



# LE TRAITEMENT DES VULNÉRABILITÉS POUR LES SOLUTIONS UCAAS CLOUD:

COMMENT FAIRE FACE À L'URGENCE ET AUX RÉGLEMENTATIONS  
?

FABIEN BRISSET  
11 MARS 2025







# QUI EST FABIEN BRISSET ?



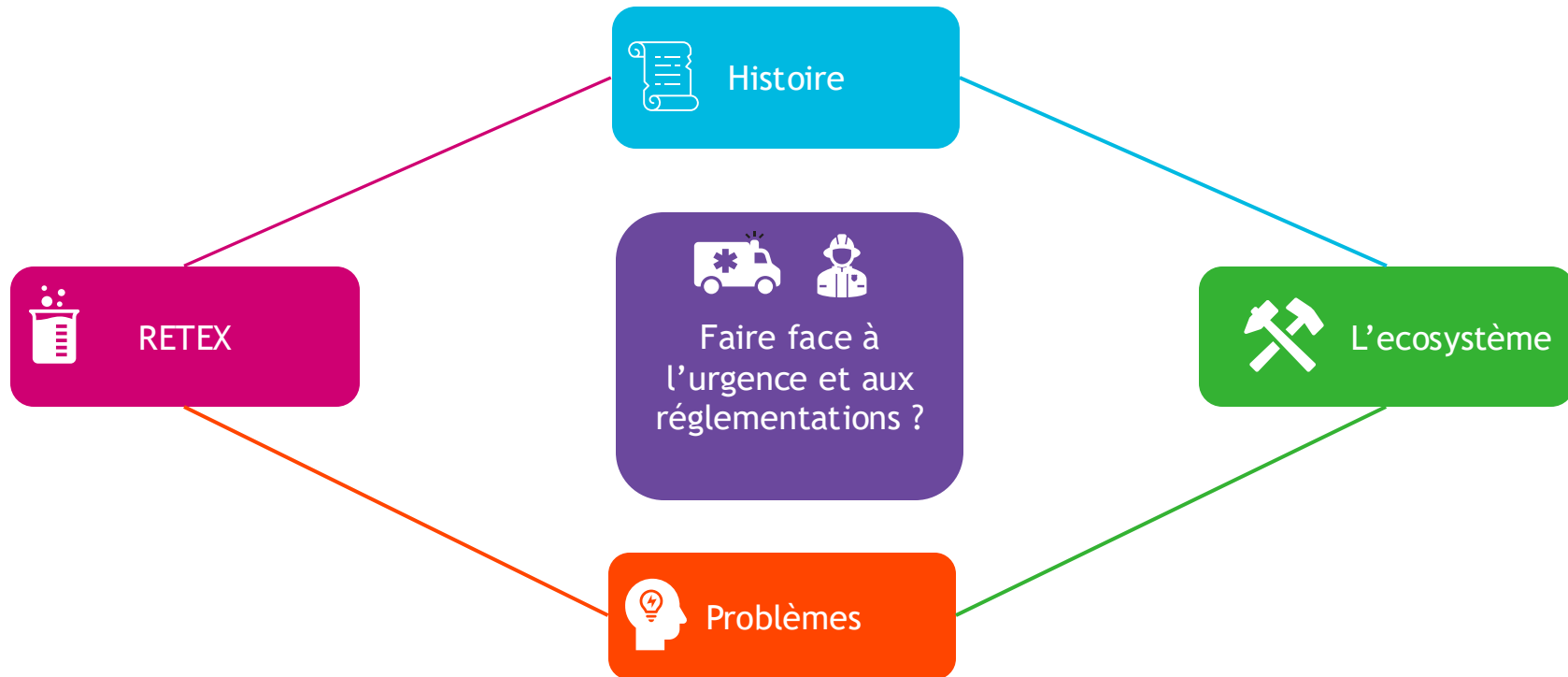
**Pseudos :** “GxFab” – “ElsassSenku”  
**Fonction :** Spécialiste Sécurité Cloud

-  @fbrisset
-  GxFab
-  Esenku
-  Blog personnel (nouveau)

-  Cybersécurité
-  Vulnérabilités
-  Cloud
-  Plateformes de CTF



# AVANT DE COMMENCER



# AUX ORIGINES,...



## Vulnérabilité

- Etymologie :
  - ✓ Dérivé de vulnérable, avec le suffixe -ité
- Définition :
  - ✓ Caractère de ce qui est vulnérable

