GOUVERNEMENT

Liberté
Égalité
Fraternité

LA E-SANTÉ FRANÇAISE

CaRE

Cybersécurité
accélération
et Résilience
des Établissements

Le plan d'action pour protéger nos établissements face à la menace cyber

La confiance et le développement des usages du numérique en santé passent par une mobilisation de tous sur la cybersécurité.

Introduction

Depuis plusieurs mois, notre système de santé fait face à une multiplication des cyberattaques en France (doublement des incidents déclarés par les établissements de santé depuis 2020)[1].

Même si le secteur de la santé n'est pas ciblé directement, l'augmentation de l'usage du numérique, et donc de son exposition, le place au troisième rang des secteurs les plus touchés, après les collectivités territoriales et les TPE/PME/ETI[2].

Les ressources compétentes pour la gestion du numérique au sein des établissements sont rares, et la mobilisation d'une enveloppe budgétaire dédiée au volet numérique permettant de répondre aux enjeux de sécurité des systèmes d'information n'est pas encore systématique.

De surcroît, les opportunités de mutualisation et de capitalisation des ressources et des moyens entre plusieurs établissements ne sont pas toujours mobilisées. La dette technologique prend de plus en plus d'ampleur, alors que les usages du numérique foisonnent et que les pirates informatiques se professionnalisent.

Plusieurs incidents ces derniers mois ont eu une résonance médiatique forte.

Les derniers retours d'expérience des établissements attaqués soulignent les impacts sur les organisations et sur la continuité de prise en charge des patients. Ils mettent en lumière les difficultés de devoir travailler en « mode dégradé » sur des périodes parfois extrêmement longues pour l'ensemble des professionnels, les pertes de chance potentielles pour les patients qui nécessitent parfois d'être transférés dans d'autres établissements par exemple. Certains évoquent aussi la détérioration de leur image et de la confiance entre l'établissement et l'usager, par ricochet des éventuels vols de données.

Depuis décembre 2022, la Délégation au numérique en santé (DNS) et l'Agence du Numérique en Santé (ANS) rassemblent et coordonnent l'ensemble des parties prenantes en charge de la cybersécurité pour le secteur au sein de la « Task Force (TF) cyber ». Ainsi chaque semaine, le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) des Ministères sociaux, la Direction Générale de l'Offre de Soins (DGOS), l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), l'Agence du Numérique en Santé (ANS), les Agences Régionales de Santé (ARS) et les Groupements Régionaux d'Appui au Déploiement de la e-santé (GRADeS) se mobilisent avec la DNS pour répondre aux enjeux de la priorité 15 de l'axe 4 de la feuille de route du numérique en santé 2023-2027 et renforcer massivement la cybersécurité des établissements sanitaires et médico-sociaux.

L'ensemble des travaux de la Task Force est conduit de manière collaborative avec les acteurs de l'écosystème (fédérations hospitalières et médico-sociales, industriels) et vise à rendre les établissements plus résilients et mieux préparés.

Le programme CaRE « Cybersécurité accélération et Résilience des Établissements » décline ainsi un plan d'action concret et ambitieux pour la période de 2023 à 2027.

Le programme, doté de plus de 230M€ sur 2023-2024, se décline en 4 axes et 20 objectifs :

1. Gouvernance et résilience

2. Ressources et mutualisation

3. Sensibilisation

4. Sécurité opérationnelle

[1] https://esante.gouv.fr/sites/default/files/media_entity/documents/ans_certsante_rapport_public_observatoire_signalements_issis_2022_vf.pdf
[2] https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/

Sommaire

Gouvernance et résilience

Page 6

Ressources et mutualisation

Page 11

Sensibilisation

Page 14

Sécurité opérationnelle

Page 16

1 Gouvernance et résilience

Le programme vise à structurer la gouvernance de la cybersécurité dans le secteur de la santé en impliquant les niveaux nationaux (ANSSI, ANS, DGOS), régionaux (ARS et GRADeS) et locaux (professionnels, établissements et aussi industriels) dans une trajectoire claire et unique, orchestrée par la Délégation au numérique en santé (DNS).

