



CAMU 2022
COLLEGE AQUITAIN DE MEDECINE D'URGENCE

28^{eme} Congrès Aquitain
de Médecine d'Urgence

6 & 7 AVRIL
PESSAC (33) INSTITUT DES MÉTIERS
DE LA SANTÉ HÔPITAL XAVIER ARNOZAN

sfmu **SFMC** **CHU BDX** CENTRE HOSPITALIER UNIVERSITAIRE BORDEAUX

l'hôpital
NORD
OUEST
Villefranche-sur-Saône
Tarare
Trévoux
St Cyr au Mont d'Or

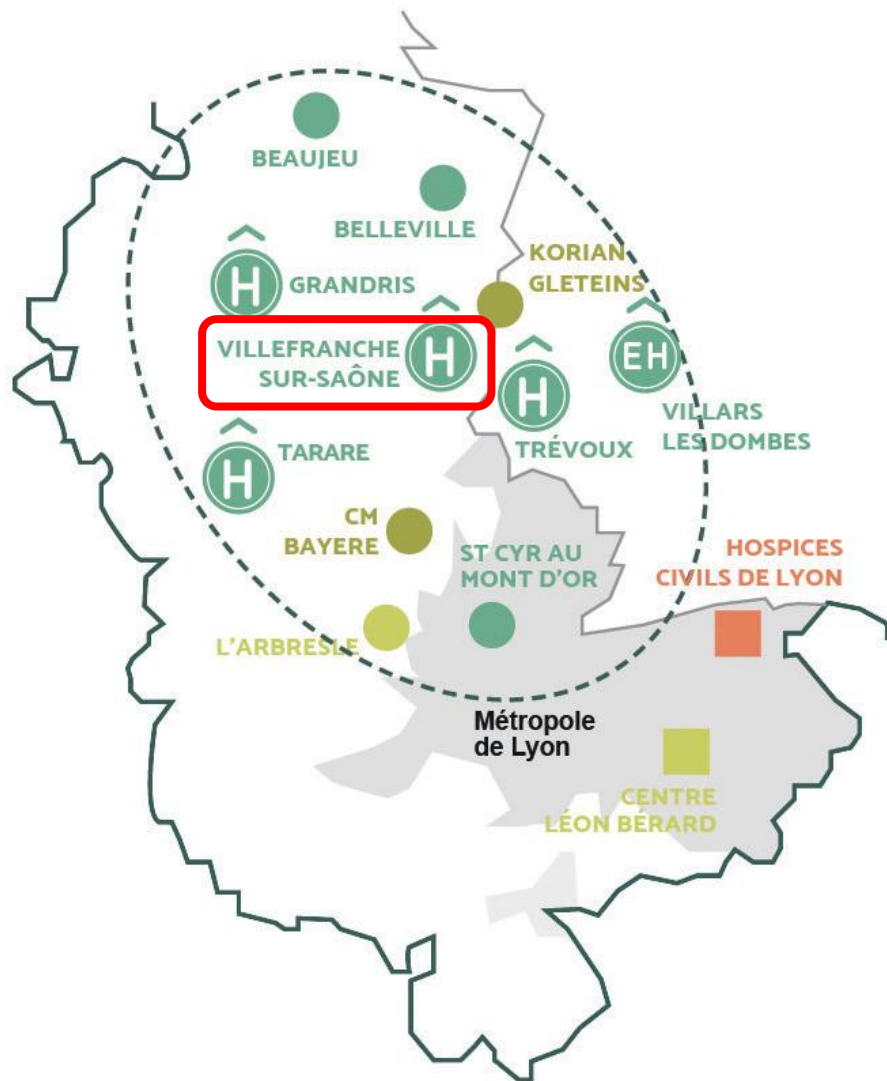


RETEX d'une cyberattaque à l'hôpital de Villefranche-sur-Saône -15 février 2021-

Dr Marc DU BESSET
Responsable SMUR.
Référent SSE
Hôpital Nord Ouest Villefranche

Dr Olivia DECLERCK
Médecin urgentiste
Hôpital Nord Ouest Villefranche

Introduction



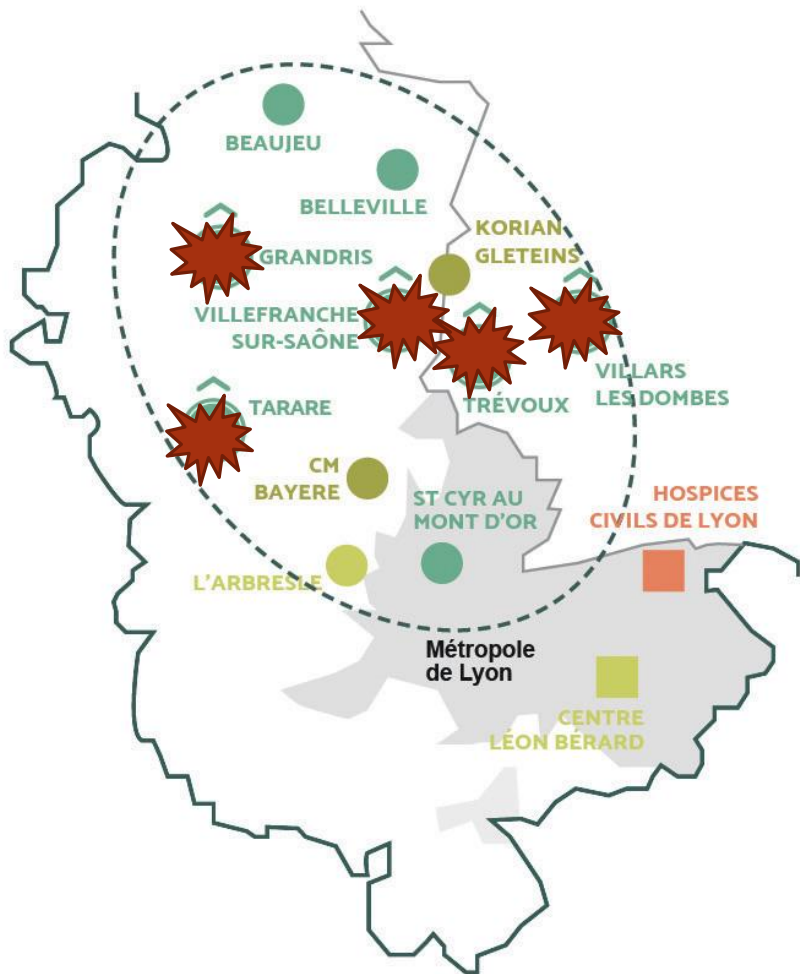
- L'hôpital de Villefranche sur Saône :
 - Etablissement de référence du nord du Rhône
 - 40 km au nord du CHU de Lyon
 - Territoire de 350 000 habitants sur 2 départements
 - 670 lits MCO avec plateau technique spécialisée
 - Urgences : 83 500 passages en 2019
- Le GHT « Rhône Nord Beaujolais Dombes »
 - 5 hôpitaux (Villefranche-sur-Saône, Tarare-Grandris, Trévoux, Belleville et Beaujeu)
 - 10 EHPAD
 - 2640 lits (50% sanitaire-50% EHPAD)

The background features several concentric, curved lines in a light brown or tan color, primarily on the left side of the page. These lines are of varying thicknesses and some are solid while others are dashed, creating a sense of depth and movement.

Une panne informatique aux urgences

J0: Le jour de l'attaque

- Lundi 15 février 2021
- 2^e semaine vacances scolaires
- Sortie de 2^eme vague Covid
- 04h45: aucun logiciel ne fonctionne
- **05h00: Alerte Cyberattaque**
- Consigne: Eteindre tout le système informatique !!!
- 5 sites du GHT concernés



J0

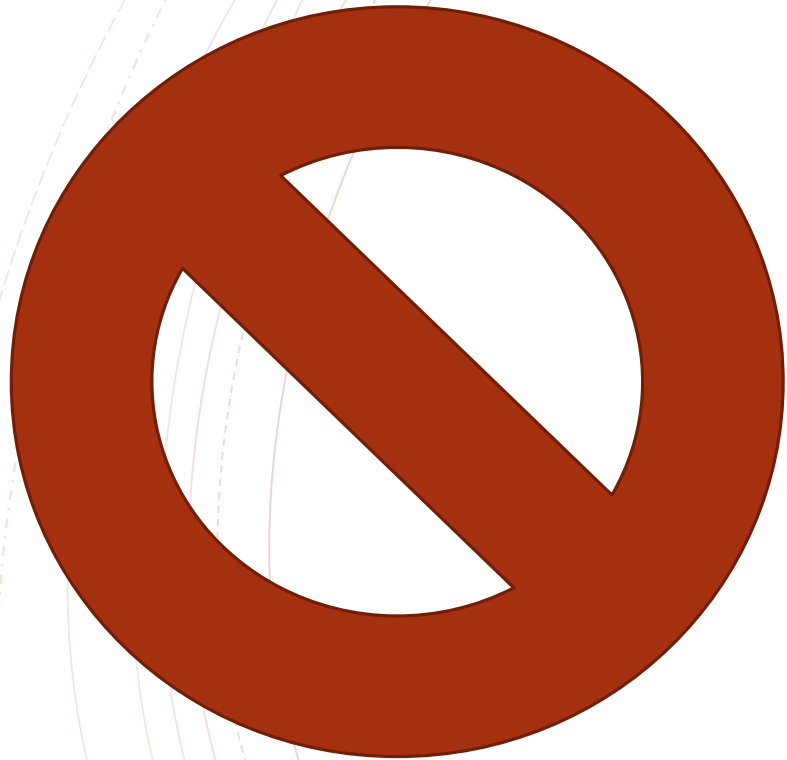
Les premiers
jours

Le
rétablissement

Forces et
limites

Conclusion

Take home
message

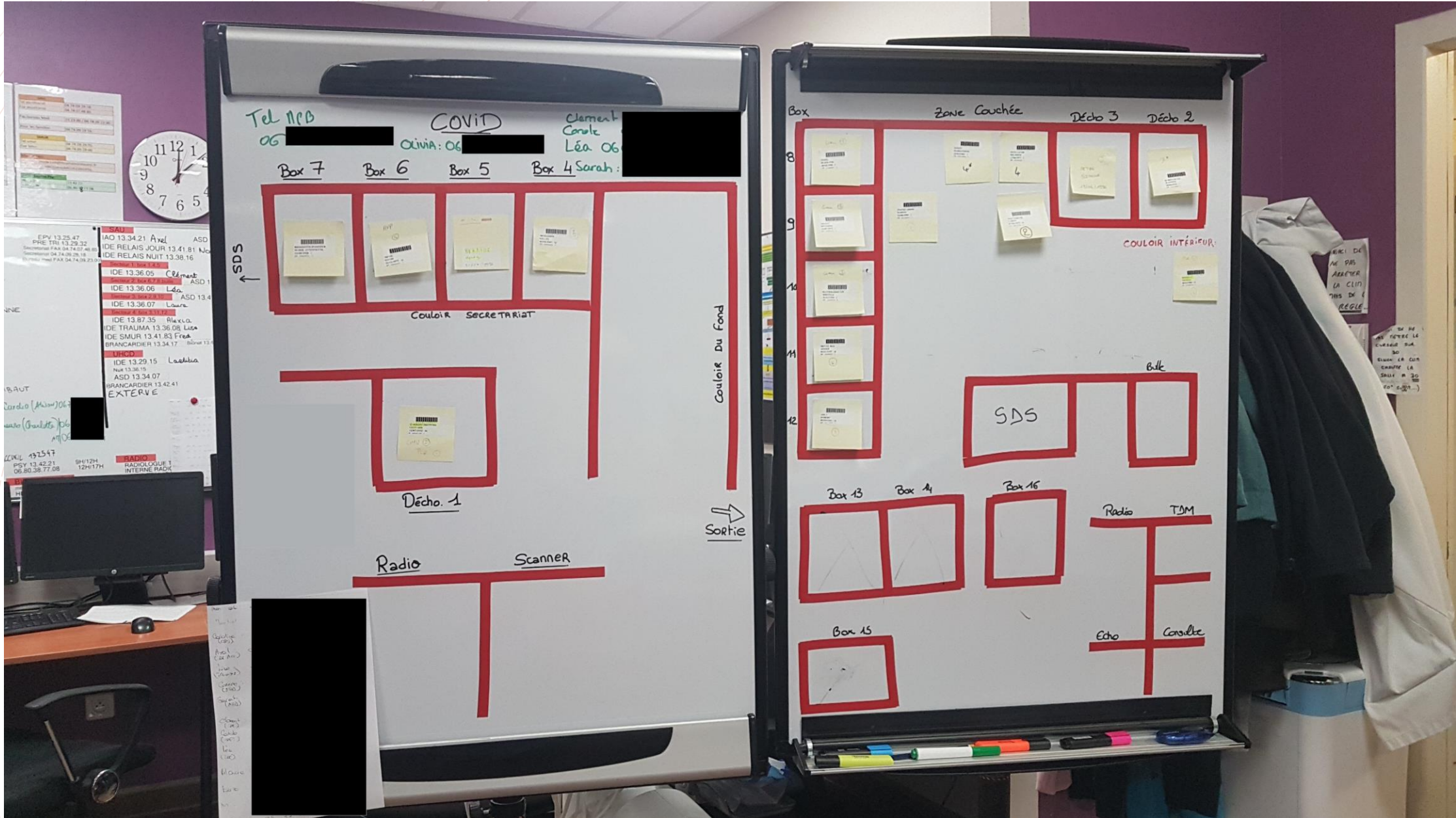


- Imagerie, laboratoire
- Report de Scope
- Dossier médical (pancarte, ATCD, prescription)
- Dossier administratif (coordonnées des familles)
- Logistique: caméra, climatisation, etc...
- Téléphonie interne et externe

Gestion de la crise :

- Protéger : débrancher tout le réseau
- Alerter
 - Les autorités : ARS, ANSSI
 - Les régulations pour détourner les flux
(pas de fermeture complète des urgences)
- Secourir : récupérer les sauvegardes
 - Récupérer les prescriptions
 - Lister et localiser les patients





Gestion de la crise:

PATIENT	BOX	MOTIF	DIAGNOSTIC	MEDECIN	IDE
			48102		
	12	Dolence à l'œil avec douleur Mo		Alice	
	13	Odeur de Hémoglobine		Camille	
	14	insomnie		Expense	
	15	Lombalgie		Elgenne	
	16	Hallucination depuis le 15/02 avec insomnie		Expense	
	17	Séq. CCN + hématurie		Expense	
	18	El pied gauche sans lésion		Clémence	
	19	Dir Hto + cholestérol + dir dans lombaire			

- Alerter les autorités
- Détourner le flux
- Lister et localiser les patients
- Procédures « papier-crayon »
- Etiquettes manuscrites et identité vigilance
- Biologie en dégradé : allongement des délais et saturation des capacités
- Imagerie: pas d'accès au PACS
- Arrêt des admissions en soins intensifs/réa

J0

Les premiers
jours

Le
rétablissement

Forces et
limites

Conclusion

Take home
message

Rétablissement du système informatique (SI)

J0

J2

- 1 poste par soins critiques

J10

- SI rétabli au SAU

J19

- Reprise flux au SAU

J45

- SI rétabli dans services de soins

M3

- Réhabilitation de l'ensemble du SI

J0

Les premiers
jours

Le
rétablissement

Forces et
limites

Conclusion

Take home
message

Éléments remarquables

- Réactivité de l'équipe SI : pas de perte des données
- Adaptabilité des soignants, improvisation
- Solidarité territoriale pour gérer l'afflux de patients

Pistes d'amélioration

- Réécriture des procédures
- Formation du personnel aux procédures et exercices
- Anticipation d'une panne plus étendue et plus durable
- Recherche d'une alternative à la téléphonie interne
- Education à l'hygiène numérique
- Renfort de la cyber sécurité hospitalière
- Importance du RETEX

Avant de conclure, un peu d'informatique..

- ▼ Les principes d'une cyber-attaque
 - Introduction dans le système par une équipe et réalisation d'une porte d'accès dérobée
 - « porte d'accès » vendue à une autre équipe qui s'occupe de crypter et demander la rançon
- Rançongiciel : cryptovirus RYUK qui chiffre les données



- A villefranche : aucune perte de donnée ni d'extraction de données
- Décision prise de reconstruction l'ensemble du SI
- Aide de l'ANSSI
- 500 serveurs - 3 000 postes informatiques à remastériser – 200 applications à remettre en service
- Priorisation de la remédiation en commençant par les services critiques

J0

Les premiers
jours

Le
rétablissement

Forces et
limites

Conclusion

Take home
message

Conclusion

- Evènement hors normes
- Déstabilisation a minima de l'ensemble de la région sanitaire
- Nombreux facteurs « chance »
- Quid d'une attaque de plus grande ampleur ? (plusieurs établissements voisins)
- Cout financier considérable. Au niveau informatique : 800 000€

J0

Les premiers
jours

Le
rétablissement

Forces et
limites

Conclusion

Take home
message

Aucun établissement n'est à l'abri

- **Protéger** : Débrancher immédiatement les câbles réseau.
- **Alerter** : Détourner rapidement le flux de patients.
- **Sauvegarder** : Récupérer les sauvegardes de prescriptions.

Intégrer le risque CYBER dans nos procédures SSE.

- Prévoir en amont tous les documents sur papier.
- Possibilité d'avoir un ordinateur + imprimante hors réseau (étiquettes de patient).

Merci de votre attention

