

Proposition du Resah sur le passage d'une sécurité périmétrique à  
une sécurisation des accès à privilèges

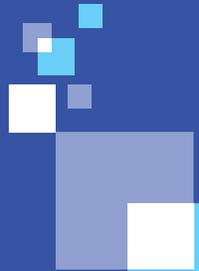
*Zero trust : le périmètre est mort, la confiance aussi !*

Hasina BESSE  
Directrice achats réseaux et télécom

Guillaume ROGER  
Chef de projet achat

Vincent BRANGER  
Consultant Expert

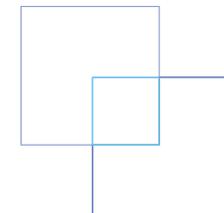
2024

resah 

# AGENDA

● Présentation du Resah

● Proposition du Resah sur le passage d'une sécurité périmétrique à une sécurisation des accès à privilèges



## Le centre de ressources et d'expertises

CONSEIL  
ÉDITIONS  
FORMATION  
SOLUTIONS  
INFORMATIQUES

guichet de l'acheteur  
hospitalier **responsable**

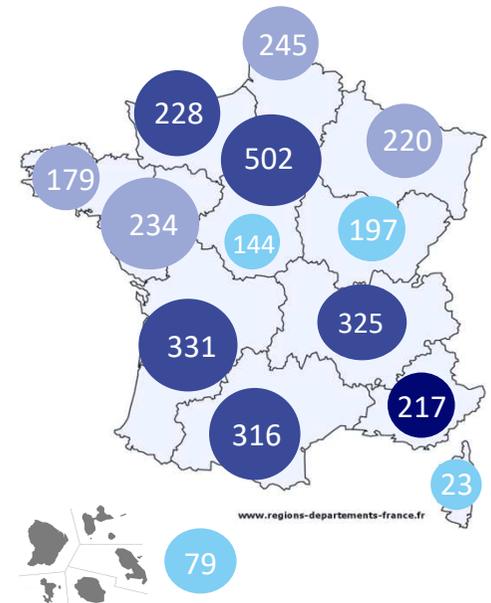


## La centrale d'achat



2 Mds €

1000



[www.regions-departements-france.fr](http://www.regions-departements-france.fr)

# Le marché 2023-R035



 Orange Cyberdefense

Fourniture de solutions – intégration – services managés – catalogue évolutif  
Accompagnement technique  
Audit de sécurité

 SPIE Capgemini

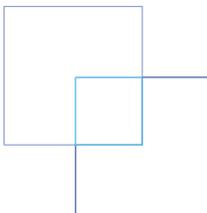
Accompagnement technique

 INTRINSEC AMOSSYS gDvens

Audit de sécurité

 France métropolitaine, DROM, COM

 Etablissements sanitaires, sociaux et médico-sociaux (+800 établissements aujourd'hui)



# Zero Trust : le périmètre est mort, la confiance aussi....

## Changement majeur de stratégie

- « Tout vérifier et ne jamais faire confiance »

## Principes essentiels :

- Aucun utilisateur, aucune machine, aucune application n'est automatiquement approuvée par défaut
- Notion de « moindre privilège » : chaque utilisateur a accès uniquement à ce dont il a strictement besoin.
- Micro-segmentation : isolation stricte des utilisateurs, réseaux, serveurs
- Authentification multi-facteur
- Contrôle strict de tout appareil ayant accès au réseau (localisation, type...)
- Management global centralisé : gestion unifiée des politiques de sécurité

## Impose la vérification de l'identité

- d'une personne et de tout matériel
- qu'il soit à l'intérieur ou à l'extérieur du réseau d'entreprise

## Processus long

- se concentrer d'abord sur les données et applications les plus critiques



# Zero Trust : attention aux mythes !

C'est juste du marketing !

Faux ! Zero Trust est une approche stratégique de cybersécurité, pas un simple buzzword.

C'est juste un produit à implémenter !

Faux ! Zero Trust est un concept, pas une solution clé en main.

C'est finalement qu'une gestion de l'identité !

Non ! Cela inclut la gestion de l'identité, mais aussi la segmentation, la surveillance....

C'est trop compliqué !

Complexe, certes, mais avec une mise en œuvre progressive, il est réalisable pour toute organisation.

Zero Trust est suffisant !

Non ! Elle doit être combinée avec d'autres mesures de défense

Zero Trust, ça ne se fait qu'une seule fois !

Faux ! C'est un processus continu qui s'adapte aux nouvelles menaces et évolue avec en permanence

Ce n'est que pour les grandes entreprises !

Non ! Toutes les organisations, petites ou grandes, peuvent bénéficier du modèle Zero Trust.



# Les offres Réseaux & Télécom



2023-R035 Sécurité des Systèmes d'Information



2024-R056 Fourniture de ressources cloud, d'hébergement sec et d'infogérance



2023-R046 Fourniture de ressources cloud et cloud de confiance



2023-R036 Services opérés de télécommunications



2021-046 Infrastructures et solutions de télécommunications



2023-R089 Fourniture et mise en œuvre de solutions multimédias en chambres



2022-025 Fourniture & mise à disposition solution logiciel de vote électronique



2022-038 Expertise indépendante vote électronique