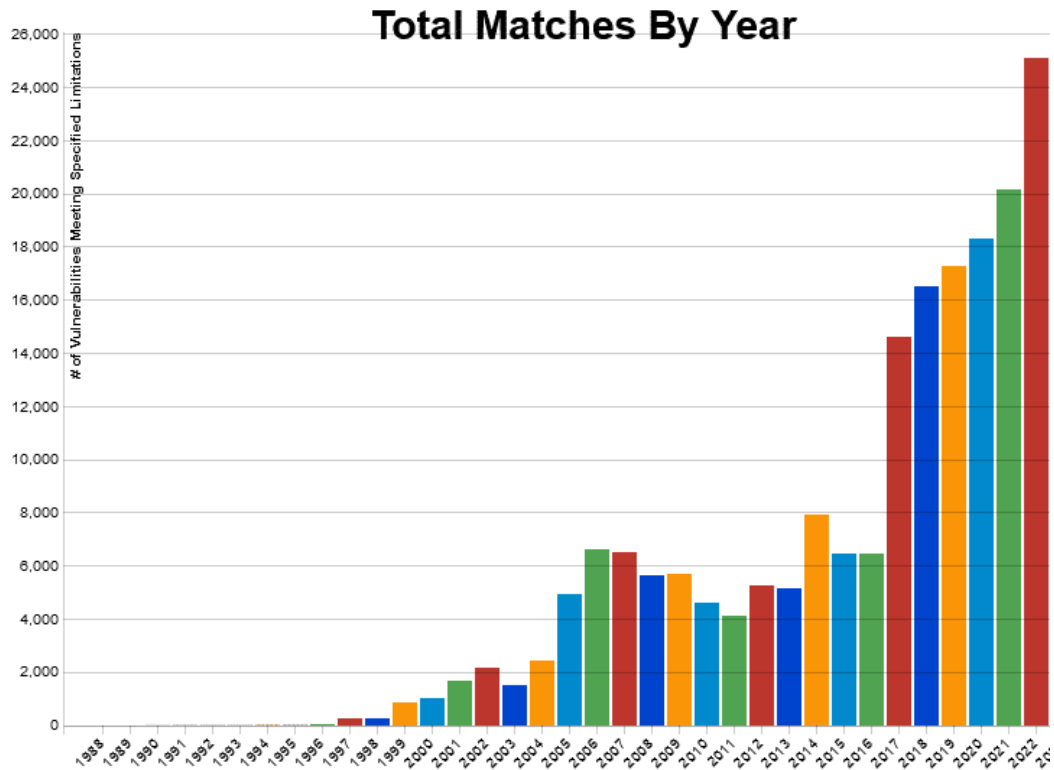
## Vulnérable

- Etymologie :
  - ✓ Du latin vulnerabilis, de vulnerare (« blesser »).
- Définition :
  - ✓ Qui peut être blessé
  - ✓ Qui peut être attaqué, qui offre prise

# MAIS QUELLE EST SA DÉFINITION EN CYBER ?



# STATISTIQUES AU FIL DES ANNÉES



Source : [Cyberwatch / NVD](#)

