LE CONSEIL DU NUMÉRIQUE EN SANTÉ

9ème Conseil du numérique en santé (CNS)

Jeudi 15 juin 2023

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

LE CONSEIL DU NUMÉRIQUE EN SANTÉ

Programme CaRE

Cyber Accélération pour la Résilience des Etablissements

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Des investissements identifiés

1. Identification de 4 domaines techniques prioritaires pour répondre à la menace de rançongiciel et d'exfiltration de données

Une démarche globale centrée sur les ES, s'appuyant sur les acteurs nationaux, régionaux, et le tissu industriel expert

- **D1 – Audits techniques**
  Annuaire technique et exposition sur internet
- **D2 – Poste de travail et détection**
- **D3 – Sécurisation des accès de télémaintenance**
- **D4 – Stratégie de sauvegarde**

Prioritaire

Les cyberattaques récentes montrent que **l'exposition internet** est l'un des vecteurs principaux de pénétration par les attaquants dans le système d'information des établissements de santé.

L'Annuaire Technique est ensuite le principal moyen de propagation, par lequel les attaquants obtiennent des privilèges élevés, leur permettant d'infliger plus de dégâts.

2. Financement "pérenne" à prévoir

Via des financements annuels conditionnés à l'atteinte d'objectifs "socle Cyber"

- Conditionné à des prérequis numériques et cyber (prérequis Ségur numérique, exercices de crise réguliers…) qui s'adaptent dans le temps aux scenarios d'attaque et à la maturité des ES
- Contribution partagée à la mission chargée de la réforme de la tarification MCO

3. Développement de l'offre de services « cyber » au niveau national et régional

Via des financements associés en cohérence avec les objectifs à atteindre par les ES

- Une offre cohérente et articulée entre l'ensemble des entités
- Appui des GRADeS dans le développement et l'homogénéisation de leurs centres de ressources régionaux (CRRC) via la définition d'un socle minimal

Genèse et ambitions de la Task Force

Multiplication des attaques dans les établissements sanitaires

- **Impacts très forts** sur la qualité et la sécurité de prise en charge des patients
- **Développement croissant** des usages du numérique dans les ES
- **Augmentation générale** de la cybermenace et professionnalisation des attaquants

x2 : nombre d'incidents déclaré par les ES depuis 2020

3ème secteur le plus touché par des attaques par rançongiciel

1,6 % : budget hospitalier dédié au numérique (part en diminution)

Lancement de la TF cyber suite à la cyberattaque du CHSF

Des ambitions :

- Concevoir un **plan massif pluriannuel** sur 2023-2027
- Une volonté **d'engager une grande majorité des ES** sur 2023-2024
- Obtenir des **résultats concrets** dès maintenant pour la résilience des ES
- **Accompagner l'ensemble des ES** dans leur montée en maturité sur la cybersécurité

Des financements :

- « **Ponctuel** » pour permettre de franchir un cap
- « **Annuel** » pour maintenir le niveau acquis et considéré comme le « Socle Cyber »
- « **Offre de services** » pour développer et coordonner l'offre de services nationale et régionale, pour un déploiement massif au sein des ES

Programme CaRE

« Une réponse collective, déterminée et coordonnée pour faire face à la menace »

LE CONSEIL DU NUMÉRIQUE EN SANTÉ

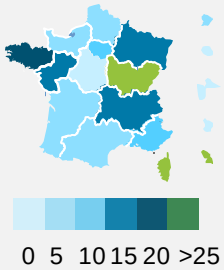
Des actions déjà engagées collectivement

1. Un effort sur la résilience

EXERCICES DE GESTION DE CRISE

% ES ayant réalisé un exercice à fin-mai sur la base des kits nationaux

415 exercices déjà réalisés



PLAN BLANC NUMERIQUE

- Volet numérique du plan blanc finalisé
- Publication imminente

PCA / PRA

- Travaux qui s'inscrivent dans la **continuité des exercices de crise** et des kits nationaux
- Lancement d'un groupe de travail pour construire **un kit clé en main pour les ES**
- **Ambition** : premiers pilotes à l'automne et publication du kit fin d'année

2. Un ancrage du numérique et de la cyber-résilience dans la certification HAS

- **Impliquer les directions d'établissement, les PCME et l'ensemble des professionnels des ES** à se préparer à la cybercrise : réalisation des exercices de crise, formalisation et mise en œuvre des PCA/PRA/modes dégradées, intégration d'un plan de formation SSI, acculturation à l'hygiène informatique, réalisation des audits réguliers

3. Une évolution des grilles RH

- **Renforcer l'attractivité des métiers de la DSI et de RSSI**

4. Un portail cyber « point d'entrée » unique

- Ouverture prochaine d'un **espace dédié** sur le portail esanté.gouv.fr
- **Référencement** de tous les outils, documents, offre de services à destination des ES

5. Des actions de communication et de sensibilisation

- **Intervention à SantExpo** via plusieurs RETEX (ES attaqués, exercices de crise) et la présentation du programme CaRE
- **Une campagne « Tous Cybervigilants »** V2 en cours de finalisation à destination des directions d'établissement puis des professionnels
- **Evènements réguliers** au niveau national et régional autour de la cyber

LE CONSEIL DU NUMÉRIQUE EN SANTÉ

HAUTE AUTORITÉ DE SANT

Un ancrage du numérique et de la cyber-résilience dans la certification HAS

Impliquer les directions d'établissement, les PCME et l'ensemble des professionnels des ES à gérer les risques numériques :

- Action de sensibilisation et acculturation à l'hygiène informatique,
- Formalisation et mise en œuvre des PCA/PRA et procédures en mode dégradée,
- Intégration d'un plan de formation aux risques d'usage du numérique en santé,
- Réalisation des exercices de crise,
- Définition de plan d'action formalisé suite à la réalisation des audits réguliers

Développer certains critères d'évaluation autour des services socles du numérique en santé (INS, DMP, MSS)

Groupe de travail d'experts → **Elaboration des critères d'évaluation** → **Concertation des parties prenantes** → **Evolution des fiches pédagogiques** → **Application des critères en 2024**

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Recrutement puis formation des experts visiteurs à compétence numérique. Diffusion de ses ajustements aux ES pour leur bonne appropriation.

