Cybersécurité

Journée des membres de l'Aster

3 décembre 2022 – Laurent Chatelain

Préambule

Pour commencer… quelques questions :

- Avez-vous déjà envisagé une coupure de votre système d'information / traçabilité ?
- Où est hébergé votre système d'information ?

- Avez-vous défini un plan d'action en cas de coupure ?
- Avez-vous testé votre plan d'action ?

- Votre système est-il sauvegardé régulièrement ?
- Qui vérifie que la sauvegarde se passe bien ?
- A quelle fréquence ?

Etes-vous bien sûr de vos réponses ??

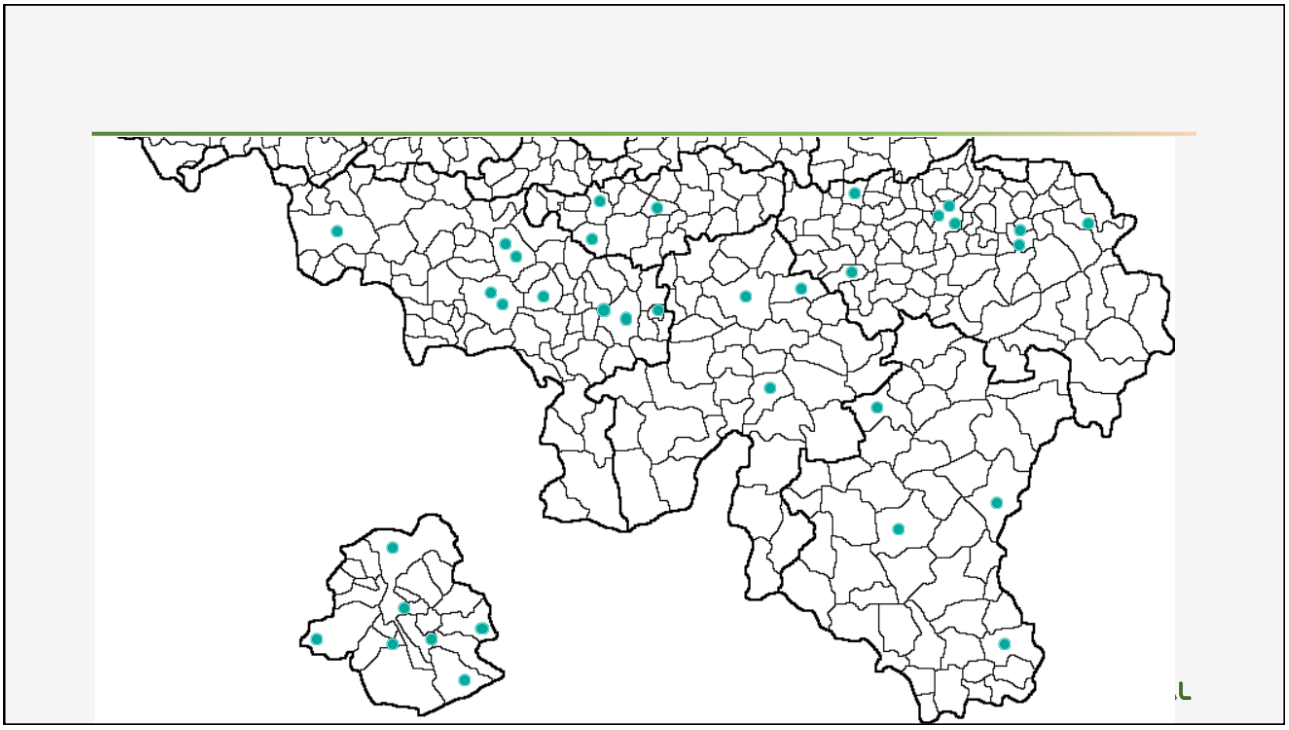
Contenu

- Aexis Medical en quelques mots
- Cyber-attaques ? Hacking ? C'est quoi ??
- Conséquences concrètes ?
- Gérer le risque…
- Mesures prises en interne
- A l'hôpital ?
- Quelques réflexions sur base des expériences passées
- Evolutions envisagées

