

# JOURNÉE RÉGIONALE CYBERSÉCURITÉ

MOT D'ACCUEIL

19/11/2024 - JEAN-CHRISTOPHE BERNADAC

**HCL**  
HOSPICES CIVILS  
DE LYON

**GCSoara**  
la santé connectée

[www.chu-lyon.fr](http://www.chu-lyon.fr)

**SECTEUR DE LA SANTÉ**  
ETAT DE LA MENACE INFORMATIQUE

TLRCLEAR

« Le secteur de la santé est un secteur **hautement critique**, soumis au triple impératif de **disponibilité**, de **confidentialité** et d'**intégrité** concernant les systèmes d'information (SI) utilisés et les données traitées.

Les incidents d'origine informatique qui l'affectent peuvent avoir des conséquences importantes sur la **continuité des soins** et des services de santé, pouvant aller jusqu'à la **mise en danger de la vie humaine... »**

**Importance de l'engagement des HCL dans la cybersécurité en tant qu'établissement de santé particulièrement exposé, et hébergeur de données de santé depuis 2013 et certifié depuis 2021**

# STRATÉGIE CYBERSÉCURITÉ DES HCL : UNE SÉCURITÉ A 360°

3

Une vision de la cybersécurité destinée à simplifier le quotidien de chacun :

- en proposant une cybersécurité « à 360° », qui répond aux points de contrôle exigés par les différentes réglementations
- en proposant une cybersécurité accessible a tous afin de préserver la confiance numérique

Axe 1



Agir pour éviter la crise

**Prévenir** : élaborer des programmes afin d'anticiper les menaces, de protéger la vie privée et de contribuer à la promesse d'une médecine d'excellence (cartographie du SI et de son environnement, sensibilisation des utilisateurs, analyse des risques...)

Axe 3



Accompagner la résilience des activités

**Assurer la résilience** des activités : développer les moyens organisationnels et techniques permettant de fonctionner sans informatique (exercices de crises cyber, PCA et PRA...)

Axe 2



Parfaire la résistance des infrastructures

**Protéger** les services numériques : mettre en œuvre des moyens technologiques et humains pour assurer la résistance des infrastructures et des logiciels (création d'une équipe Support Opérationnel en Cybersécurité)

# INVESTISSEMENT DES HCL DANS LA CYBERSÉCURITÉ OPÉRATIONNELLE

- Création en 2021 de l'équipe Support Opérationnel en Cybersécurité – 2 missions principales :
  - La détection et la réponse aux cyberattaques (SOC)
  - L'aide à la sécurisation des architectures informatiques (Cyber-architecture)
- SOC opéré en interne par les HCL
  - Outillage : EDR, SIEM, Sondes de détection d'intrusion...
  - Renfort de l'équipe en 2024 permettant la mise en œuvre d'une astreinte cybersécurité en 24/7
  - Services de cybersécurité (par exemple EDR) opéré pour les établissements du GHT Val Rhône Centre
- Protection des accès externes par MFA, mise en place de réseaux d'administration, segmentation...

# UN SOC EN EUROPE

## PROJET SOC4HEALTH PORTÉ PAR LES HCL – LES AMBITIONS

- Création et mise à disposition d'un kit "Security Operation Center" (SOC) mis à disposition des hôpitaux européens qui inclura :
  - Comment mettre en place une équipe cybersécurité opérationnelle
  - Comment internaliser à 100% un SOC dans un hôpital
- Mise en place d'une infrastructure intelligente de détection de menace et de partage d'indicateurs
  - Partenariat avec l'INRIA pour la partie Intelligence Artificielle
- Co-financé par l'UE – Permet un renforcement du SOC des HCL et de faire bénéficier la communauté de l'expertise/expérience acquise

**MERCI**

[www.chu-lyon.fr](http://www.chu-lyon.fr)



**HCL**  
HOSPICES CIVILS  
DE LYON