CyberCamp
Santé #4

Bienvenue

20 mars 2024

Bordeaux

Cité du Vin

www.cybercampsante.org

CYBERCAMP SANTE

20 mars 2024

{Ouverture}

Didier **AMBROISE**
Associé fondateur

doshas consulting

CYBERCAMP Santé

CYBERCAMP SANTE

20 mars 2024

{Introduction}

Etat de la menace Cyber

Laure **DUHESME**

Bureau Santé et Affaires sociales

CYBERCAMP Santé

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Panorama de la cybermenace en France et dans le secteur de la santé

Panorama de la menace

Panorama de la cybermenace 2023

Plusieurs points ont été soulignés par le panorama de 2023 :

- Le niveau de la **menace continue d'augmenter**, dans un contexte marqué par de nouvelles tensions géopolitiques et la tenue d'événements internationaux sur le sol français.
- En 2023, **l'espionnage stratégique et industriel** est la menace qui a le plus mobilisé les équipes de l'ANSSI. Les **attaquants continuent de perfectionner** les techniques qui leur permettent de s'introduire sur des SI, de s'y propager, d'exfiltrer des informations ou de se prépositionner, et d'éviter d'être détectés.
- Les attaques à des fins d'extorsion se sont maintenues à un niveau élevé en 2023, avec un **regain des attaques par rançongiciel** contre des organisations françaises.
- En vue des JOP, **l'ANSSI et l'ensemble des parties prenantes poursuivent les travaux visant à rehausser la sécurité des SI concernés** en cohérence avec la menace et à mettre en place un dispositif renforcé de détection et de réponse à incident.
- Répartition des victimes d'attaques par rançongiciel : **34%** TPE/PME, **24%** collectivités territoriales et **10%** établissements de santé

Des mesures cyber préventives prioritaires identifiées

- Renforcer l'authentification sur les systèmes d'information
- Sauvegarder hors-ligne les données et les applications critiques
- Accroître la supervision de sécurité
- Etablir une liste priorisée des services numériques critiques de l'entité
- S'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque
- Mettre en œuvre des politiques rigoureuses de maintien en condition de sécurité des parcs informatiques

Les types d'attaques pouvant toucher le secteur

Les rançongiciels : la menace la plus immédiate

- Une menace **persistante**
- Principalement à **visée lucrative**
- Modes opératoires : **phishing**, exploitation de **vulnérabilités** (AD, VPN, ect.)
- L'**interconnexion croissante des réseaux** augmente l'impact d'un rançongiciel sur les structures.
- Des attaques **doublées d'une exfiltration** de **données** personnelles et de santé.

Divulgations données de santé

- **Chantage** à la publication.
- **Divulgation** malveillante.
- **Revente** des données exfiltrées.

Compromissions opportunistes

- Attaque **messageries**
- **Défiguration** sites internet
- Attaques par **déni de service.**

Attaques par la *supply chain*

- Tendance **mondiale multisectorielle.**
- Accès aux SI par le biais de **solutions logicielles / matérielles compromises**

Attaques ciblées

- Les établissements de santé sont globalement, **peu, voire pas visés par les APT.**