# QUELQUES NOMS AYANT FAIT TREMBLER



1988 – "Première CVE" - Le ver Morris



2018 – Spectre – CVE-2017-5753  
CVE-2017-5715



2014 – Heartbleed – CVE-2014-0160



2018 – Meltdown – CVE-2017-5754

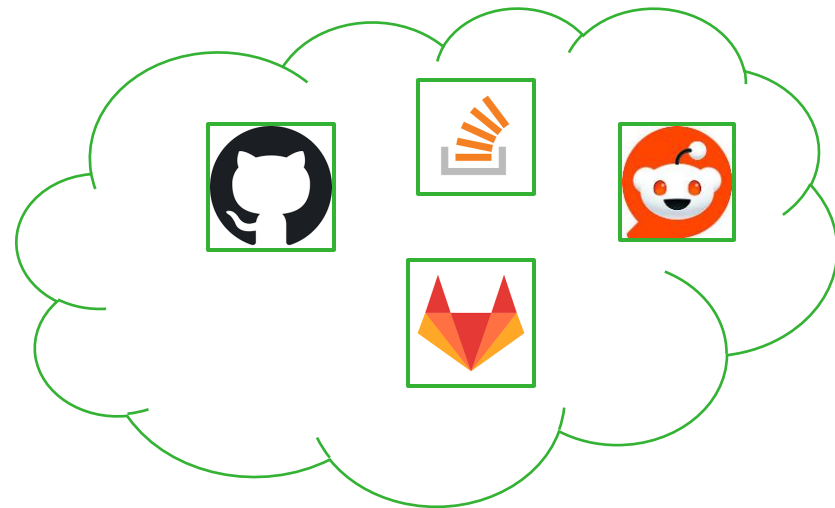


2017 – WannaCry – CVE-2017-0144



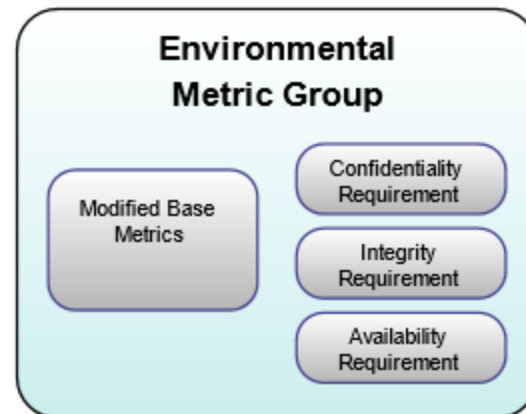
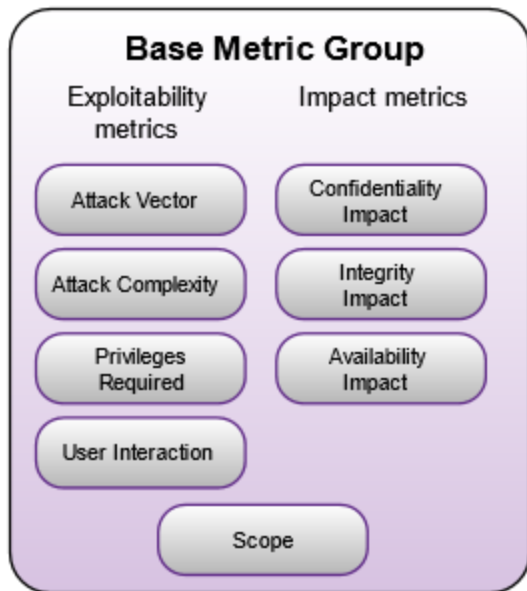
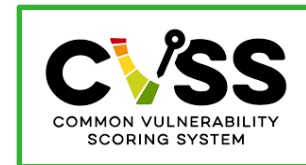
2021 – Log4Shell – CVE-2021-44228