Les enjeux de cybersécurité et la gouvernance associée doivent être pris en compte par les établissements.

Ces derniers doivent pouvoir s'approprier, décliner et déployer le programme CaRE au cœur de leur projet d'établissement et le rendre visible au travers de leurs choix stratégiques et budgétaires.

Suite aux attaques, la plupart des établissements sont contraints d'œuvrer durant de longs mois pour retrouver leur niveau d'activité d'avant crise.

La résilience des établissements en cas d'incident cyber et/ou numérique, constitue par conséquent un axe majeur d'effort.

1. Mettre en œuvre une gouvernance pérenne pour le programme CaRE et plus globalement pour la cybersécurité dans le secteur de la santé

La mise en place d'une gouvernance et d'une comitologie associée regroupant toutes les parties prenantes est la garantie que les ambitions et les objectifs du programme CaRE répondront aux besoins et aux difficultés rencontrées par les établissements (ES et ESSMS).
Ces objectifs et les travaux qui en découleront seront régulièrement évalués et ajustés durant toute la durée du programme.

1-1. Mettre en place une instance nationale regroupant toutes les parties prenantes (DNS, HFDS, FSSI, ANSI, DGOS, ANS et CERT Santé, représentants des ARS et des GRADeS).
Le COPIL CaRE rassemble toutes les parties prenantes et se réunit mensuellement.
DNS - ANS

1-2. Intégrer les représentants des ES et ESSMS dans l'élaboration du programme.
Les représentants des fédérations hospitalières et du médico-social participent aux ateliers de travail du programme.
DNS - ANS

1-3. Impliquer les associations d'usagers sur le programme.
→ Les associations d'usagers contribuent au programme, participent aux ateliers de travail et à la conception d'outils qui leur permettront de se mobiliser dans sa promotion S2 2024.
DNS - ANS

1-4. Mettre en place une instance interrégionale permettant d'animer l'écosystème régional et les correspondants SSI dans les ARS et les GRADeS.
Les ARS et les GRADeS sont mobilisés dans la conception et la mise en œuvre du programme et participent au groupe de travail territorial.
DNS - ANS

1-5. Mettre en place et animer un espace de travail communautaire collaboratif entre experts SSI.
→ La communauté RSSI participe à la conception et à la mise en œuvre du programme CaRE en participant à un groupe de travail dédié S2 2024.
ANS

1-6. Élaborer et partager avec l'écosystème la stratégie cybersécurité pour les établissements (ES et ESSMS) pour la période 2023-2027.
La feuille de route du programme CaRE est publiée et diffusée S2 2023.
DNS - ANS

1-7. Mettre à disposition de l'écosystème l'ensemble des ressources documentaires nécessaires à la mise en œuvre du programme.
La page dédiée au programme CaRE sur le site ANS est mise à jour régulièrement.
ANS

2. Intégrer la cybersécurité dans la gouvernance des établissements

La cybersécurité doit trouver sa place dans les orientations stratégiques, les budgets et la politique qualité et de gestion des risques des établissements. Pour soutenir cette action, la Haute Autorité de Santé intègre des critères numériques et cybersécurité dans le manuel de certification des établissements sanitaires et recrute une équipe d'experts visiteurs numériques.

2-1. Inciter la mise en place d'une gouvernance de la cybersécurité dans chaque établissement.
→ 70% des établissements et 100% des GHT ont un RSSI nommé et animent une comitologie dédiée S1 2025.
FSSI

2-2. Intégrer la thématique cybersécurité dans l'élaboration et le renouvellement des **Contrats Pluriannuels d'Objectifs et de Moyens (CPOM) ARS-ES**.
→ L'ensemble des CPOM signés entre ARS et établissements de santé devront intégrer au moins un objectif cybersécurité à partir de S1 2024.
DNS - ARS

2-3. Intégrer des critères numériques et cybersécurité dans le manuel de certification HAS des établissements de santé, en prévoir une mise à jour annuelle et recruter des experts visiteurs numériques pour démarrer les visites de certification dès début 2024.
La HAS participe activement à l'intégration de la cybersécurité dans la démarche qualité et gestion des risques des établissements sanitaires : elle intègre des critères numériques et cybersécurité dans le manuel de certification des établissements, et recrute des experts visiteurs numériques pour renforcer ses équipes.
→ La HAS réalise les visites de certifications dans les établissements de santé dès S1 2024 et prévoit une revue des critères annuellement.
HAS - ANS S2 2023
Financement : convention ANS-HAS 3,8M€.

2-4. Clarifier les obligations et exigences SSI pour les établissements sanitaires.
→ Une instruction synthétisant toutes les obligations et exigences SSI sera publiée pour les établissements de santé S1 2024.
HFDS - SSI

3. Préparer et accompagner les établissements à réagir et à faire face à la cybermenace

Les ARS déploient depuis plus d'un an une large campagne de réalisation d'exercices de crise cyber au sein des établissements sanitaires et des structures médico-sociales notamment grâce à une enveloppe de 10M€ octroyée début 2023 et les **kits ANS mis à disposition** à cet effet. Fin octobre 2023, 1333 exercices de crise ont déjà été organisés.
Des exercices de crise régionaux sont également en cours de déploiement sur l'ensemble du territoire, et prioritairement dans les régions qui accueilleront les Jeux Olympiques 2024, permettant de tester la capacité de réponse des acteurs régionaux à des cyberattaques de grande ampleur. Un **kit dédié à ces exercices régionaux** est mis à disposition par l'ANS, basé sur le retour d'expérience de l'ARS de La Réunion.
Dans la continuité de la généralisation des exercices de crise et du volet numérique du plan de gestion des tensions hospitalières et des situations sanitaires exceptionnelles, la DGOS a diffusé un **guide d'élaboration du plan blanc numérique**, pour aider les établissements sanitaires à adopter les mesures de prévention du risque numérique, notamment la réglementation et les outils techniques existants.
Pour donner une dimension opérationnelle à ces initiatives, et en regard des besoins exprimés par les établissements sanitaires, la Task Force CaRE a élaboré avec les fédérations et leurs représentants métiers un **kit « plan de continuité et de reprise d'activité » (PCRA)**. Celui-ci est actuellement diffusé dans sa version de travail pour ne pas ralentir les travaux de production au sein des structures : un pilote est en cours depuis mi-septembre avec la participation active de vingt-huit établissements volontaires. Cette phase permettra de consolider ce premier kit et d'identifier les leviers nécessaires à la généralisation de sa mise en œuvre effective dans tous les établissements dès 2024.

3-1. Faciliter l'intégration d'un volet numérique dans le plan blanc des établissements de santé en mettant à disposition un guide de préparation à la mise en œuvre d'un plan blanc numérique.
→ Les établissements de santé intègrent un volet numérique dans leur plan blanc S2 2024.
DGOS

3-2. Mettre en œuvre des Plans de Continuité et de Reprise d'Activité (PCRA) dans les établissements (ES et ESSMS).
→ Un kit national PCRA est conçu et mis à disposition des ES en S1 2024.
Dans l'objectif de pouvoir généraliser sa mise en œuvre dans 80% des établissements de santé sur le périmètre cible des services critiques à S1 2026, les établissements de santé devront nommer un référent plan de continuité et de reprise d'activité (PCRA) à S1 2025.
Le travail réalisé pour les ES sera adapté pour les ESSMS et un pilote sera organisé S1 2024.
ANS
Financement : pour 2024, enveloppe FIR 26M€ à répartir pour toutes les actions régionales, dont l'accompagnement à la production et mise en œuvre d'un PCRA.

3-3. Poursuivre la dynamique de la campagne de réalisation des exercices de crise et l'étendre au secteur des ESMS et aux ARS.
→ 80% des établissements de santé (maille PMSI) devront réaliser un exercice de crise d'ici S2 2024.
La réalisation annuelle de ces exercices doit être pérennisée dans tous les établissements de santé d'ici S1 2027.
Pour le secteur médico-social, les exercices de crise devront être réalisés par 90 organismes gestionnaires sur le périmètre MS1-PA-PH-Domicile-financés par un appel à projets ESMS Numérique sur 2021 et 2022 à S1 2024. 3% des OG du territoire auront réalisé un exercice de crise en 2025. Les exercices de crise cyber au niveau régional sont réalisés à S1 2024 par les ARS JOP et à S2 2024 pour les autres ARS.
ARS
Financement : 10 M€ FIR délégué aux ARS 2023.
Pour 2024 : Enveloppe FIR 26M€ à répartir pour toutes les actions régionales.

4. Engager les établissements (ES et ESSMS) dans une démarche d'auto-évaluation et d'orientation de leur feuille de route cyber

Donner aux établissements les moyens de s'auto-évaluer afin de leur permettre d'identifier les actions prioritaires à mener et de mieux orienter et piloter leur feuille de route, suivre les évolutions réglementaires et leurs impacts pour les établissements (directive NIS 2...).

4-1. Établir, en collaboration avec les établissements (ES et ESSMS), un référentiel d'auto-évaluation de leur maturité sur le volet de la cybersécurité, pour les aider à s'auto-évaluer et à définir leur plan d'actions en conséquence ainsi que les besoins associés.

→ Les établissements (ES et ESSMS) devront réaliser leur autoévaluation d'ici S1 2025. 75 % des ES s'appuient sur cette auto-évaluation pour mettre à jour leur plan d'actions cybersécurité en S1 2026.
ANS

2 Ressources et mutualisation

Le programme CaRE prend en compte la pénurie de talents et de ressources dans les établissements (ES et ESSMS) et met en exergue le besoin de s'arrêter sur l'adéquation, les compétences et la pérennisation des ressources humaines agissant dans le secteur numérique et de la cybersécurité.

Des travaux sur l'attractivité et la fidélisation des compétences sont en cours. Les réponses ne pouvant être immédiates, le programme s'appuie et favorise toutes les opportunités de convergence et de mutualisation en cherchant autant que possible à capitaliser et à embarquer l'ensemble des structures.

La Task Force s'attache à coordonner et mobiliser les acteurs de l'écosystème de manière unifiée et cohérente autour de l'ensemble des actions identifiées prioritaires et à forte valeur ajoutée.

Elle cherche à encourager le développement de l'offre de service cyber afin que chaque établissement, sans discrimination sur son type d'activité ou son lieu d'implantation, puisse bénéficier du service ou de l'accompagnement dont il a besoin pour répondre aux ambitions du programme CaRE et des évolutions réglementaires (NIS2).

Ces travaux sont réalisés sur la base du « catalogue des offres cyber » publié sur le site de l'ANS, qui collige ***plus de 400 offres proposées*** *et diffusées par l'ANSSI, l'ANS, les GRADeS et les centrales d'achat (CAHPP, CAIH, RESAH), pour les établissements autour des thématiques : prévenir, contrôler, détecter, réagir et reconstruire.*

5. Favoriser la mutualisation des ressources et des moyens entre les établissements

La mutualisation est un levier à mobiliser dans un contexte de pénurie de ressources. Du côté des établissements publics, les GHT sont déjà en place et les ressources peuvent y être mutualisées pour s'engager dans une trajectoire commune. En parallèle, le référencement de certaines prestations dans les centrales d'achat ou via les GRADeS peut apporter un premier niveau de réponse.

5-1. Impulser une trajectoire de convergence des GHT au niveau de l'établissements de santé support dans le cadre des financements CaRE.

→ L'établissement de santé support du GHT porte la candidature du GHT et l'engagement d'atteinte des objectifs pour l'ensemble des établissements de santé du GHT. Chacun des domaines liés aux appels à financement CaRE (cf. Axe 4) comporte un objectif d'atteinte en lien avec la convergence. Pour illustration, le « Domaine 1 » impose la nomination d'un chef de projet au niveau GHT et la définition d'une trajectoire de convergence des Annuaires (Active Directory).

80% des GHT sont candidats et atteignent les objectifs du domaine 1 des appels à financements CaRE S2 2025.

DNS - ANS

Financement : en partie sur l'enveloppe 65M€ pour les établissements de santé (AF D1).

6. Augmenter le nombre de personnels dédiés au SI dans les établissements

Afin de renforcer leur sécurité opérationnelle et être plus résilients face à la cybermenace, les établissements de santé doivent dimensionner leurs équipes techniques et leur DSI. L'attractivité et la fidélisation des ressources qualifiées est indispensables pour accompagner la trajectoire globale de montée en puissance des établissements.

6-1. Rendre attractives les carrières du numérique en santé au sein des établissements, et pérenniser les emplois.

Les grilles salariales des ingénieurs hospitaliers sont revalorisées S2 2023.

→ Une réflexion s'engage pour mettre à disposition des directions d'ES un guide leur permettant d'ajuster leurs équipes SI et SSI en fonction de leur organisation et de leur besoin, et de mobiliser les outils de la Gestion Prévisionnelle de l'Emploi et des Compétences pour pérenniser les emplois S2 2025.

DGOS

6-2. Proposer un ratio DSI/RSSI/ES en regard des organisations et des retours d'expérience.

→ Un guide comportant des préconisations quant aux organisations IT sera mis à disposition des directions d'établissements de santé S1 2024.

DGOS

7. Garantir dans chaque établissement un budget suffisant dédié au numérique et à la cybersécurité

La part du numérique dans le budget des établissements doit représenter 2% du budget global de l'établissement.

7-1. Amener les directions des établissements de santé à flécher 2% de leur budget sur le numérique et la cybersécurité sur la base d'une méthode de calcul uniforme et partagée.

→ 100% des établissements de santé déclarent un budget numérique et cybersécurité supérieur ou égal à 2% S1 2025.
DNS

8. Développer une offre de service répondant aux besoins prioritaires des établissements en lien avec les Centres de Ressources Cyber (CRRC) hébergés dans les GRADeS et les acteurs industriels

Le développement de l'offre de service se fera sur la base d'un recueil exhaustif de toutes les offres portées au niveau national (ANSSI, ANS, CERT Santé, Centrales d'achat) et au niveau régional (GRADeS) en les rapprochant notamment avec les besoins des établissements pour répondre à l'ambition du programme.

8-1. Élaborer une cartographie de l'offre existante afin d'identifier les éventuels besoins additionnels.
Produire et partager largement le catalogue des offres cyber.
ANS
Financement : pour 2024, enveloppe FIR 26M€ à répartir pour toutes les actions régionales.

8-2. Soutenir les régions (ARS et GRADeS) dans leurs actions d'animation et d'accompagnement de l'ensemble des établissements dans leurs territoires.
→ Les ARS sont impliquées activement dans la conception et la mise en œuvre du programme : elles sont appelées à se mobiliser dans le cadre d'une instruction détaillée S1 2024.
DNS - ANS
Financement : pour 2024, enveloppe FIR 26M€ à répartir pour toutes les actions régionales.

3 Sensibilisation

« La sécurité est l'affaire de tous », le programme nécessite donc un engagement fort de chacune des parties prenantes.

Pour cela, il est primordial de proposer à tous les professionnels de santé et à tous les personnels administratifs une formation sur le numérique et la cybersécurité, et les sensibiliser sur le cadre réglementaire et sur les bonnes pratiques à adopter.

Les directions d'établissement, en tant que décideurs, sont quant à elles garantes de la sensibilisation du personnel et de l'application des bonnes pratiques d'hygiène informatique au sein de leurs structures.

Pour soutenir cette dynamique, le programme s'attache à fournir les ressources pédagogiques nécessaires aux directions, aux RSSI et aux DSI.