CYBERCAMP SANTE

20 mars 2024

{Introduction}

Tendance des menaces 2023

Olivier **Ruet-Cros**
CERT Santé

AGENCE DU NUMÉRIQUE EN SANTÉ

CYBERCAMP Santé

CERT Santé
Evolution 2022-2023

Gestion des incidents

581 592
incidents déclarés

165 165
demandes d'accompagnement

93 101
interventions d'appui technique

Veille & audits

983 2200
alertes envoyées

50 76
cas de compromission

526 348
audits réalisés

En détails

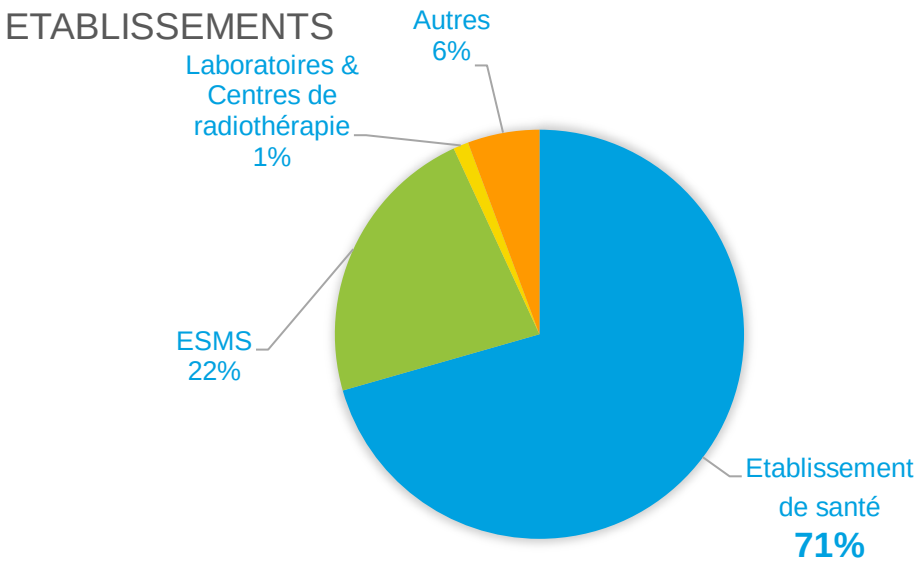
467* / 432*
structures ont déclaré au moins un incident

93* / 103*
interventions techniques d'appui (conseils techniques personnalisés, investigation numérique, remédiation, etc…)1

42* / 48*
incidents ont fait l'objet d'un suivi ou d'une prise en charge de la part de l'ANSSI

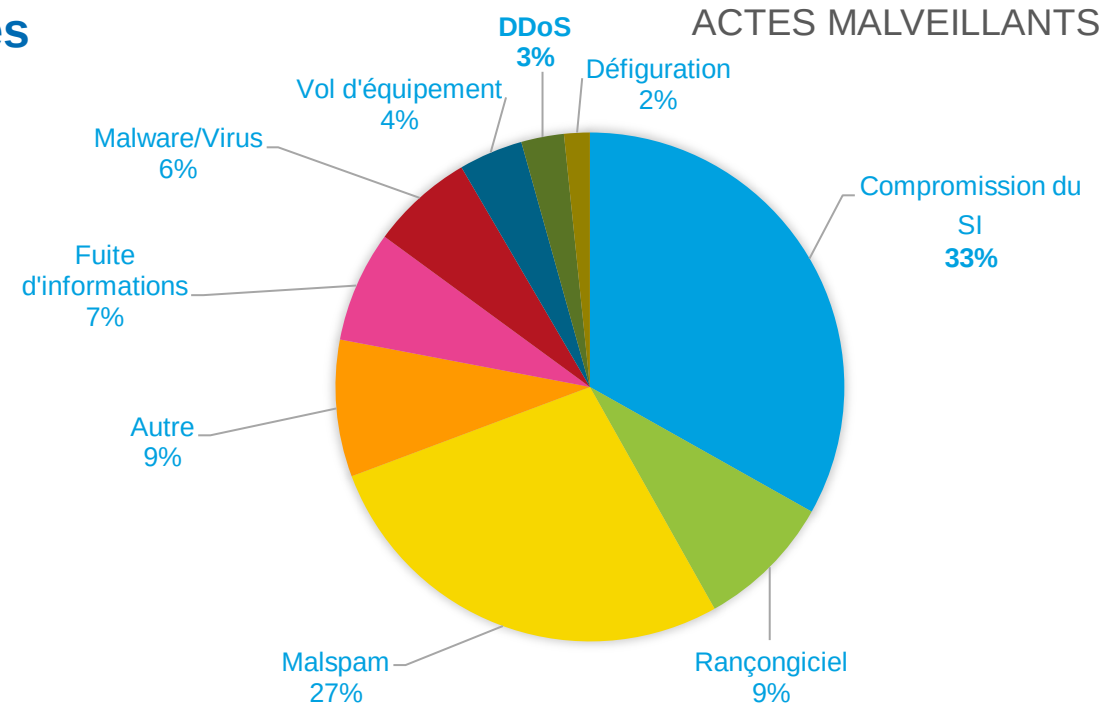
24* / 16*
incidents ont fait l'objet d'un signalement CORRUSS

