STRUCTURES DE SOINS ET D'ACCOMPAGNEMENT

CYBER SÉCURITÉ

LIVE WEBINAR

20 février 2024
10h30 - 11h30

Retour d'expérience du Centre Hospitalier Intercommunal Nord Ardennes

intervention du ComCyberGend Commandement de la Gendarmerie dans le cyberespace

Un objectif commun :
La sécurité des soins

Structure Régionale d'Appui Grand Est

Centre Hospitalier Intercommunal nord Ardennes

Gratuit - Inscription obligatoire
www.sragrandest.org
Ouvert à la Région Grand Est
Avec le soutien de l'Agence Régionale de Santé Grand Est

micro coupé

onglet 'conversation' désactivé pendant la présentation
un temps d'échanges est prévu en fin de séance

pas d'enregistrement

Les règles de déroulé du webinaire

SOMMAIRE DU WEBINAIRE

01. Pourquoi ce webinaire porté par la SRA Grand Est ?
    Anne-Sophie URBAIN - Directrice

02. Retour d'expérience du Centre Hospitalier Intercommunal Nord Ardennes
    Thomas TALEC - Directeur / Samuel LEGROS - DSI

03. Actions portées par la Gendarmerie Nationale
    Lieutenant Colonel Jean-François LALOYER

04. Questions / Réponses

La SRA Grand Est

CA VEUT DIRE QUOI SRA ?

Structure Régionale d'Appui à la qualité des soins et sécurité des patients en région Grand Est

Association Loi 1901 à but non lucratif

01

MISSION EIGS

Soutien à la déclaration et à l'analyse systémique des évènements indésirables graves associés aux soins

02

MISSION QUALITE / SECURITE DES SOINS

Contribution à la politique régionale qualité et sécurité des soins

01. Pourquoi ce webinaire porté par la SRA Grand Est ?

PLUSIEURS OBJECTIFS :

01 Acculturation à la réalité de la menace cyber dans le secteur de la santé et à la façon de protéger sa structure par le retour d'expérience

02 Prendre conscience de l'importance exponentielle de ce risque pour la sécurité des usagers et des conséquences possibles sur les prises en soins (possibles EIGS)

03 S'inscrire dans la continuité des recommandations des politiques publiques (Ségur du numérique en santé, Programme CaRE (ANS), etc.) et des dispositifs d'évaluation et certification HAS

Cyber Sécurité Une responsablité collective

CONTEXTE NATIONAL

Forte augmentation de cyberattaques des établissements de santé et des établissements sociaux et médico-sociaux
Renforcer la résilience et la sécurité numérique du système de santé

01 LE VIRAGE NUMERIQUE

Enjeu majeur pour la santé en France

02 LA GESTION DES RISQUES

Gérer les risques de cyberattaques qui impactent les prises en soins et accompagnements

03 LE COLLECTIF

Sensibiliser l'ensemble des acteurs concernés

Cyber Attaques en santé

Secteur en plus forte croissance

Quelques chiffres clés 2022

ECHELLE MONDIALE

38%

Augmentation du nombre de cyberattaques tous secteurs confondus

EN FRANCE

191%

Hausse du nombre de cyberattaques contre les acteurs du secteur de la santé en 1 an

LES 7 CRITÈRES NUMÉRIQUES DE LA V2024

Gestion des risques numériques

Critère 3.6-02 Les risques de sécurité numérique sont maîtrisés

Critère 3.6-06 L'identification des utilisateurs et des patients dans le système d'information est sécurisée

sécurisation de l'identification des professionnels dans le SI

Création de deux critères en V2024

Promotion des bons usages

Critère 2.2-05 Les équipes de soins ont accès aux informations du patient avec un système d'information adapté

Critère 3.1-07 Les modalités de communication permettent aux usagers et aux médecins de ville de contacter l'établissement aisément

Critère 3.2-09 L'établissement est organisé pour permettre au patient d'accéder à son dossier

Critère 1.1-18 Le patient reçoit une information claire et adaptée à son degré de discernement sur les modalités de sa prise en charge

information du patient sur le DMP

Critère 2.3-01 Les équipes respectent les bonnes pratiques d'identification du patient à toutes les étapes de sa prise en charge

LES 7 CRITÈRES NUMÉRIQUES DE LA V2024

Les documents <u>obligatoires</u>

- **Cartographie du système d'information applicatif**
- **Charte d'utilisation des ressources informatiques**
- **Plan de continuité d'activité (PCA) incluant le Plan de reprise d'activité (PRA)**

Autres documents pouvant être consultés

- Le schéma directeur
- La politique de sécurisation du SI
- Le plan de formation
- La matrice habilitation
- Le plan d'actions à la suite des audits sécurité numérique
- Les résultats d'un exercice de cybersécurité, etc.

