État de la menace et Programme CaRE (Cyberaccélération de la résilience des établissements)

Conférence cybersécurité

Financé par l'Union européenne NextGenerationEU

Observatoire des signalements d'incidents de SSI pour les secteurs santé et médico-social

Chiffres 2023 vs 2022

Gestion des incidents

581 592
incidents déclarés

165 165
demandes d'accompagnement

93 103
interventions d'appui technique

Veille proactive

983 2200
alertes envoyées

50 76
cas de compromission

23 22
Vulnérabilités critiques identifiées

Bulletins & Audits de cybersurveillance

106 9
Bulletins d'alerte publiées

529 348
Audits réalisés

Financé par l'Union européenne NextGenerationEU

Origines et Impacts des incidents

Chiffres 2023 vs 2022

Origine des incidents

50% 50%

Nombre d'incidents d'origine malveillante

71% 78%

Incidents de sécurité déclarés par les établissements de santé

61

C'est le nombre de structures ayant déclaré plus de 2 incidents durant l'année 2023 sur 462 structures au total. Parmi elles, il y avait 301 établissements de santé et 121 établissements et services médico-sociaux. 8 établissements de santé ont signalé au moins quatre incidents.

Impact des incidents

17 22

Nombre d'incident d'origine malveillante ayant un effet extrême ou important sur le SI de l'établissement victime

69

mises en danger patients potentielles

1 mise en danger patient avérée

53%

C'est le pourcentage de structures indiquant que l'incident n'a eu aucun impact sur son fonctionnement en 2023. Ce chiffre est en baisse par rapport à 2022 mais présente une augmentation par rapport à 2021 puis qu'il était de 38%.

Financé par l'Union européenne NextGenerationEU

Evolution de l'activité malveillante

Chiffres 2023 vs 2022

2023 2022	Ecart	Description
32 27	+18%	**Nombre de rançongiciels**
43% 38%	+8%	Compromission du SI (compte de messagerie, compte AD, comptes VPN, exploitation de CVE)
36% 45%	-23%	Message électronique malveillant (Hameçonnage, malspam)
9% 3%	x3	Fuite d'information
9% 12%	-30%	Logiciel malveillant / virus
3.5% 0.7%	x5	Attaque par déni de service

Financé par l'Union européenne NextGenerationEU

Incident en PdL et partenariat CERT-Santé /GCS e-santé

- Signalement de 50 incidents en 2023
- Intervention conjointe GRADeS / CERT-Santé sur 13 incidents
- Focus accompagnement de l'Etape Jeunes

l'étape ASSOCIATION
L'INNOVATION AU SERVICE DE L'INSERTION

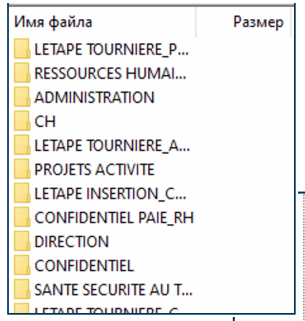
Localisation : Nantes

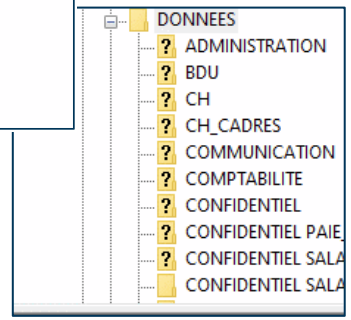
Chiffres clés : 230 salariés, 1000 personnes accompagnées, 455 logements.

Secteurs : handicap psychique, protection de l'enfance, grande précarité.

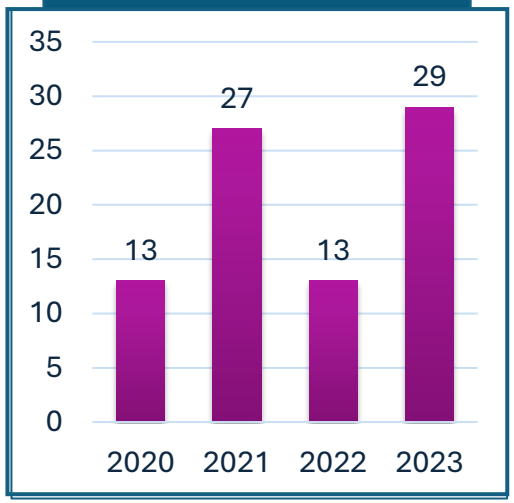
Activités : hébergement et/ou accompagnement

Architecture : hébergement interne des données, 17 serveurs, 3 éditeurs de logiciels





Soit 82 cyberattaques déclarées entre 2020 et 2023.



	2019	2020	2021	2022	2023	2024
Incidents en région PdL	36	31	54	49	50	19

Financé par l'Union européenne NextGenerationEU

Des professionnels de santé libéraux également concernés

Cas d'usurpation d'identité d'un éditeur de logiciel dédié aux pharmacies

- Information du CSIRT régional : un acteur malveillant **s'est fait passer pour le service informatique** de l'éditeur WINPHARMA, auprès de pharmacies clientes, en vue **d'obtenir leurs codes d'accès** et **installer un virus** dans leurs SI, par le biais d'une **mise à jour de sécurité**.
- Le virus semble en mesure **d'exfiltrer les données sensibles** des patients stockées dans le logiciel. La société a **prévenu ses clients** de la situation en cours (7000 sur le territoire) et a pu intervenir au moins sur une pharmacie visée. Néanmoins, d'autres pharmacies ont pu être infectées.

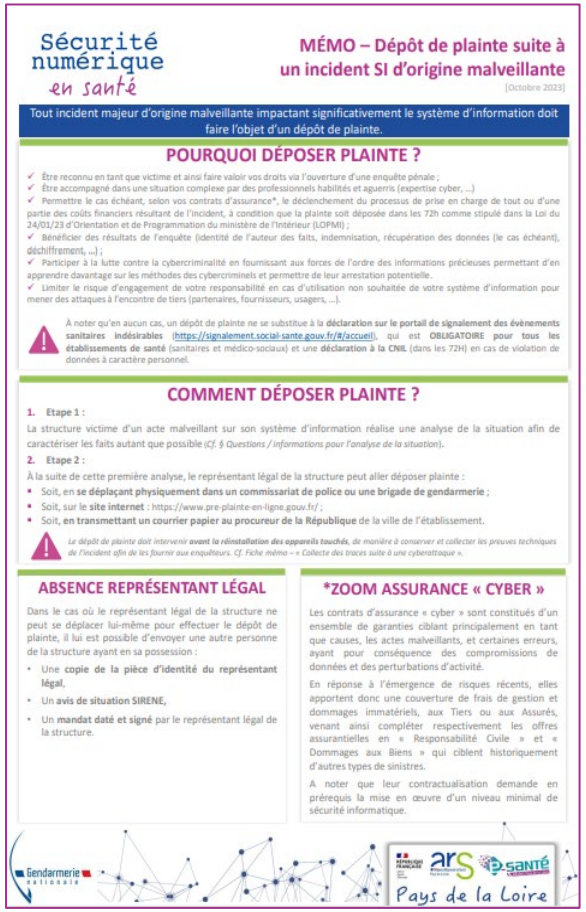
Une information transmise par le GRADeS à l'URPS pharmaciens

URPS Pharmaciens PAYS DE LA LOIRE

Financé par l'Union européenne NextGenerationEU

Partenariat Gendarmerie

- **Co-construction de deux fiches mémo :**



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 des professionnels habilités et aguerris (expertise cyber, ...)
- ✓ Permettre le cas échéant, selon vos contrats d'assurance*, le déclenchement du processus de prise en charge de tout ou d'une partie des coûts financiers résultant de l'incident, à condition que la plainte soit déposée dans les 72h comme stipulé dans la Loi du 24/01/23 d'Orientation et de Programmation du ministère de l'Intérieur (LOPMI) ;
- ✓ Bénéficier des résultats de l'enquête (identité de l'auteur des faits, indemnisation, récupération des données (le cas échéant), déchiffrement, ...) ;
- ✓ Participer à la lutte contre la cybercriminalité en fournissant aux forces de l'ordre des informations précieuses permettant d'en apprendre davantage sur les méthodes des cybercriminels et permettre de leur arrestation potentielle.
- ✓ Limiter le risque d'engagement de votre responsabilité en cas d'utilisation non souhaitée de votre système d'information pour mener des attaques à l'encontre de tiers (partenaires, fournisseurs, usagers, ...).

À noter qu'en aucun cas, un dépôt de plainte ne se substitue à la **déclaration sur le portail de signalement des évènements sanitaires indésirables** (https://signalement.social-sante.gouv.fr/#/accueil), qui est **OBLIGATOIRE pour tous les établissements de santé** (sanitaires et médico-sociaux) et une **déclaration à la CNIL** (dans les 72H) en cas de violation de données à caractère personnel.

COMMENT DÉPOSER PLAINTE ?

1. **Etape 1 :**

La structure victime d'un acte malveillant sur son système d'information réalise une analyse de la situation afin de caractériser les faits autant que possible (*Cf. § Questions / informations pour l'analyse de la situation*).

2. **Etape 2 :**

À la suite de cette première analyse, le représentant légal de la structure peut aller déposer plainte :

- Soit, **en se déplaçant physiquement dans un commissariat de police ou une brigade de gendarmerie** ;
- Soit, sur le **site internet** : https://www.pre-plainte-en-ligne.gouv.fr/ ;
- Soit, **en transmettant un courrier papier au procureur de la République** de la ville de l'établissement.

*Le dépôt de plainte doit intervenir **avant la réinstallation des appareils touchés**, de manière à conserver et collecter les preuves techniques de l'incident afin de les fournir aux enquêteurs. Cf. Fiche mémo – « Collecte des traces suite à une cyberattaque ».*

ABSENCE REPRÉSENTANT LÉGAL

Dans le cas où le représentant légal de la structure ne peut se déplacer lui-même pour effectuer le dépôt de plainte, il lui est possible d'envoyer une autre personne de la structure ayant en sa possession :

- Une **copie de la pièce d'identité du représentant légal**,
- Un **avis de situation SIRENE**,
- Un **mandat daté et signé** par le représentant légal de la structure.

*ZOOM ASSURANCE « CYBER »

Les contrats d'assurance « cyber » sont constitués d'un ensemble de garanties ciblant principalement en tant que causes, les actes malveillants, et certaines erreurs, ayant pour conséquence des compromissions de données et des perturbations d'activité.

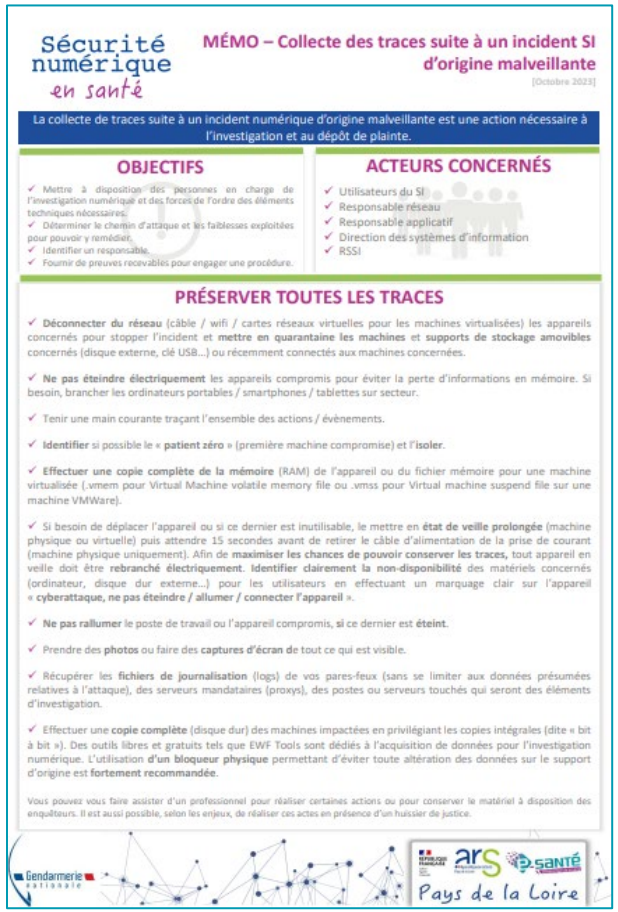
En réponse à l'émergence de risques récents, elles apportent donc une couverture de frais de gestion et dommages immatériels, aux Tiers ou aux Assurés, venant ainsi compléter respectivement les offres assurantielles en « Responsabilité Civile » et « Dommages aux Biens » qui ciblent historiquement d'autres types de sinistres.

A noter que leur contractualisation demande en prérequis la mise en œuvre d'un niveau minimal de sécurité informatique.

Gendarmerie nationale — ars Agence Régionale de Santé Pays de la Loire — e-santé Pays de la Loire

Dépôt de plainte à la suite d'un incident d'origine malveillante :

- Pourquoi déposer plainte ?
- Comment ?
- Préparer son dépôt de plainte
- Questions pour analyser la situation



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 un responsable.
- ✓ 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 pour les machines virtualisées) 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 / évènements.
- ✓ **Identifier** si possible le « **patient zéro** » (première machine compromise) et l'**isoler**.
- ✓ **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 .vmss 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 pares-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.

Gendarmerie nationale — ars Agence Régionale de Santé Pays de la Loire — e-santé Pays de la Loire

Collecte des traces à la suite d'un incident SI d'origine malveillante (à destination des équipes SI / prestataire)

- Préserver toutes les traces
- Recevabilité d'une trace en tant que preuve

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

Financé par l'Union européenne NextGenerationEU

CaRE, un programme ambitieux et inédit

Multiplication des cyberattaques (CHSF, CHV,…)

Une coordination par la DNS et l'ANS

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ | Délégation ministérielle au numérique en santé | DNS

AGENCE DU NUMÉRIQUE EN SANTÉ

Lancement des premiers appels à projet et financement

2021 → **Décembre 2022 : Lancement de la Task Force (TF) Cyber** → **Fin 2023** → **S1 2024**

Une équipe « cœur »

FSSI
DGOS
ANSSI
ARS
GRADeS

Des contributeurs

- HAS, ANAP, Fédérations Hospitalières, Fédérations Médico-Sociales, Industriels, Etablissements de santé, Centrales d'achat, représentants des Usagers, …

Publication du plan d'action Cybersécurité accélération et Résilience des Etablissements

Ce plan d'action est décliné en **4 axes** :

- **Gouvernance et résilience**
- **Ressources et mutualisation**
- **Sensibilisation**
- **Sécurité opérationnelle**

Une comitologie dédiée …

- COPIL cyber
- Comité fédérations hospitalières
- Comité régional
- Comité de suivi

… des ambitions …

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

… et des moyens :

- Au total, une **enveloppe de 750M€** envisagée **jusque 2027**
- **Investissement 2024-2025 : 250M€ déjà fléchée sur les domaines prioritaires** (notamment exposition internet, annuaires techniques, et moyens d'identification électronique des professionnels de santé) et sur les offres d'accompagnement régional

Financé par l'Union européenne NextGenerationEU

Déclinaisons opérationnelles nationales et régionales de l'axe 1

Gouvernance et Résilience

Certification HAS 2024

- *Intégration de critères numériques et cyber dans le référentiel de certification 2024 (123 ES visités au T1 2024)*
- *Recrutement de 175 experts visiteurs numériques (33 formés à fin 2023)*

Exercices de gestion de crise régionaux

Réalisation d'un premier exercice régional d'ici S1 2024 pour les régions JOP 2024

Pays de la Loire : Réalisation en février

PCA / PRA

Plan de Continuité et de Reprise d'Activité

- *Des kits méthodologiques mis à disposition sur le site de l'ANS après une phase pilote fin 2023 :*
  - Kit PCA-PRA: Cadrage
  - Kit PCA-PRA: Méthodologie d'élaboration
  - Kit PCA-PRA: Gestion du PCRA
  - Kit PCA-PRA: Exemples BIA

S'appuie sur la documentation de référence (Plan Blanc Numérique de la DGOS, guide de la continuité d'activité du SGDSN) et adopte une approche orientée métier et non SI.

CPOM

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

Exercices de gestion de crise

- *Accompagnement à la réalisation des premiers exercices de crise*
- *Un kit à disposition sur le site de l'ANS, enrichi pour s'adapter aux activités PSY et SSR et création d'un scénario dédié pour les HAD.*

61% des ES ont réalisé un exercice de crise depuis janvier 2023 pour un total de 1722 exercices

78 exercices réalisés soit 68% des ES

Financé par l'Union européenne NextGenerationEU

Exercices de crise cyber en PdL

Pas du tout satisfaisant	Peu satisfait	Satisfait	Très satisfait
0 réponses	1 réponse	69 réponses	48 réponses

99,15%

« satisfaisant ou Très satisfaisant »

85 exercices réalisés ou planifiés

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

74% des établissement de santé ont réalisé un exercice de crise cyber

Financé par l'Union européenne NextGenerationEU

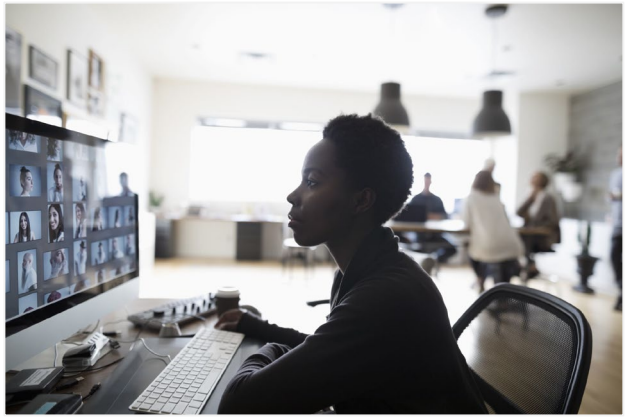
25% *OBJECTIF : 31/05/2023* Atteint le 22/06/2023

50% *OBJECTIF : 31/12/2023* Atteint le 20/11/2023

70% *OBJECTIF : 30/05/2024* Atteint le 06/02/2024

Déclinaisons opérationnelles nationales et régionales de l'axe 2

Ressources et mutualisation

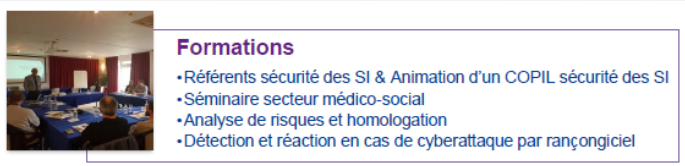


Renforcer l'attractivité des ressources en ES

➡ *Revalorisation des grilles salariales hospitalières* (*Décret n° 2024-52 du 30 janvier 2024 portant statut particulier du corps des ingénieurs hospitaliers*)

Centre de Ressources Régional Cyber

- Ces CRRC se voient attribuer plusieurs missions : 8 objectifs généraux ont été définis et 3 spécifiques, propres au secteur du médico-social.



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

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

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

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

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

Préparation à la crise cyber
- Soutien à la réalisation d'exercices de crise cyber
- Centre de ressources SSI accessible aux structures les moins dotées (ESMS)
- Synthèse de l'état de l'art de la sauvegarde des données

Veille technologique et réglementaire
- https://www.scoop.it/t/ssi-sante

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

La sécurité numérique 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

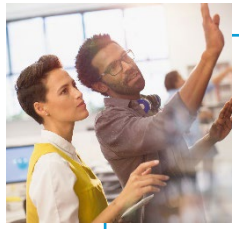
- https://www.scoop.it/t/ssi-sante

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 ressources SSI accessible aux structures les moins dotées (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

Catalogue des accompagnements du Centre de ressources SSI mutualisées à destination des ESMS

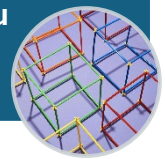
Evaluation du niveau général de maturité de sécurité du SI basée sur un questionnaire, donnant lieu à un plan d'action concret et priorisé.

1.Diagnostic de maturité de la sécurité du SI

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

Note : Modèle fourni

2.Cartographie du système d'information



Revue des versions et des configurations de sécurité des pares-feux, antivirus, sauvegardes, …

3.Diagnostic des équipements de sécurité

Revue des versions et des configurations de sécurité des pares-feux, antivirus, sauvegardes, …

4.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.

5. 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

6. Diagnostic de messagerie

Revue des droits, gestion des utilisateurs, configuration et traçabilité

6 BIS. Diagnostic plateforme collaborative Office 365

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

7. Aide à l'élaboration du plan de sauvegarde

Cadrage technique et plan d'action

Note : test non réalisé en séance, à réaliser a posteriori par la structure.

8. 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.

9. Sécurisation de la configuration Wifi

Financé par l'Union européenne NextGenerationEU

Centre de ressources SSI mutualisées à destination des ESMS

- A ce jour, **37 structures** ont intégré la démarche et bénéficié d'un premier accompagnement du centre de ressources SSI mutualisées, destiné aux ESMS.
- Un total de **53 accompagnements réalisés ou planifiés**.

Quelques retours de bénéficiaires :

« Diagnostic très instructif et utile pour le futur de l'établissement ! Un technicien très pédagogue et à l'écoute. »

Direction - EPSMS

« La compréhension et l'échange autour du plan d'action permettent une amorce rapide et accessible des premières actions d'amélioration. »

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

« 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

« Très bon partenariat avec le GCS e-santé, qui permet aux petites structures de se mettre en conformité au regard des attendus actuels en termes d'évolution des SI des ESMS. »

Direction - EHPAD

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

Direction - EPMS

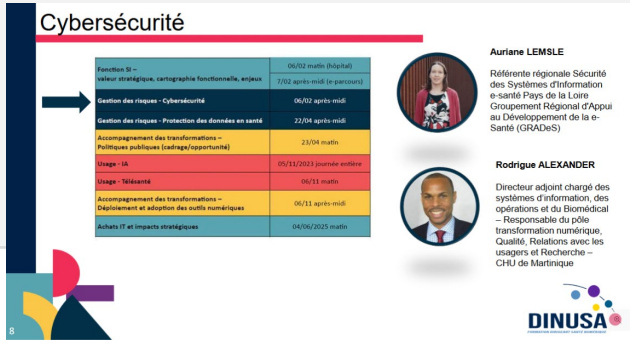
Financé par l'Union européenne NextGenerationEU

Déclinaisons opérationnelles nationales et régionales de l'axe 3

Sensibilisation

Formations

Modules obligatoires numériques et cyber (formations initiales et continues professionnels de santé et EHESP)



Formations régionales

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

Guides

Outils régionaux

Présence aux évènements nationaux et régionaux, publications

Journée régionale cyber, Participation à SantExpo 2023, au Congrès de l'APSSIS, à la Semaine européenne de la e-santé 2023, ….

Journée régionale cyber

Congrès de l'APSSIS

Semaine de la e-santé

SantExpo

Financé par l'Union européenne NextGenerationEU

Formation à la détection et réaction face à une attaque par rançongiciel

Un apport théorique …

- Panorama de la menace (zoom sur le secteur de la santé)
- Focus sur la menace de type rançongiciel (exemples du secteur)
- Conséquences d'une cyberattaque pour un établissement de santé
- Descriptif des différentes phases de l'attaque
- Cas concrets permettant d'identifier des signaux faibles en amont

… et pratique

- Pour alerter et protéger via la fiche de qualification et d'alerte

À destination des membres des équipes SI

Une demi-journée (3h)

Des supports variés

Quizz

Présentation

Vidéos

Financé par l'Union européenne NextGenerationEU

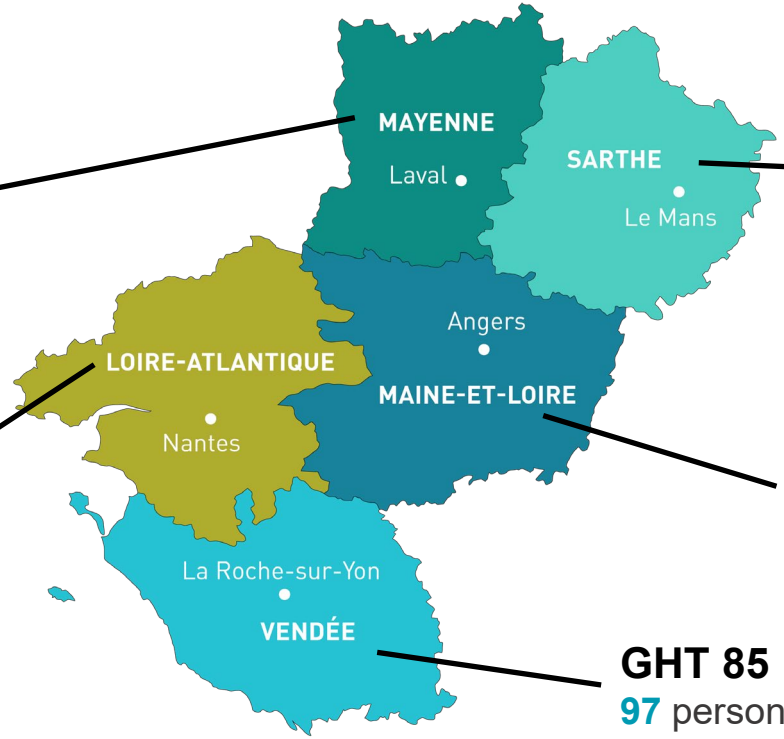
Formation à la détection et réaction face à une attaque par rançongiciel

GHT 53
30 personnes (février 2024)

LNA Santé
20 personnes (janvier 2024)

VYV3
10 personnes (juin 2024)

ELSAN
10 personnes (juin 2024)



GHT 72
69 personnes (janvier 2024)

CH Mamers
8 personnes (mars 2024)

GHT 49 & Centre Les Capucins
21 personnes (décembre 2023)

VYV3
20 personnes (juin 2024)

GHT 85
97 personnes (juin 2023)

231 personnes ont déjà bénéficié de la formation

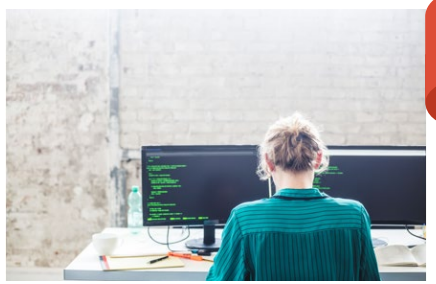
(Note de satisfaction moyenne : **9,06 / 10**)

Environ 60 personnes supplémentaires devraient bénéficier de la formation au second trimestre 2024

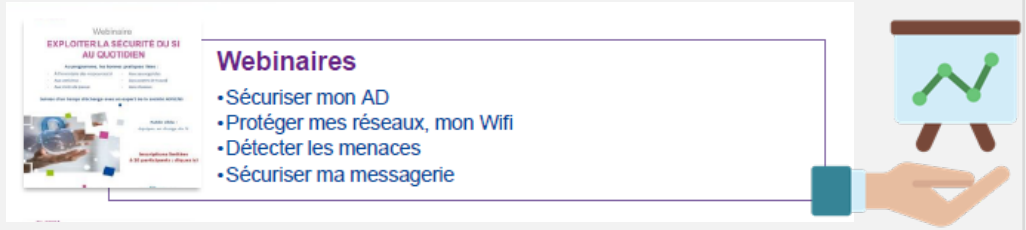
Financé par l'Union européenne NextGenerationEU

Déclinaisons opérationnelles nationales et régionales de l'axe 4

Sécurité opérationnelle



Webinaires régionaux



14 sessions réalisées

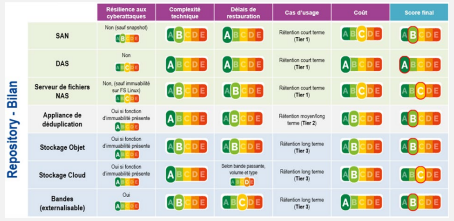
163 participations au total

Satisfaction globale

9,58 /10

Sauvegarde

Synthèse de l'état de l'art de la sauvegarde à destination des DSI, RSI, RSSI, administrateurs système et sauvegardes



Domaines de financement

Domaine 1 « Audits techniques Active Directory et exposition sur internet »

- ***L'arrêté du 18 mars** relatif à l'appel à financement du Domaine 1 a été publié au JO.*
- *Une enveloppe de 65 M€ qui concerne tous les établissements (publics et privés)*
- *La **plateforme de candidature eCaRE** est ouverte **depuis le 18 mars et jusqu'au 19/04/2024***
- ***A date du 17/04, 48 candidats, sur les 58 éligibles ont démarré une procédure de candidature.***

Domaine « Stratégie de continuité et de reprise d'activité »

- *Construction du domaine à partir de début 2024 afin de définir les objectifs demandés aux établissements pour bénéficier des financements.*
- *Des GT sont organisés à fréquence hebdomadaire : quatre objectifs sont en cours de construction sur les deux volets **sauvegarde et PCRA**.*
- *Un appel à candidature a été lancé pour travailler avec des **représentants des ESMS** sur la déclinaison médico-social du domaine.*

Domaine « Identification électronique des professionnels - HospiConnect »

- *Phase pilote pour le domaine HospiConnect (AAP ALPHA) lancée le 18 mars 2024*
- *Le guichet de candidature a été fermé le 5 avril 2024*
- *23 dossiers ont été reçus. Dont 2 de la région Pays de la Loire*
- *Pour rappel, la phase ALPHA de l' AAP est destinée à un nombre limité d'établissements (15)*

Autres domaines à venir en 2024-2025 :

- *Sécurisation des accès de télémaintenance*
- *Poste de travail et détection*
- *Autres thématiques…*

Financé par l'Union européenne NextGenerationEU

Merci

Financé par l'Union européenne NextGenerationEU