CERT Santé
Gestion des incidents - National



59%

Des incidents ont eu un impact sur les données



32%

Des incidents ont déclenché un mode dégradé

32

Incidents par rançongiciel

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

LA E-SANTÉ FRANÇAISE
CERT Santé

Tel : 09 72 43 91 25
Mail : cyberveille@esante.gouv.fr
https://www.cyberveille-sante.gouv.fr/

CYBERCAMP SANTE

20 mars 2024

{Introduction} - *Présentation de la réponse française*

Elodie **Chaudron**
Responsable programme Care

Christophe **Mattler**
Responsable programme Care

AGENCE DU NUMÉRIQUE EN SANTÉ

MINISTÈRE DU TRAVAIL DE LA SANTÉ ET DES SOLIDARITÉS
Liberté Égalité Fraternité

CYBERCAMP Santé

Programme CaRE

Cybersécurité accélération et Résilience des Etablissements

Cybercamp

Mars 2024

MINISTÈRE DE LA SANTÉ ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

CaRE, un programme ambitieux et inédit

Délégation ministérielle au numérique en santé

AGENCE DU NUMÉRIQUE EN SANTÉ

Multiplication des cyberattaques (CHSF, CHV,…)

Décembre 2022 : Lancement de la Task Force (TF) Cyber

Une **équipe « cœur »** : FSSI, DGOS, ANSSI, ARS, GRADeS

Coordonnée par la DNS et l'ANS

DIRECTION GENERALE DE L'OFFRE DE SOINS

Des **contributeurs**

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

Une comitologie dédiée

- COPIL – COSTRAT - COPROJ
- Des « comités fédérations et établissements »
- Comité Régional CaRE
- Comités opérationnels
- Ateliers de travail

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 ES** dans leur montée en maturité sur la cybersécurité

Des moyens :

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

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

Publication du plan d'action CaRE 2023-2027

Délégation ministérielle
au numérique en santé

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Nous vous invitons à (re)visionner le webinaire de présentation du programme CaRE* pour plus de détail sur le plan d'actions

** En tant compte que quelques modifications ont pu être apportées au programme depuis la diffusion de ce webinaire*

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

Mise à disposition de la Feuille de Route Cybersécurité accélération et Résilience des Etablissements (CaRE)

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

Délégation ministérielle
au numérique en santé

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Un plan d'actions décliné en 4 axes

Gouvernance et résilience

1. Mettre en œuvre une **gouvernance pérenne pour le programme CaRE** et plus globalement pour la cybersécurité dans le secteur de la santé
2. Intégrer la cybersécurité dans la **gouvernance des établissements**
3. Préparer et accompagner les établissements à **réagir et à faire face à la cybermenace**
4. Engager les ES dans une **démarche d'auto-évaluation** et d'orientation de leur feuille de route cyber

Ressources et mutualisation

5. Favoriser la **mutualisation des ressources et des moyens** entre les établissements
6. **Augmenter le nombre de personnels** dédiés au SI dans les établissements
7. Garantir dans chaque établissement un **budget suffisant** dédié au numérique et à la cybersécurité
8. Elaborer une **cartographie de l'offre existante** afin d'identifier les éventuels besoins additionnels