Ces documents sont analysés par l'Expert visiteur numérique lors de l'Audit Système

LES CRITÈRES NUMÉRIQUES DE L'EVALUATION DES ESSMS

Stratégie et outils numériques

Critère 3.15.2 L'ESSMS définit et déploie sa stratégie numérique

Critère 3.15.3 Les professionnels sont régulièrement sensibilisés et/ou formés aux outils numériques.

Stratégie numérique = 2 critères

Protection des informations et sécurisation des données relatives à la personne

Critère 2.2.7 L'ESSMS garantit la confidentialité et la protection des informations et données relatives à la personne accompagnée.

Critère 2.10.2 Les professionnels respectent les règles de sécurisation des données, des dossiers et des accès.

Protection des données = 2 critères

Éléments évalués lors de la visite d'évaluation par l'Audit Système

Éléments évalués lors de la visite d'évaluation par le Traceur Ciblé

LES CRITÈRES NUMÉRIQUES DE L'EVALUATION DES ESSMS

Éléments d'évaluation documentaires

- Projet d'établissement ou de service / PCA
  - ➤ stratégie numérique : matériels, moyens, rôles et responsabilités, DUI de la personne…
- Réglement de fonctionnement
- Procédure, protocole ou autre document
  - ➤ définissant les règles de sécurisation et des accès aux données et dossiers
- Plan de formation, feuilles d'émargement, supports de sensibilisation, ressources pédagogiques…
- Charte informatique personnalisée, affichages "bonnes pratiques", conduite à tenir en cas de…
- Liste des personnes habilitées…

Autres éléments d'évaluation

- Actions visant à garantir la confidentialité des données, la sécurisation du réseau : sécurisation des locaux et des postes informatiques, gestion des mots de passe, gestion de la messagerie, sauvegardes, anti-virus…
- Observation des pratiques, respect des règles de confidentialité et de protection des données : conditions d'accès aux dossiers des personnes…
- Journées à thème, RETEX…

Merci
pour votre attention

Un objectif commun :
La sécurité des soins

WEBINAIRE du 20 février 2024: Cybersécurité dans les établissements de santé

Retour d'expérience du Centre Hospitalier Nord Ardennes (et GHT nord Ardennes)

- **Thomas TALEC, directeur du GHT Nord Ardennes**
- **Samuel LEGROS, DSI du GHT nord Ardennes**

Groupement Hospitalier de Territoire Nord-Ardenne

Centre Hospitalier Intercommunal Nord Ardennes

Centre Hospitalier Bélair
Établissement Public de Santé du Département des Ardennes

