AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Retour d'Expérience

Un établissement victime du chiffrement d'une partie de ses environnements virtualisés

Contexte d'intervention

Caractéristiques de l'organisation ciblée

- **Groupement d'intérêt public :**
  - Conception, déploiement et hébergement de systèmes d'information
  - **Plusieurs centaines** de collaborateurs sur l'ensemble du groupement
  - accompagne plusieurs **centaines** d'établissements de santé et collectivités

Origine(s) de la crise

- Intrusion sur le SI suite **à l'exploitation d'une mauvaise configuration du pare-feu** et la compromission d'un compte de l'Active Directory (AD) par une attaque par **force brute**
- Une **compromission d'un compte à privilège de l'AD** a ensuite été effectuée
- Accès au **serveur de sauvegarde**, avec l'utilisation d'un script de l'éditeur

Impacts et Risques identifiés

Impacts

- **Chiffrement** des disques virtuels sur lesquels étaient stockés les VM

Risques

- **Exfiltration** de données

Chronologie détaillée de l'incident

Compromission et actions illégitimes

15 février 2024 – 12:30-12:49

Accès initial

- Attaque par force brute de différents comptes
- Connexion réussie sur un compte AD

15 février 2024 – 12:56

Tentatives de connexion

- Plusieurs tentatives de connexion depuis le compte administrateur vers le serveur Oracle

15 février 2024 – 13:55-14:21

Connexion sur le serveur de sauvegarde

- Connexion de l'attaquant en RDP sur le serveur de sauvegarde
- Activités de reconnaissance

15 février 2024 – 14:39-14:46

Déploiement d'outils

- Tentative de téléchargement d'outils malveillants
- Dépôt de l'outil de chiffrement

15 février 2024 – 14:46-14:49

Chiffrement

- Chiffrement du serveur de sauvegarde
- Chiffrement du serveur BDD

Actions de l'établissement

15 février 2024 – 14:39

Première Détection antivirale

- Détection par l'anti-virus d'un exécutable (bloqué)

15 février 2024 – 15:10

Déclenchement de la cellule de crise

- Alerte du SOC

15 février 2024 – 15:25 – 19:15

Nouvelle Détection antivirale

- Les VMs encore fonctionnelles ont été redémarrées
- Qualification de l'incident