# SOURCES D'INFORMATIONS



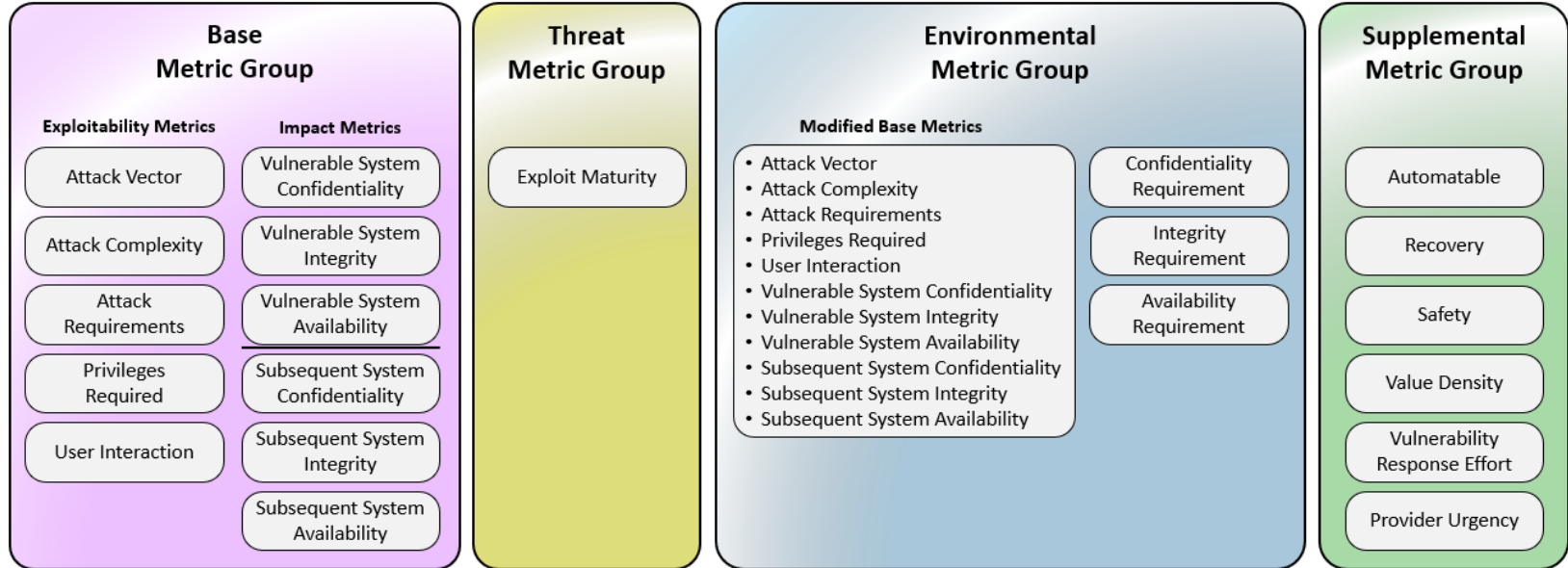


# SYSTÈME DE NOTATION : CVSS 3.1



Source : <https://www.first.org/cvss/v3.1/specification-document>

# SYSTÈME DE NOTATION : CVSS 4.0



Source : <https://www.first.org/cvss/v4.0/specification-document>

# SYSTÈME DE NOTATION



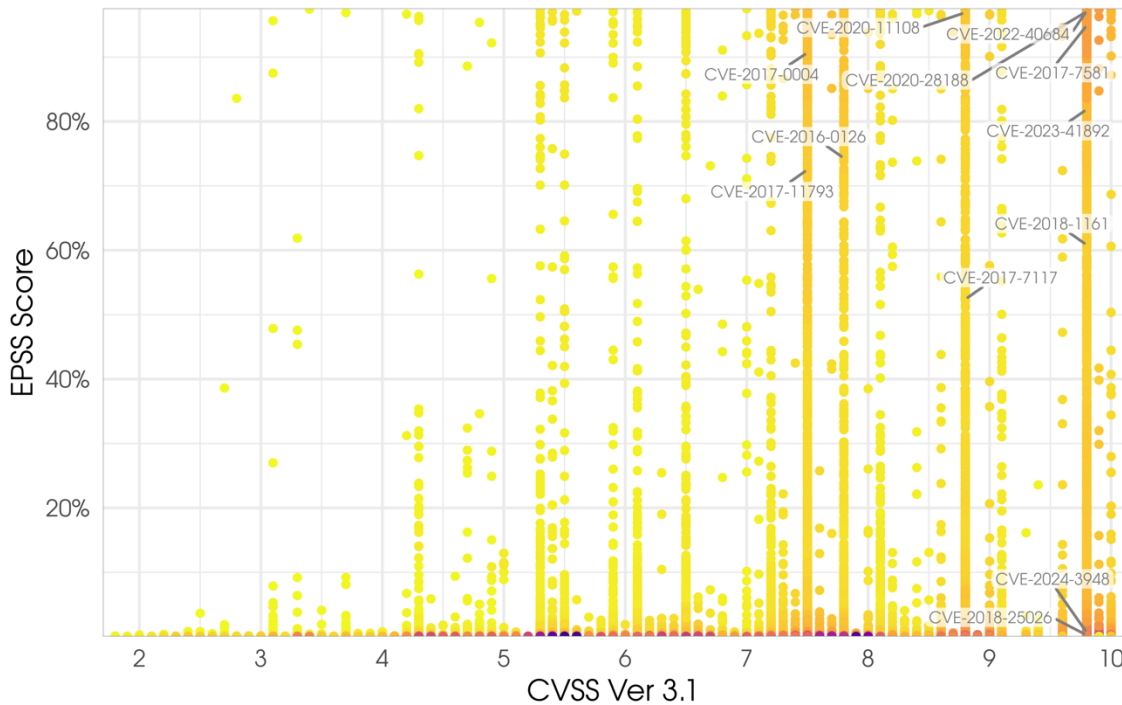
- Compris entre 0 et 1
- Un score et un percentile
- Score calculé à l'aide d'un modèle statistiques qui prend en compte :
  - Les caractéristiques de la vulnérabilité
  - L'historique de l'exploitation
  - Les renseignements sur les menaces
  - La disponibilité d'un exploit
  - La gravité intrinsèque de la vulnérabilité
  - Le vecteur d'attaque
  - L'impact métier

# SYSTÈME DE NOTATION



## EPSS score compared to CVSS Base Score (NVD)

Point density is represented by color, yellow is less dense going through red to a deep purple for the most dense areas. Labeling a random sample of CVEs with higher values for reference.