Résidence Porte de France
Le bien-être sur un plateau

Territorial Ardenne Nord GCS
Groupement de Coopération Sanitaire

PLAN de l'intervention

1) Contexte général du GHT

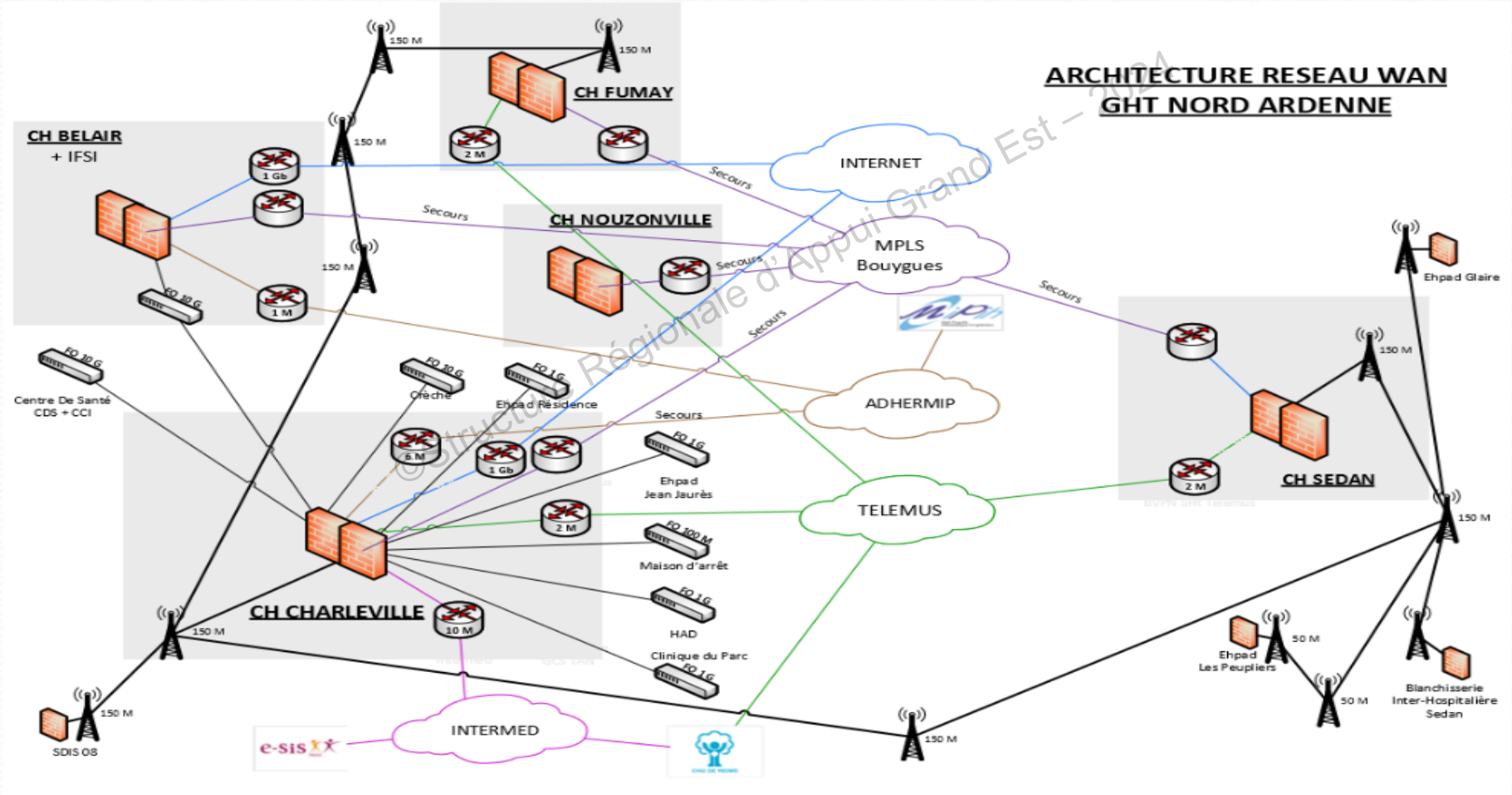
2) Déroulement et gestion de la gestion de crise

3) Le travail de remédiation…un marathon voire un ultra trail!

1) Contexte général du GHT

- Fusion de 4 hôpitaux au 1er janv 2020, en mode accéléré, puis crise covid
- Montée en puissance des besoins SI suite à la fusion: forte mobilisation équipe SIH
- Directeur unique sur le GHT
- DSIH unique sur le GHT
- Centralisation des serveurs sur 2 sites (CHINA et CH Belair)
- Recours au télétravail ++ depuis la crise covid
- Juste avant la crise:
  - ✓ Septembre 2022, perte de 2 administrateurs systèmes et réseau, reste 2 agents dont RSSI spécialisé réseau et un nouvel agent arrivé en janvier 2022, perte très forte de l'historique
  - ✓ 2 nouveaux agents en congés

1) Contexte général du GHT



2) La survenue de la crise et sa gestion

30 Septembre 2022 fin de matinée

Alerte de nos systèmes sur CH Bélair

Analyse de l'alerte :
Installation illicite à 22h le 29/09 d'un agent en télétravail sur un appareil critique

Contact utilisateur ➔ pas de télétravail depuis Août

Alerte faite à Cyberveille (CERT Santé)