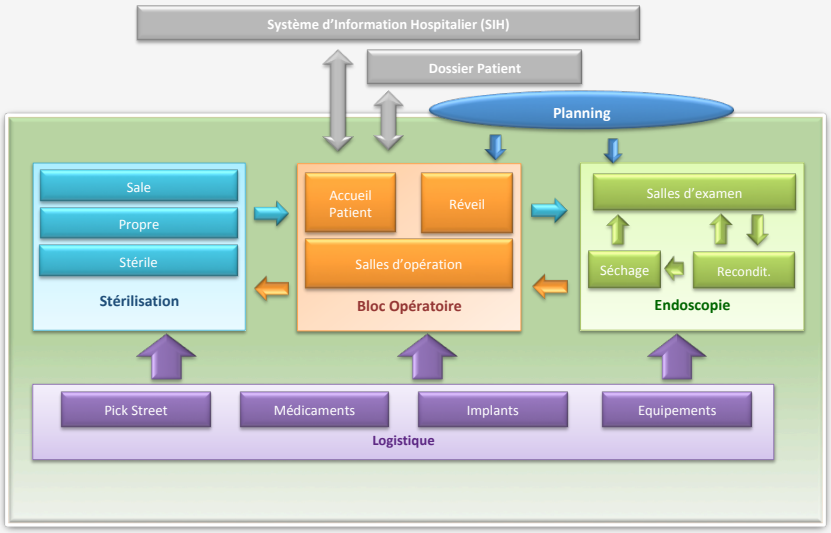
Aexis Medical

- Société belge fondée en 2004
- Solutions pour les départments hospitaliers
  - Sterilisation Centrale (2004) : +100 hôpitaux (75% marché belge)
  - Bloc + Logistique (2008) : +75 hôpitaux
  - Endoscopie (2015) : + 20 hôpitaux
  - Autres : ~ 10 hôpitaux
- Tout types d'institutions : Universitaires, Publics, Privés, 1:N, N:N sites

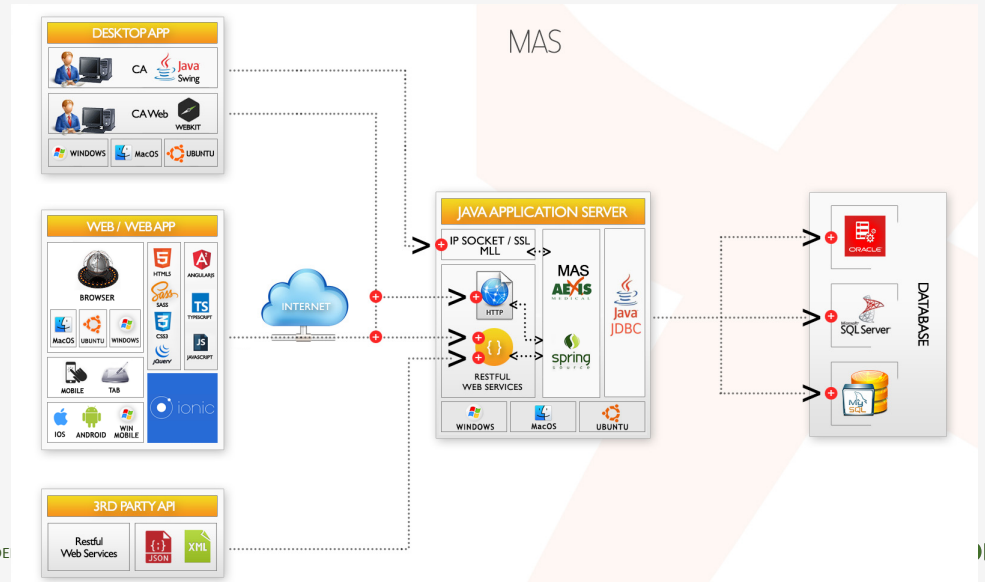
- 34 sites hospitaliers utilisateurs de SteriLine en Wallonie / Bxl



Platforme XLine



Architecture Platforme XLine



Aexis Medical

- 2 implantations : Tirlemont (Belgique) – Colombo (Sri Lanka)
- 22 personnes en Belgique – 42 personnes au Sri Lanka
- 12 Serveurs physiques
  - Code Source, Bases de Données, Développement, …
  - Tests automatisés
  - Stockage de fichiers et Backup
  - Instances d'accès à distance chez les clients
- 87 Workstations
- Cloud :
  - Email - Office
  - Logiciel ITSM (Helpdesk, Base de connaissances, Gestion de projet)
  - Comptabilité
  - Téléphonie

Cyberattaques : Pourquoi ? Comment ? Sur qui ?

