MARDI 3 décembre 2024
de 9h à 17h30
Centre de congrès d'Angers

JOURNEE REGIONALE E-SANTE

Pour les professionnels du social et du médico-social des Pays de la Loire

Quels outils numériques pour quels usages ?

RÉPUBLIQUE FRANÇAISE
ars Agence Régionale de Santé Pays de la Loire
l'Assurance Maladie
e-santé GRADeS Pays de la Loire
Collectif SI Médico-Social Pays de la Loire
CaRE Cybersécurité accélération Résilience des Etablissements
Financé par l'Union européenne NextGenerationEU

Plénière Cybersécurité

« ESSMS et cybersécurité, enjeux et perspectives pour les prochaines années »

Mehdi ZINE, *Agence du Numérique en Santé*

Julien NTANGA, *Agence Régionale de Santé*

Solène MANSOURI, *EPMS de l'Anjou*

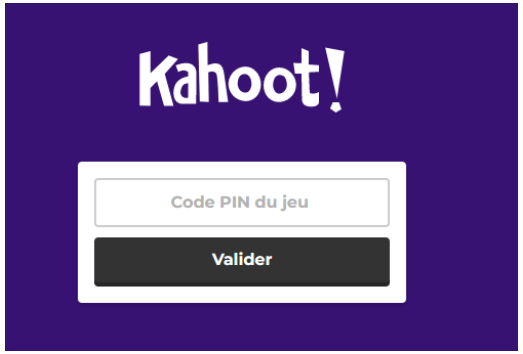
Auriane LEMESLE, *GRADeS Pays de la Loire*

Financé par l'Union européenne NextGenerationEU

Faisons connaissance

La cybersécurité au sein de votre structure, où en êtes-vous ?

Accédez à l'adresse https://kahoot.it/ et rentrer le code PIN



→

Choisissez un pseudonyme (jusqu'à 3 propositions)

→

A vous de jouer !

Menaces pesant sur le secteur

Attaques à finalité lucratives

- **Chiffrement des données via rançongiciels à des fins d'extorsion**
- **Exfiltration de données à des fins d'extorsion et / ou revente**

Compromissions à des fins de fraudes

Vol d'accès de professionnels de santé pour établir de faux documents (exemples : passes sanitaires, ordonnances…)

Espionnage

Données médicales d'individus ou données de recherche

Déstabilisation

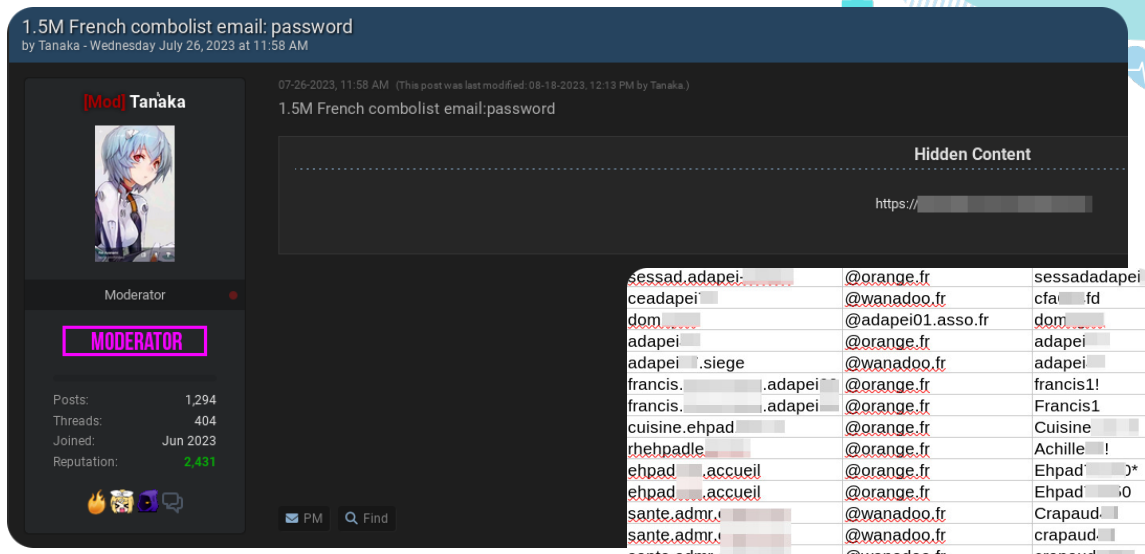
- Déni de service distribué
- Défiguration de sites web
- Exfiltration de données pour divulgation publique

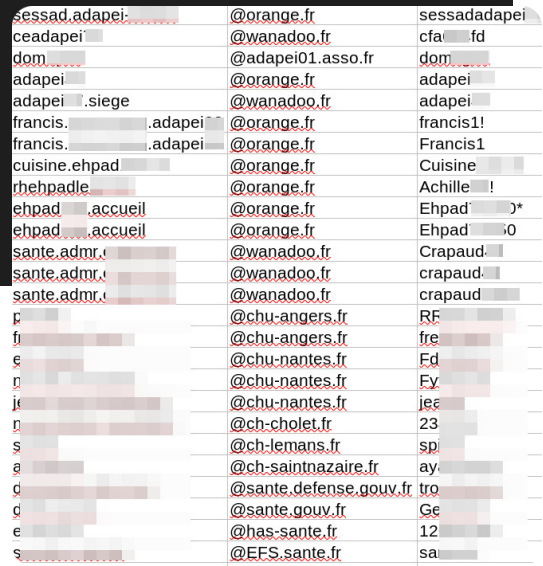
Portes d'entrée sur vos SI

Vol d'identifiants de connexion au SI

Internes (collaborateurs)

Externes (prestataires et partenaires)





Comptes compromis via des "Infostealers"

Equipements vulnérables exposés sur Internet

Services VPN (télétravail, télémaintenance)

Serveurs applicatifs (DUI, serveur de fichiers)

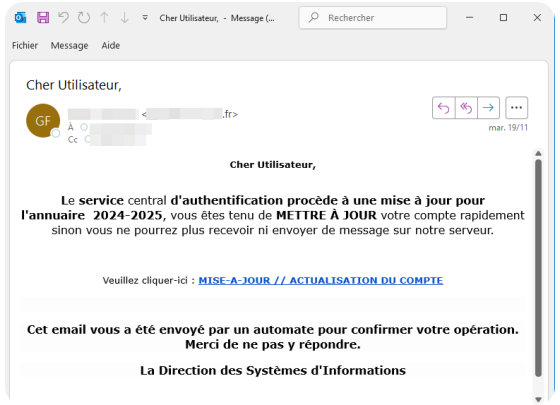
19 novembre 2024

Exploitation en cours de vulnérabilités critiques affectant les pares-feux Palo Alto

Le CERT Santé et le CERT-FR de l'ANSSI nous informent qu'une vulnérabilité critique est activement exploitée dans les pares-feux de la marque Palo Alto.

En plus de l'application du correctif de sécurité mis à disposition par l'éditeur le 18 novembre 2024, il est recommandé de vérifier que l'accès à l'interface d'administration est restreinte aux administrateurs et qu'elle n'est pas exposée sur Internet. Dans le cas où elle serait ou aurait été exposée, le CERT-FR recommande d'isoler l'équipement et réaliser un gel des données (pour investigations) avant de reconstruire la solution à partir d'une version à jour et en suivant les recommandations de sécurité de l'éditeur pour le déploiement de l'interface d'administration.

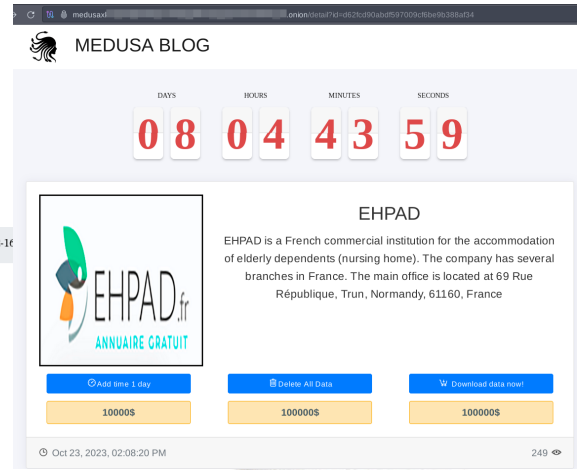
Mail frauduleux : hameçonnage

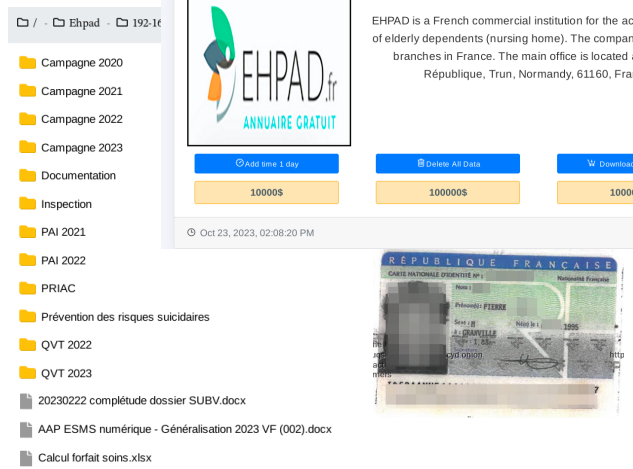


Impacts

Manche : Un Ehpad attaqué par des cybercriminels demandant une rançon de 95.000 euros

- Perturbation activité / prise en soin et de l'accompagnement des personnes
- Coûts importants de remédiation
- Réputation





Moselle

Farébersviller : l'Ehpad victime d'une cyberattaque avec demande de rançon

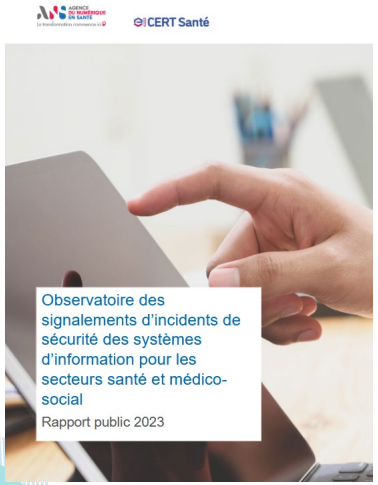
L'Ehpad Saint-Jean-Baptiste de Farébersviller a fait l'objet d'une cyberattaque de grande ampleur, avec demande de rançon. Tout le système informatique, en particulier le logiciel de suivi des résidents, est paralysé. Des données personnelles ont probablement été piratées. Une plainte a été déposée.

Stéphane Mazzucotelli – 10 févr. 2024 à 05:00 | mis à jour hier à 09:46 – Temps de lecture : 3 min

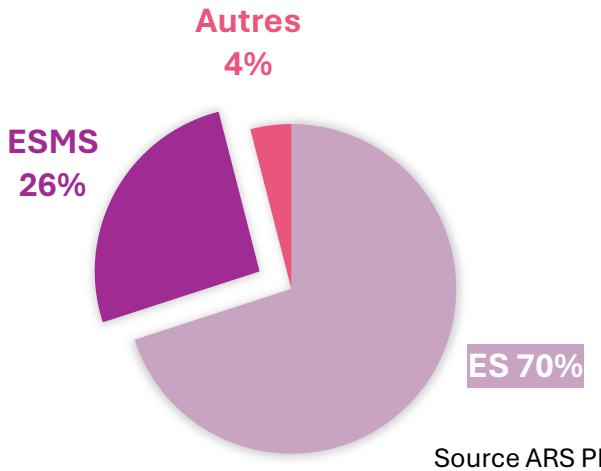
Incidents en Pays de la Loire

Nombre de signalements réalisés via le portail de signalement (à fin novembre 2024) :

	2019	2020	2021	2022	2023	2024
National	392	369	733	592	*581*	
Régional	36	31	54	49	50	52



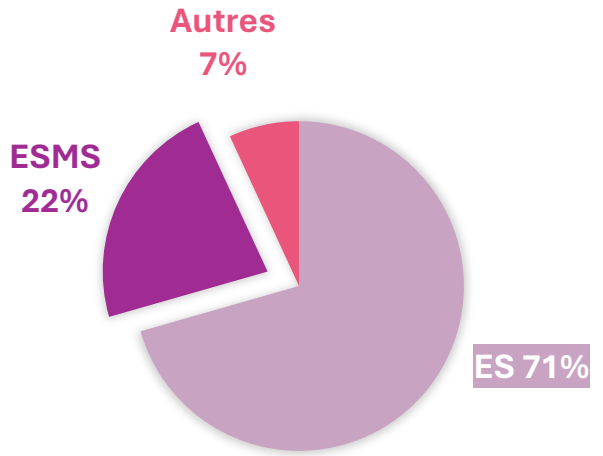
Répartition des incidents déclarés en 2023 en Pays de la Loire :



Source ARS PDL

58% d'origine malveillante

Répartition des incidents déclarés en 2023 en France :



Source CERT Santé

50% d'origine malveillante

La genèse du programme CaRE

2021 - 2022

Les établissements de santé et médico-sociaux ont été la cible de nombreux actes de cybermalveillance

1321

Déclarations d'incidents de cybersécurité dans les ES ont été enregistrés en 2021 et 2022 (CERT Santé), **dont 675 d'origine malveillante**

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

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER
MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
MINISTÈRE CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES TÉLÉCOMMUNICATIONS

21 décembre 2022

Réunion interministérielle pour de nouveaux engagements pour renforcer la cybersécurité des ES

Décembre 2023

Présentation par le ministre de la Santé et de la Prévention au CH de Versailles du Plan d'action CaRE
Cybersécurité accélération et Résilience des Etablissements
pour renforcer la cybersécurité des ES et des ESSMS

1. Gouvernance et résilience
2. Ressources et mutualisation
3. Sensibilisation
4. Sécurité opérationnelle

Implication de toutes les parties prenantes

- Une **équipe « cœur »** : DNS, FSSI, DGOS, ANSSI, ANS, ARS, GRADeS
- Des **contributeurs** : Fédérations Hospitalières, Fédérations Médico-Sociales, Etablissements de santé, Industriels, Centrales d'achat

AGENCE DU NUMÉRIQUE EN SANTÉ
MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Délégation ministérielle au numérique en santé DNS

Décembre 2022

Lancement de la Task Force (TF) Cyber constituée d'une équipe cœur, et des contributeurs et pilotée par l'ANS et la DNS

Une feuille de route en 4 axes

> **Une réponse collective, déterminée et coordonnée pour faire face à la menace**

Gouvernance et résilience

Structurer la gouvernance de la cybersécurité dans le secteur de la santé en impliquant les niveaux nationaux, régionaux et locaux.

Ressources et mutualisation

Prise en compte de la pénurie de talents et de ressources dans les établissements, et mise en avant du besoin de mutualiser et de pérenniser les ressources humaines.

Sensibilisation

Encourager un engagement fort de chacune des parties prenantes de la cybersécurité dans les établissements de santé.

Sécurité Opérationnelle

Soutenir financièrement les investissements jugés prioritaires via des « Domaines » (via des appels à financements et/ou appels à projets).

Financé par l'Union européenne NextGenerationEU

Axe 1 : Déclinaisons opérationnelles nationales et régionales

Gouvernance et Résilience

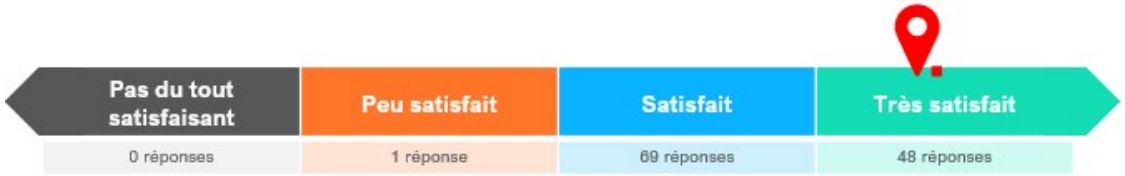
Exercices de crise dans les Etablissements de Santé ESMS

Objectif : 80% des ES d'ici S2 2024 réalisent un exercice de crise, démarche qui doit devenir annuelle

- Plus de 2220 exercices réalisés ou planifiés soit **78 %** des ES (FINESS PMSI).
- **À l'échelle régionale, 93** exercices ont été réalisés ou planifiés soit **86%** **des ES** (FINESS PMSI) et les premiers ESMS se sont lancés dans la démarche.

Exercices de crise en Pays de la Loire

93 exercices réalisés ou planifiés



99,15%

« satisfaisant ou Très satisfaisant »

86% **des établissement de santé ont réalisé un exercice de crise**

Au-delà d'une **très bonne satisfaction globale**, une véritable **prise de conscience des impacts** d'une crise cyber **sur la continuité des soins** est observée par tous les participants aux exercices de crise cyber

Et maintenant ?

Soutien aux ESMS dans la réalisation d'un 1er exercice de crise

Pour en savoir plus

Assistez à l'atelier « Crise cyber : se préparer pour mieux la traverser »

Adapeila

Axe 1 : Déclinaisons opérationnelles nationales et régionales

Gouvernance et Résilience

Exercices de crise dans les Etablissements de Santé ESMS

Objectif : 80% des ES d'ici S2 2024 réalisent un exercice de crise, démarche qui doit devenir annuelle

- Plus de 2220 exercices réalisés ou planifiés soit **78 %** des ES (FINESS PMSI).
- **À l'échelle régionale, 93** exercices ont été réalisés ou planifiés soit **86% des ES** (FINESS PMSI) et les premiers ESMS se sont lancés dans la démarche.

Exercices de crise régionaux

Objectif : Réalisation d'un premier exercice régional d'ici S2 2024

- **Toutes les régions ont réalisé ou planifié leur exercice.**
- Exercice réalisé le 21/02/2024 pour les Pays de la Loire.

Plan de Continuité et de Reprise d'Activité

Objectifs : Mettre en œuvre des Plans de Continuité et de Reprise d'Activité (PCRA) dans les établissements (ES et ESSMS).
Un objectif spécifique PCRA a été inclus dans l'appel à financement « Domaine Stratégie de continuité et de reprise d'activité » en cours de co-construction.

- Kit PCRA disponible sur le site de l'ANS
- Des modules de formations e-learning sont en cours d'élaboration
- Déclinaison du kit prévue pour le médico-social
- Le PCRA est intégré au Domaine 2 : « nommer un responsable PCRA » est un prérequis et « mettre en place une gouvernance qui y est dédiée puis le formaliser » sont des objectifs à atteindre

Certification HAS 2024

Objectif : Intégration de critères numériques et cyber dans le référentiel de certification v2024 et recrutement d'experts visiteurs numériques

- **175 EVN** recrutés et formés et **369 ES visités** à S1 2024
- Intégration de critères concernant la stratégie numérique et la sensibilisation des utilisateurs au numérique au **Référentiel d'évaluation de la qualité des ESSMS**

CPOM

Construction en cours d'une trame d'objectifs cyber à intégrer dans les CPOM ARS-ES

- Initiative de l'ARS Pays de la Loire de l'insertion d'objectifs numérique et cyber dans les CPOM ARS-ESMS

Référentiel Maturin-SMS

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

En établissant 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.

La version 2024 est accessible en ligne sur le site de l'Agence du Numérique en Santé (ANS) : Publication du référentiel maturité numérique « Maturin SMS »

1 **Référentiel MaturiN-SMS**

Outil d'évaluation de la maturité numérique des établissements et services du secteur médico-social, construit autour de 7 dimensions thématiques

Dimension 5 « Sécurité des SI » spécifique des questions cyber

16 indicateurs découpés en **5 niveaux de maturité**

Exemple d'un indicateur de la Dimension 5 « Sécurité des SI » du référentiel MaturiN-SMS

Thématique	Indicateur	Niveaux de maturité
5.1 : Sécurité des différentes composantes du SI	5.1.1 Sécurité organisationnelle et stratégique	Sélectionner votre réponse parmi les propositions suivantes (plusieurs réponses sont possibles) : 0 - Pas de procédures dégradées ni de charte de sécurité SI 1 - Charte/document SI diffusé et actions de sensibilisation et de formations régulières 2 - Existence d'un plan de continuité d'activité (PCA) formalisé spécifique au SI (PCI), élaboré en partenariat avec l'éditeur du DUI 3 - Existence d'un plan de reprise d'activité (PRA) formalisé spécifique au SI, élaboré en partenariat avec l'éditeur du DUI 4 - Plan global de sécurité des systèmes d'informations formalisé -Conforme au référentiel PGSSI-S (à renouveler tous les 3 ans)

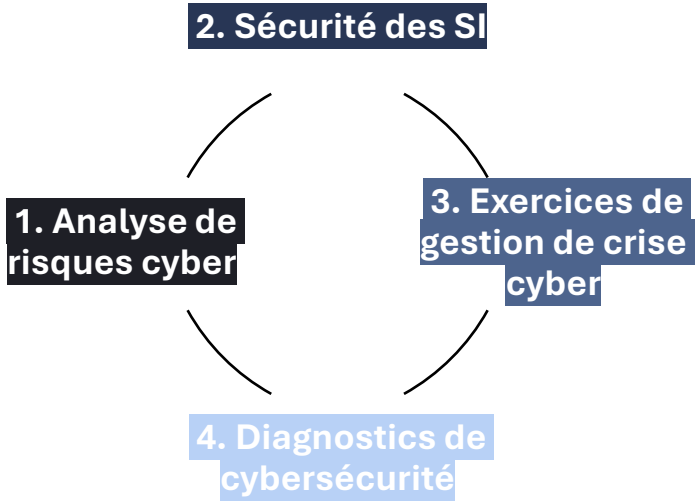
Observatoire Permanent de la Sécurité des SI du secteur Médico-Social (OPSSIMS)

2

Outil d'observation des pratiques de sécurité des SI

des établissements et services du secteur médico-social

Questionnaire axé autour de 4 thématiques



- Lancement à venir de la **phase pilote,** menée par la DNS et l'ANS, pour **tester le contenu** de ce dernier afin de :
  - **Évaluer la pertinence et la clarté des questions de l'observatoire**
  - **Recueillir les suggestions d'amélioration**

- Modalités de la phase pilote :

09 décembre 2024 au 20 janvier 2025

3 à 5 OG volontaires en Pays de la Loire

1 fichier Excel à compléter

Un interlocuteur pour accompagner les pilotes (temps d'échange via Teams)

Axe 2 : Déclinaisons opérationnelles nationales et régionales

Ressources et mutualisation

Catalogue des offres cyber

Objectif : Recensement de l'ensemble des offres existantes à destination des ES / ESMS dans un catalogue dédié disponible sur le site de l'ANS.

- 467 offres publiques recensées
- 168 offres d'industriels recensées

Renforcer l'attractivité des ressources en ES

Objectif : Identifier les leviers pour renforcer l'attractivité des ressources en ES

Revalorisation des grilles statutaires des ingénieurs hospitaliers

Mutualiser les ressources

Objectif : Favoriser toutes les opportunités de convergence et de mutualisation en cherchant autant que possible à capitaliser et à embarquer l'ensemble des structures

- Grappes ESMS
- GCSMS

Financement de la cybersécurité en région (CRRC)

Objectif : Mise en place des centres de ressources cyber (CRRC) qui vont développer une offre de services répondant aux besoins prioritaires des établissements.

Ces CRRC se voient attribuer plusieurs missions :

- 8 objectifs généraux
- 3 objectifs spécifiques, propres au **secteur du médico-social**.

Financé par l'Union européenne NextGenerationEU

Sécurité numérique en Pays de la Loire

TOUS CYBER VIGILANTS EN PAYS DE LA LOIRE

Formations

- Référents sécurité des SI & Animation d'un COPIL sécurité des SI
- Séminaire secteur médico-social
- Analyse de risques et homologation
- Détection et réaction en cas de cyberattaque par rançongiciel

Journées régionales

- Partager les actualités, nouvelles réglementations et expériences avec les acteurs en région

Appui à la gestion des incidents

- Diffusion alertes
- Soutien en cas d'incident
- Aide à la mise en œuvre d'un outil de supervision réseau

Veille technologique et réglementaire

- https://www.scoop.it/topic/ssi-sante

Webinaires

- Sécuriser mon AD
- Protéger mes réseaux, mon Wifi
- Détecter les menaces
- Sécuriser ma messagerie

Base documentaire régionale

- Modèles de documents
- Mémos thématiques
- Base documentaire en ligne

Préparation à la crise cyber

- Soutien à la réalisation d'exercices de crise cyber
- Centre de ressource SSI mutualisées à destination des ESMS
- Synthèse de l'état de l'art de la sauvegarde des données

Outils de sensibilisation

- Affiches
- Fonds d'écran
- Escape game
- Badges métalliques
- e-learning
- Vidéos de sensibilisation
- Flyer de sensibilisation des entrepreneurs
- Datablockers
- Faux phishing

Financé par l'Union européenne NextGenerationEU

Diagnostic de maturité de la sécurité du SI

Opportunité de bénéficier d'un **panorama à 360°** sur les **menaces** et d'**un état des lieux** de votre positionnement par rapport aux référentiels nationaux.

Accessible au travers du **centre de ressources SSI mutualisées** à destination des ESMS adhérents du GCS e-santé.

Entretien de 3h, en distanciel, avec un intervenant indépendant.

Guide cyber dédié au social et médico-social

Référentiels applicables

Ce que ça m'apporte :

- **Savoir où je me situe**
- **Cibler mes priorités**
- **Faire un état des lieux complet**
- **Partager les constats**
- **Mieux comprendre les sujets liés au SI**
- **Obtenir des livrables personnalisés**

Financé par l'Union européenne NextGenerationEU

Retour d'expérience

Partage de l'EPMS de l'Anjou sur son accompagnement par le centre de ressources SSI mutualisées.

Par Solène MANSOURI, *Directrice*.

EPMS DE L'anjou
ÉTABLISSEMENT PUBLIC
MÉDICO-SOCIAL

Les accompagnements du centre de ressources SSI mutualisées à destination des ESSMS

Initiation ou mise à jour de l'inventaire des composants du SI (matériels, logiciels, applications, ...)

Modèle fourni

Cartographie du système d'information

Revue des composants essentiels de sécurité du SI : pares-feux, antivirus, sauvegardes, ...

Diagnostic des équipements de sécurité

Rappel des bonnes pratiques de revue des pares-feux et révision des règles en place sur votre matériel

Accompagnement revue des règles de pare-feu

Vérification de la posture de sécurité de votre AD avec plan d'action correctif pour la revue de la configuration

Diagnostic de l'Active Directory

Vérification du maintien en condition de sécurité et du paramétrage permettant de limiter la réception de messages indésirables et les usurpations d'identité

Diagnostic de messagerie

Revue des droits, gestion des utilisateurs, configuration et traçabilité

Diagnostic plateforme collaborative Office 365

Cartographie des données, des technologies utilisées, planification des sauvegardes et restauration

Aide à l'élaboration du plan de sauvegarde

Cadrage technique et plan d'action

Test non réalisé en séance, à réaliser a posteriori par la structure.

Préparation réalisation d'un test de restauration

Vérification du niveau de sécurité mis en place sur les Wifi professionnel et usager / résident avec plan d'action priorisé pour la remédiation.

Sécurisation de la configuration Wifi

Centre de ressources SSI mutualisées à destination des ESMS

49 **structures** ont intégré la démarche et bénéficié d'un premier accompagnement du centre de ressources SSI mutualisées, destiné aux ESMS.

68 **accompagnements réalisés ou planifiés**.

Pour les structures ayant fait un retour au questionnaire de satisfaction :

L'accompagnement réalisé a « *Totalement* » répondu à leurs attentes pour 90,9 % d'entre elles.

92,8% des structures s'estiment « ***Très satisfaites*** » par la **clarté du plan d'actions fourni**.

Quelques retours de bénéficiaires

« Accompagnement de très bonne qualité. Merci de cette aide précieuse, à recommander à toutes les structures n'ayant pas de service informatique."

Ingénieur Qualité / Gestion des risques / RSI - EHPAD

« Réelle écoute des questions, reformulation des termes techniques très appréciable. »

Direction - EPMS

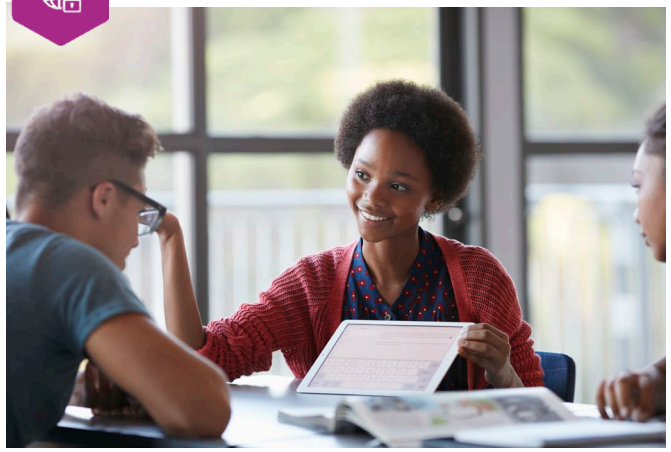
« La démarche est l'occasion de remettre à plat nos outils et nos utilisations. J'ai aussi bien entendu l'importance des actions de prévention et sensibilisation, avec des sources documentaires intéressantes. Prestation pertinente et efficace. »

Direction - SSIAD

Financé par l'Union européenne NextGenerationEU

Axe 3 : Déclinaisons opérationnelles nationales et régionales

Sensibilisation



Campagnes de sensibilisation

Objectif : Réaliser des campagnes de sensibilisation à destination des publics prioritaires, aux niveaux national et régional.

- **Outils régionaux :**
  - Affiches, fonds d'écran, badges, stickers, datablockers
  - Sant'escape – Sécurité numérique
  - Vidéos de sensibilisation
  - Plateforme e-learning & faux-phishing

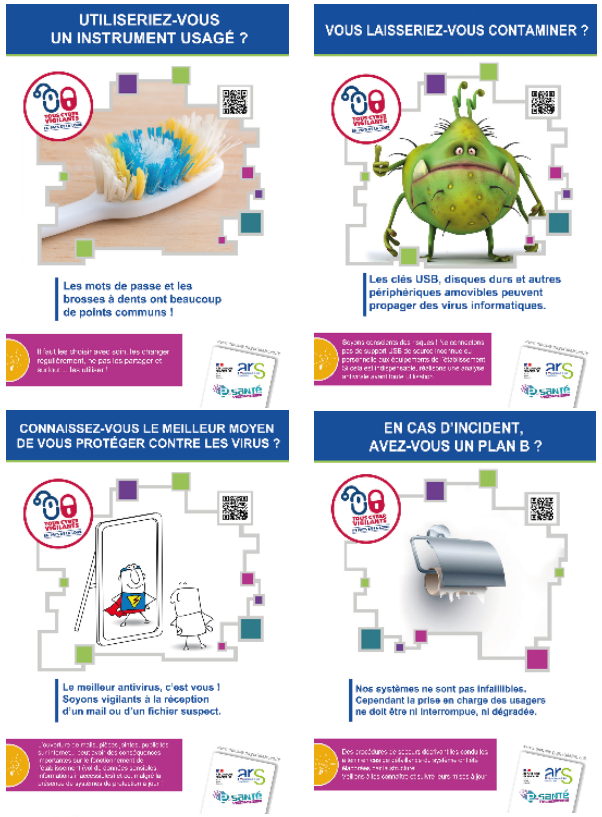
Des accessoires ludiques et pratiques

Datablocker

Jeu de l'oie

Protège carte

Des visuels déclinés sous différents formats



Financé par l'Union européenne NextGenerationEU

Plateforme de e-learning et faux-phishing

- Accessible aux adhérents, via **2 modes d'accès** (opéré ou autonome) après signature d'une **convention de service**.
- **Contenus contextualisés** au domaine de la **santé** et au **social et médico-social**.

En 2024 :

11 campagnes

24 bénéficiaires
dont 19 ESMS

3900 destinataires en moyenne (e-learning)

71,2% des bénéficiaires déclarent une **atteinte totale des besoins** en sensibilisation des utilisateurs

81% de satisfaction sur la **préparation** des campagnes de **faux-phishing**

81% de satisfaction sur les **thématiques de e-learning**

Pour vous inscrire à **l'édition 2025 du programme opéré** par le GCS e-santé PdL, des formulaires sont disponibles au stand cyber.

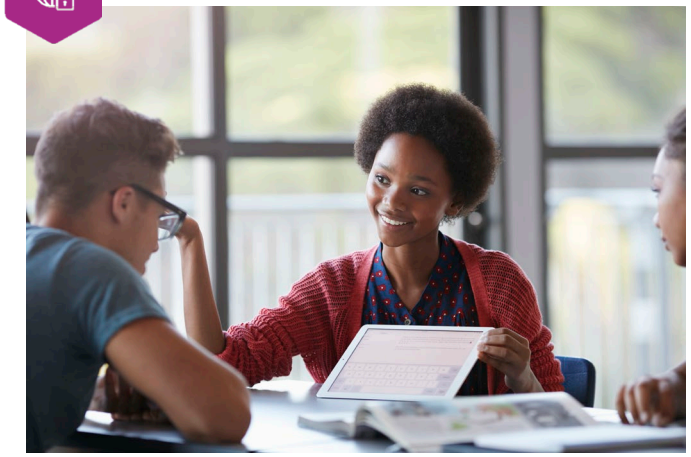
Programme e-learning 2025

- **Janvier** – *Enjeux de la cybersécurité*
- **Février** – *1 session, 1 utilisateur*
- **Mars** – *Clés USB*
- **Avril** – *Authentification à double facteur*
- **Mai** – *Session ouverte*
- **Juin** – *Phishing*
- **Juillet – Août** – *En dehors du temps d'activité*
- **Septembre** – *Stockage mot de passe navigateur*
- **Octobre** – *Cybermoi/s*
- **Novembre** – *Utilisation Wi-Fi public*
- **Décembre** – *Fraude faux support technique*

+ 4 campagnes de faux-phishing

Axe 3 : Déclinaisons opérationnelles nationales et régionales

Sensibilisation



Campagnes de sensibilisation

Objectif : Réaliser des campagnes de sensibilisation à destination des publics prioritaires, aux niveaux national et régional.

- **Outils régionaux :**
  - Affiches, fonds d'écran, badges, stickers, datablockers
  - Sant'escape – Sécurité numérique
  - Vidéos de sensibilisation
  - Plateforme e-learning & faux-phishing

Formation

Objectif : Former l'ensemble des professionnels de santé et/ou administratifs dans les établissements (ES et ESSMS) aux enjeux cyber.

- **Modules obligatoires numériques et cyber dans les formations initiales et continues professionnels de santé et à EHESP**

- **Plateforme e-learning ANS-Formation :** [ANS-Formation] - Coorpacademy
- **Offre de formations régionales à destination des adhérents**

Animations & Présence aux évènements nationaux et régionaux, publications

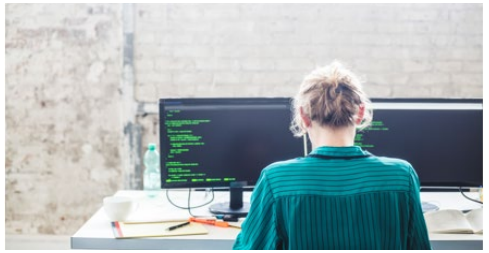
Objectifs :

- Promouvoir le programme CaRE au sein de l'écosystème et sensibiliser aux enjeux de la Cyber.
- Poursuivre l'animation régionale réalisée par les ARS et les GRADeS avec les acteurs SI et SSI dans les territoires.

- **Organisation de Webinaires d'information et relai des Webinaires ANS** (Webinaire présentation programme, Webinaire PCRA, Webinaire HospiConnect, Webinaire atteinte des objectifs D1, etc…)

Axe 4 : Déclinaisons opérationnelles nationales et régionales

Sécurité opérationnelle



Domaine Annuaires techniques et exposition sur internet

Objectif : Maîtriser les risques d'exposition sur internet et la sécurisation de leurs annuaires.

- **Une enveloppe de 65 M€** qui concerne tous les établissements sanitaires (publics et privés)
- **53** candidatures à l'échelle régionale
- **La phase opérationnelle en cours** qui s'étend jusqu'à juin 2025

Domaine Stratégie de continuité et de reprise d'activité

Objectif : Reconstituer rapidement les services critiques en cas d'incident et assurer la continuité et reprise d'activité.

- Co-construction en cours avec la Task Force et des représentants des ES / ESMS : définition des objectifs et des prérequis
- Objectifs techniques autour de la sauvegarde et organisationnels autour du PCRA
- Lancement prévu au T4 2024 pour une enveloppe prévisionnelle de 45 M€

Synthèse de l'état de l'art de la sauvegarde

Aide à l'élaboration du plan de sauvegarde

Préparation réalisation d'un test de restauration

Domaine Sécurisation des accès distants

Objectif : Sécuriser l'ensemble des accès distants, couvrant à la fois les fournisseurs et les accès du personnel des établissements.

- Conception du domaine en cours. Lancement prévu T2 2025
- Co-construction en cours avec la Task Force et des représentants des ES / ESMS ainsi qu'avec des éditeurs - fournisseurs responsables de la télémaintenance.

HospiConnect

Objectif : Simplifier et sécuriser l'accès des professionnels aux services numériques sensibles.

- Lancement du domaine HospiConnect (**AAP ALPHA**) **18 mars 2024**
- **1 candidat en région** pour la phase pilote **sur 15 structures** retenues à l'échelle nationale

Adapeila

Webinaires techniques

Envie d'en savoir plus ?

Atelier cybersécurité

« Crise cyber : se préparer pour mieux la traverser. »

L'équipe cyber est présente aujourd'hui

Puisqu'une démo vaut 1000 mots, RDV sur notre stand !

Pour lutter contre le piratage de vos appareils et carte sans contact, venez vérifier ***l'efficacité de nos accessoires de sensibilisation****.*

Pour sensibiliser les utilisateurs de votre SI, venez visualiser des exemples de ***vidéos de e-learning et les mails de faux-phishing*** *dont vous pourriez bénéficier.*

Pour mesurer la rapidité à laquelle un mot de passe peut être « craqué », venez avec nous ***vous mettre dans la peau d'un « hacker ».***

Financé par l'Union européenne NextGenerationEU

Merci pour votre attention

« La cyber : avant, c'est trop cher…

... après, c'est trop tard ! »

Financé par l'Union européenne NextGenerationEU