30 Septembre 2022 12h30

Analyse rapide CERT Santé avec description des outils

➔ C'est une attaque évoluée et très sérieuse

Confirmation à DG de l'attaque à 12h45

Organisation cellule de crise à 13h30 sur CH Bélair

Décision quasi immédiate d'isoler le CH Bélair

30 Septembre 2022

Organisation cellule de crise à 14h30 sur CHINA

Découverte des impacts de l'isolation

Choix d'un prestataire de remédiation ➔ OCD

Envoi des fichiers pour analyse experts

Gestion des impacts, mise en œuvre procédures dégradés (impression des dossiers régulièrement)

Analyse des connexions distantes CHInA

Forte suspicion attaque GHT

1 Octobre 2022 12h30

Cellule de crise GHT

2 Octobre 2022 8h30

Confirmation impact GHT

Passage à un niveau supérieur car OSE
Renforcement OCD + CERT Santé + ANSSI

Cellule de crise 3 fois par jour

Isolation totale du GHT

Renfort du personnel pour gestion de la crise

Chronologie semaine du 3 Octobre 2022

Arrivé sur site agents OCD

Finalisation des analyses et contrôle de l'isolation

Remonté au fur et à mesure des soucis par les services, priorisation lors des cellules de crises

Etat entre deux. Procédures dégradées papiers et doublons avec le SI
Mise en place de PC 4G

Mise en place messagerie extérieure GMAIL en moins de 48h pour l'ensemble des utilisateurs

Confirmation que la menace est contrôlée et que l'attaquant n'a plus la main

Proposition d'OCD sur un planning de remédiation

- Com interne +++ (un message général/jour)
- Com externe sur 48-72hr

2) La survenue de la crise et sa gestion

Résultats de cette gestion de crise (terme immédiat)

- 0 donnée volée, 0 donnée cryptée, 0 donnée perdue
- 0 patient transféré
- 0 déprogrammation

3) Le travail de remédiation…un marathon voire un ultra trail!

- **Contrôle et correction PC** (Vérification présence Antivirus et EDR / Mise à jour poste / Administrateurs du postes)
- **Contrôle Serveurs** (Vérification présence Antivirus et EDR / Mise à jour OS / Administrateurs du postes / liste de l'ensemble des services et tâches lancés par un utilisateurs du domaine)
- **Changement des anciens PC** (remplacement des postes Windows 7 et antérieures)
- **Changement des anciens serveurs** Windows 2003 puis Windows 2008 (Contact éditeur, installation et isolement dans environnement sécurisé, planification modification, correction et gestion de la panne éventuels avec le prestataire, validation)
- **Mise à jour des serveurs de messagerie** (mise à jour des serveurs de messagerie)
- **Réinstallation OS Compromis** (Contact éditeur, installation et isolement dans environnement sécurisé, planification modification, correction et gestion de la panne éventuels avec le prestataire, validation)
- **Mot de passe utilisateurs** (Obligation de changer tous les mots de passes utilisateurs et compte d'ouverture de PC et serveurs)
- **Liste blanche internet** (L'accès en liste blanche pour l'ouverture sur internet reste une solution temporaire de remédiation et non de construction d'une nouvelle infrastructure. Il permettra en mode dégradé de donner des accès à internet, contrôlés et strictement nécessaires aux agents du GHT, site par site)
- **Nouvel antivirus**(Mise en place du blocage par l'outil, actuellement simplement en mode lecture)
- **Suppression domaine parc.fr et sedan.fr**
- **Changement équipements de sécurités** (Mise en place d'un nouveau PareFeu (ceux actuels sont utilisées pour de la sécurisation et les échanges internes des serveurs)
- **Tiering** réseau à minima serveurs annuaires.

