Programme Cyber Accélération et Résilience des Etablissements (CaRE)

Task Force Cyber

Journée de la cybersécurité en Ile-de-France

Task Force Cyber – Présentation générale

La création d'une Task Force Cyber a été annoncée au cours de la RIM du 21/12/2022. L'objectif premier de cette Task Force est de construire un plan cyber pluriannuel massif (2023-2027). La co-construction de ce plan va mobiliser à la fois les institutions nationales et les acteurs régionaux.

Composition et structuration de la Task Force

Participants

Pilotes : DNS (pilotage) + ANS (co-pilotage)

Membres : FSSI, DGOS, ANSSI, ANS, ARS, GRADeS

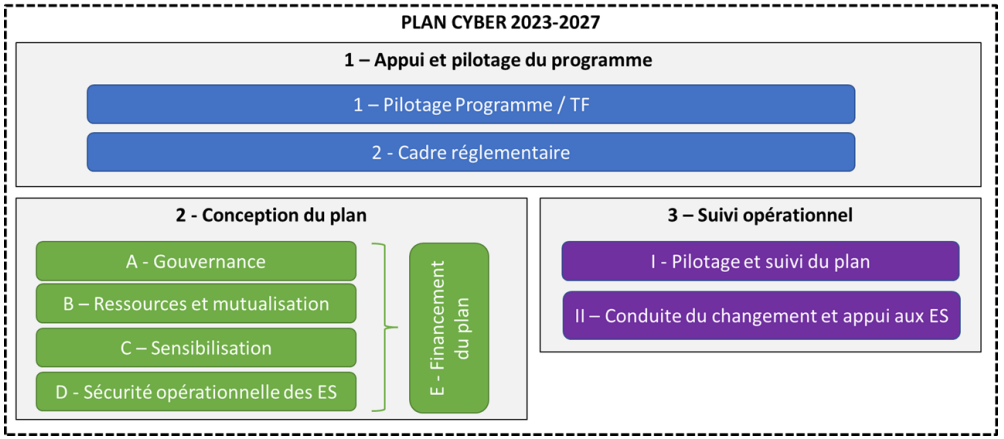
Points de contact :

- Jean-Baptiste LAPEYRIE (DNS)
- Elodie CHAUDRON (ANS)
- Sponsors régions : Steven GARNIER, Djamil VAYID, Fabian RICHARD (ARS), Auriane LEMESLE, Rémi TILLY, Thierry NAVARETTE (GRADeS)

Principaux livrables

- **Fin avril** : Formalisation d'un plan d'action comprenant notamment des actions court terme à destination des ES
- **Fin juin** : Plan de financement pluriannuel pour la mise en œuvre du plan d'action

Structuration des travaux



Les lignes directrices de construction du plan cyber établissements

✓ **Une hausse très sensible (au moins x2) des dépenses Cyber (et numériques) et sur le très long terme :**

- Cette visibilité est absolument nécessaire avant d'embarquer les acteurs dans un plan ambitieux et très attendu
- Le financement de la cyber ne peut pas durablement être envisagé comme une intervention de la puissance publique mais doit s'intégrer à la gestion globale des risques des établissements (sur le long terme)

✓ **Un financement à destination principale des établissements avec deux composantes :**

- Un financement pérenne annuel lié à l'atteinte d'objectifs socle cyber
- Un financement d'investissement afin d'accompagner l'écosystème dans le franchissement d'un palier

✓ **Le développement de l'offre de service nationale / régionale afin d'aider et accompagner les établissements**

- Portée par l'ANSSI, le CERT-Santé et les GRADeS, et centrales d'achat
- Comprenant aussi les capacités de mesure et de pilotage du programme

✓ **La nécessité de démarrer vite (et si possible « fort ») dès maintenant**

- Car le retard accumulé par les établissements vis-à-vis de la menace est inquiétant
- Afin de mettre en mouvement l'écosystème, démontrer qu'il est possible d'avoir une action systémique
- Sous condition de visibilité sur des financements pérennes….

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
Liberté Égalité Fraternité

Task Force Cyber – Les modalités d'intervention de la puissance publique

Délégation ministérielle au numérique en santé

AGENCE DU NUMÉRIQUE EN SANTÉ

Modalités d'intervention de la puissance publique

- **Objectif de financement direct des établissements pour la majeure partie du plan :**

  Financement pérenne annuel (pour financer RH, licences, etc.)

