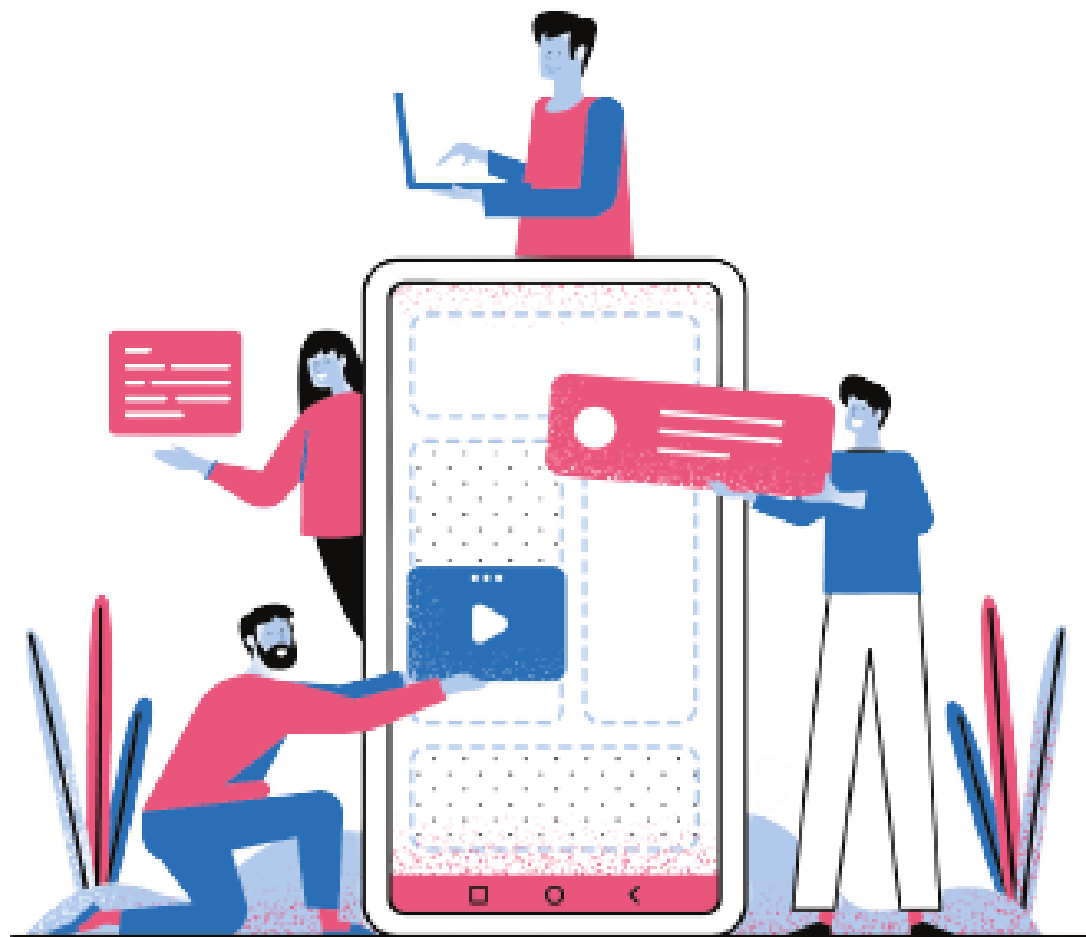


ESMS : le virage numérique

*Journée régionale
9 novembre 2023*



Temps forts de la journée

 9h - Café d'accueil

 9h30 - Plénière

- 9h30 – Mot d'ouverture
- 10h – Le **numérique** au service du médico-social
- 10h15 – L'**intelligence artificielle** en santé

 10h45 – Pause / Visite des stands

 11h15 – Ateliers & retours d'expérience

- **Coordination des soins et de l'accompagnement** avec la solution régionale parcours
- Présentation de **Mon Espace Santé**
- Déploiement de **MSSanté** en structure médico-sociale
- La **télesanté**, un levier pour l'accès aux soins

 12h15 – Pause déjeuner / Visite des stands

 12h45 - Conférence

Risques numériques et enjeux de la **cybersécurité** pour le médico-social


 14h30 – Ateliers & retours d'expérience

- **Coordination des soins et de l'accompagnement** avec la solution régionale parcours
- Présentation de **Mon Espace Santé**
- Déploiement de **MSSanté** en structure médico-sociale
- La **télesanté**, un levier pour l'accès aux soins

 15h30 – Pause / Visite des stands

 15h45 – Table ronde

Regards croisés sur le **déploiement du Dossier Usager Informatisé** par trois ESMS

 17h - Clôture

Mot d'ouverture par le Collectif Systèmes d'Information Médico- social

Les membres du Collectif SI médico-social



- **16 membres** dont 8 font partie du comité restreint
- Des **professionnels du secteur** qui sont des Directeurs d'ESSMS ou Responsables des Systèmes d'informations
- Des représentants de Fédérations et d'Organismes Gestionnaires sur le territoire.



La vision du Collectif SI MS

Le numérique comme **levier** majeur pour soutenir la **transformation** de l'offre des établissements sociaux et médico-sociaux



Les missions du Collectif SI médico-social

ACCULTURER ET SENSIBILISER

Les responsables (OG et Directions) des ESSMS aux **enjeux** des systèmes d'information

ANIMER LA COMMUNAUTE

Mettre en relation les ESSMS et recueillir **les besoins du terrain** afin de les remonter au niveau national et régional

FACILITER LA MUTUALISATION ET LA COOPERATION

Des ESSMS et les **orienter** vers les dispositifs et ressources existants

Mot d'ouverture



Rémi Barba

Chargé de projets ESMS Numérique
ARS Pays de la Loire

Mot d'ouverture



Odile Jamet

Directrice de projet médico-social
Délégation ministérielle du Numérique en Santé



Didier Alain

Responsable du programme ESMS Numérique
Caisse Nationale de Solidarité pour l'Autonomie

Le numérique au service du médico-social



Anne-Alexandra Babu

Directrice
GCS e-santé



Julie Tan

Responsable de pôle ESMS
GCS e-santé



Auriane Lemesle

*Responsable de pôle sécurité et conformité
numériques et référente régionale SSI*
GCS e-santé

Le GCS e-santé Pays de la Loire



Un GRADeS, groupement régional d'appui au développement de la e-santé : opérateur préférentiel de l'ARS qui favorise la **coopération entre le privé et le public, et entre la ville et l'hôpital.**



**AU SERVICE
DE NOS MEMBRES**

Des professionnels spécialisés dans le numérique en santé

- aident à mettre en œuvre votre projet,
- équipent en outils numériques,
- forment et accompagnent dans les usages.



**UNE PROXIMITÉ
TERRITORIALE**

5 sites départementaux pour être au plus proche de vous :

- contact de proximité,
- disponibilité et réactivité.



NOTRE MISSION

Soutenir le déploiement du **numérique en santé** au bénéfice **des professionnels de santé et du médico-social** pour apporter **une meilleure coordination dans la prise en charge et le suivi des patients et usagers**

La Télésanté : un levier pour faciliter l'accès aux soins



La Télésanté : un levier pour faciliter l'accès aux soins

SOLUTION RÉGIONALE TÉLÉSANTÉ



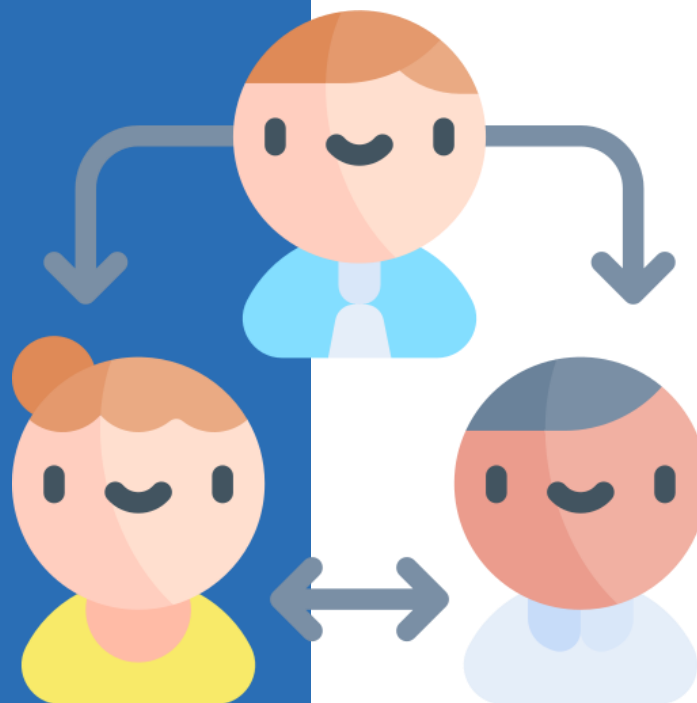
L'Agence Régionale de Santé des Pays de la Loire met à disposition une **plateforme régionale de télésanté** et finance votre projet de télésanté (équipements)

- Plus de 30 spécialités : cardiologie, gériatrie, infectiologie, soins palliatifs...

Accompagnement personnalisé :

- avant-projet et cadrage,
- conseil et expertise,
- installation des équipements,
- formation aux outils,
- suivi des usages, support, formation

L'outil Parcours : pour la coordination des professionnels autour de parcours complexes



SOLUTION RÉGIONALE PARCOURS



- Accessible en ligne, elle est composée de différents modules. Elle facilite la coordination entre les professionnels de la santé afin de **garantir la continuité de prise en charge des personnes suivies**.
- L'Agence Régionale de Santé des Pays de la Loire met à disposition la solution régionale Parcours et finance vos projets de coordination.

Accompagnement personnalisé :

- accompagnement à l'expression des besoins et à la mise en place du plan d'actions,
- mise en œuvre du parcours,
- conseils et formation,
- suivi des usages, support et formation.

La Messagerie Sécurisée de Santé





Moyen rapide et sécurisé pour échanger des informations sensibles entre professionnels de santé et avec les usagers via la messagerie sécurisée de Mon Espace Santé.

Pour les échanges :

- Ville - ESMS
- Hôpital - ESMS
- ESMS à ESMS

Notre solution E-santé MAIL :

- une messagerie MSSanté, financée par l'ARS
- notre équipe vous accompagne dans sa mise en œuvre



Les outils d'orientation au service d'une réponse pour tous



Les outils d'orientation au service d'une réponse pour tous



L'outil d'aide et de suivi des orientations

Fiabilisons les données pour réduire les files d'attente et le délai de prise en charge



Le référentiel unique de l'offre de santé et d'accompagnement

Fiabilisons les données pour une meilleure visibilité de l'offre



MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

*Liberté
Égalité
Fraternité*

Service d'Accès aux Soins
Un service de Santé.fr



RÉPUBLIQUE
FRANÇAISE

*Liberté
Égalité
Fraternité*

Santé.fr

La dynamique Ségur et ESMS Numérique : pour faciliter la coordination des acteurs et un parcours fluide pour les personnes accompagnées

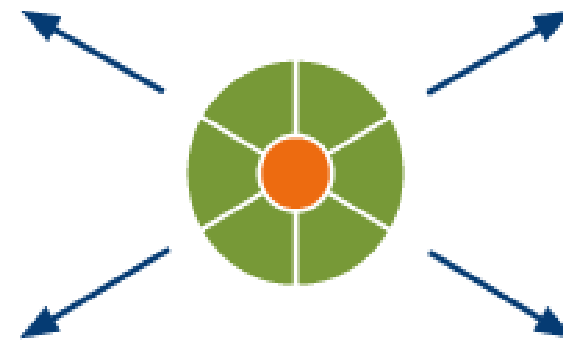


Le volet numérique du Ségur pour le médico-social

Le volet social et médico-social du Ségur numérique vise à **équiper tous les établissements et services sociaux et médico-sociaux d'un logiciel, dossier usager informatisé (DUI), conforme au virage du numérique en santé.**

mon
ESPACE
SANTÉ

Identité Nationale
de Santé
INS
Bien identifié-e,
bien soigné-e.



du **Dossier Usager Informatisé (DUI)**
interopérable
et communicant;

MS
Santé

PRO SANTE
CONNECT

Les financements disponibles pour les ESMS

Programme ESMS Numérique



Des aides pour l'acquisition et le renouvellement de votre Dossier Usager Informatisé (DUI).

Système ouvert non sélectif (SONS)



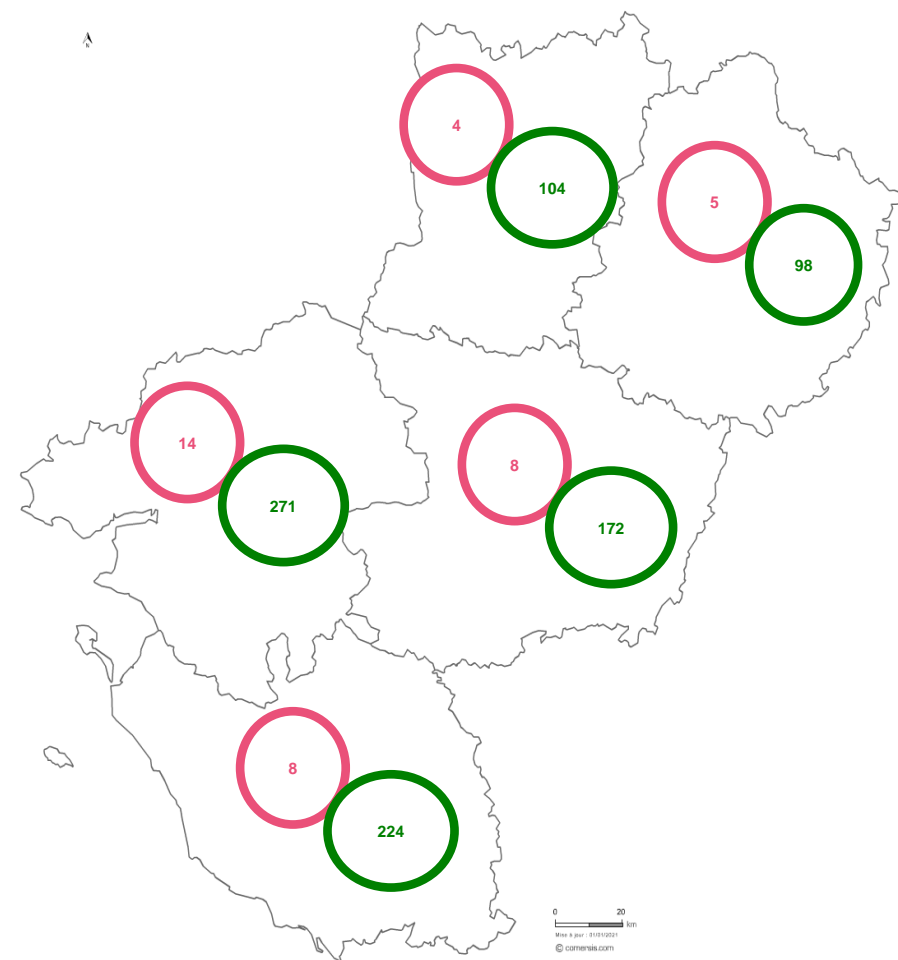
La montée de version de votre Dossier Usager Informatisé (DUI), **prise en charge par l'État.**

- Date butoir : 10/01/2024
- Bon de commande à demander à votre éditeur

La dynamique ESMS numérique en Pays de la Loire

+ 900 ESSMS embarqués

+38 porteurs de projet actifs
(dont 2 nationaux)



Le GCS informe, sensibilise et accompagne les ESSMS pour concrétiser leur transformation numérique



Le GCS accompagne le Collectif SI MS Pays de la Loire
dans la réalisation de ses travaux
& **les ESSMS de la région** à prendre le virage numérique.



Nos actions et notre accompagnement :

- **Webinaires** et actions de **sensibilisation**
- Organisation d'**événements** (tour des départements, ...)
- Création d'**outils** (cartographie DUI, Kit Démarches Simplifiées, ...)
- Animation de la **communauté des porteurs** (Groupe de travail porteurs, ...)
- **Accompagnement** pour vos **projets ESMS Numérique** (candidature et mises en œuvre des pré-requis (RPPS+, certificats, ...) au déploiement DUI et services socles, ...)

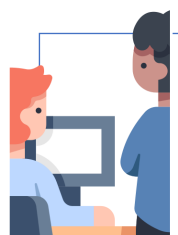
La Sécurité des Systèmes d'Information : l'incontournable



La Sécurité des SI : l'incontournable



Le GCS e-santé Pays de la Loire accompagne ses adhérents à l'amélioration de la sécurité numérique :



e-learning / faux phishing



Escape Game cyber



Affiches, fonds d'écrans



Stickers, badges métalliques



Centre de ressources cyber dédié ESMS



Base documentaire



ssi@esante-paysdelaloire.fr



Appui à la gestion des incidents



L'intelligence artificielle en santé : Quelles perspectives pour le secteur médico-social ?



Antony Escudié

*Chef de projet Data & Innovation Numériques
CHU Angers*



Bastien Le Hyaric

*Directeur des Systèmes d'Information et de la
Transformation Numérique
ADAPEI 44*

Pause

ATELIERS A PARTIR DE 11H15 :

- **Coordination des soins et de l'accompagnement avec la solution régionale parcours**
→ **SALLE 1**
- **Présentation de Mon Espace santé**
→ **SALLE 2**
- **Déploiement de MSSanté en structure médico-sociale**
→ **SALLE 3**
- **La télésanté, un levier pour l'accès aux soins**
→ **SALLE 4**



Deux ateliers successifs à 11h15 et 11h45 choisissez vos sujets !

Risques numériques et enjeux de la cybersécurité pour le médico-social



Auriane Lemesle

Responsable de pôle sécurité et conformité numériques et référente régionale SSI
GCS e-santé



Emilie Prioux

Cheffe de projet cybersécurité
GCS e-santé



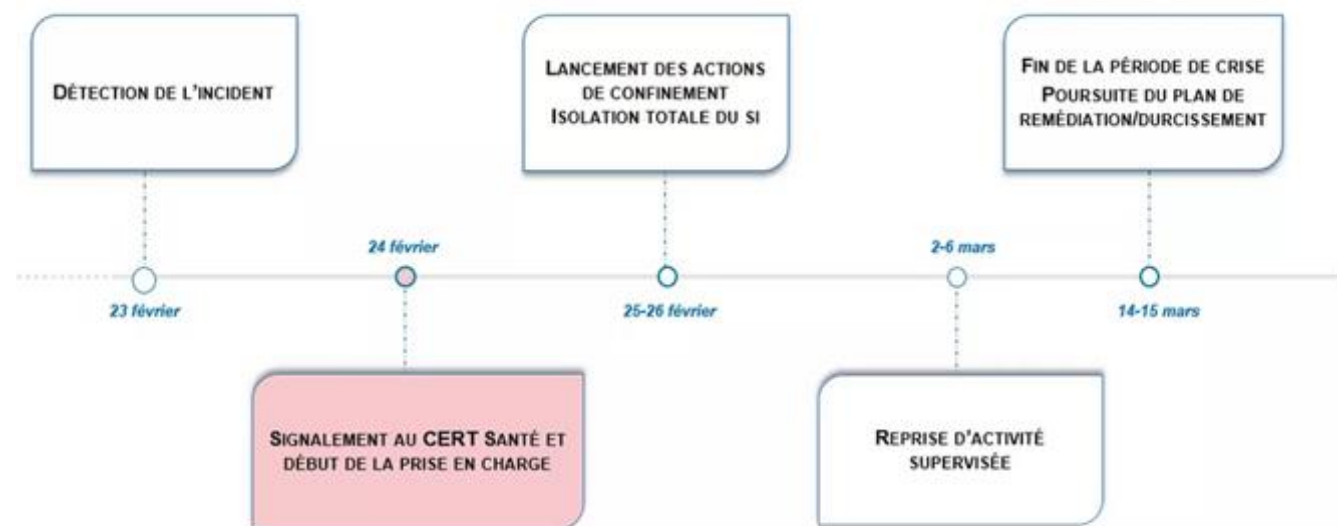
Myriam Jock

Assistante Chef de projet Cybersécurité
GCS e-santé

Actualités cyber tourmentées

- Structure répartie sur 35 communes, 20 établissements et services, + de 500 postes utilisateurs, 55 machines virtuelles, 8 serveurs physiques.
- **Attaque par rançongiciel** via connexion avec des privilèges depuis un accès VPN (exploitation vulnérabilité critique non corrigée).
- Incident rapidement détecté, mise en place d'une **cellule de crise** au sein de la structure, **débranchement réseau** des équipements compromis.
- Conséquences pour l'établissement :
 - Prise de contrôle à distance des équipements avec compromission de comptes à privilèges,
 - Perte irréversible de données/ressources comptables et administratives.

Février 2023



<https://www.cyberveille-sante.gouv.fr/retours-dexperience>

Actualités cyber tourmentées

Septembre 2023



Système d'information

La Fondation Vincent-de-Paul a été victime d'une cyberattaque rapidement maîtrisée

Publié le 06/09/23 - 15h01



La Fondation Vincent-de Paul qui gère dans le Grand-Est une quarantaine de structures (hôpital et cliniques, établissements et services médico-sociaux et sociaux) a été victime d'une cyberattaque dans la nuit du 6 au 7 septembre. "Cette attaque a touché notre système central. Tous les secteurs de la fondation sont donc concernés mais notre direction des systèmes informatiques et organisation (DSIO) est intervenue extrêmement rapidement. En moins de deux heures, toutes les connexions ont été coupées et le système sécurisé. Depuis nous fonctionnons en mode dégradé, sans informatique connectée. Les patients et usagers sont toujours accueillis mais les dossiers sont manuscrits, et cela prend du temps. Mais tout fonctionne à 100% y compris les urgences et les blocs opératoires", explique à Hospimedia la fondation.

- Cyberattaque ayant touché **plusieurs cliniques** à Strasbourg mais aussi une **quinzaine d'établissements du secteur enfance** et **15 EHPAD** en Alsace et Lorraine.
- Actions entreprises :
 - **Déconnexion** de l'intégralité du **réseau**,
 - Mise en œuvre d'une **cellule d'investigation**,
 - Activation du **mode dégradé** dans les établissements,
 - **Dépôt de plainte** auprès de la police judiciaire,
 - Et **déclaration CNIL**.
- Impacts organisationnels :
 - Continuité des prises en charge assurée (urgences, blocs opératoires, admission des patients/usagers) mais avec une messagerie indisponible,
 - Retour au dossier 100% papier pendant plusieurs jours (temps d'adaptation nécessaire pour les professionnels).

Actualités cyber tourmentées

- Alerte du CERT-Santé sur l'envoi d'un courrier alarmiste contenant des cartes SD ou clé USB à des établissements de santé (**phishing par courrier**).
- L'expéditeur conviait à consulter les supports pour avoir de plus amples informations sur une nouvelle menace sanitaire en cours.
- **Bonnes pratiques à suivre dans ce cas :**
 - Ne pas utiliser les supports, ne pas les connecter au SI.
 - Les isoler et les conserver pour traces (idéalement, sous clé ou dans un coffre).
 - Alerter le CERT-Santé (portail de déclaration des incidents).

Octobre 2023



Actualités cyber tourmentées

23 octobre 2023

MEDUSA BLOG

DAYS: 08 HOURS: 04 MINUTES: 43 SECONDS: 59

EHPAD

EHPAD is a French commercial institution for the accommodation of elderly dependents (nursing home). The company has several branches in France. The main office is located at 69 Rue République, Trun, Normandy, 61160, France

Obtain data now 180000\$

Obtain All Data 1000000\$

Download data now 1000000\$

Oct 23, 2023, 02:08:20 PM

249

REPUBLIC FRANÇAISE
CARTE NATIONALE D'IDENTITÉ n° 1
Nom: FIEBEE
Sexe: M
Date de naissance: 1995
Lieu de naissance: CHARVILLE
N° de carte: 1 23 45 67 89 01010

EHPAD Les Hortensias (Manche)

- Etablissement de 65 lits.
- Cyberattaque revendiquée par le collectif MEDUSA avec demande de **rançon de 100 000\$** (95 000€ env.).
- **Fuite de données avérée** : publication sur le darknet de plusieurs fichiers informatiques appartenant à l'EHPAD (documents administratifs internes et pièces d'identité de résidents).
- **Impacts** pour la structure :
 - Maintien du fonctionnement normal de l'établissement.
 - Fichiers médicaux et comptabilité non impactés car externalisés.
 - Dépôt de plainte auprès de la gendarmerie.
- Enquête en cours, refus de paiement de la rançon.

Actualités cyber tourmentées

5 novembre 2023

The screenshot shows a website with a red header containing the LockBit 3.0 logo and navigation links: LEAKED DATA, TWITTER, HOW TO BUY BITCOIN, CONTACT US, PRESS ABOUT US, AFFILIATE RULES, and MIRRORS. The main content area features a large red box with the text 'UNTIL FILES 12D10H02M36S PUBLICATION'. Below this, a red box indicates the deadline: 'Deadline: 19 Nov, 2023 21:13:58 UTC'. A section for 'letillet.btprrms.com' includes a logo for 'PRÉNOM N. INFIRMIÈRE BTP-RMS' and the text 'ALL AVAILABLE DATA WILL BE PUBLISHED !'. It also shows upload and update timestamps: 'UPLOADED: 05 NOV, 2023 07:14 UTC' and 'UPDATED: 07 NOV, 2023 10:58 UTC'. At the bottom, there are download options: '*Download archive', '*Download files tree', and '*Download torrent', each with a file size of '12D 11H 02M 36S' and a download icon.

PRO BTP Résidences Médico-Sociales

- La clinique SSR située à Le Tillet (Oise) semble être le seul établissement du groupe impacté.
- Cyberattaque revendiquée par le collectif LockBit avec annonce de **publication des données** prévue le **19 novembre 2023**.

Incidents en Pays de la Loire

- Les signalements des structures en Pays de la Loire :

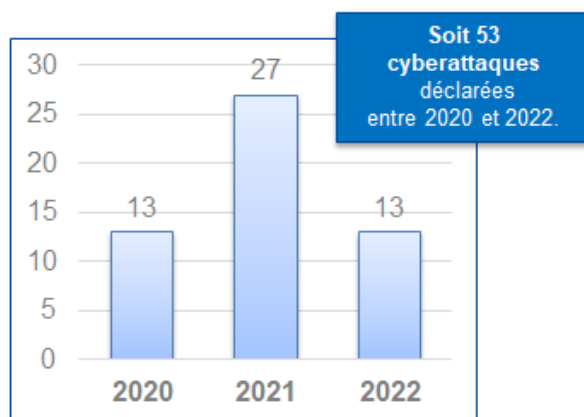
(sur la base des éléments déclarés au CERT-Santé)

(*) données disponibles à novembre 2023

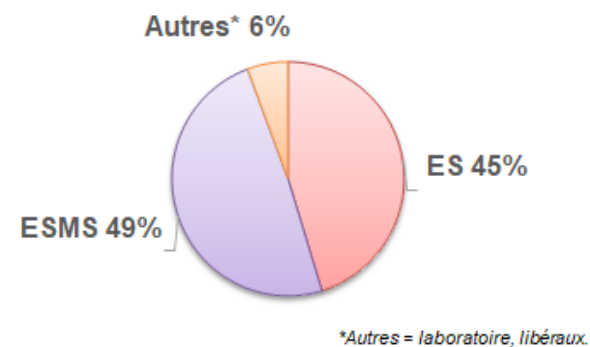
	2019	2020	2021	2022	2023(*)
National	392	369	733	592	
Régional	36	31	54	49	43

- Focus sur les chiffres concernant les incidents d'origine malveillante, dénommées "cyberattaques" :

Nombre de cyberattaques déclarées sur les Pays de la Loire 2020 - 2022



Répartition des déclarations entre 2020 et 2022, par type de structure



*Autres = laboratoire, libéraux.

Plan de renforcement Cyber 2021



Le Directeur de cabinet
SHPDS - 2021 - 40

Paris, le 30 JUIN 2021

NOTE

aux directeurs généraux des agences régionales de santé

Objet : Plan de renforcement 2021 de la cybersécurité des établissements de santé.

Réf. : Note ministérielle du 23 juillet 2019 relative au plan de renforcement de la cybersécurité des établissements de santé.
Instruction 2016-740 du 4 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé.
Instruction 109 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information dans les structures de santé.

PI : Feuille de route cyber 2021 - 2022 des agences régionales de santé

Dans les derniers mois, le secteur de la santé a déploré une multiplicité de cyberattaques par rançongiciel, et d'incidents numériques provoquant la fuite de données personnelles de santé. Cette situation entraîne dans certains territoires une perturbation du fonctionnement des services médicaux, aggravé par le contexte de la crise sanitaire.

Comme l'a souligné le Président de la République dans la présentation de la stratégie nationale pour la cybersécurité le 18 février 2021, le niveau de menace cyber auquel notre pays est actuellement confronté nous impose une réaction supplémentaire à la hauteur des enjeux, sous peine d'assister à une désorganisation de notre système de santé.

J'ai évoqué avec vous le 2 juillet dernier les nouvelles mesures de renforcement de la stratégie ministérielle de cybersécurité en santé prises en 2021, avec le rôle clé confié aux ARS dans leur déclinaison territoriale. Il s'agit notamment de s'assurer que l'ensemble des responsables des structures de santé soit mobilisé pour faire face aux risques cyber, qui vont continuer à s'accroître.

En cohérence avec le Ségur de la santé et la feuille de route stratégique du numérique en santé de « Ma santé 2022 », le plan de renforcement 2021 de la cybersécurité est prioritairement orienté vers les établissements de santé, en étroite coordination avec l'ANSSI.

Pour autant, les actions de sensibilisation et d'accompagnement sur la cybersécurité s'adressent à l'ensemble des acteurs de santé et du médico-social, comme le montre la campagne nationale de communication sur la cybersécurité en santé « Tous cyber vigilants », lancée par le ministre des Solidarités et de la Santé le 9 juin dernier. Cette campagne de communication, qui va se dérouler sur toute l'année 2021, doit permettre de sensibiliser l'ensemble du secteur aux enjeux de sécurité numérique.

Dans le cadre de la gouvernance en matière de cybersécurité installée en mars 2021, la mise en œuvre effective des actions du plan de renforcement est suivie par le cabinet du ministre chargé de la santé, au travers du comité de pilotage cyber santé mensuel, dans lequel les ARS sont représentées.

14 AVENUE DUQUESNE - 75350 PARIS 07 SP
TÉLÉPHONE : 01 40 56 60 00

- Suite aux annonces présidentielles du 18/02/21 après les incidents des CH de Dax et Villefranche sur Saone.
- Sur la base de plusieurs constats :
 - Poursuites des cyberattaques par rançongiciels avec des impacts potentiels graves sur la prise en charge des usagers.
 - Nécessité de renforcer la prise de conscience de la menace qui pèse sur le secteur santé social (dont le risque systémique).
 - Faible niveau de maturité cyber de nombreux ES et ESMS.
 - Sensibilisation des personnels à renforcer.
 - Réponse à incident cyber à renforcer.
- Des actions territoriales à conduire autour de 4 thématiques :
 - Sensibilisation aux risques cyber
 - Animation territoriale
 - Appui des structures de santé
 - Contrôle

CaRE - Cybersécurité accélération et Résilience des Etablissements



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 »



Une TF regroupant toutes les parties prenantes

Une équipe cœur

- DNS
- FSSI
- DGOS
- ANSSI
- ANS
- ARS
- GRADeS



Et des contributeurs

- Fédérations Hospitalières
- Fédérations Médico-sociales
- Etablissements de santé
- Industriels
- Centrales d'achat



Une feuille de route déclinée en 4 axes

AXE 1 - Gouvernance et résilience

AXE 2 - Ressources et mutualisation

AXE 3 - Sensibilisation

AXE 4 - Sécurité opérationnelle



Analyse de l'exposition aux risques cyber des ESMS - 2023

- Exposition variable en fonction de différents facteurs ou dimensions :



Caractéristiques du SI et degré de maturité en sécurité numérique

Augmentation de la numérisation des ESMS (nombre d'applications, services numériques utilisés, données échangées) amène de nouveaux risques à considérer.



Taille de l'organisme gestionnaire

SI des organismes de petite taille (96% du secteur) sont plus fragiles : peu ou pas de ressources SI internes, forte dépendance prestataires informatiques externes.



Couverture territoriale de l'organisme gestionnaire

Outils informatiques centralisés : risque accru d'un impact SI majoré en cas de propagation d'une cyberattaque.



Capacité de réaction et de remédiation des structures

*Connaître son SI pour mieux mesurer les impacts et actions à lancer.
Sensibiliser les utilisateurs pour limiter les risques.
S'appuyer sur le cadre réglementaire et l'environnement cyber en cas d'incident.*

CaRE – Chantier médico-social

Contexte

- Le numérique est devenu **incontournable** dans le secteur médico-social. Il permet le décloisonnement et une meilleure coordination des professionnels du secteur.
- Aujourd’hui, la **menace cyber est réelle** : il n’est plus possible de faire de la cybersécurité une variable d’ajustement des SI

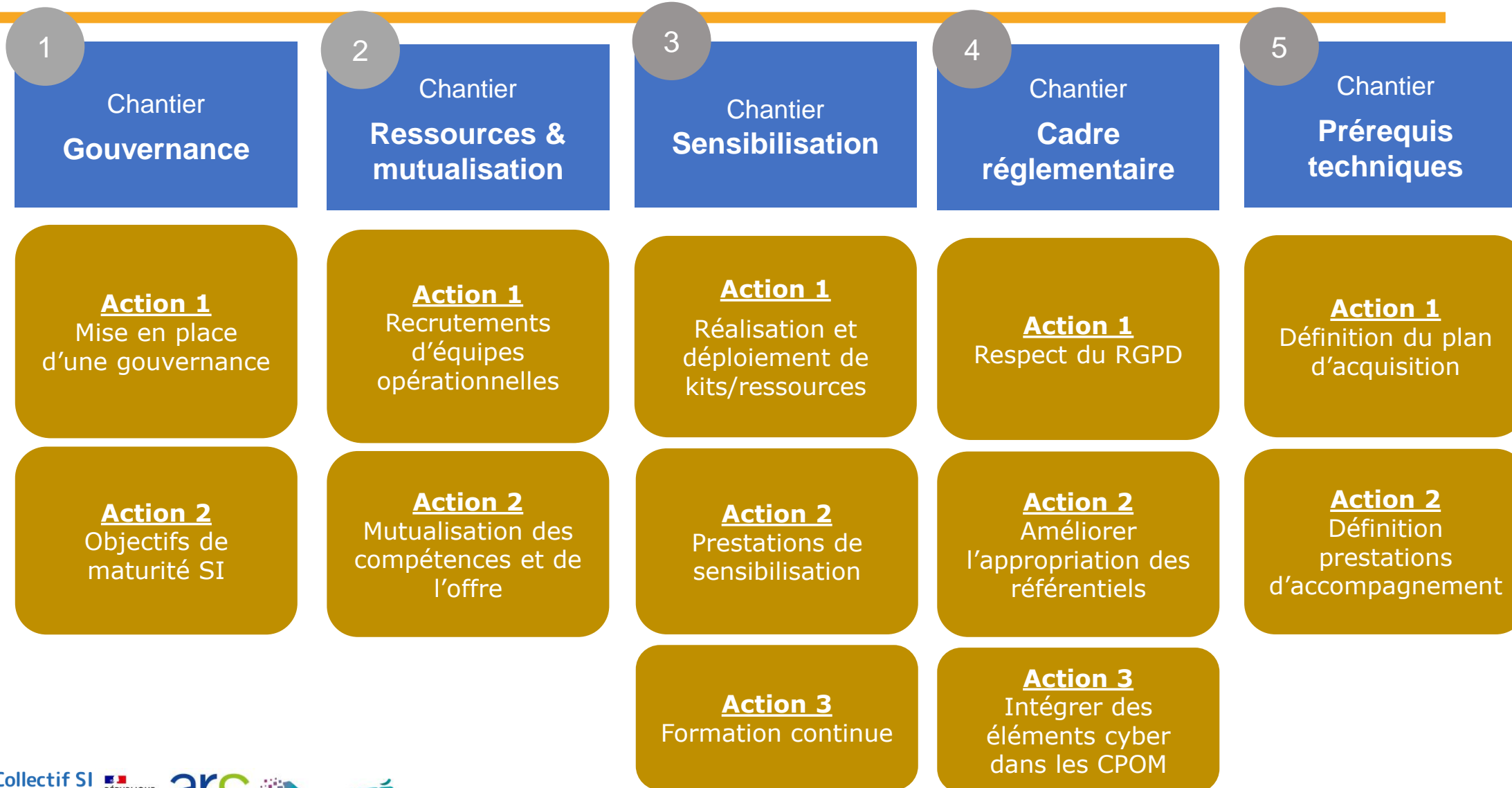
Objectifs

- Le secteur social et médico-social doit être en mesure de pouvoir **comprendre, évaluer, anticiper et maîtriser ces risques**, qui sont in fine une exposition pour la qualité des soins et des accompagnements ainsi que pour la confiance des utilisateurs.

Méthodologie

- Cette TF comporte un **chantier ESSMS** (pilotage DNS, DGCS, CNSA, ANS, ANAP, HFDS) dans lesquels s’inscrivent ces travaux.
 - Construire **collectivement** cette feuille de route pour qu’elle réponde aux enjeux et s’inscrive rapidement dans les pratiques
 - Assurer de la cohérence et de la convergence avec la feuille de route **sanitaire**

Feuille de route cyber MS : Structure générale



Un guide pour aider les ESMS sur la cybersécurité



https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_GUIDECYBER_PHASE%201-EXE%20-V2.pdf

- Le guide cybersécurité à destination des établissements et services médico-sociaux.
- Présente en 13 questions/thématiques des mesures accessibles afin d'accroître le niveau de sécurisation des SI des ESMS et sensibiliser les professionnels aux bons gestes à adopter.
- Articulation avec l'Observatoire MaturiN-SMS :
 - Objectif d'accompagner les ESMS dans leur montée en maturité en matière de numérique.
 - Lien fait le cas échéant entre les questions du guide et les indicateurs cyber contenus dans l'Observatoire.

Un guide pour aider les ESMS sur la cybersécurité

- Les 13 questions abordées dans le guide cybersécurité pour les ESMS



1. Connaissez-vous suffisamment votre parc informatique ?

• Inventorier :

- les équipements et services
- les logiciels utilisés
- les données et traitements de données
- les droits et les accès
- les interconnexions



2. Effectuez-vous des sauvegardes régulières ?

- Identifier les données à sauvegarder
- Déterminer le rythme des sauvegardes
- Choisir le ou les supports à privilégier pour la sauvegarde
- Évaluer la pertinence du chiffrement des données



3. Appliquez-vous régulièrement les mises à jour ?

- Utiliser des solutions matérielles et logicielles maintenues
- Activer la mise à jour automatique des logiciels et des matériels



4. Utilisez-vous un antivirus ?

- Déployer un antivirus sur tous les équipements
- Centraliser la gestion des antivirus



5. Avez-vous implémenté une politique d'usage de mots de passe robuste ?

- Formaliser des exigences en matière de complexité des mots de passe
- Définir des fréquences régulières de changement des mots de passe



6. Avez-vous activé un pare-feu ?

- A minima, activer le pare-feu préinstallé sur le poste de travail et son paramétrage par défaut
- Installer sur tous les postes de travail un pare-feu local (qu'il soit intégré au système d'exploitation ou qu'il soit une solution logicielle tierce)



7. Comment sécurisez-vous votre messagerie ?

- Sensibiliser les professionnels
- Proscrire la redirection de messages professionnels vers une messagerie personnelle
- Disposer d'un système d'analyse antivirus
- Activer le chiffrement de la couche de transport (Transport Layer Security-TLS)



8. Comment séparez-vous vos usages informatiques ?

- Créer des comptes utilisateurs dédiés à chaque salarié et ne disposant pas de privilège d'administration
- Au départ d'un collaborateur, faire l'inventaire de ses accès et les révoquer



9. Comment maîtrisez-vous le risque numérique lié au nomadisme des professionnels ?

- Sauvegarder régulièrement ses données
- Conserver son matériel informatique
- Réduire voire supprimer l'utilisation des clés USB



12. Avez-vous fait évaluer la couverture de votre police d'assurance cyber ?

- Contacter son assurance en vue de souscrire à une clause permettant de se prémunir de certains risques d'origine numérique (cyber malveillance, cyberattaques)



10. Comment vous informez-vous ? Comment sensibilisez-vous vos collaborateurs ?

- Formaliser une charte informatique
- Prévoir des formations à la cybersécurité



11. Savez-vous comment réagir en cas de cyberattaque ?

- Organiser des exercices de crise cybersécurité
- En cas d'incident, déconnecter son équipement ou SI d'internet mais ne pas éteindre ou modifier les ordinateurs et matériels affectés par l'attaque
- Porter plainte

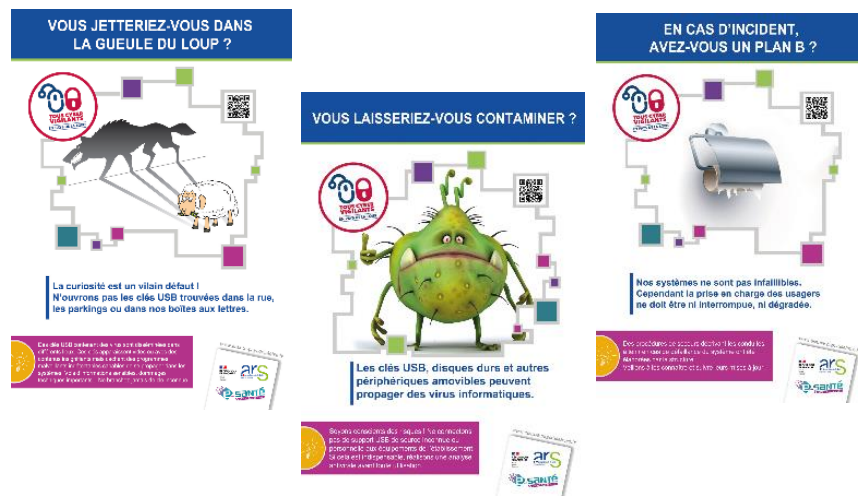


13. Maîtrisez-vous les risques numériques liés à vos relations avec des tiers ?

- Identifier et décrire dans les contrats les missions confiées à des tiers
- Formaliser des exigences de sécurité et les annexer au contrat avec les prestataires
- Identifier les membres de l'organisation assurant le lien avec les fournisseurs
- Documenter les moyens mis en œuvre par les prestataires pour respecter les exigences de sécurité

Démarche régionale

- L'Agence Régionale de Santé des Pays de la Loire est engagée depuis plusieurs années dans l'amélioration de la sécurité des SI des structures de santé.
- La mise en œuvre de la sensibilisation et des accompagnements en région est confiée au GCS e-santé Pays de la Loire (GRADeS)



<https://www.esante-paysdelaloire.fr/>



Outil de e-learning / faux phishing

• Quoi :

- Plateforme composée de 2 modules :
 - e-learning : contenus génériques et contextualisés santé (vidéo, sondage, quizz, saynètes, ...) pour sensibiliser les utilisateurs.
 - Faux-phishing (simple ou avancé) : modèles de mails prêts à l'envoi ou contextualisables.

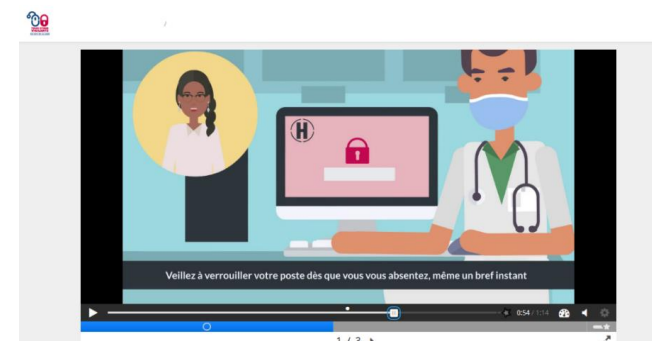
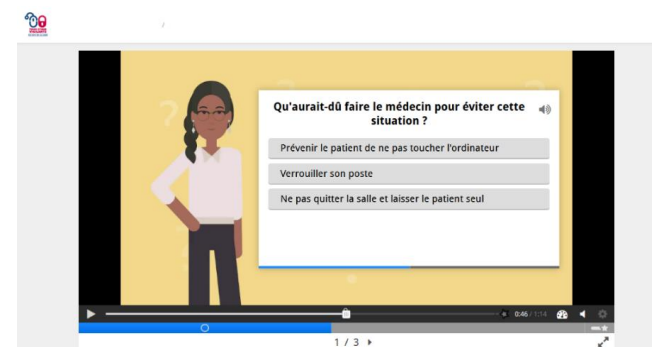
• Prérequis :

- Être adhérent au GCS e-santé PdL.
- Signature convention de services.
- Avoir 1 adresse de messagerie / utilisateur (recommandation).
- Être en capacité de mettre en œuvre des paramètres techniques (garants de la bonne réception des mails envoyés depuis la plateforme)

• Note :

- Frais d'acquisition plateforme, maintenance et abonnement pris en charge par l'ARS et le GCS.
- 2 modalités d'accès : autonomie ou mode opéré.

E-learning



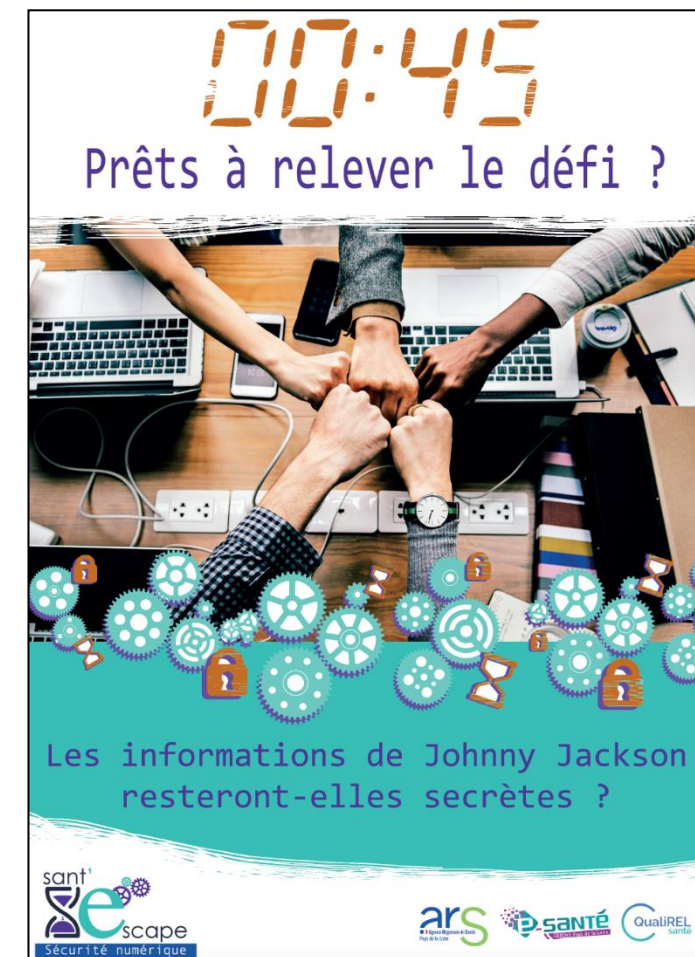
Faux-hameçonnage

De : GCS esanté PDL <gcs-esante-pdl@teams.com>
Date: mer. 20 avr. 2022 à 13:03
Subject: Vous avez reçu une invitation Teams



Sant'escape – Sécurité numérique

- **Quoi :**
 - Escape game basé sur un scénario adapté et contextualisé au domaine de la santé.
- **Objectifs :**
 - Sensibiliser à la cybersécurité et aux bonnes pratiques de sécurité SI de façon ludique, innovante et impliquante.
 - Développer le travail en équipe.
- **Comment :**
 - Les participants se mettent dans la peau des « méchants » et exploitent les mauvaises pratiques d'utilisation du SI.
 - 45 minutes de jeu (+ introduction et sensibilisation post-séance).
 - 2 possibilités de mise en œuvre :
 - Animation ponctuelle de sessions par le GCS e-santé (3 animateurs formés, 2 parcs informatiques configurés)
 - Autonomie des structures dans la mise en œuvre : formation animateur(s) et remise d'un KIT de ressources.
- **Cible :**
 - Tous publics, ne nécessite aucune connaissance technique particulière.



Accessoires de protection

Datablocker

- Permet le rechargement USB en empêchant les échanges de données et les attaques potentielles sur des prises USB non maîtrisées.
- Protège les ordinateurs / smartphones lors des connexions USB nécessitant uniquement une alimentation électrique.



Protège carte bancaire

- Permet de protéger votre carte bancaire du **télé-pickpocketing** (piratage de CB à distance pratiqué dans les espaces publics – ex : transports en commun, grands magasins).
- Bloque la lecture de la puce de votre carte bancaire via flux NFC empêchant ainsi toute transaction / collecte d'informations sans contact.

Cache webcam

- Se fixe sur la webcam de votre ordinateur afin de la masquer lorsque vous ne l'utilisez pas.
- Permet de protéger votre droit à l'image / intimité en cas de piratage de votre ordinateur / webcam.



Affiches de sensibilisation, stickers et badges métalliques

- 16 affiches déclinées en cartes postales.



- Et en fonds d'écran

- En stickers et badges métalliques :



<https://www.esante-paysdelaloire.fr/nos-services/securite-numerique-en-sante-99-111.html>

Centre de ressources SSI mutualisées pour les ESMS

- Permettre un accès aux structures les moins dotées à des compétences rares sur les thématiques cybersécurité
- L'ARS et le GCS e-santé PdL prennent en charge la mise à disposition des adhérents ESMS du GRADeS plusieurs profils :
 - Organisationnel
 - Technique
 - Juridique / conformité
- Un accompagnement complémentaire aux actions déjà conduites en région et dont le maître mot est la capitalisation :
 - Les documents produits sont mis à la disposition de l'ensemble de la communauté.
 - Le catalogue est enrichi en fonction des besoins exprimés par les structures

Centre de ressources SSI mutualisées pour les ESMS

- Les accompagnements proposés dans ce centre de ressources sont accessibles :
 - aux adhérents du GCS e-santé,
 - prioritairement pour les structures non pourvues ou ayant peu de ressources SI internes.
- Nous encourageons chaque établissement bénéficiaire à :
 - Respecter la planification des rendez-vous afin de ne pas pénaliser l'accès au service pour d'autres structures (faciliter la planification du report en cas de déprogrammation).
 - Concrétiser une partie du plan d'action remis suite à l'accompagnement (% d'actions) ou mettre en œuvre plusieurs axes d'améliorations identifiés.
- Un même établissement peut demander la réalisation de plusieurs accompagnements.
- Pour toute demande sur le centre de ressources SSI mutualisées :
 - cyber.esms@esante-paysdelaloire.fr

Centre de ressources SSI mutualisées pour les ESMS



En distanciel
(visioconférence)



Durée de 1 à 3h
(selon accompagnement)



Animé par un partenaire
(ressources expertes en cybersécurité)



Aucune action de prise en main
sur le SI n'est réalisée par le
partenaire.



Présence ressource(s) avec
connaissance configurations /
paramétrages / informations
(sur thématique choisie)



Réunion de restitution
*(1h en visio, M+1 après accompagnement,
selon la thématique)*

Centre de ressources SSI mutualisées pour les ESMS

- Catalogue des accompagnements disponibles à date :

1

Diagnostic de maturité de la sécurité du SI : questionnaire > rapport complet + plan d'actions priorisé et outil de suivi

2

Cartographie du système d'information : inventaire des composants (matériels, logiciels, ...) du SI

3

Diagnostic des équipements de sécurité (pare-feu, antivirus, sauvegarde...) : revue des contions de sécurité et des configurations

4

Diagnostic messagerie : vérification du maintien en condition de sécurité et du paramétrage permettant de limiter la réception de message indésirables et les usurpations d'identité

4bis

Diagnostic plateforme collaborative Office 365 : revue des droits, utilisateurs, configuration et traçabilité

5

Aide à l'élaboration du plan de sauvegarde : cartographie des données, des technologies utilisées, planification des sauvegardes et restauration

6

Préparation à la réalisation d'un test de restauration : cadrage technique et plan d'actions

Base documentaire régionale

Modèles de documents

- Politique de sécurité du SI
- Charte utilisateurs
- Procédure de gestion des incidents
- Fiche réflexe signalement d'incident

Sécurité numérique en santé

CLAUSES DE SECURITE CONTRATS PRESTATAIRES SI

Modèle à adapter et contextualiser

Insérer le logo de la structure

Date de dernière mise à jour	20/04/2020
Version	2.2
Classification	Interne
Nombre de pages	15

MIS hors formulaire du DOCUMENT

Version	Date	Description
1.0	20/03/2020	Initialisation du document
2.0	20/04/2021	Appel de clauses OSI

Sécurité numérique en santé

CHARTRE D'UTILISATION DES TECHNOLOGIES NUMERIQUES

Utilisateurs

Insérer le logo de la structure

Date de dernière mise à jour	30/11/2017
Version	1.0
Classification	Interne
Nombre de pages	14

HISTORIQUE DU DOCUMENT

Version	Date	Description

Mémos

- Synthétisent en une page les bonnes pratiques à mettre en œuvre : gestion des mises à jour, des antivirus, des mots de passe...
- Les sources renvoient vers les guides ANSSI, PGSSI-S, CNIL, etc.

Sécurité numérique en santé

MÉMO – Antivirus et pare-feu

Les antivirus et les pare-feu sont des solutions essentielles et souvent complémentaires permettant de se prémunir contre les risques d'infection et d'intrusion dans les systèmes d'information.

ANTIVIRUS

PARE-FEU

EN FONCTION DES BESOINS

TOUT BLOQUER PAR DÉFAUT

RÈGLEMENTAIRE MIS À JOUR

SCAN PERMANENT

CONTRÔLER LES SOURCES EXTERNES

VERIFIER LE RÉGLAGE

Sécurité numérique en santé

MÉMO – Gestion des sauvegardes

La sauvegarde des informations du système d'information est vitale et permet de garantir la continuité des activités et la disponibilité des données en cas d'incident.

RISQUES À COUVRIR

ACTEURS CONCERNÉS

IDENTIFIER LES BESOINS

EXTERNALISATION ET SUPPORT

RESTAURATION ET CONTRÔLE

GARANTIR LA CONFIDENTIALITÉ

CONTRÔLER LE FLUX D'INFORMATIONS

JOURNALISATION

TYPE DE SAUVEGARDE



À venir : un nouvel outil en 2024 !

Appui à la gestion des incidents

Rappel des actions déclaratives à réaliser en cas d'incident sur votre SI

- **Déclarer l'incident** sur le portail dédié (obligation réglementaire), sans délai : <https://signalement.social-sante.gouv.fr>
 - Le CERT-Santé hébergé par l'Agence du Numérique en Santé (ANS), l'Agence Régionale de Santé (ARS) et le GCS e-santé PdL sont informés du signalement effectué.
 - Aide au signalement disponible sur le portail de cyberveille : <https://www.cyberveille-sante.gouv.fr/faq>
 - Permanence téléphonique du CERT-Santé 24h/24 et 7j/7 en cas d'urgence : 09 72 43 91 25.
- Si l'incident est **d'origine malveillante** :
 - Effectuer un **dépôt de plainte** auprès de la gendarmerie ou de la police.
 - **Recueillir toutes les traces** possibles et **lister les actions** techniques et fonctionnelles mises en œuvre sur le SI.
 - Suivre la recommandation gouvernementale de **ne pas payer la rançon** demandée (le cas échéant).
- En cas de **violation de données à caractère personnel, potentielle ou avérée** :
 - Effectuer une déclaration auprès de la **CNIL** dans les **72 heures** après survenue de l'incident.

Appui à la gestion des incidents

Sécurité
numérique
en santé

MÉMO – Dépôt de plainte suite à
un incident SI d'origine malveillante

[Octobre 2023]

Tout incident majeur d'origine malveillante impactant significativement le système d'information doit faire l'objet d'un dépôt de plainte.

POURQUOI DÉPOSER PLAINTE ?

- ✓ Être reconnu en tant que victime et ainsi faire valoir vos droits via l'ouverture d'une enquête pénale ;
- ✓ Être accompagné dans une situation complexe par :
- ✓ Permettre le cas échéant, selon vos contrats d'assurance, de bénéficier des résultats de l'enquête (identité de délégués, ...)
- ✓ Participer à la lutte contre la cybercriminalité en apprenant davantage sur les méthodes des cybercriminels
- ✓ Limiter le risque d'engagement de votre responsabilité en cas de poursuites judiciaires

Sécurité
numérique
en santé

MÉMO – Collecte des traces suite à un incident SI
d'origine malveillante

[Octobre 2023]

La collecte de traces suite à un incident numérique d'origine malveillante est une action nécessaire à l'investigation et au dépôt de plainte.

OBJECTIFS

- ✓ Mettre à disposition des personnes en charge de l'investigation numérique et des forces de l'ordre des éléments techniques nécessaires ;
- ✓ Déterminer le chemin d'attaque et les faiblesses exploitées pour pouvoir y remédier ;
- ✓ Identifier les responsables ;
- ✓ Fournir de preuves recevables pour engager une procédure.

ACTEURS CONCERNÉS

- ✓ Utilisateurs du SI
- ✓ Responsable réseau
- ✓ Responsable applicatif
- ✓ Direction des systèmes d'information
- ✓ RSSI

PRÉSERVER TOUTES LES TRACES

- ✓ Déconnecter du réseau (câble / wifi / cartes réseaux virtuelles) les appareils concernés pour stopper l'incident et mettre en quarantaine les machines et supports de stockage amovibles concernés (disque externe, clé USB...) ou récemment connectés aux machines concernées.

- ✓ Ne pas éteindre électriquement les appareils compromis pour éviter la perte d'informations en mémoire. Si besoin, brancher les ordinateurs portables / smartphones / tablettes sur secteur.

- ✓ Tenir une main courante traçant l'ensemble des actions / événements.

- ✓ Identifier si possible le « patient zéro » (première machine compromise) et l'isolier.

- ✓ Effectuer une copie complète de la mémoire (RAM) de l'appareil ou du fichier mémoire pour une machine virtualisée (.vmem pour Virtual Machine volatile memory file ou .vmsx pour Virtual machine suspend file sur une machine VMWare).

- ✓ Si besoin de déplacer l'appareil ou si ce dernier est inutilisable, le mettre en état de veille prolongée (machine physique ou virtuelle) puis attendre 15 secondes avant de retirer le câble d'alimentation de la prise de courant (machine physique uniquement). Afin de maximiser les chances de pouvoir conserver les traces, tout appareil en veille doit être rebranché électriquement. Identifier clairement la non-disponibilité des matériels concernés (ordinateur, disque dur externe...) pour les utilisateurs en effectuant un marquage clair sur l'appareil « cyberattaque, ne pas éteindre / allumer / connecter l'appareil ».

- ✓ Ne pas rallumer le poste de travail ou l'appareil compromis, si ce dernier est éteint.

- ✓ Prendre des photos ou faire des captures d'écran de tout ce qui est visible.

- ✓ Récupérer les fichiers de journalisation (logs) de vos pare-feux (sans se limiter aux données présumées relatives à l'attaque), des serveurs mandataires (proxys), des postes ou serveurs touchés qui seront des éléments d'investigation.

- ✓ Effectuer une copie complète (disque dur) des machines impactées en privilégiant les copies intégrales (dite « bit à bit »). Des outils libres et gratuits tels que EWF Tools sont dédiés à l'acquisition de données pour l'investigation numérique. L'utilisation d'un bloqueur physique permettant d'éviter toute altération des données sur le support d'origine est fortement recommandée.

Vous pouvez vous faire assister d'un professionnel pour réaliser certaines actions ou pour conserver le matériel à disposition des enquêteurs. Il est aussi possible, selon les enjeux, de réaliser ces actes en présence d'un huissier de justice.

COMMENT

1. Etape 1 :

La structure victime d'un acte malveillant sur S

caractériser les faits autant que possible (cf. 9 Ques

2. Etape 2 :

À la suite de cette première analyse, le représenta

• Soit, en se déplaçant physiquement dans un o

• Soit, sur le site Internet : <https://www.pre-plainte>

• Soit, en transmettant un courrier papier au pn

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.



Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

Le dépôt de plainte doit intervenir avant la réin

de l'incident afin de les fournir aux enquêteurs. Cf.

• Documentation – Fiches mémo

- **Dépôt de plainte** suite à un incident d'origine malveillante
- **Collecte des traces** suite à un incident SI d'origine malveillante (à destination des équipes SI / prestataire).

=> <https://www.esante-paysdelaloire.fr/nos-services/securite-numerique-en-sante-99-115.html>

• Aide et accompagnement dans la déclaration au CERT-Santé

- Facilitation des échanges entre la structure, le CERT Santé et le prestataire informatique de la structure (éventuellement)
- Conseils techniques et organisationnels



18 octobre 2023

Vulnérabilité exploitée et non corrigée dans les systèmes Cisco IOS XE

Le CERT Santé et l'ANSSI informent d'une vulnérabilité activement exploitée qui pourrait permettre à un attaquant non authentifié de créer un compte administrateur sur le système. Aucun correctif n'est disponible pour l'instant.

Cisco - CVE-2023-20198

Un défaut de gestion de privilèges dans Cisco IOS XE permet à un attaquant non authentifié, en envoyant des requêtes spécifiquement forgées, de créer un compte administrateur sur le système. Cette vulnérabilité présente un score de dangerosité (CVSSv3.1) de 10/10 et est déjà exploitée.

Risques

Exécution de code arbitraire à distance.

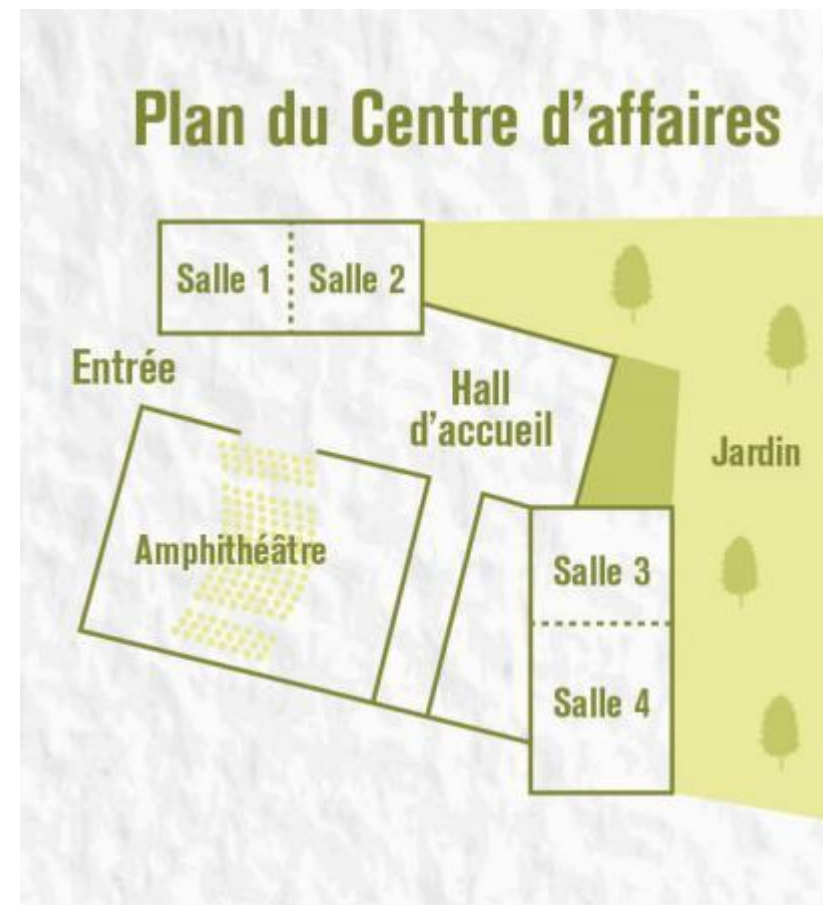
• Relai d'alertes du Ministère

- Vulnérabilités critiques, attaques en cours, conduites à tenir, veille...
- Rappel des modalités de signalement,
- ...

Pause

ATELIERS DE 14H30 à 15H30 :

- **Coordination des soins et de l'accompagnement avec la solution régionale parcours**
→ **SALLE 1**
- **Présentation de Mon Espace santé**
→ **SALLE 2**
- **Déploiement de MSSanté en structure médico-sociale**
→ **SALLE 3**
- **La télésanté, un levier pour l'accès aux soins**
→ **SALLE 4**



Deux ateliers successifs à 14h30 et 15H00 choisissez vos sujets !

Regards croisés sur le déploiement du Dossier Usager Informatisé

Retours d'expérience



François Le Brun

Directeur de projets

SYNAPPSE pour l'ADAPEI ARIA 85



Isabelle Redon

Directrice

EHPAD Bellevue



Nicolas Sorin

Chef de projet ESMS Numérique

GCSMS 53



Anne-Flore Pujos

Responsable qualité et gestion des risques

VYV3

Animateur



Rémi Barba

Chargé de projets ESMS Numérique

ARS Pays de la Loire

Regards croisés sur le déploiement du Dossier Usager Informatisé



François Le Brun

Directeur de projets

SYNAPPSE pour l'ADAPEI ARIA 85



Isabelle Redon

Directrice

EHPAD Bellevue



Nicolas Sorin

Chef de projet ESMS Numérique

GCSMS 53



Anne-Flore Pujos

*Responsable qualité et gestion des risques
VYV3*



- **Projet ADAPEI ARIA VENDEE**
- **Financé en 2021**
- **Mise en conformité**
- **DUI Ogyris**
- **49 ESMS PH**



- **Projet GCSMS 53**
- **Financé en 2021**
- **Acquisition**
- **DUI Netsoins**
- **15 ESMS PA**



- **Projet VYV3**
- **Financé en 2021**
- **Mise en conformité**
- **DUI Imago DU**
- **29 ESMS PH**

Résumé théâtral des moments forts de la journée.



Merci pour votre participation !

Donnez-nous votre avis sur la journée