Source: [https://first.org/epss/data\\_stats, 2025-03-07](https://first.org/epss/data_stats, 2025-03-07)

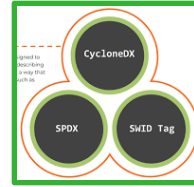
# SYSTÈME DE NOTATION

- *Catalogue de vulnérabilités activement exploités*
- *Intérêt d'un tel catalogue :*
  - *Informé sur les risques immédiats*
  - *Liste détaillée des vulnérabilités exploitées*
  - *Actualisation continue*
  - *Aide à la priorisation*

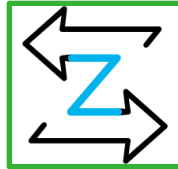
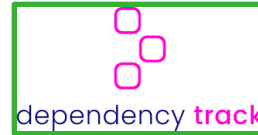


# BRIQUES LOGICIELLES

## Scanners Actifs



## Logiciels de gestion



## Analyseurs de code

## Scanners Passifs

# VEILLE DE MENACE

- Participe aussi à l'écosystème de gestion des vulnérabilités
- Processus essentiel pour aider les organisations
- Six intérêts :
  - *Détection précoce*
  - *Priorisation des actions*
  - *Connaissance des tactiques d'attaque*
  - *Amélioration des capacités de défense*
  - *Réduction des risques*
  - *Collaboration et partage d'informations*

