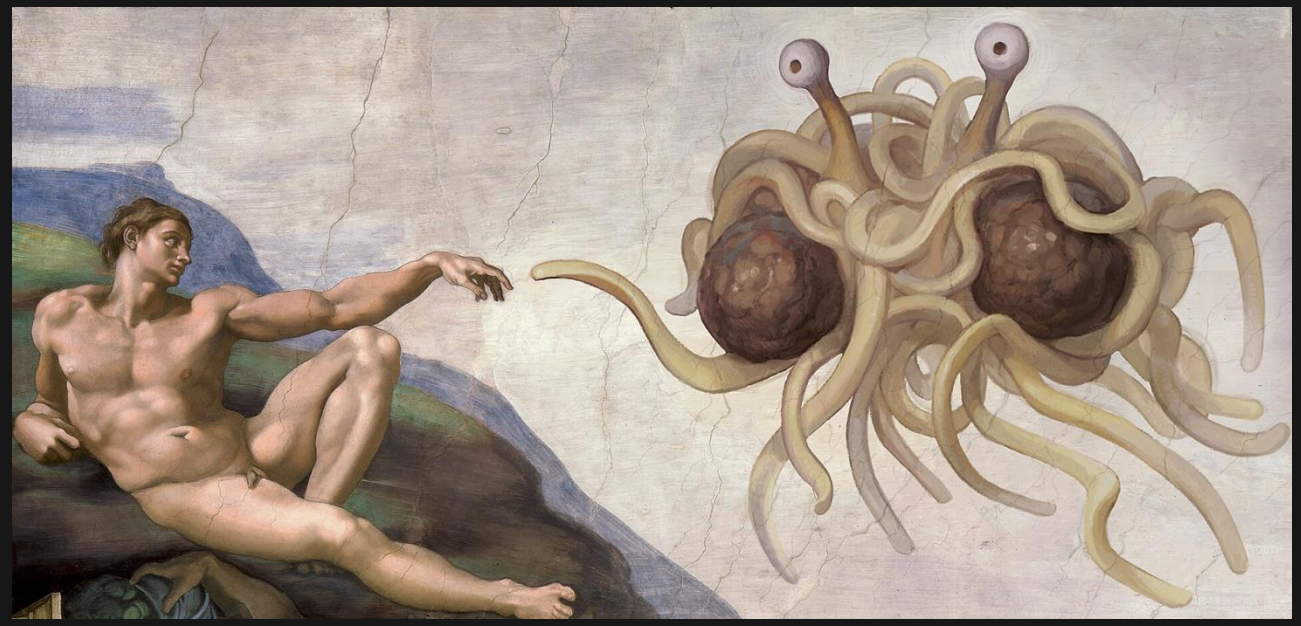
- Un aspect essentiel : la **consommation** et les émissions CO_2
- **Sobriété** énergétique, sobriété des traitements, des données stockées
- Mais *effet rebond (paradoxe de Jevons)* : accroissement de la consommation provoqué par la réduction des coûts / de l'énergie consommée
- Le cloud peut être un atout – mutualisation et maximisation de l'usage des ressources matérielles… ou pas: études partielles, épuisement des ressources…

