AGENCE DU NUMÉRIQUE EN SANTÉ

GHT DE LA RÉUNION
Groupement Hospitalier de Territoire

CERT Santé

# Retour d'Expérience

## Incident du GHT La Réunion

# Contexte d'intervention

## CHU de La Réunion

/ Région : **La Réunion**

/ **1900 lits, 7330 professionnels (dont 1014 ETP médicaux)**

/ **1014 ETP médicaux, 686 médecins seniors**

/ **Architecture**

- **3 domaines**
- **15 établissements concernés rattachés à l'AD**
- **900 serveurs**

## Origine(s) de la crise

- **Signalement du 06/02/2023 au CERT Santé**
- Systèmes concernés : Serveur AD, serveurs applicatifs (Citrix), postes de travail
- Incident détecté par le SoC :
  - **Scan réseau**
  - **Exécution de Mimikatz**
  - **Déploiement de RAT (Atera)**

## Risques identifiés*

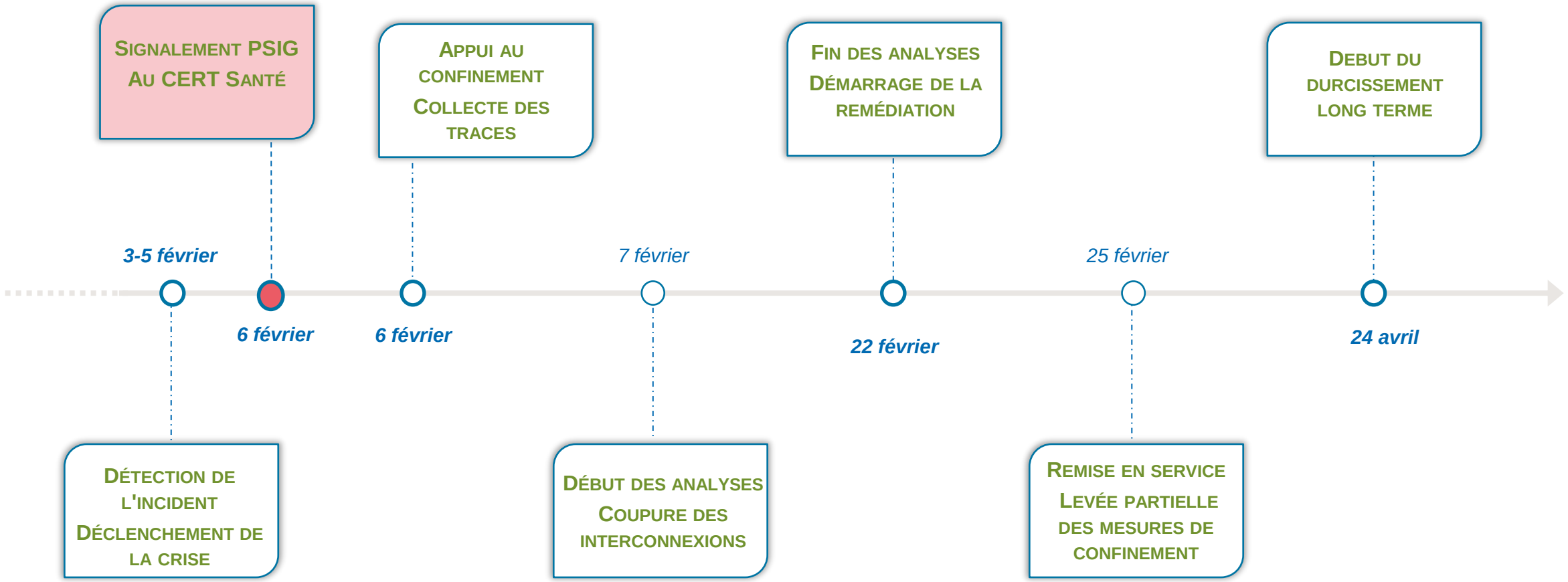
- **Prise de contrôle à distance** des équipements
- **Compromission d'identifiants sur plusieurs comptes à privilèges**
- **Compromission globale du domaine, risque de chiffrement**
- **Risque d'exfiltration de données : interconnexion avec les domaines du CHU**