Sensibilisation

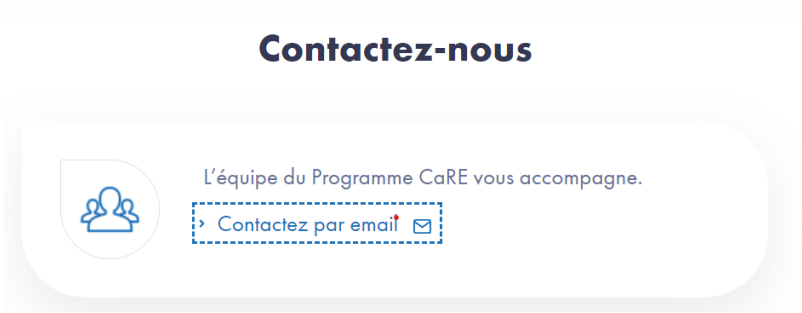
9. **Sensibiliser les DG et les PCME** sur les risques cyber et leurs impacts
10. Animer une **communauté des RSSI** d'établissements
11. **Sensibiliser et former** l'ensemble du personnel des établissements

Sécurité opérationnelle

12. Soutenir les ES dans les **domaines identifiés comme prioritaires** pour faire face à la cybermenace
13. **Maitriser les risques** d'exposition sur internet et sécuriser les annuaires d'établissement
14. **Superviser les postes de travail** et détecter les intrusions
15. **Sécuriser les accès au SI** depuis l'extérieur (télémaintenance)
16. **Reconstituer rapidement les services critiques** en cas d'incident
17. Disposer d'une équipe dédiée au **contrôle des ES** permettant d'attester l'atteinte des objectifs tels que définis dans les différents domaines
18. **Maintenir le niveau acquis** via l'atteinte d'objectifs considérés comme le « Socle Cyber »
19. **Limiter les risques d'usurpation de l'identité numérique** des professionnels pour l'accès aux services sensibles, conformément au Référentiel d'identification électronique de la PGSSI-S

Points de contacts

Pour toute demande autour du programme :



Page web dédiée au Programme CaRE sur le site de l'ANS :

https://esante.gouv.fr/strategie-nationale/CaRE

CYBERCAMP SANTE

20 mars 2024

{Table ronde}

Animation :

Cécile **JOUANEL**
Associée

doshas consulting

Intervenants :

Adrien Bourdon

Vincent Génot

Laure Duhesme

Jean-François Laloyer

Sylvain Faugieras

Jean-Arnaud Elissalde

CLUB RSSI SANTÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI

Com CyberGend

SantéCité

France Assos Santé
La voix des usagers

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS 2

CONTEXTE ET PRÉSENTATION

Pourquoi NIS 2 ?

- Une suite de la première réglementation européenne en matière de cybersécurité NIS 1, publiée en 2016 et transposée en droit français en 2018. Environ 300 entités désignées « Opérateurs de Services Essentiels » (OSE) – dont 142 ES – sous NIS 1.

- NIS 2 : une réglementation pour aller vers la cybersécurité de masse :
  - Face à un **niveau élevé de menace cyber**, une multiplication des attaques par rançongiciel et un besoin de sécuriser la *supply chain*, NIS 2 a pour ambition un plus large champ d'application ainsi qu'une application harmonisée au sein de l'UE.
  - Publication fin 2022 du texte de la directive européenne. La France, comme les autres États membres, doit transposer la directive NIS 2 en droit national avant le 17 octobre 2024 et prévoit d'intégrer pleinement le principe de proportionnalité entre les exigences et les enjeux et les capacités des entités concernées.

De NIS 1 à NIS 2 : les évolutions majeures

Périmètre

- Intégration de nouveaux acteurs, au-delà des 142 OSE existants. La plupart des établissements de santé, privés comme publics seraient notamment concernés
- Disparition de la notion d'OSE et du mécanisme de désignation unitaire, et mise en place de **2 catégories d'entité** déterminées sur critères (secteurs d'activités, nombre d'employés, chiffre d'affaires, etc.) : **Entités Importantes (EI) et Entités Essentielles (EE)**

Relations entre opérateurs et ANSSI

- Notification à l'autorité nationale compétente (ANSSI)
- Communication des informations de contact
- Déclaration des incidents majeurs en plusieurs étapes
- Capacités renforcées de supervision, de contrôle et de sanction