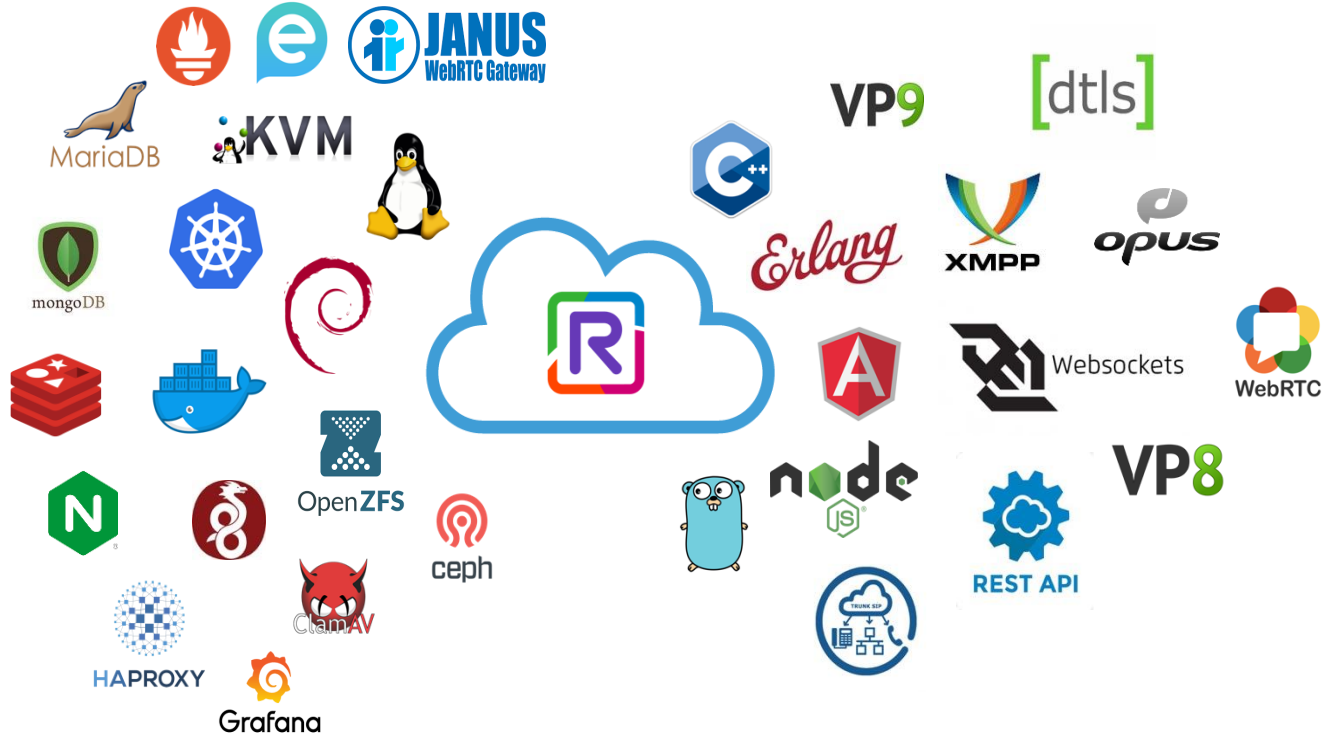


# EXEMPLE DE SOLUTION UCAAS

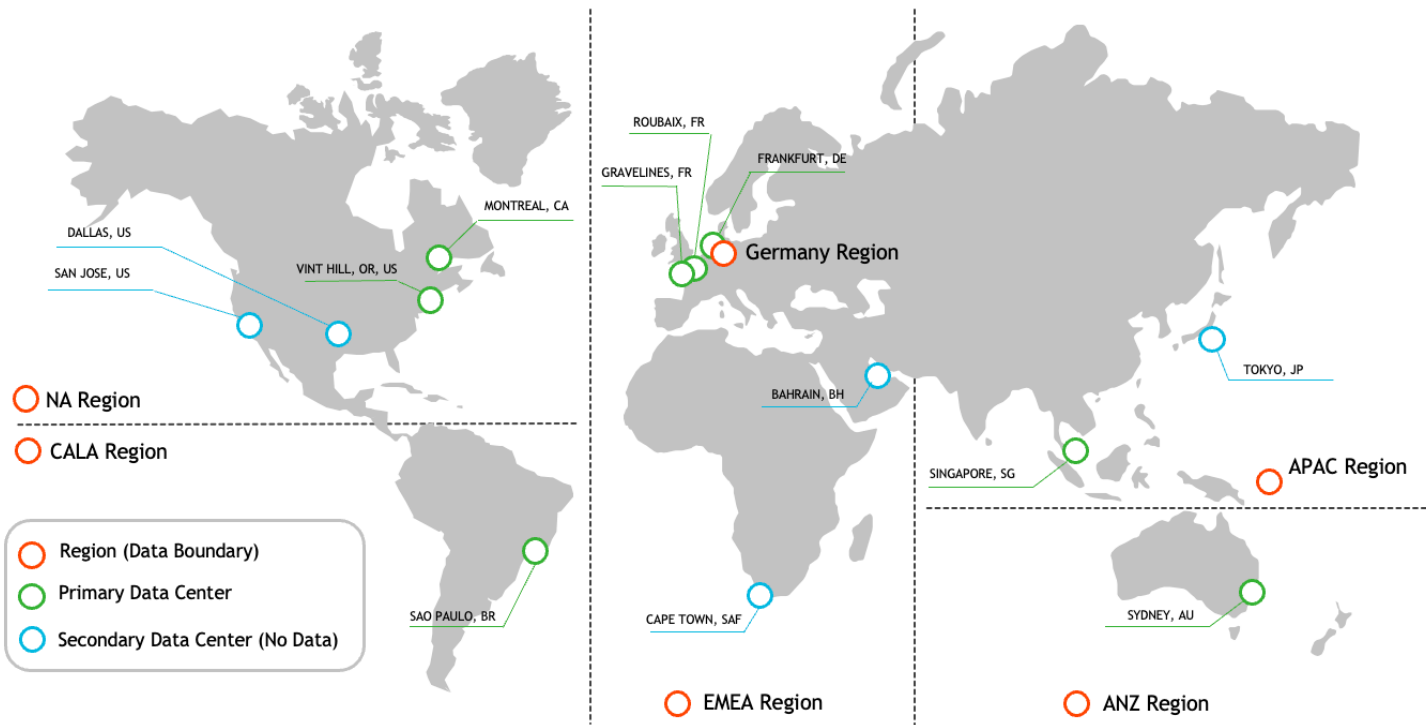




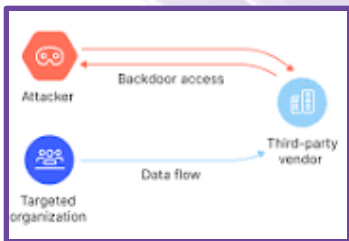
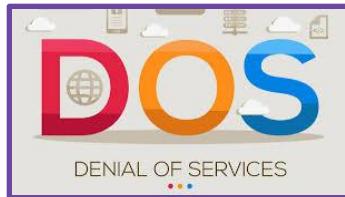
# UNE MASSE DE TECHNOLOGIES : OSS OU NON