9. Sensibiliser les Directeurs Généraux et les Présidents des Commissions Médicales d'Etablissements (PCME) sur les risques cyber et leurs impacts

La sensibilisation des directions d'établissement est une priorité du programme : leur implication est indispensable pour la mise à niveau de la SSI dans les structures.

9-1. Réaliser des campagnes de sensibilisation à destination des publics prioritaires, au niveau national et au niveau régional.
→ Le programme met à disposition un nouveau kit « tous cybervigilants » complémentaire à celui de 2021, facilement déclinable à l'échelon régional et local S1 2024.
Il s'agira de mesurer l'impact de cette campagne, notamment, par le biais de la diffusion de ce kit S1 2025.
ANS

9-2. Partager des **retours d'expériences** sur les impacts d'une cyberattaque.
Les établissements de santé victimes de cyberattaques témoignent et sont ambassadeurs du programme. Ils sont sollicités pour réaliser des retours d'expérience lors d'évènements régionaux, nationaux, ou par le biais d'autres canaux comme le site ANS.
DNS - ANS - ARS - GRADeS

10. Animer une communauté des RSSI d'établissements

L'animation des RSSI des structures est un enjeu fort du programme pour renforcer la visibilité de leur action auprès de leur direction et créer un espace de partage et d'échange de bonnes pratiques et des difficultés rencontrées au quotidien.

10-1. S'appuyer sur un Groupe de travail RSSI pour identifier les freins, les belles réussites, les besoins prioritaires à instruire dans le programme.
→ L'ensemble des productions est réalisé en adéquation avec les besoins du terrain. L'ensemble des travaux du programme est partagé et coconstruit avec les experts, en s'appuyant sur un groupe de travail rassemblant les RSSI et la mise en place d'un espace de travail collaboratif S1 2024.
ANS

10-2. Poursuivre l'animation régionale réalisée par les ARS et les GRADeS avec les acteurs SI et SSI dans les territoires.
Les instances régionales entre ARS (avec l'appui des GRADeS) et DSI/RSSI des établissements de santé se réunissent de manière trimestrielle.
ARS
Financement : pour 2024, enveloppe FIR 26M€ à répartir pour toutes les actions régionales.

11. Sensibiliser et former l'ensemble du personnel des établissements

Instaurer une culture de la sécurité informatique au sein des établissements via des actions de sensibilisation et de formation de leur personnel.

11-1. Former l'ensemble des professionnels de santé et/ou administratifs dans les établissements (ES et ES-SMS).
Les référentiels de compétences intègrent un module obligatoire «numérique et cyber» :

- **Dans les formations initiales des professionnels de santé médicaux et non médicaux, (universités) et des personnels administratifs (EHESP) S2 2023**
- **Dans les formations continues des mêmes professionnels S2 2023.**

DNS

4 Sécurité opérationnelle des établissements

Dans le contexte des attaques actuelles (utilisation de rançongiciels et exfiltration de données par des acteurs professionnalisés), un effort important sur les infrastructures doit être réalisé au sein des établissements pour :

- *Remédier aux faiblesses (vulnérabilités) des établissements, afin de limiter ces intrusions dans les SIH et empêcher ou rendre plus difficile la latéralisation ;*
- *Déployer des technologies permettant de mieux détecter les signaux de compromission en cas d'intrusion ;*
- *Améliorer la capacité de reprise informatique en cas d'une telle compromission.*

Par conséquent, le programme CaRE a identifié des «domaines» d'investissement prioritaires avec l'écosystème pour que les établissements puissent pallier leur dette technologique.

En complément, le programme HospiConnect est dédié au domaine de l'identification électronique des professionnels, afin de sécuriser l'accès aux services numériques sensibles et de limiter les risques d'usurpation de l'identité numérique des professionnels dans le système d'information des établissements.

Il est envisagé à terme d'octroyer un financement plus pérenne aux établissements qui maintiendraient le niveau acquis, en regard des priorités de la feuille de route CaRE.

12. Soutenir les établissements de santé dans les domaines identifiés comme prioritaires pour faire face à la cybermenace

Les établissements de santé sont financés pour pallier leur dette technologique sur les domaines identifiés comme prioritaires. Un premier appel à financement dit pour le domaine « audits techniques exposition internet et annuaires techniques » (Domaine 1) est lancé.
Les prochains appels à financement suivront rapidement. Parmi les priorités déjà identifiées : « Poste de travail et détection » (Domaine 2), « Sécurisation des accès de télémaintenance » (Domaine 3), et « Continuité d'activité et stratégie de sauvegarde » (Domaine 4).

12-1. Élaborer le dispositif juridique et administratif nécessaire à la mise en œuvre des appels à financement.
→ L'arrêté pour le Domaine 1 est publié à S2 2023.

Les établissements de santé pourront se porter candidats à S1 2024 et seront financés à l'atteinte des objectifs en S2 2024.
DNS - ANS

13. Maitriser les risques d'exposition sur internet et sécuriser les annuaires d'établissement

Les cyberattaques récentes montrent que l'exposition sur 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.

13-1. Mettre en place les moyens nécessaires pour que les établissements de santé évaluent rgulièrement et amliorent significativement leur niveau de sécurité de leurs annuaires techniques (Active Directories - AD) et de leur surface exposée.
→ 90 % des établissements de santé candidats CaRE D1 atteignent les objectifs du domaine S1 2025.
DNS - ANS
Financement : 65 M€ pour les ES.

14. Superviser les postes de travail et détecter les intrusions

L'objectif est de détecter au plus tôt une tentative d'intrusion ou une intrusion dans le système d'information, pendant la phase où les attaquants cherchent à s'introduire, se propager et à contrôler le SIH. L'ambition est aussi d'engager une approche communautaire, et de permettre à tous les établissements de santé de bénéficier des signaux.

Les actions et indicateurs qui relèvent de cet objectif sont en cours de co-construction avec les parties prenantes de la Task Force.
Financement : 60 M€ pour les ES.

15. Sécuriser les accès au SI depuis l'extérieur (télémaintenance)

Le nombre important de fournisseurs nécessitant des liens avec les solutions déployées au sein des établissements de santé (plusieurs dizaines pour certains établissements de santé) induit un risque important d'intrusions d'attaquants via ces « portes ouvertes ».
L'ambition consiste donc à mettre en œuvre des «portes sécurisées, maitrisées et exploitées» pour ces liens avec les fournisseurs.

Les actions et indicateurs qui relèvent de cet objectif sont en cours de co-construction avec les parties prenantes de la Task Force.
Financement : 60 M€ pour les ES.

16. Reconstituer rapidement les services critiques en cas d'incident

Lors d'une attaque de type rançongiciel (une des principales menaces), les attaquants cherchent à chiffrer les données des ES, mais aussi les sauvegardes, rendant la reprise d'activité particulièrement complexe, avec des pertes de données massives et critiques.
Un effort particulier doit être porté sur la capacité des établissements à se préparer, s'organiser et à réagir dans le cadre d'une cyberattaque, notamment dans la mise en place de sauvegardes non contaminables et restaurables pour toutes les applications critiques.

Les actions et indicateurs qui relèvent de cet objectif sont en cours de co-construction avec les parties prenantes de la Task Force.
Financement : 45 M€ pour les ES.

17. Disposer d'une équipe dédiée au contrôle des ES permettant d'attester l'atteinte des objectifs tels que définis dans les différents domaines

Cette mesure exhaustive de l'atteinte des objectifs par les établissements de santé, réalisée par le biais d'audits, complétée par une opération de contrôle est fondamentale pour la réussite du programme.
Cela permet aux établissements de s'assurer que les solutions et les actions de remédiation sont efficaces. D'autre part, la synthèse de ses mesures facilite et éclaire le pilotage du programme en mettant en exergue les difficultés rencontrées par les acteurs nécessitant un soutien complémentaire.