  Financement des appels à projet cyber pour tous les établissements sur des thématiques prioritaires (postes de travail et détection, Active Directory, passerelles pour les accès des prestataires, sauvegardes)

  Et l'ambition :

  - D'intégrer le numérique et la cyber (niveau cyber socle) à la certification HAS des établissements de santé
  - *"à terme" de concevoir un "forfait numérique" récurrent dédié au numérique sous conditions d'atteinte du socle cyber*

- **Avec un financement (pour une petite partie du plan) pour** :

  - Le développement de l'offre nationale et régionale
  - Le pilotage du programme
  - Les éditeurs (via les exigences SSI du programme Ségur numérique vague 2)

Objectifs à atteindre considérés comme le "Socle Cyber" avec des **financements pérennes annuels**

Lancement d'Appels à projet spécifiques avec un financement des investissements / transformation sur des thématiques prioritaires

Développement et renforcement d'une offre de service nationale et régionale
- Veille et centres de ressources régionaux
- Formation et sensibilisation
- Prévention et protection
- Réponse à incidents

Un plan pluriannuel décliné avec des objectifs de maturité annuels

		2023	2024	2025	2026	2027	
ES	Objectifs à atteindre = "Socle Cyber"	1. .. 2. ..	1. .. 2. ..	1. .. 2. ..	1. .. 2. ..	1. .. 2. ..	Forfait annuel Financement pérenne
	AAP spécifiques Investissement / Transformation	1. ..	1. ..	1. ..	1. ..	1. ..	Forfait AAP 1
		4. ..	4. ..	4. ..	4. ..	4. ..	Forfait AAP 4
Offre nationale/régionale	Offres mises à disposition	1. .. 2. ..	1. .. 2. .. 3. ..	1. .. 2. .. 3. ..	1. .. 2. .. 3. .. 4. ..	1. .. 2. .. 3. .. 4. ..	
Editeurs		Ségur – Art. 53 du PLFSS 2023					

Objectifs 2023-2024

Domaines	Objectifs 2023	Objectifs 2024
Gouvernance	➔ **Gouvernance stratégique sur la cyber en place** • Reprise des prérequis SSI du programme Ségur Usage Numérique (SUN-ES) : RSSI, PSSI, gouvernance, etc • Mis en oeuvre par 70% des ES • Recrutement de 17 référents régionaux SSI MS + 1 national (pour 5 ans) ➔ **Exercices de crise** • 100% OSE, 50% des ES MCO • 3 exercices au niveau régional • Réalisation de 500 exercices/an ➔ **PCA / PRA + dimension cyber "plan blanc/ORSAN"** • Définition d'une première trame nationale déployée sur ~150 ES ➔ **Certification HAS** • Définition des critères et du financement des visiteurs	➔ **Gouvernance stratégique sur la cyber en place** • Audit de type "test d'intrusion" récent (< 1 an) • Ordre du jour minimal imposé pour le comité Cyber avec la direction de l'établissement ➔ **Exercices de crise** • 100% ES ont réalisé un exercice de crise • 90% des futures EE sont sur un rythme annuel d'exercices • Un exercice au niveau régional pour chaque ARS • Réalisation de diagnostics et feuille de route cyber pour 1000 ESMS/an • Réalisation de 500 exercices an ➔ **PCA / PRA + dimension cyber "plan blanc/ORSAN"** • Déploiement de la première trame sur les futures EE (voire EI ?) ➔ **Certification HAS** • Mise en œuvre des critères cyber pour la campagne 2024
Financements	➔ **Engager les fonds Ségur numérique** ➔ **Fonds pour le plan jusqu'à 2027** • Valider le financement pluri-annuel du plan cyber ➔ **Financement pérenne** • Proposer une modalité dans la refonte de la tarification	➔ **Fonds pour le plan jusqu'à 2027** • Affectation des crédits dédiés au plan ➔ **Financement pérenne** • Financement numérique et cyber fléché et avec un ratio minimal dans le budget des ES

Plan cyber – Rappel des objectifs

Domaines	Objectifs 2023	Objectifs 2024
Ressources & Mutualisation	➔ **Mutualisation GHT** • Instruction à destination des ES publics pour une feuille de route à 2 ans sur la convergence des infrastructures • Intégration de ces objectifs dans les financements ➔ **Mutualisation ES "Privés" :** • Pas de perspective évidente à ce stade ➔ **Mutualisation MS :** • 17 ETP SSI sur 5 ans ➔ **Plan RH** • Identification du total ETP RSSI • [...]	➔ **Mutualisation GHT** • 75% des GHT ont une équipe Cyber mutualisée • 75% des GHT ont une équipe poste de travail mutualisée • 75% des GHT ont une équipe réseau mutualisée • Conditionnement de tout plan de financement numérique à l'atteinte des objectifs de mutualisation • Mise à jour de la feuille de route à 2 ans ➔ **Mutualisation MS :** • 17 ETP SSI sur 5 ans ➔ **Plan RH** : [...] • Augmenter le total ETP RSSI