# UNE INFRASTRUCTURE IMPORTANTE



# Veille de menace solution UCaaS : quelles stratégies ?

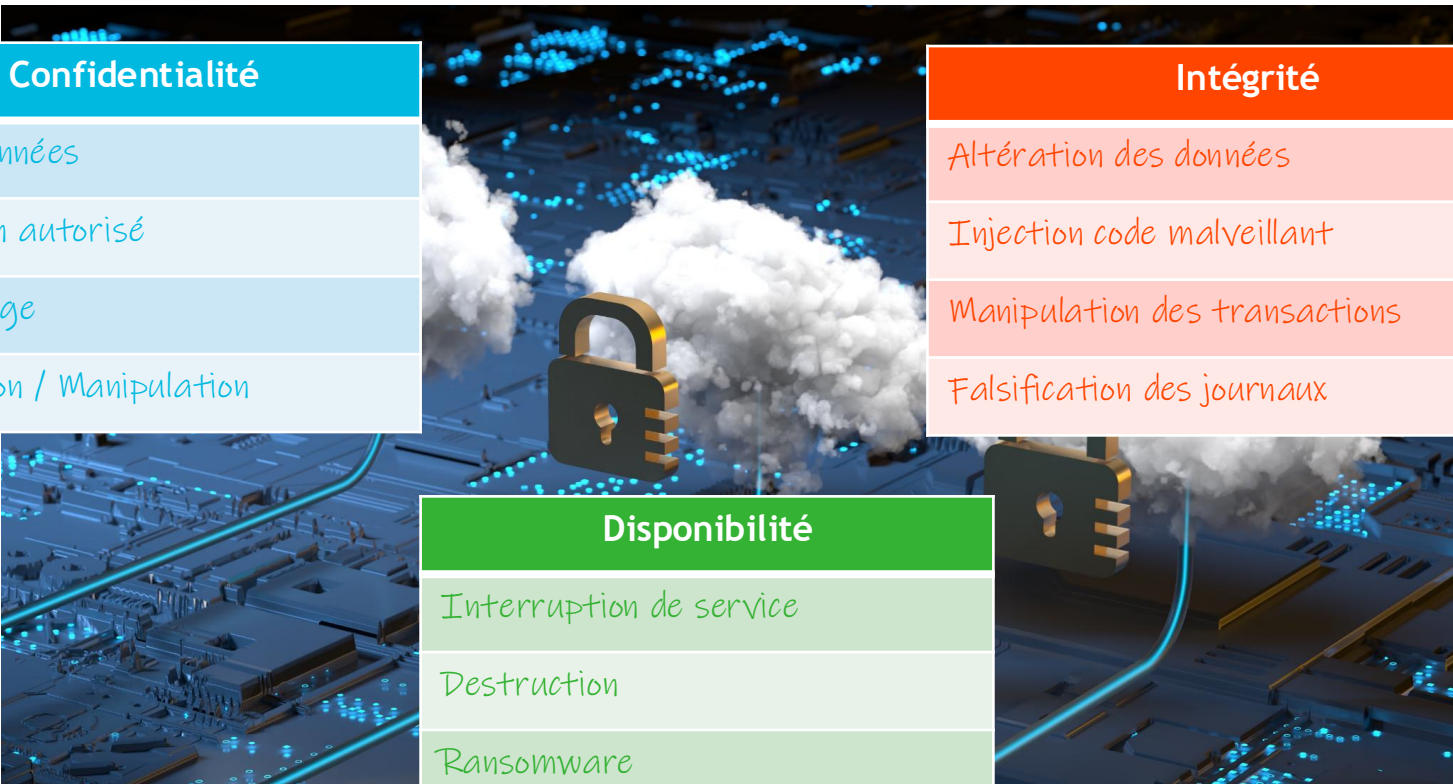


# Veille de menace solution UCaaS : les acteurs ?

Quelques groupes recensés pour notre domaine :

- LockBit
- BlackCat
- APT29 (Russie)
- APT42 (Iran)
- Lazarus Group (Corée du Nord)

# LE PROBLÈME DU CLOUD : LA DONNÉE



## Confidentialité

Vol de données

Accès non autorisé

Espionnage

Altération / Manipulation

## Intégrité

Altération des données

Injection code malveillant

Manipulation des transactions

Falsification des journaux

## Disponibilité

Interruption de service

Destruction

Ransomware

Défaillance des systèmes

# LE PROBLÈME DU CLOUD : LES NIVEAUX DE SERVICE DES VULNS

## Accord sur le niveau de service

Niveaux attendus par les clients

Signifie des engagements contractuels

**1 - Temps de réponse initiale**

**2 - Application correctifs critiques en x h**

## Objectif sur le niveau de service

Objectifs spécifiques et mesurables

Définissent des objectifs clairs

**1 - Temps de résolution des incidents critiques**

**2 - Taux de succès des correctifs appliqués**

## Indicateur sur le niveau de service

Métriques quantifiables pour mesure le respect de ONS

Permettent d'auditer les performances

**1 - Temps moyen de résolution des incidents**

**2 - Pourcentage des systèmes vulnérables après x délai**

# LE PROBLÈME DE LA RÉGLEMENTATION



# LE PROBLÈME DE LA RÉGLEMENTATION DE PLUS PRÈS

Règlementation	Point à observer
LPM 2024-2030	Article 66 LPM Obligation de notification à l'ANSSI pour les éditeurs de logiciels des vulnérabilités significatives
SecNumCloud 3.2	Article 12.11 sur la gestion des vulnérabilités techniques : mise en place d'un processus de veille
NIS2	Selon le document de travail de la transposition de l'ANSSI de la directive, on va retrouver l'ensemble des objectifs de sécurité
DORA	Principe de détection préventive des faiblesses i.e "vulnérabilités"
CRA	Obligation pour les fabricants de porter une attention particulière aux vulnérabilités