17-1. Construire et mobiliser une équipe dédiée aux opérations de contrôle pour vérifier l'atteinte des objectifs par les ES pour tous les domaines prioritaires du programme CaRE.
→ L'équipe de contrôle est opérationnelle à S1 2024.
DNS - ANS
Financement : 3M€ 2024 et 6 M€ 2025.

18. Maintenir le niveau acquis via l'atteinte d'objectifs considérés comme le « Socle Cyber »

La définition de ce «socle cyber» minimum, dont les objectifs seront plus ambitieux chaque année, est de permettre aux établissements de santé de maintenir le niveau acquis et de poursuivre les efforts en continu.

Les actions et indicateurs qui relèvent de cet objectif sont en cours de co-construction avec les parties prenantes de la Task Force.

19. Limiter les risques d'usurpation de l'identité numérique des professionnels pour l'accès aux services sensibles, conformément au Référentiel d'identification électronique de la PGSSI-S

Sécuriser l'accès des professionnels aux services numériques sensibles du SI des établissements et aux services socles nationaux du numérique en santé (par exemple le DMP), sur la base :

- D'un identifiant sectoriel unique après enregistrement au RPPS (concerne tous les professionnels intervenant dans le système de santé depuis l'Arrêté du 23 septembre 2022),
- De l'utilisation de moyens d'identification électronique (MIE) à double-facteur d'authentification (2FA), en particulier les dispositifs proposés par la fédération Pro Santé Connect (cible niveau eIDAS substantiel),
- De la mise en œuvre de solutions d'Identity & Access management (IAM) pour améliorer la gestion des habilitations et de briques de Single Sign On (SSO) pour simplifier l'authentification des professionnels.

Actions envisagées :
Mise en œuvre du programme HospiConnect, pour accélérer l'adoption par les établissements de solutions conformes au référentiel d'identification électronique de la PGSSI-S, par l'intermédiaire d'appels à projets, dotés de financements dédiés à l'atteinte des cibles mentionnées : utilisation de MIE sécurisés (2FA, Pro Santé Connect ou eIDAS substantiel), IAM, SSO.

Un premier appel à projets est prévu pour quelques établissements pilotes début 2024, en vue d'une généralisation à partir de 2025.
→ En 2027, les professionnels des établissements sanitaires et médico-sociaux disposent de moyens d'authentification à deux facteurs pour se connecter à leurs applications sensibles (objectif 8.5 de l'axe 2 de la feuille de route du numérique en santé 2023-2027).

20. Intégrer la cybersécurité dans l'élaboration des référentiels sectoriels pour toutes les solutions utilisées par les établissements (ES et ESSMS) et par les professionnels de santé

Les solutions utilisées par les professionnels de santé (PS) et déployées en établissement contribuent directement au niveau de sécurité globale et à la protection des données de santé à caractère personnel, en particulier les EHR (Electronic Health Record) et le DME (Dossier Médical Electronique). Les référentiels sectoriels regroupent les exigences que doivent respecter les solutions d'un secteur d'activité (DPI, Dossier patient informatisé, par exemple) par rapport à la feuille de route du numérique en santé et la doctrine technique associée.
En conséquence, les référentiels sectoriels concernant ces solutions intègreront progressivement des exigences cyber. Cela permet ainsi de mener une action globale, tant au niveau des établissements que des solutions déployées, tout en s'inscrivant à part entière dans la réglementation européenne en cours ou à venir (EHDS, Cyber Resilience Act, etc). Sont typiquement concernées toutes les actions de référencement et de labellisation, comme les référencements Ségur, les certificats délivrés pour les solutions de télésanté ou de téléconsultation.

20-1. Construire et faire évoluer un référentiel transverse d'exigences cyber pour les solutions, en intégrant un test d'intrusion par un auditeur PASSI S1 2024.

→ Nombre de solutions référencées sur un référentiel sectoriel comprenant des exigences en cybersécurité.

Délégation ministérielle au numérique en santé - DNS
Conception, création et design : l'agenceverte
Décembre 2023