16 février 2024

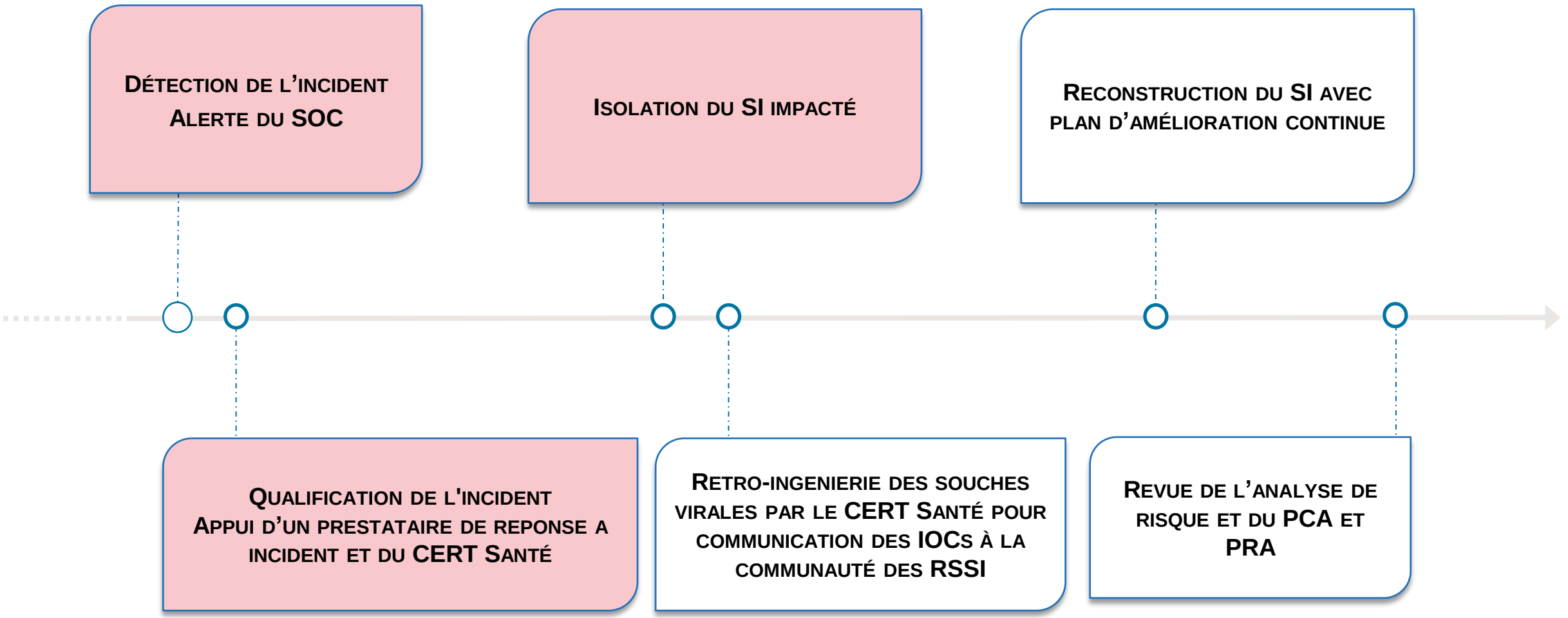
Lancement Intervention

- Intervention d'un prestataire de reponse a incident et du CERT Santé

Chronologie des actions post-détection

DURANT LA CRISE

SUITE À LA CRISE



*Evènements identifiés à postériori grâce à l'investigation

Accompagnement post- crise

FÉVRIER 2024

ACTIONS MISES EN ŒUVRE EN SOUTIEN DE LA CRISE

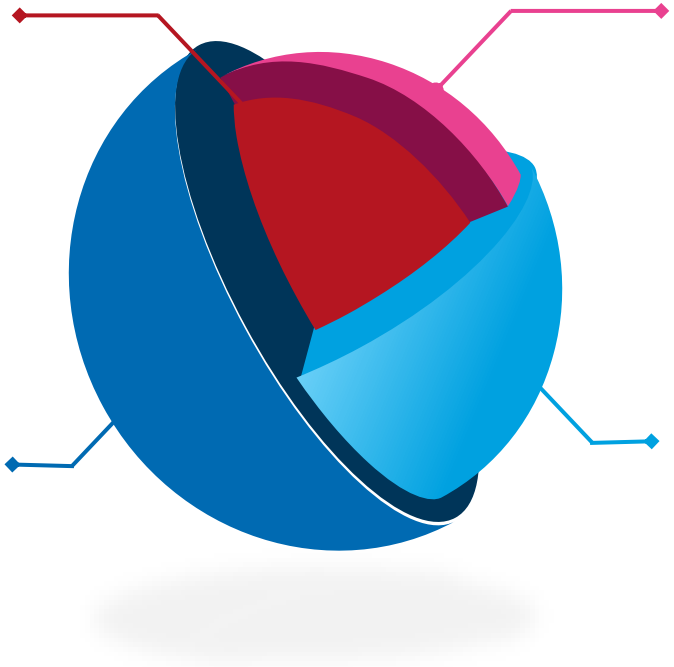
/ Les principaux **axes mis en œuvre** sont :

- **Transmission de consignes** de remédiation
- **Relais de communication** aux RSSI Santé
- **Co-pilotage des actions** d'investigation
- **Analyse des souches virales** transmises et **partage du compte-rendu** à la communauté

Les étapes du déploiement du plan de remédiation

1. Alerter les entités compétentes

Alerter le SOC, le prestataire de réponse à incident et le CERT Santé pour assister à la gestion de la crise



2. Isolation du SI

Empêcher une propagation de l'attaque sur le reste du SI

3. Revue de l'analyse de risques

Revoir l'analyse des risques en prenant en compte les leçons de la crise

4. Renforcement du PRA et PCA

Renforcer le PRA et PCA suite à l'incident et aux leçons apprises.

Bilan de l'accompagnement durant la crise

Rappel de la chronologie des évènements

12:30 - 12:49 :
Connexion réussie sur un compte AD en brut forçant avec différents comptes

12:56 :
Tentatives de connexion sur le serveur BDD

13:55 :
Connexion en RDP sur le serveur de sauvegarde

14:46 :
Tentative de déploiement d'outils
Dépôt de l'outil de chiffrement

14:46 - 14:49 :
Chiffrement du serveur de sauvegarde
Chiffrement du serveur BDD

15:10 :
Alerte du SOC

Résultats et éléments clés

L'attaquant **a exploité une mauvaise configuration du pare-feu** puis a réalisé une attaque par **force brute d'un compte de l'Active Directory** pour avoir un accès initial au SI.

L'ensemble des **disques virtuels sur lesquels étaient stockées les VM est chiffré**. Un redémarrage de certaines machines a permis à l'attaquant de couper complètement l'accès aux machines virtuelles.

Points à retenir

1. Importance de **vérifier la pertinence de la configuration des outils de surveillance et d'assurer** la prise en charge des **alertes**

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

   Réalisation d'analyses afin de confirmer les hypothèses de la compromission et travail conjoint sur les mesures de remédiation suite à l'identification des faiblesses du SI

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé