
ADN Santé - ADN Cyber
13/12/2022
18h30-20h30
SIB, Rennes

Déroulé

Au programme :

Une présentation de la menace Cyber pesant sur le secteur de la santé
par Nicolas Jolivet (Responsable Protection des Données et Cybersécurité au SIB)

Une présentation de l'accompagnement territorial Cybersécurité en santé pour la région Bretagne proposés
par Elodie Chaudron de l'ANS (Agence du Numérique en Santé), Lionel Lecomte de l'ARS Bretagne (Agence Régionale de Santé) et Gilles Larroche, chef de projet DPO du GCS eSanté-Bretagne

2 retours d'expérience d'établissements de santé par :
> la Fondation Bon Sauveur de Bégard, par Dimitri Martinescu, DSI, et Casandra Devemy, Responsable de la protection et de la sécurité des données personnelles / DPO / RSSI

> Le Groupe HSTV (Hospitalité Saint Thomas de Villeneuve) par Nicolas Milleville (RSSI)

Un cocktail dinatoire vous sera proposé pour clôturer la soirée.

Cet événement sera animé par Hervé Guillou-Hély de Wavestone, animateur au sein de la communauté santé d'ADN Ouest

ADN Ouest : Agir pour le Développement du Numérique en Pays de la Loire et en Bretagne

UN LARGE RÉSEAU

- +640 Structures adhérentes
- +3700 Membres
- 100 Évènements
- 2 Régions

4 ENJEUX MAJEURS

- Emploi et formation
- Transition Numérique
- RSE
- Innovation

7 COMMUNAUTÉS THÉMATIQUES

- Numérique Responsable
- Santé
- Infra & services
- Cybersécurité
- Stratégie Digitale
- Data
- Management

DES PROGRAMMES AU SERVICE DE LA FILIÈRE

- 2 Observatoires : métiers et compétences numériques / économie et investissements
- 1 Fonds de Dotation : ADN Solidarity
- 1 accélérateur de projets innovants : ADN Booster

DES PÔLES TERRITORIAUX

ADN 44
ADN 85
ADN 49
ADN 56
ADN 35
ADN 22
ADN 29

DES CERCLES METIERS

- DPO
- DSI
- CMO

La communauté #ADNCyber

10 thématiques

- Sécurité et Ressources Humaines
- Normes et méthodes
- Audits, détection et réaction aux incidents de sécurité
- Sécurité et Innovation
- Protection des données et RGPD
- Gestion des identités et des accès
- Technologies et solutions de sécurité
- Cloud et sécurité
- Sécurité des infrastructures physiques
- Gouvernance et écosystème de la cybersécurité

Notre modèle

- Des discussions thématiques
- Des documents de référence

Nos projets 2022

- **Les Forums & Cyber Meets**
- **Podcast "Innover en toute cybersécurité"**
- **Et toutes vos bonnes idées !**

Notre histoire

13-14/01/2020
Lancement de la communauté

Podcast #1 : Innover en toute Cybersécurité

WEBINAIRES
Avril : Cybersécurité : les bons conseils en temps de crise
Mai : Redémarrez sans faille...de sécurité
Juin : L'intelligence artificielle au service de la cybersécurité
Sept : Présentation du label Expertcyber

04/02/2021
Afterwork virtuel de la communauté

16/09/2021
Attaques cyber : c'est arrivé près de chez vous

Podcast #2 : Innover en toute Cybersécurité

16/11/2021
Forum Cyber & santé (Nantes)

WEBINAIRES
Janv : Assurance cyber : pourquoi et comment ?
Mars : Quand l'industrie rencontre la cybersécurité
Mai : Panocrim : table ronde régionale

FORUMS
Mai : Sensibilisation SSI (Nantes)
Octobre : Sécurisation Active Directory (Nantes)
Décembre : Cyber & santé (Rennes)

CYBER MEET
Fév : analyse de risques
Mars : sensibilisation SSI
Avril : PCA/PRA
Septembre : PCA/PRA
Octobre : formations cyber
Novembre : vulnérabilités

Podcast #3 : Innover en toute Cybersécurité

WEBINAIRES
Janv : Norme ISO 27001 : Quels apports pour le management de la sécurité ?
Avril : Comprendre et appréhender le facteur humain dans le risque cyber
Novembre : sujet à définir

2020 | 2021 | 2022

La communauté #ADNSanté

4 thématiques

- Comprendre les enjeux du numérique en santé
- Mieux coordonner les parcours
- Mieux accompagner la prise en charge
- Mieux prévenir et diagnostiquer

Nos projets

- Panorama IA
- Handicap et citoyens
- Hackathon Hacking Health
- Cartographie des acteurs

Marianne Allanic
Althenas
Sponsor

Christophe Cantin
Weliom
Pilote

Notre histoire

2020

Lancement de la communauté 30/09/2020

Afterwork virtuel de la communauté 01/12/2020

2021

11/03 : E-santé : coordonner les parcours des patients
07/04 : De l'Intelligence Artificielle en santé
09-11/04 : Hacking Health Nantes
09/06 : Cartographie des acteurs
21/09 : Innover en santé : trouvons les conditions du succès
14/10 : 1 an de la communauté
16/11 : Cybersécurité dans la santé : quelles solutions ?
22/11 : Rencontre Club Innovation Santé Domicile & Digital

2022

27/01 : L'IA au service de la santé
28/03 : Club Innovation Santé : Handicap
05/04 : Pitchs de solutions innovantes e-santé
24-26/06 : Hacking Health Nantes
08/09 : Afterwork des communautés
05/10 : 2 ans de la communauté *(Nantes)*
14/11 : Club innovation Santé : oncologie *(Nantes)*
13/12 : Cybersécurité dans la santé *(Rennes)*

2023

Nos prochains événements :

Janvier : Sport, santé et objets connectés (Nantes & Brest)
23-26 janv : Hacking Health

Services numériques

Santé & Collectivités

SIB

entreprise publique

50
ANS

450
COLLABORATEURS

650
CLIENTS


ASSEMBLÉE NATIONALE

Editeur

Numérique responsable

DATA

Cyber Sécurité

entreprise publique

Hébergeur

Innovation

Services numériques

Santé & Collectivités

Nicolas Jolivet,

Responsable Protection des Données et Cybersécurité

(SIB)

L’état de la menace cybersécurité

ADN Ouest – 13/12/2022

384775

Sommaire

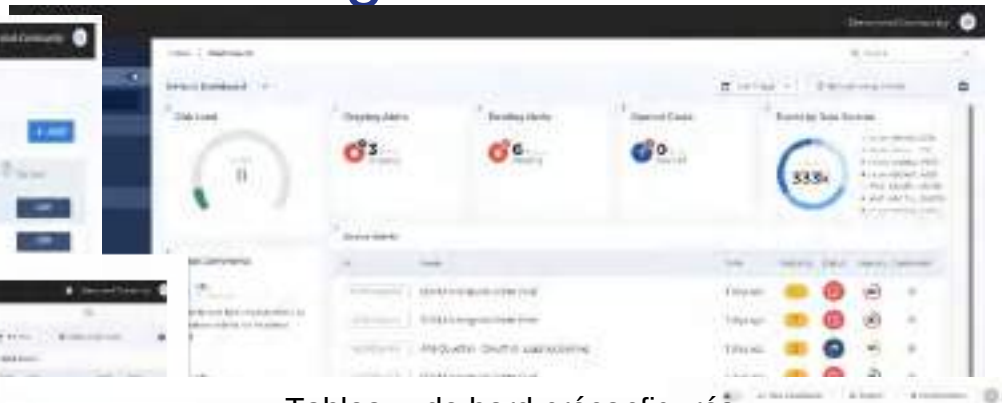
L’offre SIB

Et dans la cyber?

EDR et SOC Manager

Gestion des actifs

Analyse en temps réel des données



Tableaux de bord préconfigurés

Les attaques dans les organismes publics Français

http://umap.openstreetmap.fr/fr/map/attaques-cybersecurite-aupres-dorganismes-publics_821557#6/46.127/6.284

Observatoire des signalements 2021

Source : rapport annuel de l’ANS

Chiffres clés des signalements déclarés pour la période 2020-2021

733* / 369*
incidents déclarés sur le portail des signalements

582* / 290*
structures ont déclaré au moins un incident

189* / 90*
Demandes d'accompagnement par le CERT Santé

80* / 32*
interventions techniques d'appui (conseils techniques personnalisés, investigation numérique, remédiation, etc...)1

17* / 7*
incidents ont fait l'objet d'un suivi particulier de la part du FSSI

36* / 14*
incidents ont fait l'objet d'un suivi ou d'une prise en charge de la part de l'ANSSI

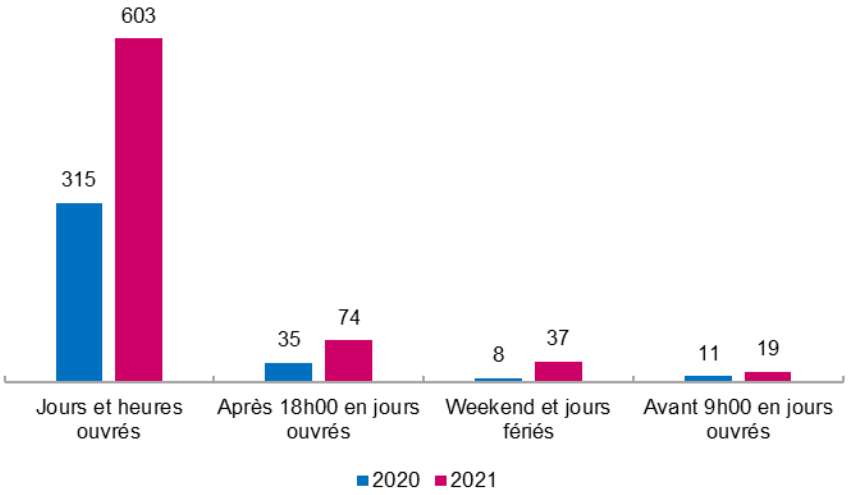
CORRUSS

17* / 4*
incidents ont fait l'objet d'une information au CORRUSS

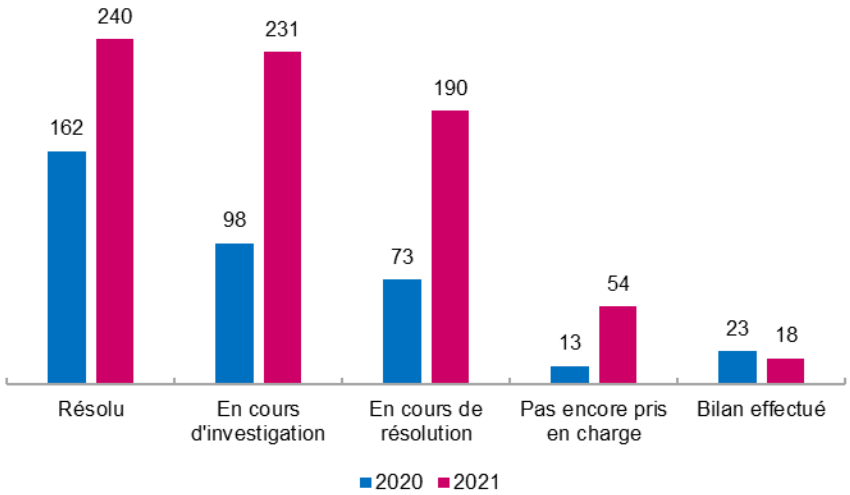
* : Ici sont présentées les données de 2021 en rose et les données de 2020 en bleu
1 : appui pouvant mobiliser un ou plusieurs experts durant plusieurs jours

Quand sont déclarés les signalements ?

Répartition des signalements selon l'horaire et le jour de leur dépôt



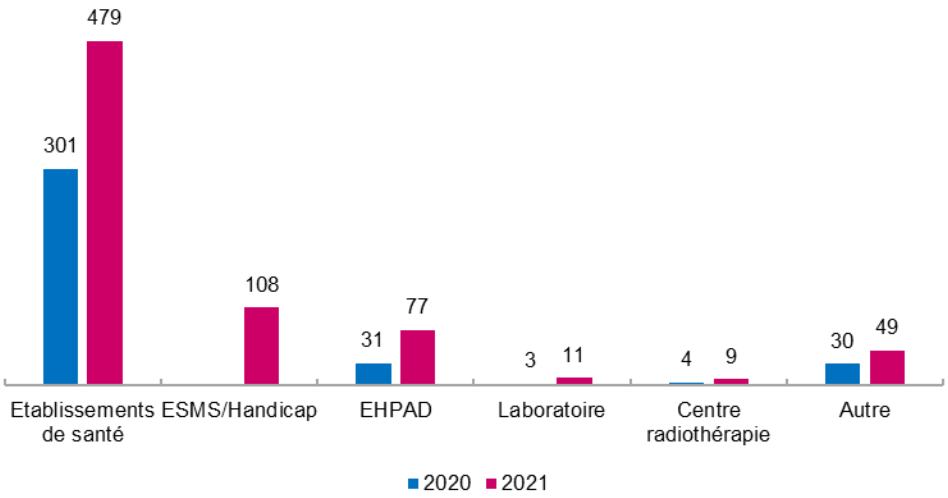
Etat des incidents lors de leur signalement



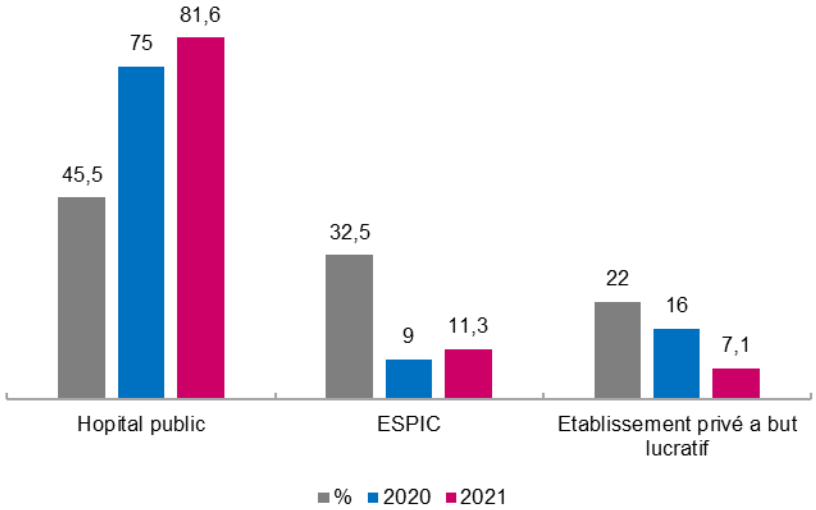
26% des signalements sont accompagnés d'une demande d'accompagnement en 2021. Il est stable par rapport à 2020 (27%)

Qui signale?

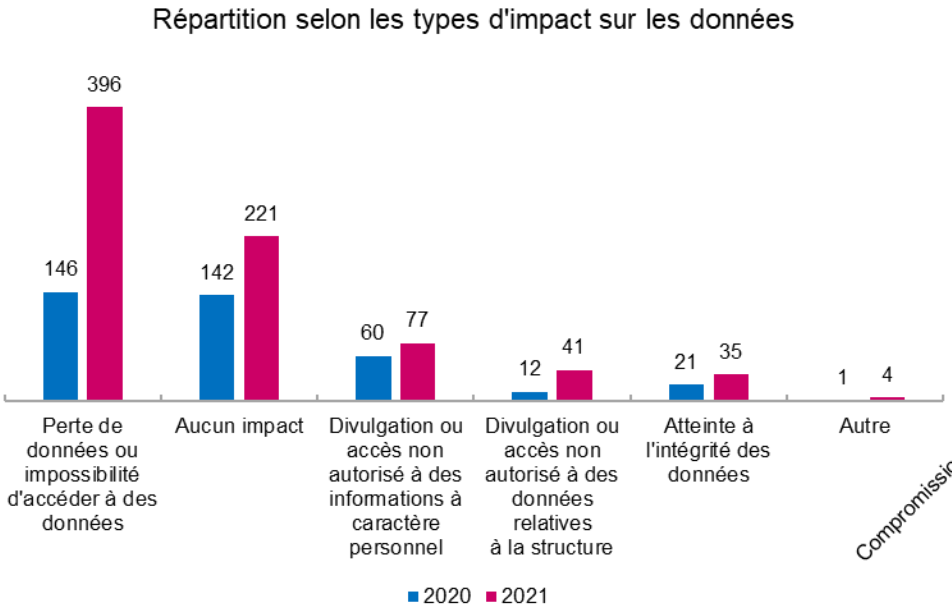
Répartition des signalements selon le type de structure

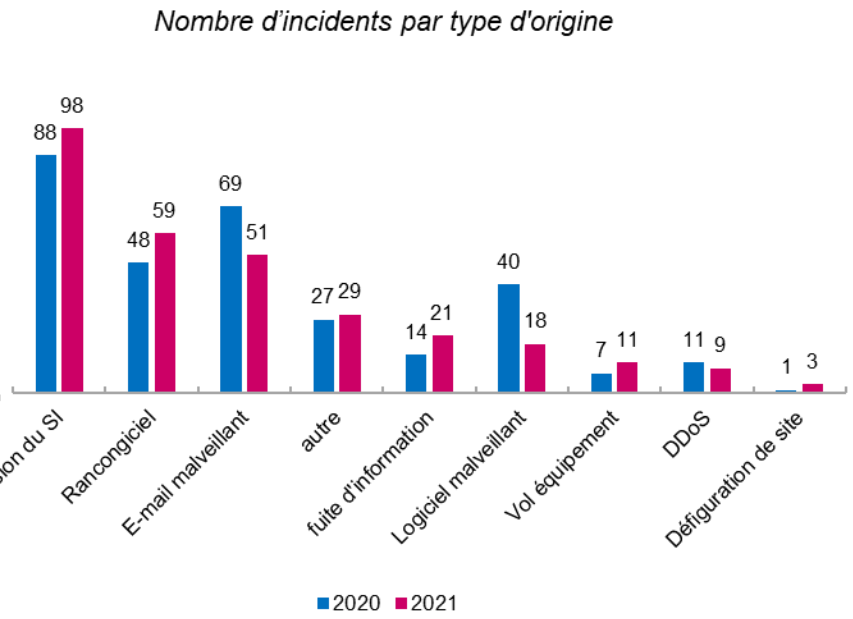


Part des signalements comparée à la part des établissements selon leur raison sociale



Pourquoi ?





52% des incidents déclarés sont d'origine malveillante.
Ce chiffre a diminué de 8% depuis l'année précédente


Un réseau complexe
Patients
Soins
Interconnecté
Administratif
Industriel

Les faiblesses du SI

Active directory unique et trop exposé

Applicatifs et Dispositifs médicaux obsolètes

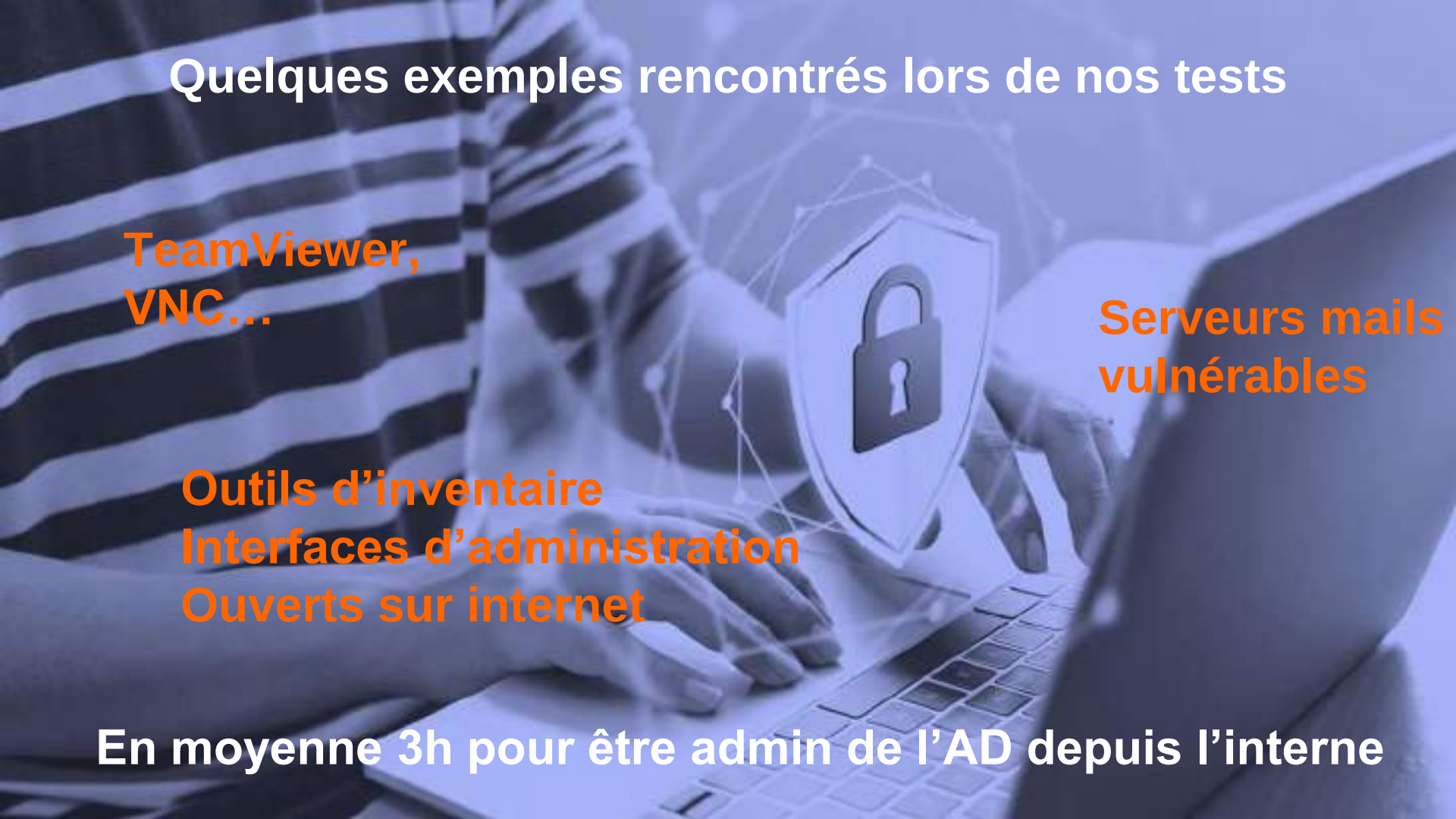
Outils de sécurité non maitrisés

La gestion des droits et des accès

Partages réseaux

Comptes applicatifs

Dispositifs médicaux



Quelques exemples rencontrés lors de nos tests

TeamViewer,
VNC…

Serveurs mails
vulnérables

Outils d’inventaire
Interfaces d’administration
Ouverts sur internet

En moyenne 3h pour être admin de l’AD depuis l’interne


Par ou rentrent-ils?
Documents malveillants
Intrusion physique
Exploitation de Vulnérabilités

Avez-vous des questions ?

Lionel Lecomte,
Coordinateur du ségur numérique
(ARS Bretagne)

Elodie Chaudron,
Responsable du développement territorial
(ANS)

Gilles Larroche,
Chef de projet
(CGS e-santé Bretagne)

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

ADN Ouest

13 décembre 2022

L'ANS accompagne la transformation numérique du système de santé aux côtés de tous les acteurs concernés des secteurs sanitaire, social et médico-social, privés comme publics, professionnels ou usagers.

L'ANS au cœur de la transformation numérique en santé | esante.gouv.fr

Régulateur

Nous améliorons la performance numérique grâce à des règles communes de régulation et d'échanges.

Opérateur

Nous concevons de grands e-programmes nationaux pour un service public de santé efficace et solidaire.

Promoteur, valorisateur

Nous stimulons, accompagnons et évaluons toutes les initiatives de e-santé pour les faire grandir

Membres fondateurs

Ministère des Solidarités et de la Santé

L'Assurance Maladie

cnsa

Dr Jacques Lucas, Président de l'Agence du Numérique en Santé

Annie Prévot, Directrice générale de l'Agence du Numérique en Santé

Une gouvernance au plus proche du terrain

ars Agence Régionale de Santé

Collège des GRADeS

Service réactif

Qualification
Analyse technique
Réponse aux incidents

Signalez l'incident
signalement.social-sante.gouv.fr

Profitez d'une prise en charge
H24 7/7
09 72 43 91 25
cyberveille@esante.gouv.fr

Service préventif

Audit de cyber-surveillance
Aide à la prévention des risques
Tests en ligne (messagerie)

Contactez nous
cyberveille@esante.gouv.fr

Veille & Sensibilisation

Portail cyberveille-santé
Indicateurs
Communauté cyber
Webinaires

cyberveille-sante.gouv.fr

Salon Tchap CERT Santé

Un contexte cyber pour les régions

Des attaques cyber de plus en plus fréquentes auprès des structures de santé

Intégration des sujets cyber par les régions afin de mieux prévenir et mieux agir

Mise en œuvre d'actions de prévention, de sensibilisation par les régions

Une inscription des sujets cyber à travers différentes feuilles de route nationales

Un discours présidentiel impulsant le plan de renforcement de la cybersécurité pour les établissements de santé #Touscybervigilants

Un questionnaire adressé aux 18 régions pour :

- **Recenser les initiatives instaurées,**
- **Évaluer leur niveau de maturité**
- **Connaitre les besoins du terrain**

Les besoins remontés par les 18 régions :

1. Gestion de crise /continuité des services (40%)
2. Sensibilisation (15%)
3. Maintien en condition de sécurité
4. Appui organisationnel
5. Partage de bonnes pratiques entre les régions

Création et lancement du Groupe de Travail Territorial (GTT) pour répondre aux besoins remontés par les collèges ARS et GRADeS

Objectif : créer un collectif abordant de :
- La continuité d'activité
- La sensibilisation et la prévention
- Les retours d'expériences sur les initiatives

Inscription du GTT dans une démarche globale :
Accompagnement PRC et Ségur

Le Groupe de Travail Territorial (GTT)

Présentation

Une démarche dynamique

Les GTT sont des points de rendez-vous pour les régions dédiés au sujet de la cybersécurité. C'est espace de collaboration et de co-construction qui a pour ambition d'emmener collectivement les régions vers les objectifs définis par le national.

Le GTT assure l'intégration des GRADeS et ARS à la gouvernance de l'ARS en tant que membres.

Organisés toutes les 6 semaines, les GTT abordent :

- L'état d'avancement des chantiers en cours
- Le partage des bonnes pratiques sous forme de retours d'expérience
- Les prochains travaux à mener.

Attendus

Les objectifs

1. Accélérer les actions de lutte contre les cybermenaces dans les territoires
2. Impulser la mise en œuvre du plan de renforcement cybersécurité des ES
3. Aider les régions les moins avancées sur les sujets cyber

Les livrables

Chantier 1 :

- Création de 3 kits : débutant, intermédiaire et confirmé
- Stratégie de déploiement des kits auprès des régions
- Création d'indicateurs de suivi relatif au PRC
- Note de clarification

Chantier 2

- Catalogue des guides et référentiels nationaux liés à la SSI et à la cyber
- RETEX des initiatives régionales en terme de sensibilisation et prévention des sujets cyber
- Alignement d'une feuille de route pour le secteur du médico-social

Les sponsors et participants

4 Sponsors :

- Steven GARNIER – ARS Bourgogne Franche Comté
- Djamil VAYID – ARS La Réunion
- Auriane LEMESLE – GRADeS Pays de la Loire
- Rémi TILLY – GRADeS Ile-de-France

La participation des ARS & GRADeS (toutes régions confondues)
Profil des participants : RSSI, DPO, responsable de projet, CMSI, etc.

Leurs rôles :

- Mobiliser les régions en portant plus spécifiquement le sujet auprès d'elles
- Principaux référents de l'ANS : orientations, points d'étapes sur les travaux lors des Collèges ARS et GRADeS.

AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'Agence du Numérique en Santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante

Quelles réponses régionales face aux menaces et aux risques cyber en santé ?

Cybersécurité dans la santé : quelles solutions ?

ADNOuest

Le 13 décembre 2022

1ER Constat des risques Cyber en région Bretagne

Breizh Cyber Tour (T2 2022) : rencontre individuelle ARS/GCS avec chaque RSSI des 8 OSE Bretons (Opérateurs de Services Essentiels)

- **Des équipes en SSI sous-dimensionnées (manque parfois jusqu'à 60% des besoins en RH)**
- **Une grande hétérogénéité des applications à administrer et sécuriser (parfois plus de 200 applications au sein d'un seul GHT)**
- **Une convergence IT encore faible à l'échelle des GHT**
- **Des solutions logicielles vulnérables, pour les métiers de la santé comme pour les infrastructures des établissements, entrainant un effort permanent de gestion des mises à jour**
- **Des résultats (score) d'audit ADS et Cybersurveillance insuffisants : nécessité de sécurisation rapide par les ES de leurs infrastructures bureautiques (réseaux, serveurs bureautiques, annuaires, messagerie, etc.) qui constituent les principales cible des attaques.**

Quelles réponses régionales face aux menaces et aux risques cyber en santé ? (1)

Le Plan de Renforcement Cyber : annoncé par le Président de la République le 18 février 2021 dans le cadre de la « Stratégie nationale de cybersécurité ». Demande au Ministre de la santé et de la prévention de prendre des mesures immédiates pour réduire les risques cyber

> Un plan d'action cyber qui couvre l'ensemble des structures de santé et s'appuie sur le renforcement des dispositifs existants (4 axes principaux - 23 actions)

> Une gouvernance :

- Ministérielle : Copil cyber réunissant tous les acteurs engagés dans le PRC
- Territoriale :
  - ARS & GCS → Animation territoriale de la e-santé et suivi de mise en œuvre de la politique de renforcement CYBER
- Locale :
  - GHT → Garant de la politique de sécurité partagée et de la cible de mutualisation des ressources humaines, techniques, etc.
  - DG → Responsable de la démarche globale de management des risques, dont la prise en compte effective de la cybersécurité

Quelles réponses régionales face aux menaces et aux risques cyber en santé ? (2)

Le rôle des ARS : en appui du pilotage national et de la mise en œuvre réalisée au sein des établissements (4 axes)

Sensibiliser aux risques cyber

Animer

- **Faciliter le partage des pratiques** et les actions de mutualisation (région et GHT) ;
- **Accompagner financièrement**

Appuyer les structures de santé : en lien avec la chaîne d'alerte nationale (CERT Santé) et territoriale (ARS/établissements de santé) et organiser la réponse territoriale à l'incident cyber ;

Contrôler par :

- la prise en compte de la protection des données et de la SSI, dans les projets SI-e-Santé et dans les investissements SI ;
- la préparation des ES (PCA numérique et plan de réponse à incident, prise en compte effective des prérequis cyber (financement HOPEN, SUN-ES, ESMS numérique…)

Bilan à fin 2022

- **Bonne dynamique régionale**
  - **Développement** des actions sur l'ensemble des 4 axes
  - Mise à disposition des ES d'une **offre de services**
  - **Relation de partage et d'entraide** au sein de la région pour avancer collectivement sur les actions du PRC (ARS – GCS – ES)

Ambitions 2023

- **EN REGION :**
  - Faire que la **cybersécurité soit considérée comme la priorité n°1** par l'ensemble des acteurs de l'offre de soins
    - Exercices de continuité d'activité en mode dégradé réalisés pour tous les ES
    - Audit ADS et Cybersurveillance bi-annuels pour tous les OSE
    - Renseignement de l'OPSSIES par tous les ES
    - Mise en place d'un centre de ressources « cybersécurité » au sein du GRADeS

- **AU NATIONAL :**
  - Définir les **programmes de financement** qui prendront la relève de HOP'EN et SUN-ES
  - Trouver un **mécanisme de financement** de la SSI en ES dans la durée

Les moyens d'actions (1)

L'animation régionale : Le Comité Régional SSI & Protection des données

Les objectifs de cette démarche régionale collective

- Fédérer les acteurs de la Sécurité des Systèmes d'Information (SSI) et de la protection des données de l'ensemble des structures de santé de la région ;

- Co-construire les actions relatives à la Sécurité des Systèmes d'Information (SSI) et à la protection des données en région.

Les moyens d'actions (2)

Les formations & ateliers thématiques

Les objectifs :

- Renforcer le développement des connaissances en matière de cybersécurité, de cyber-résilience et de protection des données des professionnels IT des structures de santé ;

- Maîtriser les impacts et évolutions règlementaires, juridiques, technologiques en matière de SSI & de Protection des données.

Les moyens d'actions (3)

Les outils et supports de sensibilisation

Les objectifs :

- Diffuser les bonnes pratiques ;
- Prévenir les risques de cybermalveillance ;
- Développer une culture de cybersécurité et de cyber-résilience.

Plateforme numérique de sensibilisation

TEST DE PHISHING
(ou D'HAMECONNAGE)

MODULES E-LEARNING SENSIBILISATION

Cyber Héros {Cybermoi/s 2022}

Vidéo retour d'expérience de professionnels du CH de Dax victime d'une cyberattaque en février 2021

[Lien vidéo 1](#) (version courte ~40s)
[Lien vidéo 2](#) (version longue ~33 min)

5 Thématiques

- Le jour J : la sidération
- Les impacts de la cyberattaque dans les services : le chaos
- Les premières mesures mises en place pour faire face à la crise : l'intelligence collective et la débrouillardise
- Les impacts de la cyberattaque à moyen terme : l'inscription dans un temps long
- Les enseignements de la cyberattaque : l'anticipation et la préparation

Les moyens d'actions (4)

Les actions et prestations régionales de cyber-résilience

Les objectifs :

Mettre à disposition des structures de santé, des actions et prestations leur permettant de :

- Se préparer à la gestion d'incidents de Sécurité et de cyber crises, et plus particulièrement à travers la réalisation d'exercices de cyber crise ;

- Bénéficier d'un appui à la résolution et à la gestion d'incidents potentiels (ex. levée de doutes) ou avérés de sécurité au sein de leur système d'information.

Les moyens d'actions (5)

L'accompagnement au développement et à l'expérimentation de démonstrateurs de cybersécurité

GOUVERNEMENT

PROJET <BALISE>

Lauréat Appel à Manifestation d'Intérêt

« Sécuriser les territoires »

Lancement de démonstrateurs territoriaux de cybersécurité

Développement d'un démonstrateur de cybersécurité concernant **la protection, la détection, la remédiation et le repérage de fuite de données sensibles** issues des Systèmes d'Information des Structures de Santé de la région

PROTÉGER	DÉTECTER	REMÉDIER	REPÉRER
Protéger les données de santé de fuites potentielles via un **dispositif de marquage** Utilisation de techniques permettant d'identifier et de marquer ces données quel que soit leur nature, leur état et indépendamment de la production de ces données	Surveiller, qualifier et alerter des fuites potentielles de données sensibles identifiées **avant qu'elles ne sortent du système d'information** de la structure de santé	Résoudre et bloquer des fuites potentielles de données sensibles identifiées **avant qu'elles ne sortent du système d'information** de la structure de santé	Rechercher et localiser les fuites de données de santé identifiées **en dehors du système d'information** de la structure de santé permettra de retrouver la provenance de ces fuites

Avez-vous des questions ?

Dimitri Martinescu
(DSI)
La Fondation Bon Sauveur de Bégard

Casandra Devemy
(DPO/RSSI)
La Fondation Bon Sauveur de Bégard

Démarche SSI - Retex

Retour d'expérience sur la démarche SSI en établissement de santé

ADN Ouest – 13/12/2022

Dimitri Martinescu – DSI – FBS Bégard
Casandra Devemy – RSSI DPO – FBS Bégard & AHB Plouguernevel

20'

La Fondation Bon Sauveur de Bégard – Pôle de santé mentale

La Fondation Bon Sauveur de Bégard – Pôle de santé mentale

Qui sommes-nous ?

Un centre hospitalier spécialisé

- 2 pôles adultes
- 1 pôle pour enfants et adolescents

Une prise en charge graduée en ambulatoire et en hospitalisation

Un pôle médico-social et social

- 3 établissements pour personnes en situation de handicap (Foyer d'Accueil Médicalisé, Maison d'Accueil Médicalisée, Foyer de Vie)
- 1 Service d'Accompagnement à la Vie Sociale
- 1 Service d'Accompagnement Médico-Social pour Adultes Handicapés
- 1 EHPAD
- 1 Centre de Soins, d'Accompagnement et de Prévention en Addictologie

La Fondation Bon Sauveur de Bégard – Pôle de santé mentale

Organisation de la DSI : composition de l'équipe

6 ETP internes

- 1 directeur des SI
- 2 chefs de projets SI
- 1 ingénieur systèmes et réseaux
- 2 techniciens

1 RSSI DPO mutualisé (0,5 ETP)

1 ETP externe

- 1 technicien hotline / proximité (prestataire)

Enjeux et problématiques de la DSI

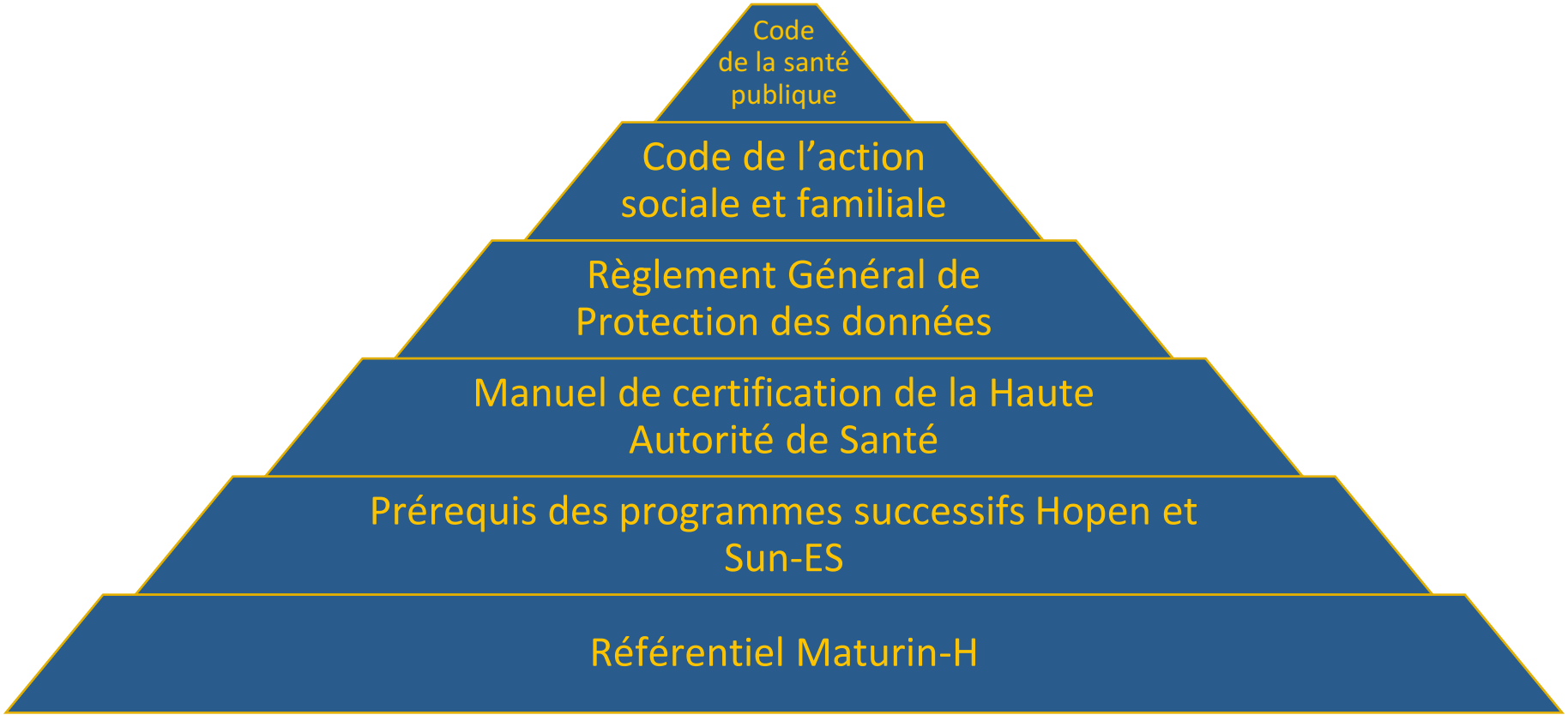
Les enjeux

- Être aligné sur l'enjeu de la Fondation : prendre soin des personnes accompagnées
- Optimiser le fonctionnement des services supports
- S'adapter au contexte réglementaire et aux enjeux de sécurité du système d'information

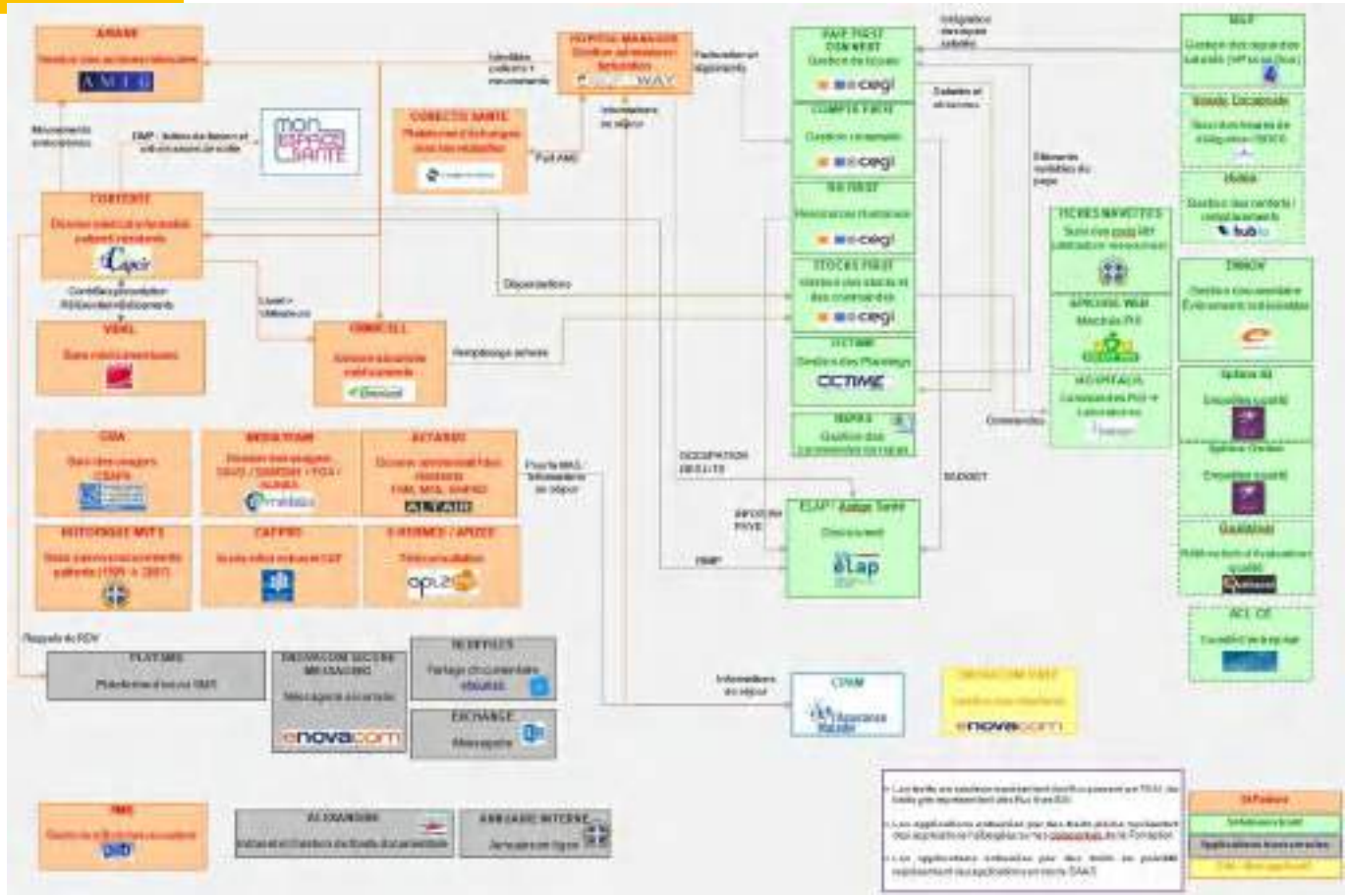
Les problématiques

- Jongler entre ressources internes / externes
- Être en réflexion permanente sur les ressources et la priorisation des projets
- Développer les coopérations / mutualisations / délégations
- Savoir « augmenter le SI » …
- …et réussir à le maintenir

Contexte législatif et réglementaire



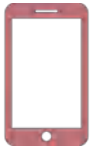
Contexte métier et applicatif



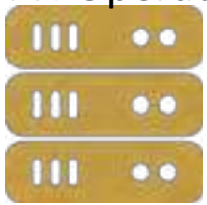
Contexte technique en quelques chiffres

25 sites interconnectés
Réseau en étoile – VPN Opérateur

650 ordinateurs



160 smartphones et tablettes

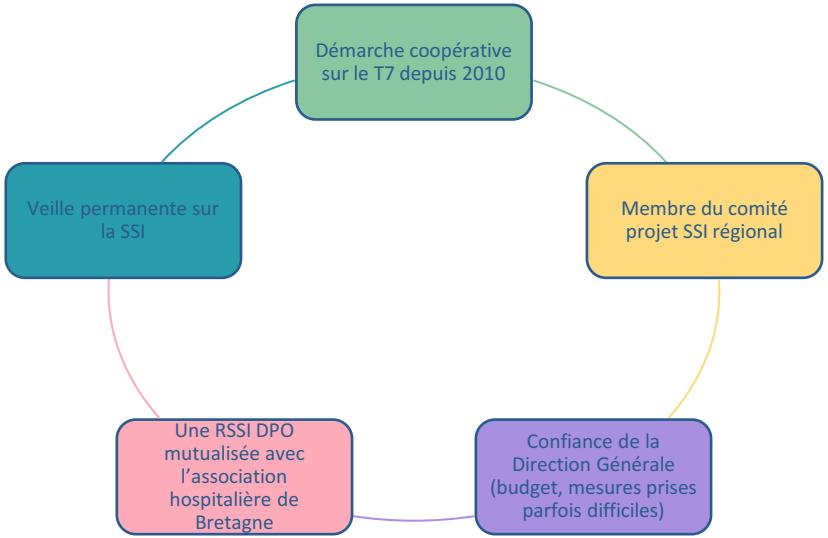


130 serveurs

120 imprimantes

4800 appels tracés par an

Démarche SSI : au niveau institutionnel et au niveau projets



- **2010**
  - Documents cadres démarche territoriale
- **2015**
  - Actualisation des documents cadres
- **2016**
  - Élaboration des procédures dégradées
- **2018**
  - Charte informatique, capacity planning, projets techniques
- **2019**
  - Actualisation des documents cadres
- **2020**
  - Audit d'intrusion
  - Analyse des vulnérabilités de la messagerie
- **2021**
  - Audit cyber
- **2022**
  - Campagne de phishing

Démarche SSI : focus sur la technique…

Une partie de la charge mentale de la DSI…

- **Se protéger vis-à-vis…**
  - **Des virus, des cryptos, et de l'indisponibilité**
    - Migration des systèmes obsolètes
    - Antivirus et EDR
    - Redondance des systèmes et services
  - **D'Internet et de la fuite de données**
    - Pare feu et VPN
    - Bastion d'administration
    - Isoler la messagerie
    - Chiffrement des disques des PC
    - Sécurisation de la flotte mobile (MDM)
  - **Du hameçonnage**
    - Vade
    - Sensibilisation
    - Renouvellement des mots de passe
    - Revue des comptes
  - **Des intrusions**
    - Bastion
    - VLAN, Radius, LAPS
    - Revues Active Directory

Démarche SSI : …et préparer la crise

- **…et être prêt à affronter la crise**

- **Continuité d'activité**
  - Procédure dégradée
  - Plan de continuité d'activité
  - Plan de reprise d'activité
  - Plan de sécurité des établissements (PSE) incluant un chapitre sur la crise cyber

- **S'exercer**
  - Exercices de crise cyber

- **Remédier**
  - Pouvoir compter sur un PRIS
  - Disposer de sauvegardes hors ligne / hors domaine
  - Solidarité entre établissements (compétences et matériels)

Conclusion - Quelles perspectives ?

- Nécessité de **savoir piloter la SSI** (copilotage DSI – RSSI nécessaire + développer l'acculturation des directions aux sujets techniques SSI)

- Disposer de moyens suffisants au sein des DSI **pour piloter les sujets**

- Disposer d'un **budget** suffisant (confiance DG)…
- …et **pouvoir le consommer** ☺

- **Travailler les coopérations à tous les niveaux :** GCS entre établissements, conventions entre structures de santé, au sein des territoires, développer l'offre ARS – GCS eSanté Bretagne pour assister **tous les acteurs de santé**

- Développer les **espaces d'échanges techniques** entre les techniciens du SI, développer la **formation continue** sur les sujets techniques

Avez-vous des questions ?

Nicolas Milleville

(RSSI)

Groupe HSTV

HOSPITALITÉ
Saint-Thomas de Villeneuve

Les Chiffres :

3000 Salariés,

15 établissements sur 3 régions:

- Bretagne,
- Pays de la Loire,
- Provence.

Activités :

- 50 % Sanitaire : MCO, SSR, PSY,
- 50 % Médico-sociale : Ehpad, Foyer de vie.

HOSPITALITÉ
Saint-Thomas de Villeneuve

L'organisation de la DSI

Support/Exploitation : 10 ETP

Transformation Numérique : 7 ETP

Protection des données : 1,5 ETP

Rattaché à la Direction Générale

HOSPITALITÉ
Saint-Thomas de Villeneuve

Le Système d'Information

Quelques chiffres :

1700 postes informatiques

30 hyperviseurs pour 300 serveurs virtuels

500 imprimantes

15 Firewalls

35 applications métiers et 115 applications diverses *(EAI, ETL, bureautique,...)*

100taine prestataires

HOSPITALITÉ
Saint-Thomas de Villeneuve

Le Sécurité des SI

Gouvernance :

Un Comité Sécurité SI :
- Piloté par le Responsable SSI
- Composé par les directeurs d'établissements, les directions des soins et les directions des services supports

Missions :
- Suivre le plan d'action Sécurité SI,
- Définir les grandes orientations,
- Valider les priorités

HOSPITALITÉ
Saint-Thomas de Villeneuve

Le Sécurité des SI

Opérationnel :

Contribution du RSSI aux projets informatiques
(mode dégradé, analyse de risques, gestion des flux, filtrage, …)

Sensibilisation dans les établissements,

Le suivi des sauvegardes en lien avec les équipes de la DSI,

La remontée d'alerte des incidents de sécurité,

…

HOSPITALITÉ
Saint-Thomas de Villeneuve
Prendre soin, c'est d'abord créer un lien

Avez-vous des questions ?

Votre avis compte !

Aller vers

app.klaxoon.com

TSZTHTQ

app.klaxoon.com/join/TSZTHTQ

Vous êtes au ♡ du numérique !

www.adnouest.org

Partagez votre expérience : #JNR2022

@adnouest