** Enumération des risques identifiés en cas de succès de l'attaque.*

# Chronologie de la crise

Accompagnement du CERT Santé

Actions du CENTRE HOSPITALIER



# Chronologie de l'attaque

**03/02/2023 07:41**

**Login compte de service**

- Connexion depuis l'exterieur
- Non légitimée
- Compte de service

**03/02/2023 19:35**

**Login compte utilisateur**

Action non légitimée

- Ip extérieure non reconnue

**03/02/2023 23:04**

**Première instance d'Atera observée**

- Outil non légitimé par la DSI
- Traces d'exécution

**05/02/2023 15:19**

**Connexion admin entre deux postes**

- Latéralisation compte admin entre 2 postes de travail

**05/02/2023 16:03**

**Login compte admin sur poste de travail**

- Action non légitimée
- Relais vers une connexion DC

**05/02/2023 16:18**

**Login compte admin compromis sur DC**

- Compromission totale du domaine

**05/02/2023 09:49**

**Latéralisation compte de service sur serveur de fichiers**

**06/02/2023 14:50**

**Exécution de mimikatz sur serveur DC**

- Exfiltration d'identifiants
- Compromission du domaine

# Aide à la reconstruction

**22/2/23**

**DÉFINITION D'UN PLAN DE REMÉDIATION ET ACCOMPAGNEMENT DU CERT SANTÉ**

/ Les principaux **axes mis en œuvre** sont :

- **Segmentation réseau** du système d'information
- **Réduction de l'obsolescence** du parc informatique (plus particulièrement sur les machines/équipements critiques)
- **Durcissement** des machines/équipements
- **Changement** des **pratiques** d'administration du système d'information
- Déploiement de nouveaux **outils de sécurité**

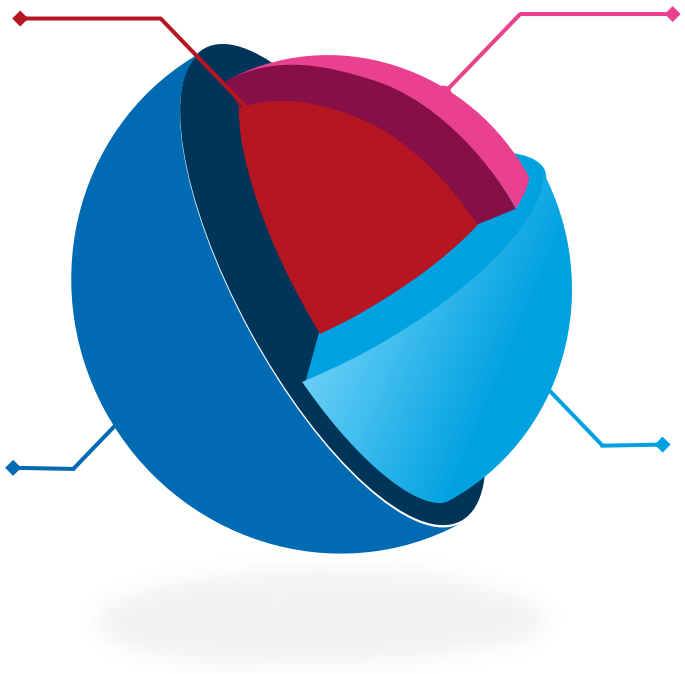
## Les étapes du déploiement du plan de remédiation

### 1. Services critiques / socle SI

S'assurer que le cœur de l'infrastructure est sécurisé

### 2. Services métiers

Contrôler les périmètres métiers et reprendre peu à peu un usage standard



### 4. Interconnexions et services exposés

Rétablir les connexions extérieures et les solutions de surveillance

### 3. Postes de travail

Remettre en service les postes de travail pour tous les collaborateurs

# Bilan de l'accompagnement

Rappel de la chronologie des évènements

***5 février 2023 :***
*Déclenchement de l'incident et ouverture d'une cellule de crise par le GHT*

***6 février 2022 :***
*Prise en charge par le CERT Santé*
*Début de l'investigation*

*7 février 2023 :*
*Application des mesures de confinement*
*Coupure des interconnexions*

***22 février 2023 :***
*Fin de la phase d'analyse et démarrage de la remédiation*

*25 février 2023 :*
*Levée partielle des mesures de confinement*

***24 avril 2023:***
*Début de la phase de durcissement*

## Résultats et éléments clés

La réactivité du CERT Santé, l'investissement du GHT La Réunion & de ses prestataires ont permis d'**éviter une sur-compromission du système d'information** de l'établissement

**Plusieurs identifiants et comptes ont été exfiltrés** au cours de l'incident

Des postes de travail ont été compromis et **accédés depuis l'extérieur**. Aucune fuite de données n'a été observée

## Points à retenir

1. **Une mise à disposition d'experts en cybersécurité pour les établissements** afin de les accompagner et les aider face à ces situations complexes

   Accompagnement au déploiement des capacités et moyens nécessaires afin de réaliser des investigations plus poussées

2. Importance de la **collaboration** pour la **résolution d'incident** de sécurité

   Travail conjoint sur les mesures de remédiation suite à l'identification des faiblesses intrinsèques au SI et réalisation d'investigation afin de confirmer les hypothèses de la compromission