Règles de cybersécurité

- Proportionnalité entre les exigences EI et EE
- Abandon de la notion de « service essentiel » utilisée pour définir un « système d'information essentiel »
- Extension du périmètre des systèmes d'information à sécuriser

Transposition de la directive NIS 2 en droit national prévue d'ici octobre 2024

Page d'information dédiée : https://cyber.gouv.fr/la-directive-nis-2

Texte de la directive : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555

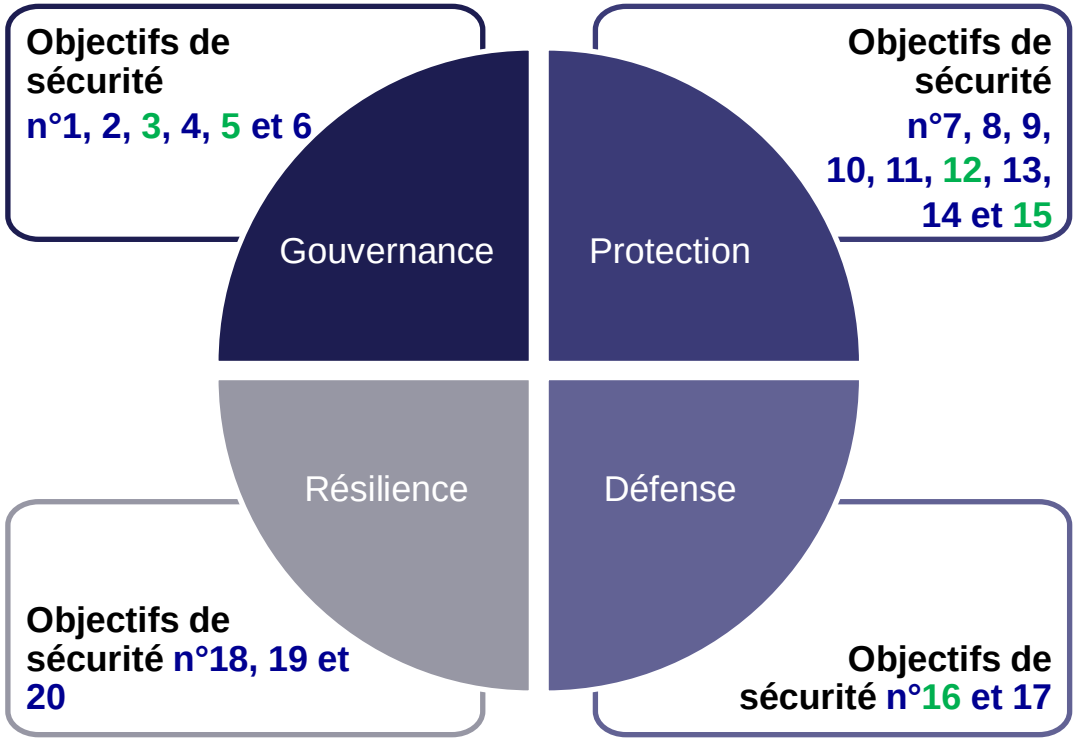
Synthèse des entités concernées par NIS 2 dans le secteur de la santé et des affaires sociales

Présentation simplifiée (les travaux de définition précise du périmètre sont en cours)

<table>
<tr><th>Périmètre spécifique santé</th><th>> 250 employés</th><th>50 à 250 employés</th><th>< 50 employés</th></tr>
<tr><td>Prestataires de soins de santé</td><td rowspan="2">Entités essentielles</td><td rowspan="3">Entités importantes</td><td rowspan="3">Hors périmètre NIS 2</td></tr>
<tr><td>R&D ou fabrication de produits pharmaceutiques</td></tr>
<tr><td>Fabrication de dispositifs médicaux (DM)</td></tr>
<tr><th colspan="4">Périmètre lié mais non spécifique santé</th></tr>
<tr><td>Administration publique</td><td rowspan="3" colspan="2">Entités essentielles</td><td rowspan="3">Hors périmètre NIS 2</td></tr>
<tr><td>Fournisseurs de cloud et services TIC</td><td rowspan="2">Entités importantes</td></tr>
<tr><td>Organismes de recherche</td></tr>
</table>