https://www.greenit.fr/2015/03/02/le-cloud-est-il-green/
https://www.ademe.fr/

Finalement, *to cloud or not to cloud?*

S’il faut monter – ou rester – dans les nuages…

Reste à déterminer lesquels, pour y faire quoi exactement et comment

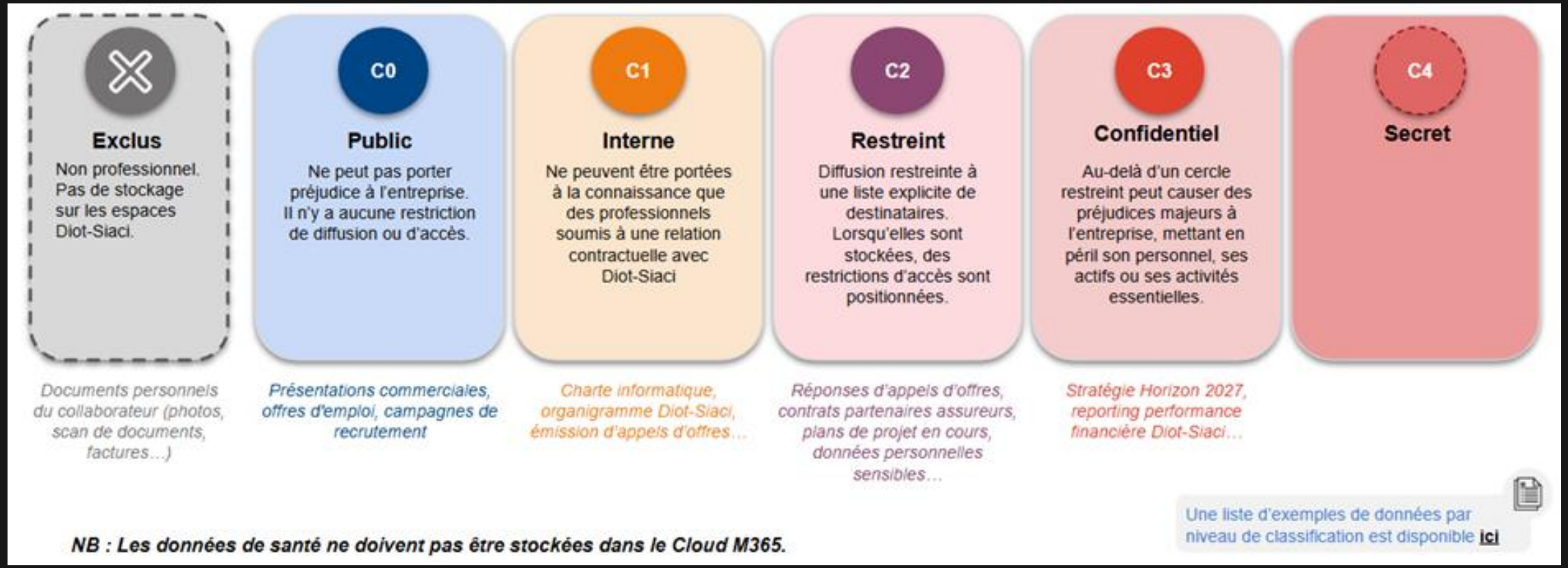


(Touché par Son Appendice Nouillesque, inspiré de La Création d'Adam de Michel-Ange, est une représentation iconique du Monstre de spaghetti volant)

Stratégie de sécurisation des nuages

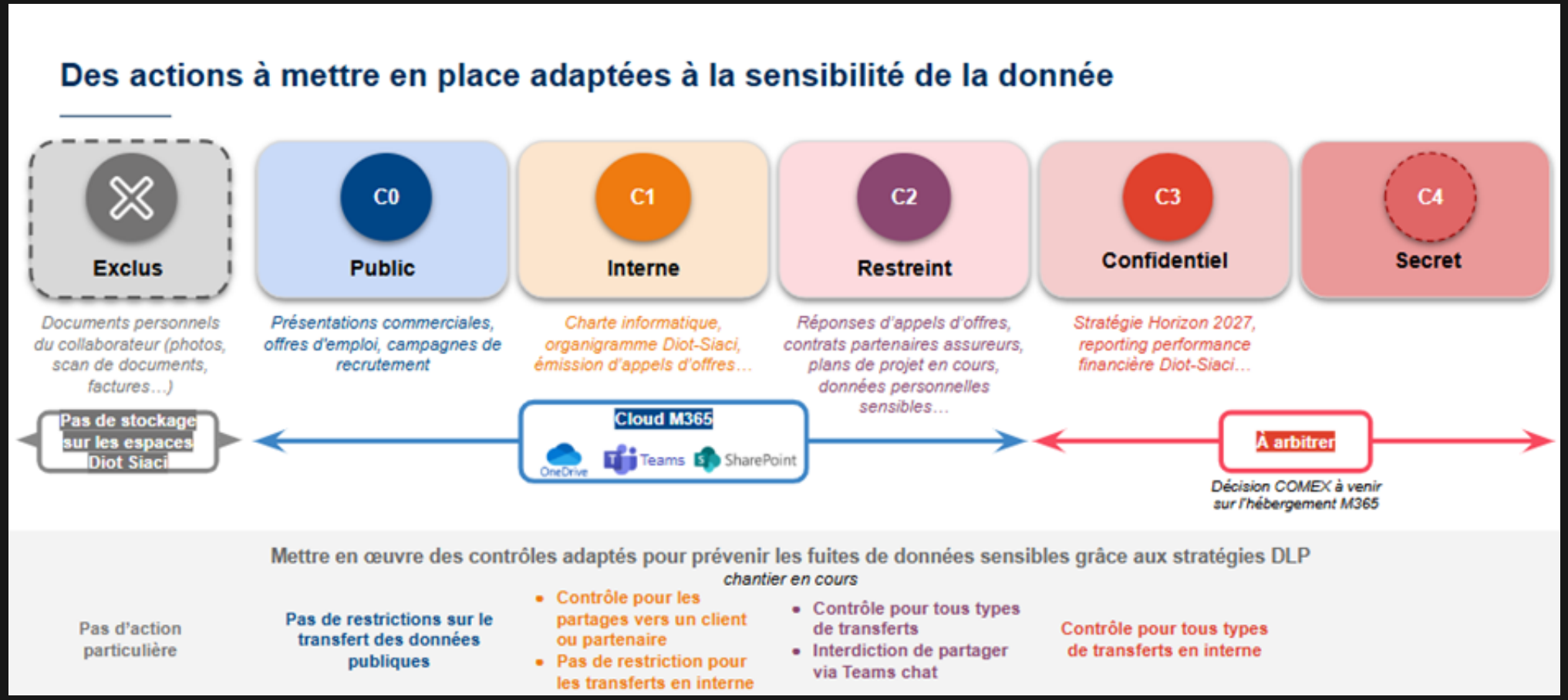
- Penser **services** et non produits
- Pas forcément choisir les plus gros – US – quitte à **réduire** les **exigences fonctionnelles**
- Par défaut, **retirer la responsabilité** de la sécurité aux utilisateurs
- Si possible, **chiffrer** les données localement
- **Classification**, maitrise et contrôles des données | Données des clients
- Faire accepter les risques
- Embaucher & former - **compétences** en interne