Merci de votre attention

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

Gendarmerie nationale

UNCyber
Direction des opérations et de l'emploi

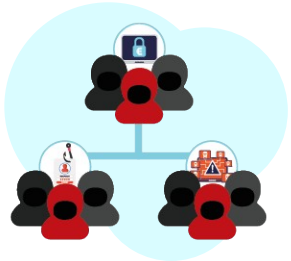
CYBERSÉCURITÉ

ENJEUX & RISQUES

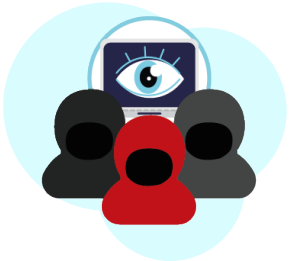
LIEUTENANT COLONEL
JEAN-FRANCOIS LALOY

L'ÉTAT DE LA MENACE

PROFIL DES CYBERDÉLINQUANTS OBSERVÉS



Groupes structurés et autonomes *(rançongiciels, botnets, vol de données, Caas,…)*



Réseaux d'opportunistes *(pédocriminalité, commerces illicites,…)*

Groupes d'activistes en ligne *(manipulation de l'information, espionnage,…)*

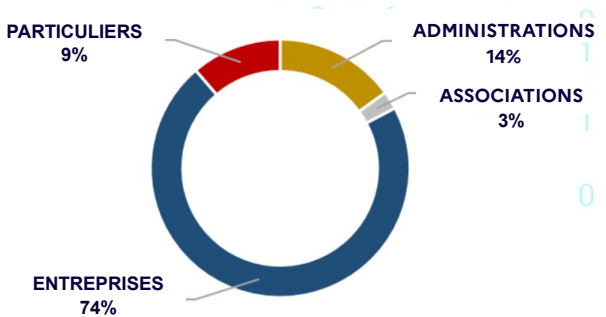
Groupes dépendant d'un état étranger *(volonté de déstabilisation)*

Escroqueries

Haine en ligne et atteintes aux personnes

Atteintes aux systèmes d'informations

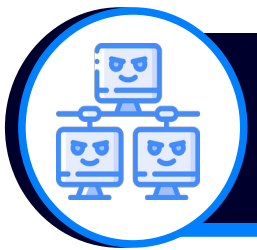
Répartition des victimes de rançongiciels en 2022
(source : rapport d'analyse des cybermenaces 2023)



MENACES EN SURVEILLANCE 2024

SUPPLY CHAIN

Les pirates considèrent toujours davantage les intégrateurs, développeurs ou éditeurs comme des intermédiaires, pour atteindre l'infrastructure et les données de leurs cibles ultimes.



NOUVEAUX RÉSEAUX DE BOTNETS

On pourrait voir l'émergence de nouveaux réseaux de botnets à grande échelle, en mesure de lancer des attaques ciblées. Ces réseaux de PC zombies présentent de l'intérêt pour les organisations APT car il est difficile pour les cibles de déterminer l'identité et les motivations des attaquants

APPAREILS MOBILES ET OBJETS CONNECTÉS TOUJOURS PLUS CIBLÉS

Les cybercriminels agissant pour le compte d'Etats pourraient toujours plus avoir recours à l'exploitation de failles se logeant dans différents devices. Mais aussi dans les objets connectés et autres appareils domotiques dits intelligents, souvent lacunaires en termes de mises à jour et de configurations sûres.

MENACES EN SURVEILLANCE 2024

HACKING EN TANT QUE SERVICE

offres de piratage à la location (hack-for-hire). Ces services se spécialisent dans la pénétration des systèmes et dans le vol de données. Des cyber-mercenaires.

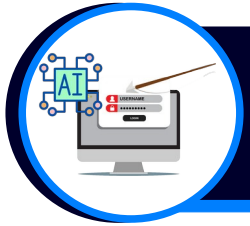
PIRATAGES ÉTATIQUES

il faut s'attendre à ce que cette tendance s'accentue, avec une hausse des cyberattaques menées par des acteurs parrainés par un Etat. Celles-ci devraient toucher non seulement les infrastructures critiques, les agences gouvernementales et les armées du monde entier, mais aussi les entreprises de médias.

LES ROOTKITS DE KERNEL

Microsoft a tenté de réduire la prévalence des rootkits et des attaques de bas niveau en introduisant de nouvelles fonctions de sécurité telles que l'architecture Secure Kernel dans les dernières versions de Windows. Toutefois, ces mesures n'empêchent pas les acteurs de la menace d'exécuter avec succès leurs logiciels malveillants dans le mode noyau des ordinateurs ciblés.

MENACES EN SURVEILLANCE 2024



GENAI ET SPEAR-PHISHING

Les acteurs de la menace créent leurs propres chatbots dopés à la GenAI basés sur des solutions licites. Cette évolution va probablement faciliter la production en grande quantité de messages de spear-phishing (hameçonnage ciblé), qui servent souvent de point de départ à des attaques de type APT ou autres.

DEEPFAKE ET HACKTIVISME

2024 verra un pic de ce type d'activisme, axé sur la désinformation. Mais aussi via des attaques DDoS, le vol ou la destruction de données, ou encore via du vandalisme sur des sites web.

BURN-OUT DES ÉQUIPES

Les JO, le stress, le poids des responsabilités, les sous-effectifs et les insuffisances budgétaires, voici le cocktail dévastateur qui guette les collaborateurs des équipes de cybersécurité, créant ainsi une vulnérabilité humaine.

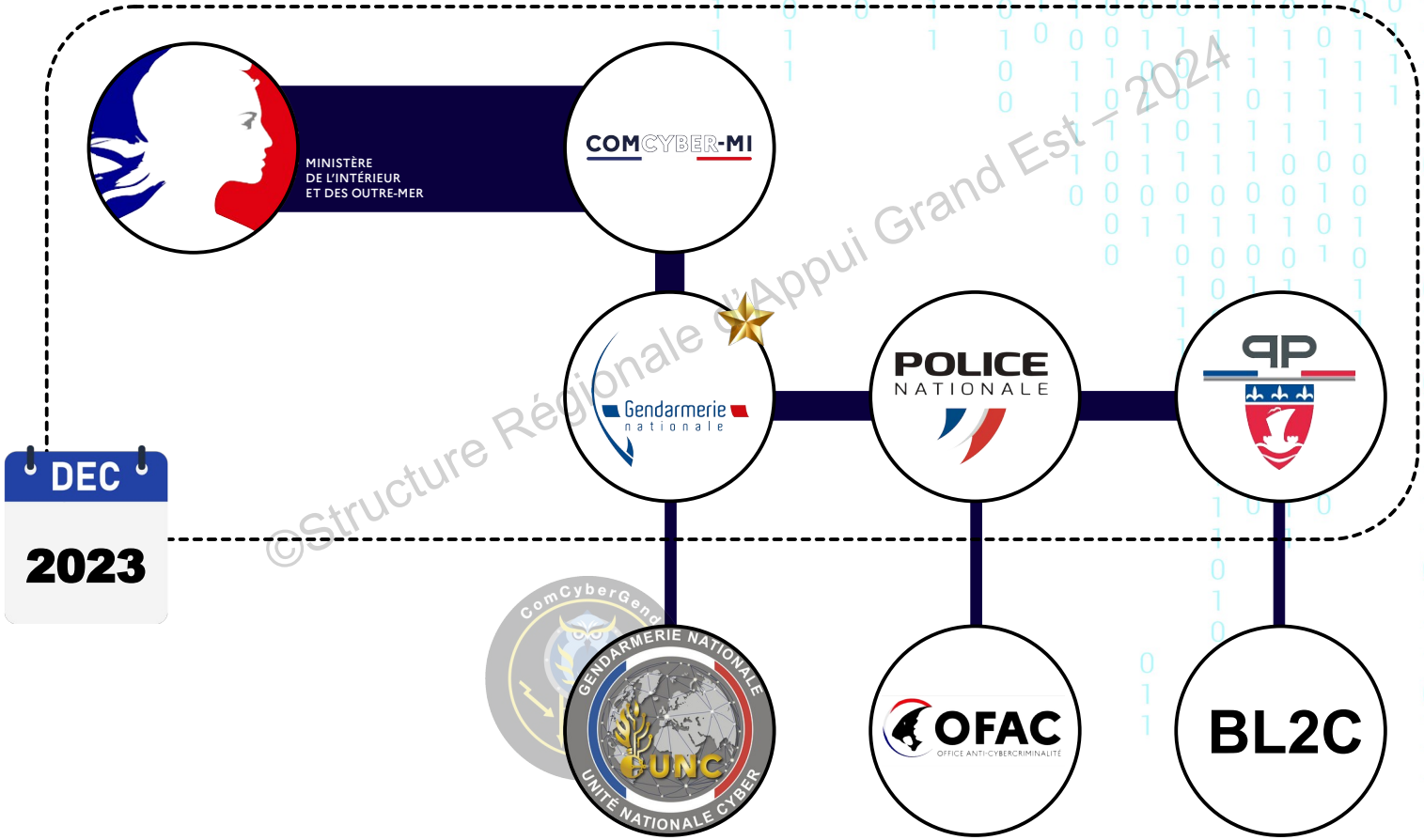
ORGANISATION

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

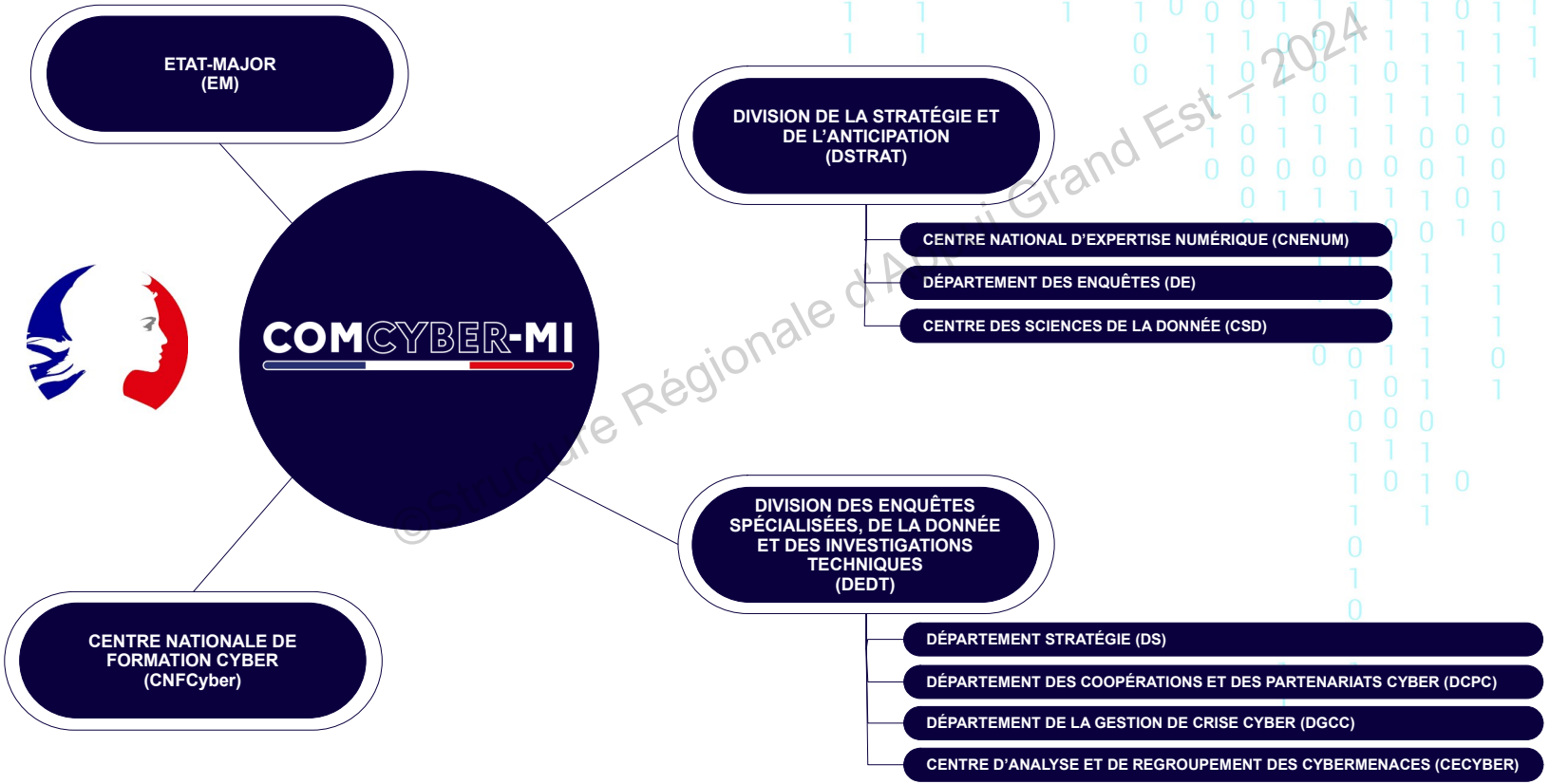


MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER
Liberté
Égalité
Fraternité