Présentation de la cible à atteindre

- La cible fixée vise à maîtriser et réduire les risques en lien avec la cybercriminalité, tout en prenant en compte le mécanisme de proportionnalité
- Les objectifs de sécurité, définis pour répondre à la cible, s'inscrivent dans le modèle déjà existant :
  - **Gouvernance**
  - **Protection**
  - **Défense**
  - **Résilience**
- Ces objectifs répondent aux obligations des articles 20 et 21 de la directive



Les objectifs en **vert** sont applicables exclusivement aux **entités essentielles**

CYBERCAMP SANTE

20 mars 2024

{Table ronde}

Animation :

Cécile **JOUANEL**
Associée

doshas consulting

Intervenants :

Adrien Bourdon

Vincent Génot

Laure Duhesme

Jean-François Laloyer

Sylvain Faugieras

Jean-Arnaud Elissalde

CLUB RSSI SANTÉ

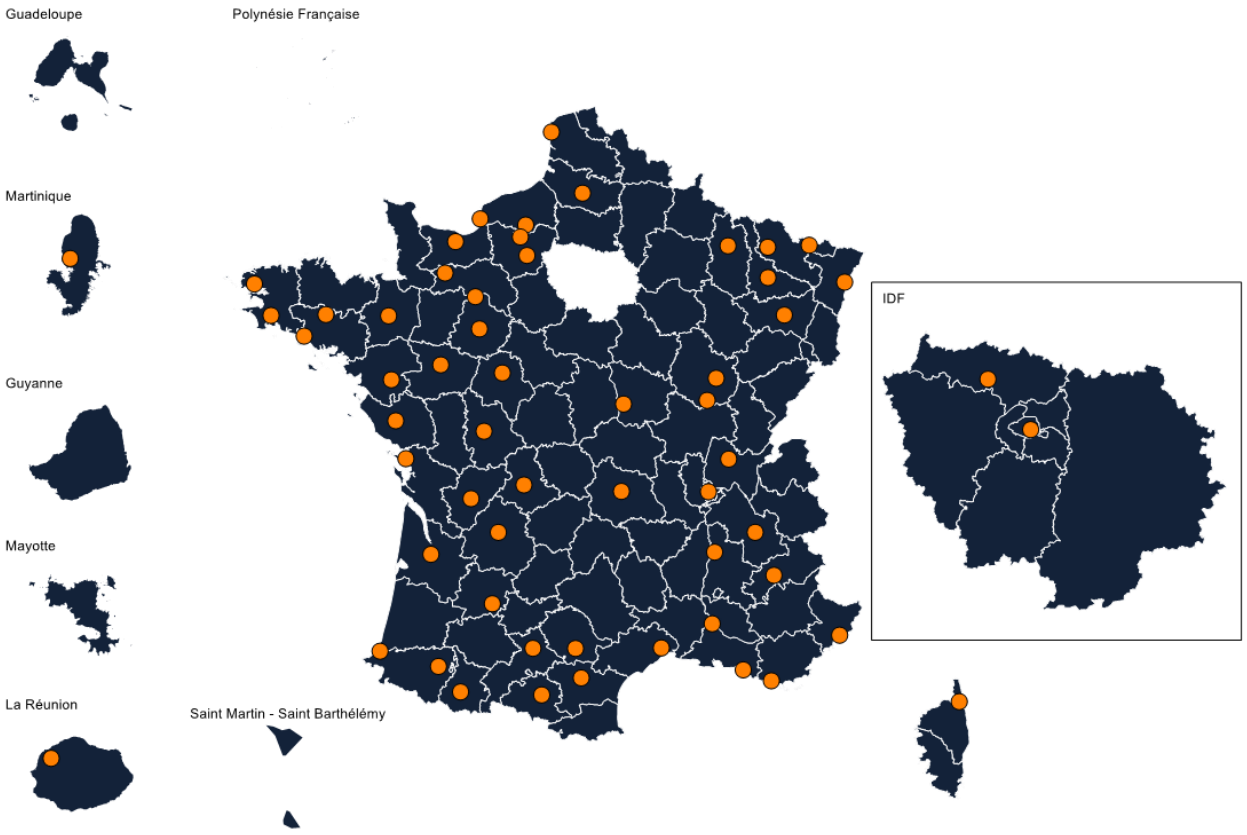
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI

Com CyberGend

SantéCité

France Assos Santé
La voix des usagers

Présentation du Club RSSI Santé



79 établissements de santé représentés

Dont 4 hors France

93 RSSI et RSSI adjoint membres du Club RSSI Santé à ce jour.
+ FSSI

Missions et production du Club

Béatrice BERARD

Les missions du Club

- Représenter la communauté des RSSI des établissements publics de santé
- Apporter un soutien moral, éventuellement matériel et des moyens aux RSSI
- Constituer des groupes de travail ou de réflexion sur des thématiques actuelles
- Organiser et animer le cercle d'échange
- Assurer la liaison avec les organismes tiers et les autorités

Quelques réalisations en 2023 :

- Mise à disposition d'un clausier sécurité pour la C.A.I.H et UNIHA
- Organisation de deux groupes de travail
  - Élaboration d'un tableau de bord SSI
  - Finalisation du clausier sécurité
- Mise à disposition d'outils de communication (Tchap, Osmose, Wiki)

CYBERCAMP SANTE

20 mars 2024

{Table ronde}

Animation :

Cécile **JOUANEL**
Associée

Intervenants :

Adrien Bourdon

Vincent Génot

Laure Duhesme

Jean-François Laloyer

Sylvain Faugieras

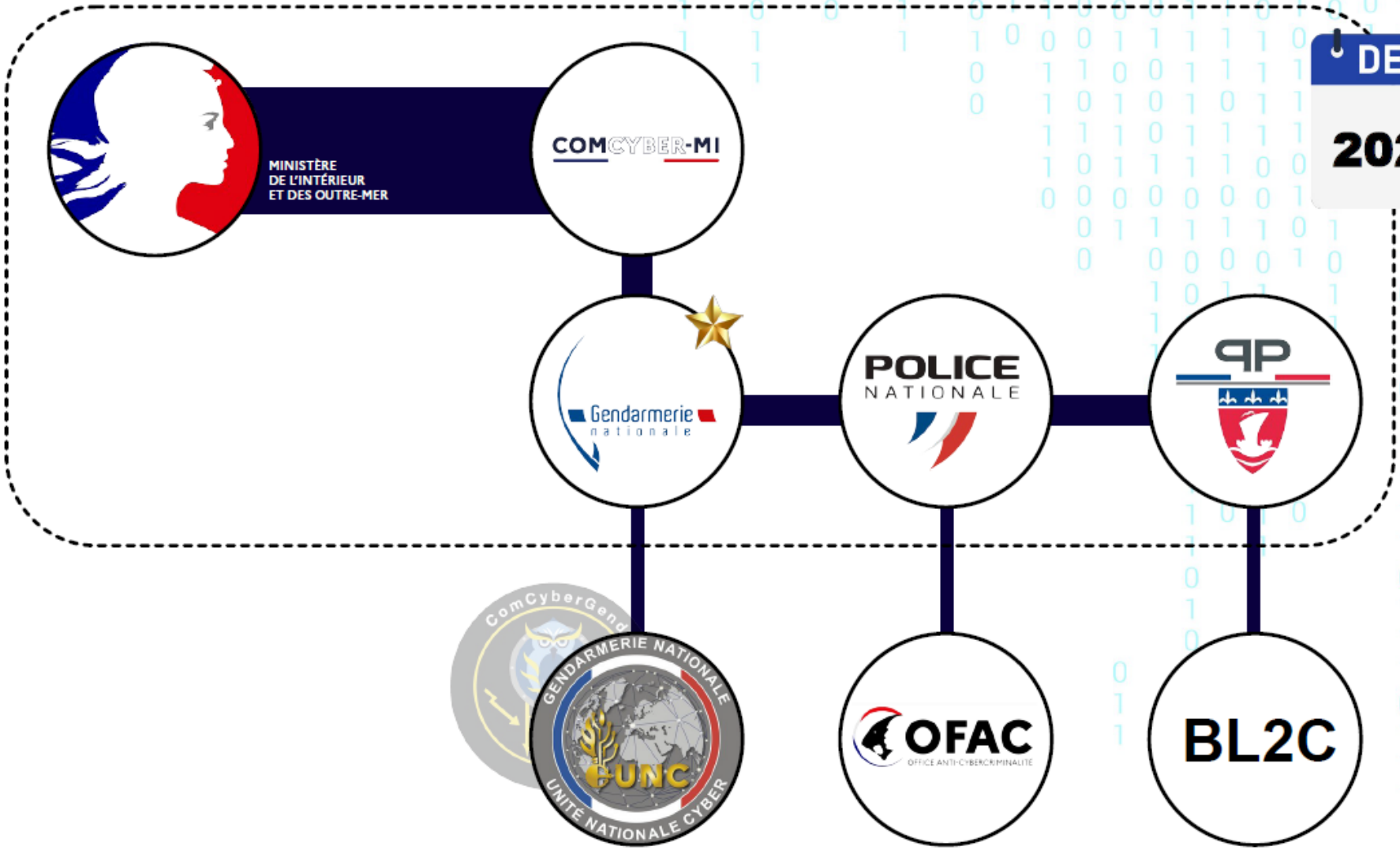
Jean-Arnaud Elissalde

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

UNCyber
Direction des opérations et de l'emploi

ORGANISATION DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ



CYBERCAMP SANTE

20 mars 2024

{Table ronde}

Animation :

Cécile **JOUANEL**
Associée

doshas consulting

Intervenants :

Adrien Bourdon

Vincent Génot

Laure Duhesme

Jean-François Laloyer

Sylvain Faugieras

Jean-Arnaud Elissalde

CLUB RSSI SANTÉ

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ANSSI

Com CyberGend

SantéCité

France Assos Santé
La voix des usagers

CYBERCAMP SANTE

20 mars 2024

{Présentation de la suite du programme}

Didier **AMBROISE**
Associé fondateur

doshas consulting

CYBERCAMP Santé

CYBERCAMP SANTE

20 mars 2024

Temps d'échanges et partage / cocktail déjeunatoire puis *.... 4 ateliers thématiques animés par :*

Souveraineté numérique

Maître Florence *Eon-Jaguin*

WITHLAW
SOLUTIONS JURIDIQUES DE SECURITE

Programme Care / Déclinaison régionale

Damien Teyssier
Référent Cyber

ESEA
e-santé en action
NOUVELLE AQUITAINE

Démonstration de solutions sur NIS 2

Vincent Génot
RSSI GHT Dordogne

CLUB RSSI SANTÉ

Démonstration Active Directory

Adel Allam
Auditeur Sécurité

ELYSIUM SECURITY
RootMe PRO

CYBERCAMP SANTE
20 mars 2024

Temps d'ateliers : de 13h45 à 16h45 (3h)
Chaque atelier dure 45 min

Les salles de réunion ne pouvant accueillir tout le monde, les ateliers se dérouleront en parallèle pour pouvoir répartir les participants dans les salles.
Toutes les 45 min, les participants doivent changer de salle pour assister à un autre atelier.

En prenant en compte les temps de changement de salle (15 min), il sera possible de faire 3 rotations.
Par conséquent, chaque participant pourra suivre jusqu'à 3 ateliers maximum.

Les ateliers feront l'objet d'une restitution en fin de journée (sauf l'atelier démo Root Me)

Avec le soutien de ...

CYBERCAMP
Santé

contact@CyberCampSante.org

@CyberCampSante

www.cybercampsante.org