- Vol de données (médicales, bancaires, …)
- Bloquage de l'organisation - Nuisances
- Convictions ou Gains financiers - $$$

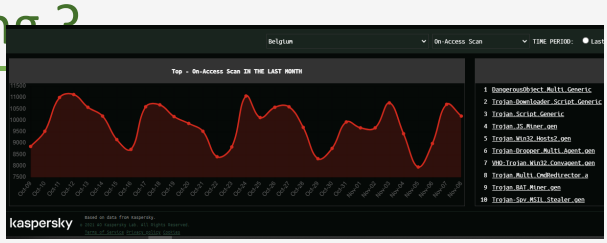
- Intrusion
- Suppression de services
- Encryption des stockages

- Particuliers
- Organisations commerciales
- Organisations (non-)gouvernementales
- Autres…

Cyber Attaques ? Hacking ?

- Chevaux de Troie / Phishing
  - Interception d'identifiants
  - Redirection vers de "faux" sites web

9000 à 11000 détections par jour en BE



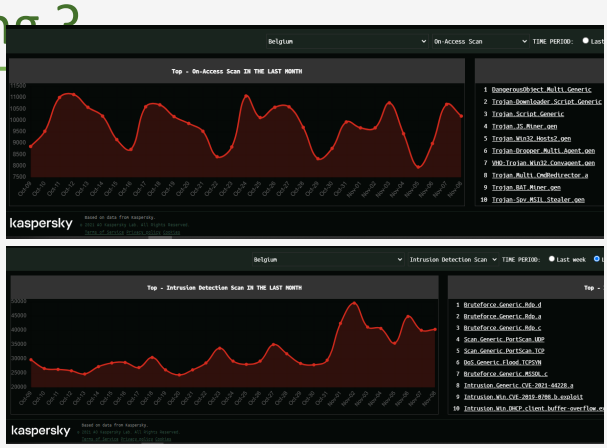
Cyber Attaques ? Hacking ?

- Chevaux de Troie
  - Interception d'identifiants
  - Redirection vers de "faux" sites web

  9000 à 11000 détections par jour en BE

- Tentatives d'intrusion (Bruteforce / PortScan)

  35000 à 50000 détections par jour en BE



Cyber Attaques ? Hacking ?

- Chevaux de Troie
  - Interception d'identifiants
  - Redirection vers de "faux" sites web

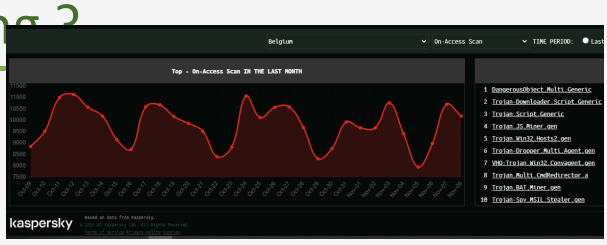
  9000 à 11000 détections par jour en BE

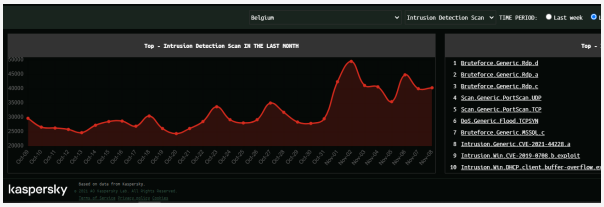
- Tentatives d'intrusion (Bruteforce / PortScan)