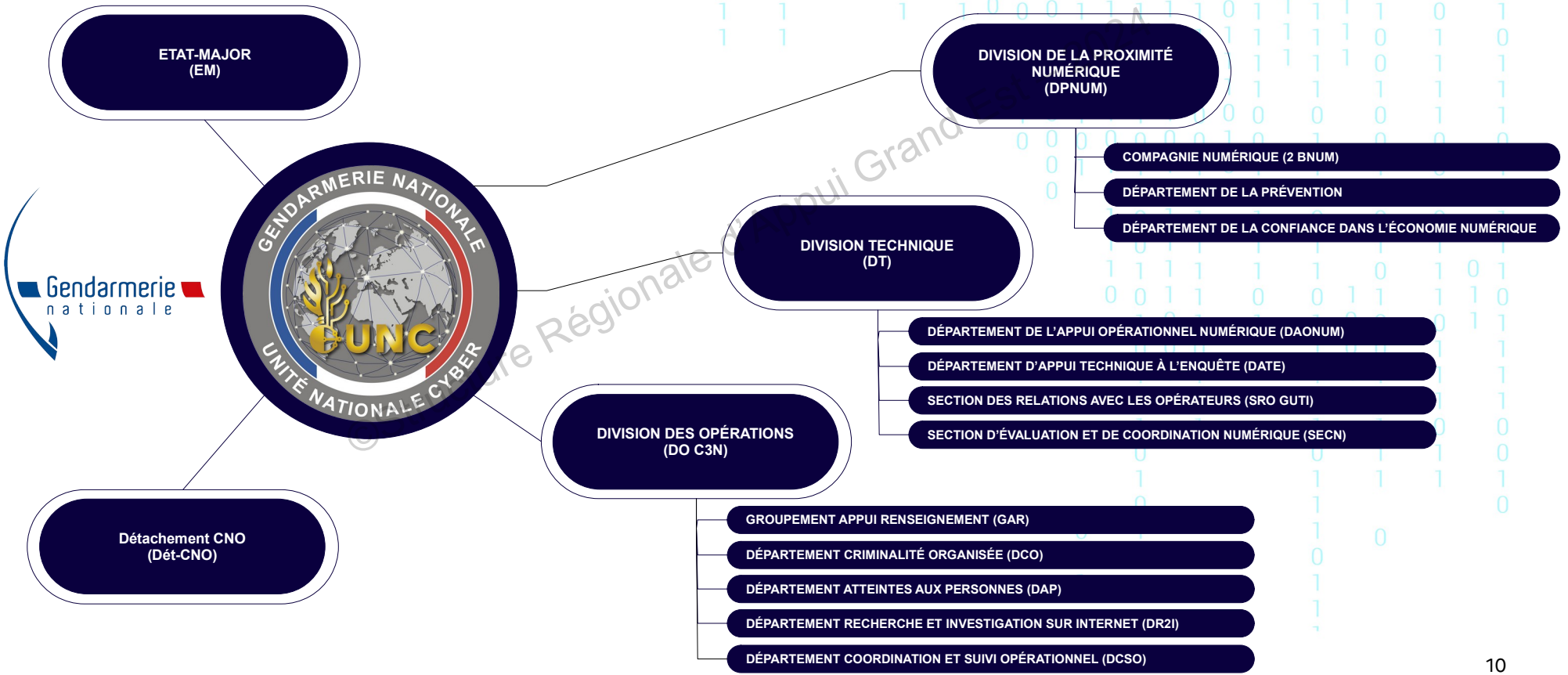
Gendarmerie nationale

UNCyber
Direction des opérations et de l'emploi

COMMANDEMENT DU MINISTÈRE DE L'INTÉRIEUR DANS LE CYBERESPACE

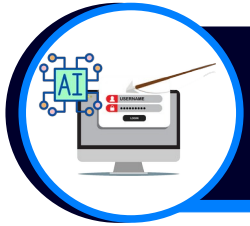


UNITÉ NATIONALE CYBER



SE PROTÉGER

COMMENT LUTTER CONTRE LES CYBERDÉLINQUANTS



C'est une question technique

C'est une question organisationnelle

C'est une question de sensibilisation

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

Gendarmerie nationale

MERCI,
POUR VOTRE ATTENTION

DES QUESTIONS ?