# RETEX

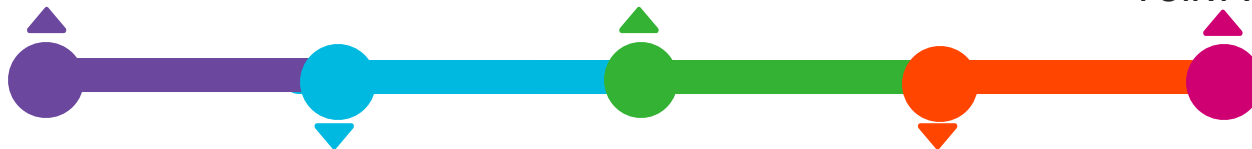




1er Juillet 2024  
Alerte du CERT-FR de  
l'ANSSI et analyse

4 Juillet 2024  
80% du parc du SI  
avec le correctif

16 Juillet  
Communication du  
bulletin de sécurité du  
PSIRT ALE



1er Juillet 2024

Correctif appliqué  
aux actifs critiques

8 Juillet

Annonce des médias  
sur de faux scripts  
d'exploitation

# RETEX



12 Janvier 2024

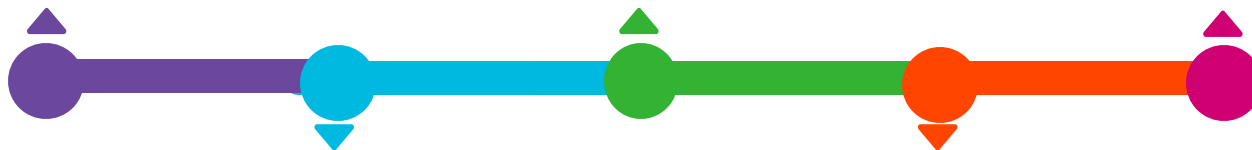
Alerte du CERT-FR de l'ANSSI et analyse

15 Janvier

Redémarrage sous conditions

18 Janvier

Mise à jour sécurisée vers instance corrigée



14 janvier

Isolation du serveur même si non affecté

15-18 Janvier

Audit complet du GitLab

# COMMENT FAIRE FACE A TOUT ÇA ?

## 1 – Définir une politique de gestion des vulnérabilités :

- **Fait partie de la PSSI**
- **Est associé à la cartographie des actifs de la solution**
- **Prévoit déjà les moyens de notifications des clients**
- **Doit prendre en compte les indicateurs de la solution en nuage (ANS, ONS, INS)**

# COMMENT FAIRE FACE A TOUT ÇA ?

## 2 – S'équiper en conséquence

- **Connaître ses capacités financières, matérielles et humaines**
- **Choisir les logiciels adaptés aux produits, technologies utilisés**
- **Ne pas tomber dans la surenchère d'outils**
- **Un VOC simple est un VOC efficace**

# COMMENT FAIRE FACE A TOUT ÇA ?

## 3 – Pratiquer des exercices de mises en condition

- **Plusieurs exercices par an de tous types**
- **Peut paraître chronophage mais bénéfique pour les équipes**
- **Revoir les procédures de remédiation pour limiter les impacts et accélérer le correctif final**
- **Permet aussi de sensibiliser tous les acteurs de la chaîne**

# COMMENT FAIRE FACE A TOUT ÇA ?

## 4 – Pratiquer une veille réglementaire :

- **Surveiller les publications des instances gouvernementales ou Européennes**
- **Permet d'anticiper des changements majeurs de la politique de gestion des vulnérabilités**
- **Permet de revoir ses indicateurs avant l'entrée en vigueur de lois**
- **La proactivité est la clé pour ne pas se laisser dépasser**

# THANK YOU

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE.

Alcatel-Lucent  
Enterprise 



# C O N T A C T U S



## WEBSITE

[www.al-enterprise.com](http://www.al-enterprise.com)

Follow us on:

