Présentation des activités du CERT Santé

Mars 2025

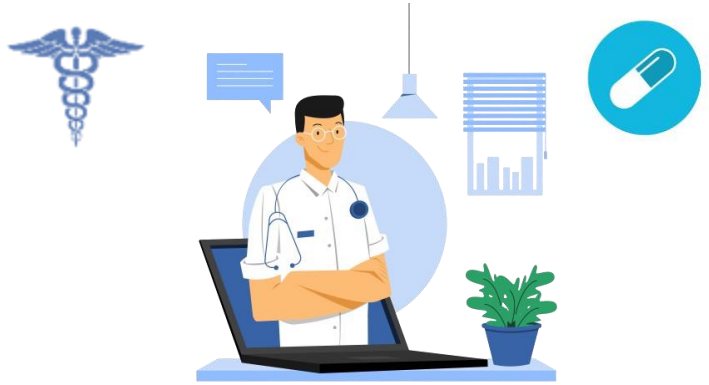
Bénéficiaires du CERT Santé

2211 ES* publics
(dont 898 regroupés en 135 GHT*)
1482 ES privés lucratifs
880 ES privés à but non lucratifs

35 000 établissements sociaux et médico-sociaux, centres de radiothérapie, 500 laboratoires de biologie médicale

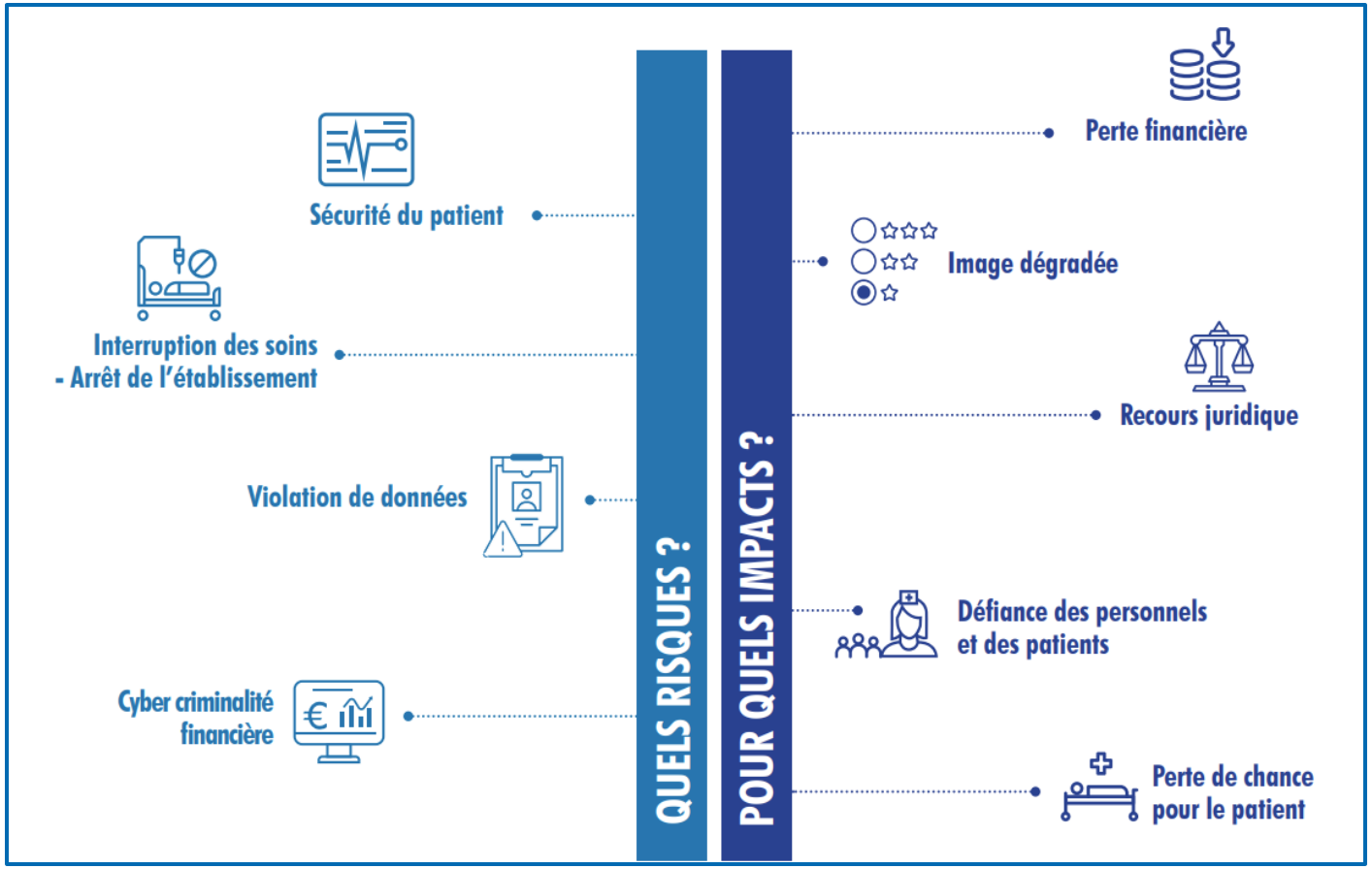
… au service de plus de
67,8 millions d'usagers citoyens

Ne font pas partie de nos bénéficiaires



2 millions de professionnels de santé libéraux,
20000 officines, 2000 centres de santé

- Une menace continue et en croissance
  des tensions internationales et un appel au « renforcement de la vigilance cyber »
- Une exposition réelle des établissements de santé et du médico-social
  victimes d'attaques par rançongiciel par ex
- Des impacts importants en cas d'incident
  Interruption prolongée des applications
  Perte irréversible de données
  Travail en mode dégradé pendant plusieurs semaines



Sources : Observatoire des incidents et des vulnérabilités du CERT Santé

Les missions du CERT Santé

Réponse à incidents

- Traitement des déclarations d'incidents de sécurité
- Intervention d'urgence à distance H24 7j/7

https://signalement.social-sante.gouv.fr

Intelligence de la menace & veille proactive

- Veille sur les vulnérabilités / campagnes d'exploitation / fuites de données
- Envoi d'alertes

https://www.cyberveille-sante.gouv.fr

Sensibilisation - partage

- Animation d'une communauté de RSSI/DSI autour de la SSI en santé

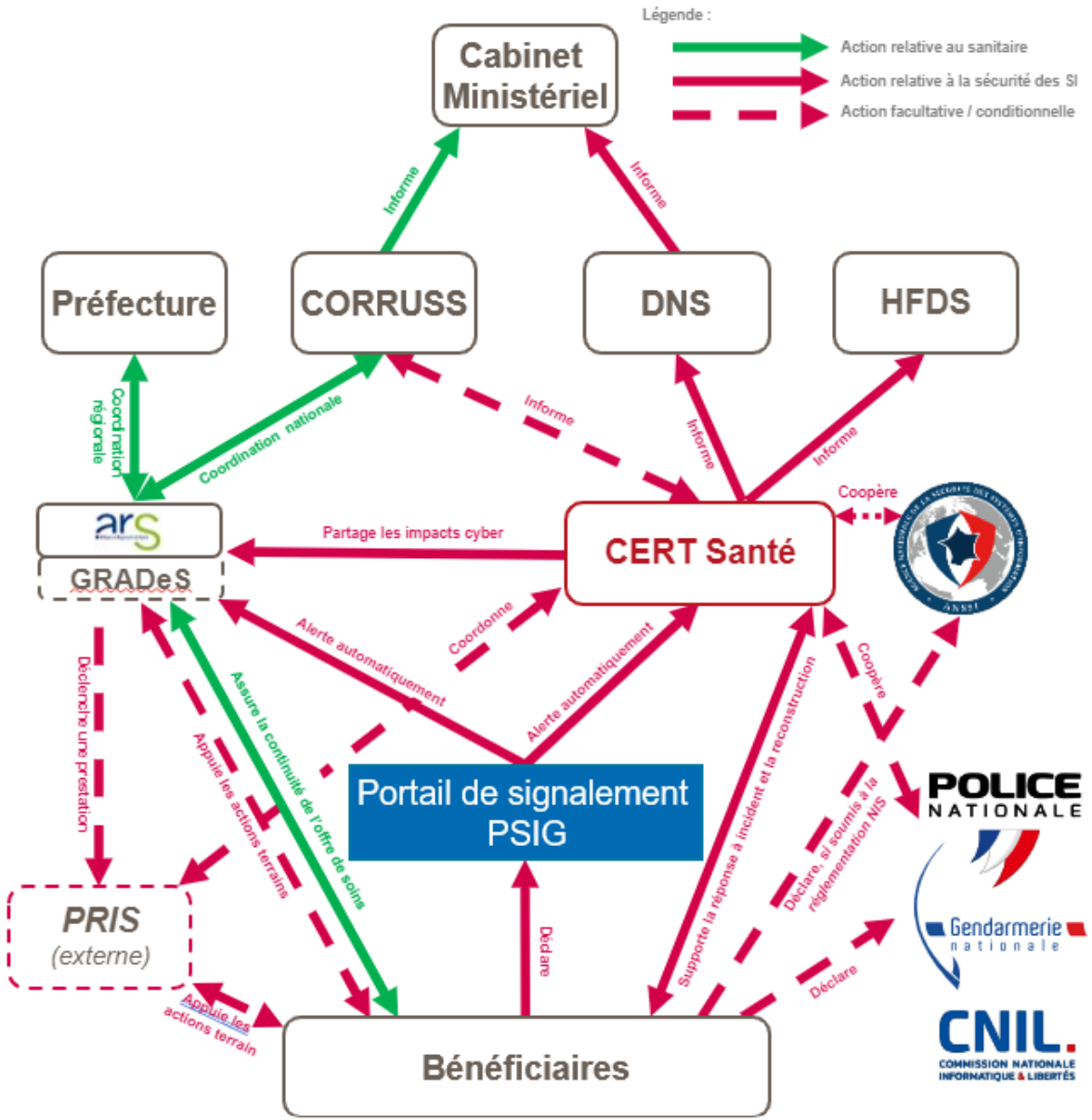
Audits

- Exposition sur Internet des SI des ES et ESMS

Présentation des services :
https://www.cyberveille-sante.gouv.fr/les-services

Règlementation relative au signalement des incidents de sécurité

- Article L. 1111-8-2 du code de la santé publique prévoit **l'obligation de signalement des incidents de sécurité.**
- Le décret n° 2022-715 du 27 avril 2022 décrit les **conditions selon lesquelles sont signalés les incidents graves** de sécurité des systèmes d'information.
- L'arrêté d'application du 30 octobre 2017 relatif **aux modalités de signalement et de traitement** des incidents



Les grandes étapes de la réponse à incidents

QUALIFICATION

1

Réaliser une première **évaluation d'un incident** et de ses impacts avérés ou potentiels, et de le partager si nécessaire

CONFINEMENT

2

Partager un ensemble de recommandations pour **isoler une partie du SI** en cas d'incident de cybersécurité

INVESTIGATION

3

Rechercher les origines et les modalités d'une attaque informatique, ainsi que les éléments du SI qui sont compromis

REMEDIATION

4

Mettre en place les premières mesures permettant de sécuriser à nouveau le système d'information afin de bloquer l'attaquant

En fonction du contexte, ces étapes peuvent être réalisées simultanément

DURCISSEMENT

5

Renforcer la sécurité afin d'**être plus résilient face** à la menace cyber existante

Accompagnement optionnel et dépendant du niveau de sécurité du SI

En fonction de la criticité de l'incident et du diagnostic défini, le CERT Santé peut éventuellement accompagner sur la reconstruction du système d'information compromis

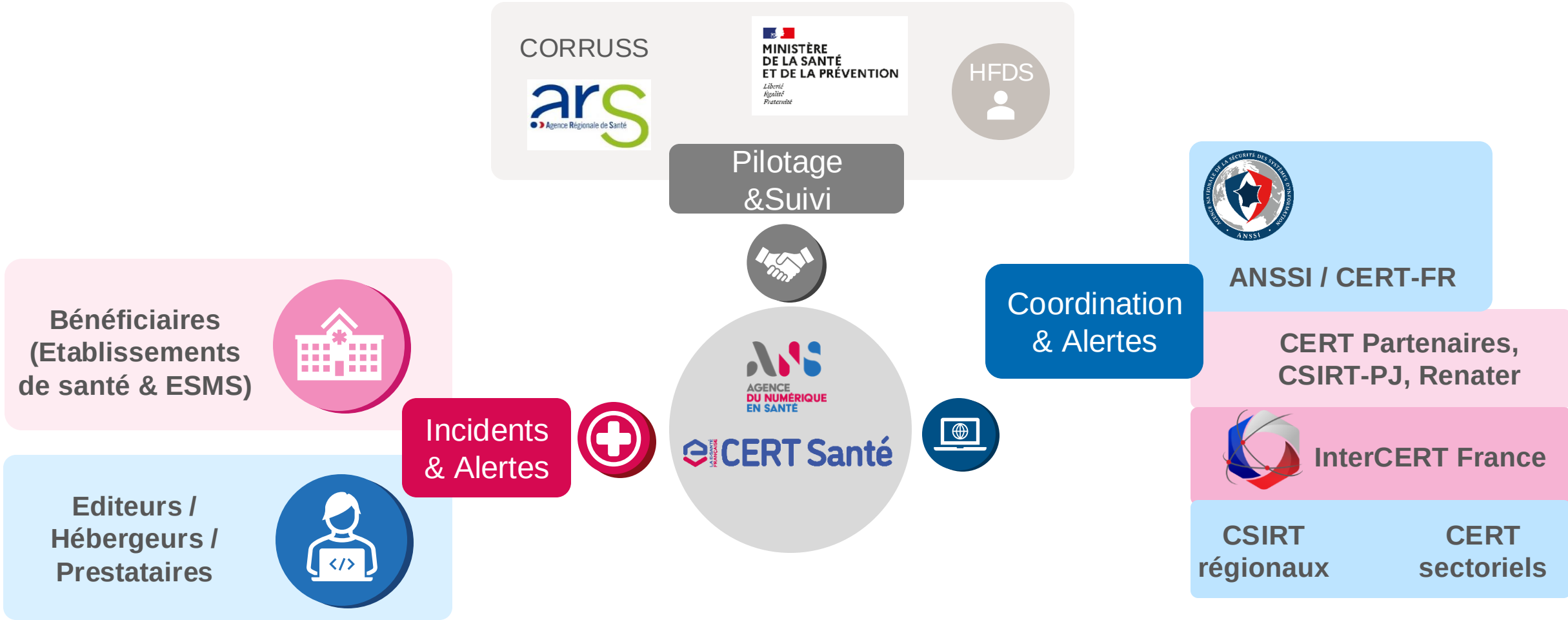
Une veille quotidienne afin d'alerter les structures dès la publication de la vulnérabilité

Des vulnérabilités permettant d'exécuter du code arbitraire, de réaliser des dénis de service, etc.

95

alertes critiques publiées sur le portail cyberveille-santé

Panorama des acteurs de l'écosystème



Exposition

Lister et maîtriser les services et ports exposés

MFA

Mettre en place de l'authentification double facteur sur les accès critiques ou exposés

Sauvegardes

Sécuriser et structurer ses protocoles de sauvegarde

Journaux

Centraliser la gestion des journaux

Cartographie

Etablir et maintenir à jour la cartographie du SI

Comptes

Mise en place d'une gestion des comptes et utilisateurs

Anticiper les incidents

Sensibiliser

Sensibiliser les agents et équipes aux risques de sécurité afin **d'augmenter sa résilience et sa réactivité**

Maintenir à jour

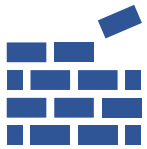
Améliorer le **suivi** et la **correction des vulnérabilités classiques**

Analyser les logs

Analyser **régulièrement les journaux de ses systèmes** et **équipements périmétriques**

Exercices de crise

Réaliser des exercices de crise **répétés** et de **formats différents** permet de se **préparer** au mieux en cas de **véritable incident**.



Outils tiers

Anticiper les **vulnérabilités et failles** d'outils tiers en **adaptant son architecture et ses usages** à leur fonctionnement.

Gestion des prestataires

Inclure un engagement du prestataire sur le **maintien en conditions de sécurité de son infrastructure**

En cas d'incident il est impératif de **solliciter rapidement le CERT Santé**. Plus tôt l'incident est signalé, plus grande est la probabilité de **contenir et de résoudre la situation de manière rapide** afin de garantir la continuité des services de santé.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

CERT Santé

Tel : 09 72 43 91 25
Mail : cyberveille@esante.gouv.fr
https://www.cyberveille-sante.gouv.fr/