Evolution de la certification HDS

- **Une certification qui a fait ses preuves :** 238 hébergeurs certifiés, de la start up à la multinationale par 8 organismes certifiés COFRAC depuis juillet 2018.

- **Des axes d'amélioration :** activité 5 d'administration et d'exploitation du système d'information, périmètre des prestations couvertes par la certification,…

- Prendre en compte les **évolutions** du contexte normatif (ISO 27001) et réglementaire (SecNumCloud,…)

- **Risque de transfert de données** Hors de l'Espace Economique Européen et souveraineté : règles de transparence avant un renforcement de ces règles en 2027

Déc 2022	Fin de concertation
Mai 2023	Saisine CNIL
Juil. 2023	Publication et Notification à l'Union Européenne
Oct. 2023	Publication de l'arrêté approuvant le nouveau référentiel

LE CONSEIL DU NUMÉRIQUE EN SANTÉ

Une accélération des exercices de gestion de crise

Une dynamique qui se confirme sur le terrain et des ambitions fortes

- **Industrialisation des exercices** via la mise à disposition de kits nationaux avec 3 niveaux de maturité
- L'objectif est **d'atteindre 50% des ES à fin 2023** et **100% fin 2024**
- Démarche qui **doit devenir annuelle** au sein des ES
- De premiers **exercices à l'échelle régionale** commencent à se tenir

Des retours extrêmement positifs

- **Atteinte des objectifs fixés en amont de l'exercice**
- **Simulation réaliste d'une crise cyber**
- **Identification des axes de progression**

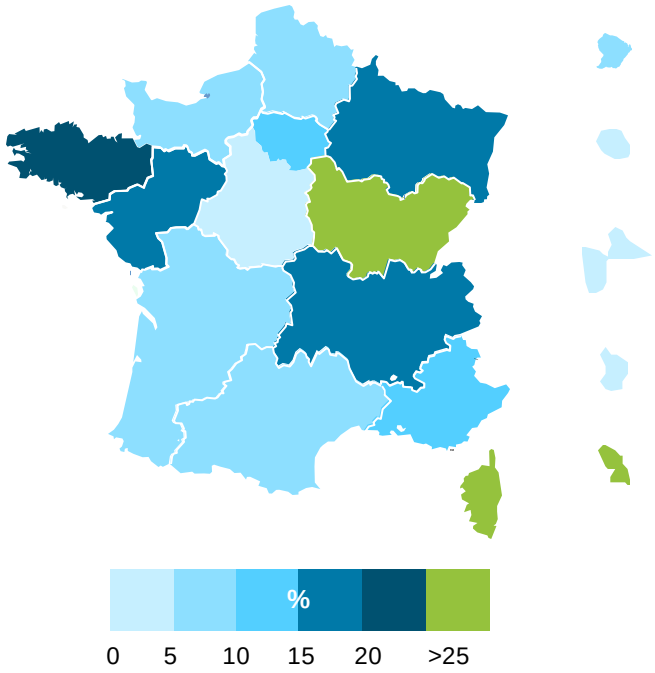
85%

Satisfaction globale des participants en Pays-de-la-Loire

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Exercices réalisés à fin mai 2023



- **15% des ES** ont réalisé un exercice à fin mai 2023 (dont 78% des OSE)
- Rappel de l'objectif des DDG Régions : 25% à fin mai pour les ES et 100 % pour les OSE

Une feuille de route cybersécurité pour le médico-social

La transformation numérique du secteur social et médico-social s'accompagne d'une exposition croissante au risque cyber. **Le risque est avéré** pour les ESMS et les personnes accompagnées.

Au premier semestre 2023, le chantier **cybersécurité social et médico-social** a permis de mener :

- Une concertation auprès **de 60 organismes gestionnaires**
- **8 ateliers de co-construction** avec les acteurs du secteur
- Un **plan d'action 2023/2027 ambitieux, adapté, et cohérent** avec la feuille de route sanitaire.

87 incidents signalés par des ESMS en 2022

Une feuille de route cybersécurité pour le médico-social

1	2	3	4	5
Gouvernance du plan cybersécurité	**Stimuler la mutualisation des ressources cyber**	**Sensibiliser l'écosystème**	**Accompagner la mise en conformité réglementaire**	**Accompagner l'acquisition d'outils**
Une dynamique portée collectivement par les acteurs du secteur	Un levier pour investir dans la sécurité des structures	Former et acculturer les professionnels du secteur	Un cadre à adapter en lien avec les spécificités des ESSMS	Fournir les outils nécessaires à la cybersécurité

LE CONSEIL
DU NUMÉRIQUE
EN SANTÉ

Contact
contact@cns.com
06.00.00.00.00