Plan cyber – Rappel des objectifs

Domaines	Objectifs 2023	Objectifs 2024
Sensibilisation	➔ **Sensibilisation des DG** • Parvenir à toucher 50% des DG	➔ **Sensibilisation des DG** • Parvenir à toucher 75% des DG ➔ **Animation de la communauté des RSSI d'établissements** • Aider à organiser et animer la communauté des RSSI d'établissements (en s'appuyant sur le noyau actuel du club RSSI) • Proposer un plan d'embarquement spécifique pour les nouveaux RSSI d'établissement ➔ **Sensibilisation des personnels** • 90% des futures Entités Essentielles (NISv2) ont intégré un plan de sensibilisation de leurs personnels
Ségur SONS Vague 2 à l'hôpital	➔ **Dispositif SONS pour DPI, RIS, SGL** • Inclure un test d'intrusion dans les exigences	➔ **Dispositif SONS pour DPI, RIS, SGL** • Référencer les solutions • Déployer sur 50% du parc

Plan cyber – Rappel des objectifs

Domaines	Objectifs 2023	Objectifs 2024
Infrastructure bureautique et postes de travail **Exposition Internet** **Hébergement & Sauvegardes** **Gestion des identités**	➔ **<u>« Subvention » (investissement) pour un rattrapage sur des enjeux techniques précis</u>** • Intégration des enjeux de souveraineté et de convergence • Déploiement d'une solution technique (« équipement ») et de pratiques SSI associées ➔ **<u>« Subvention » Modalités d'un financement pérenne actuel conditionné à l'atteinte d'objectifs pour 2024</u>** • Intégration des enjeux de convergence, des prérequis de HOP-EN/SUN-ES, de la réalisation d'exercices de crise (mesures prioritaires) ➔ **<u>Outillage de suivi et de pilotage (dont budgétaire)</u>** • Outillage mis en place pour les « subventions » ci-dessus	➔ **<u>« Subvention » (investissement) pour un rattrapage sur des enjeux techniques précis</u>** • 50% des ES à la fermeture ➔ **<u>« Subvention » Modalités d'un financement pérenne actuel conditionné à l'atteinte d'objectifs pour 2024</u>** • 66% des ES sur le socle 2024 ➔ **<u>Outillage de suivi et de pilotage (dont budgétaire)</u>** • Intégration du volet cyber des ES dans l'observatoire de la e-santé

Financement Cyber

Ambitions

✓ Permettre à un **maximum d'établissements de franchir un palier en termes de SSI**, sur des domaines opérationnels identifiés, en lien avec les principales menaces identifiées, en mettant en œuvre des capacités opérées et pérennes :

- Réduction de la surface des infrastructures exposées sur Internet
- Durcissement des annuaires *Active Directory*
- Sécurisation des liens avec les différents fournisseurs / prestataires via des bastions d'administration
- Sécurisation des sauvegardes
- Développement d'une capacité de détection au niveau des postes de travail et serveurs (EDR + SoC)

ü Créer et accompagner **une dynamique et une synergie** avec l'ensemble des acteurs, avec une approche itérative / 'petits pas'

ü Engager la **stratégie de convergence** et surtout **de responsabilité unique sur les infrastructures** au sein des GHT

=> Financements) : Accompagner au maximum les ES sans les mettre en compétition

Enjeux

✓ Pouvoir ensuite intégrer dans le « socle cyber » ces nouvelles capacités

✓ Différencier la cible de ce financement (nouvelle capacité opérée et pérenne) et la réduction nécessaire de la dette technologique (postes de travail et serveurs)

✓ S'inscrire dans la continuité des précédents financements (AAP 2022 « France Relance »), en focalisant les thématiques couvertes par ce nouvel AAP sur **les infrastructures IT des ES/ESMS**.

✓ **Etendre cette logique à l'ensemble des ES de façon à créer un 'espace de confiance sanitaire'**, en veillant à prendre compte la situation initiale des ES (point de départ) en construisant une trajectoire de convergence différenciée

Financement Cyber

Structuration AAP

Prérequis généraux

✓ Désignation d'un **responsable au niveau GHT** avec :

- Une lettre de mission
- Un pilotage à minima fonctionnel de l'ensemble des équipes des établissements du GHT
- Un budget associé sur le budget G

4 domaines « techniques »

D1
Audits techniques : Active Directory et exposition sur internet

D2
Poste de travail

D3
Sécurisation des accès de télémaintenance

D4
Stratégie de sauvegardes

Avancée des travaux

✓ Travaux en cours

- Exercices de gestion de crise
- Certification HAS
- Sensibilisation
- Volet RH
- Plan Blanc / PCA / PRA

Merci de votre attention !