Classification, maitrise et contrôles des données | Données des clients



TLP : GREEN

Classification, maitrise et contrôles des données | Données des clients



TLP : GREEN

Classification, maitrise et contrôles des données | Données des clients

TLP : GREEN

Stratégie de sécurisation des nuages

- Appliquer des référentiels – CIS Controls | ANSSI | CLUSIF… (questionnaire pour déterminer meilleure solution | 15 critères de souveraineté)
- Œuvrer à changer les paradigmes sécurité – via de la régulation (comme DORA, NIS2) / des référentiels comme SecNumCloud

https://cyber.gouv.fr/publications/recommandations-pour-lhebergement-des-si-sensibles-dans-le-cloud
https://clusif.fr/wp-content/uploads/2025/01/20240627-Souverainete-et-confiance-numerique.pdf

TLP : GREEN

Stratégie de sécurisation des nuages

Besoin	Questions relatives à la solution ou au service numérique visés	Niveau de besoin 1	2	3	4
	Contexte				
1.	Le service métier ou le service d'hébergement recherché est-il **important** pour votre activité ?	Il est accessoire	Les activités seraient fortement perturbées	Les activités en dépendent totalement	Je ne sais pas
2.	Si un sinistre venait à atteindre votre service métier ou service d'hébergement recherché, causant un dysfonctionnement ou une perte de données, quelles seraient **les conséquences en interne** pour vos activités ?	Les conséquences internes d'un sinistre seraient négligeables	Les conséquences internes d'un sinistre seraient significatives	Les conséquences internes d'un sinistre seraient graves, voire fatales	Je ne sais pas
3.	Si un sinistre venait à impacter la sécurité de votre service métier ou service d'hébergement recherché (il ne fonctionne plus ou pas bien, vol d'informations…), quelles seraient **les conséquences pour l'extérieur** (pour vos usagers, clients, administrés…) ?	Les conséquences d'un sinistre pour l'extérieur seraient négligeables	Les conséquences d'un sinistre pour l'extérieur seraient significatives	Les conséquences d'un sinistre pour l'extérieur seraient graves, voire fatales	Je ne sais pas

	Thème	Somme recueillie	Besoin de sécurité du système	Cloud et/ou infrastructure (lambda)	Cloud et/ou infrastructure de confiance	Coud souverain	Infrastructure souveraine
Interprétation des résultats	*Contexte*	De 3 à 5	1 – Élémentaire	x	x	x	x
		De 6 à 9	2 – Moyen		x	x	x
		De 10 à 12	3 – Renforcé			x	x
	Gravité des conséquences potentielles	De 3 à 5	1 – Élémentaire	x	x	x	x
		De 6 à 9	2 – Moyen		x	x	x
		De 10 à 12	3 – Renforcé			x	x
	Sensibilité des données du système[40],	De 5 à 9	1 – Élémentaire	x	x	x	x
		De 10 à 14	2 – Moyen		x	x	x
		De 15 à 32	3 – Renforcé			x	x
	Base d'estimation des	De 4 à 7	1 – Élémentaire	x	x	x	x

Thèmes	#	Critères et exigences liées à la Souveraineté		Description
Locaux - Réseaux - Hébergement - Services	1	Localisation physique des Datacenters	P1[42]	Localisation en France ou en Europe suivant l'offre, choix ou contraintes liées à réglementations spécifiques. *Note : le drapeau Européen traduit tout pays membres dans l'Union Européenne.*
	2	Localisation des données (transit, repos, utilisation)		
	3	Localisation des services et applications tierces		
	4	Localisation des équipes d'exploitation		
	5	Localisation des sous-traitants de premier rang		
	6	Localisation si chaîne de sous-traitance		
	7	Localisation des personnes à accès à privilèges		
	8	Localisation des supervisions / sauvegardes	P2	
	9	Localisation du siège de la société		
Légal - Juridique - Financier	10	Certifications pour l'hébergeur		Reconnues ou établies au niveau Européen[43],[44]
	11	Nationalité du ou des hébergeurs	- A défaut Autres*	*Nationalité des personnels non soumises aux lois extraterritoriales (cf. chapitre 4.4)
	12	Nationalité des personnels à accès techniques		
	13	Nationalité des fonds de capitaux		*Investisseurs étrangers non majoritaires[45]
	14	Montage juridique de la société / entité		*Entité indépendante de relations[46] avec des Etats soumis aux lois extraterritoriales
	15	Nationalité des services ou produits utilisés		*Services ou produits maîtrisés en matière d'exposition (réseau privé, déconnecté, …)

https://clusif.fr/wp-content/uploads/2025/01/20240627-Souverainete-et-confiance-numerique.pdf

TLP : GREEN

Merci
À vous la parole

(vous remarquerez que je n'ai – presque? – pas parlé d'IA ou de chiffrement homomorphe)

TLP : GREEN