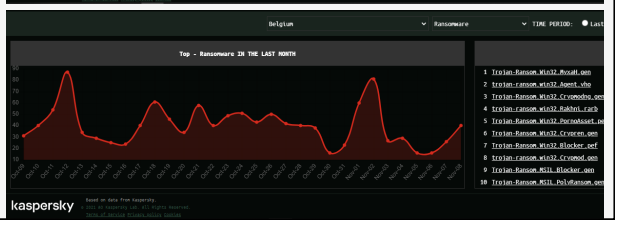
  35000 à 50000 détections par jour en BE

- Ransomware

  30 à 90 détections par jour en BE







CONFIDENTIAL – DO NOT DISTRIBUTE

Cyberattaques : Quels effets ? Conséquences ?

- Divulgation de données sensibles
- Interruption des services fournis par l'organisation au monde extérieur
- Perte d'accès aux données internes à l'organisation (comptabilité, connaissances, état des lieus, bases de données, …)

- Isolation de l'entité attaquée du monde extérieur (coupure des accès internet)
- Segmentation du réseau
- Coupure des serveurs applicatifs / base de do

→ Empêche le fonctionnement normal de l'orga
→ Coût opérationnel et financier (rançon / perte


ACCUEIL • SOCIÉTÉ

La cyberattaque de décembre 2021 a coûté 2,25 millions à la Défense

Une importante cyberattaque contre le ministère de la Défense l'avait obligé à couper Internet et cesser le trafic de courriels vers l'extérieur pendant plusieurs semaines.

Cyberattaques : Concrètement à l'hôpital…

Suite aux cyberattaques, nous avons dû procéder à certaines annulations.

Nous vous enverrons un pigeon pour vous informer du nouveau rendez-vous!

Cyberattaques : Concrètement à l'hôpital…

- Coupure Internet
  - Accès aux emails
  - Accès aux plateformes / fournisseurs externes
    - Commandes de linge, Matériel ancillaire, Stérilisation externalisée, Catalogues
  - Accès des patients (Prise de RDV, Dossier Médical, …)
  - Accès des médecins externes (Résultats Labos, Protocoles, …)
  - Accès des fournisseurs (Support, …)
  - Accès du personnel depuis l'extérieur (Consultations à domicile, Télétravail, …)

Cyberattaques : Concrètement à l'hôpital…

- *Nos appareils sont maintenant sécurisés à 100%*
- *Comment y-es-tu arrivé ?*
- *Je les ai tous éteints…*

Cyberattaques : Concrètement à l'hôpital…

- Coupure Internet
  - Accès aux emails
  - Accès aux plateformes / fournisseurs externes
    - Commandes de linge, Matériel ancillaire, Stérilisation externalisée, Catalogues
  - Accès des patients (Prise de RDV Dossier Médical, …)
  - Accès des médecins externes (Résultats Labos, Protocoles, …)
  - Accès des fournisseurs (Support, …)
  - Accès du personnel depuis l'extérieur (Consultations à domicile, Télétravail, …)
- Coupure de systèmes internes
  - Patients dans l'hôpital ? Traitements en cours ?
  - Patients planifiés ? Quelle intervention ? Quel RDV ?
  - Enregistrement des prestations ? Facturation ?
  - Appareillage lié au réseau ? Fonctionnement autonome ?

Cyberattaques : Concrètement à l'hôpital…

- Encryption des données
  - Ré-installation des serveurs
    → Utilisation de backups → Perte de données (?)
  - Ré-installation des postes de travail
  - Ré-installation des imprimantes
    → Re-configuration de l'architecture de la sterili
  - Re-déploiement des interfaces avec systèmes / appareillage tiers
    → Consistance des données entre systèmes

Cyberattaques : Que faut-il en penser ?

- Comment suis-je protégé ?
- Comment se protéger ?
- Que faut-il envisager en plus ?

Tôt ou tard… “Sh!@# happens…”

- Quelle sera la situation si (lorsque) cela arrive ?
- Que fera-t-on / pourra-t-on faire / devra-t-on faire lorsque ça arrive ?

Réflexion et discussion… Le début de la solution !

Tôt ou tard…

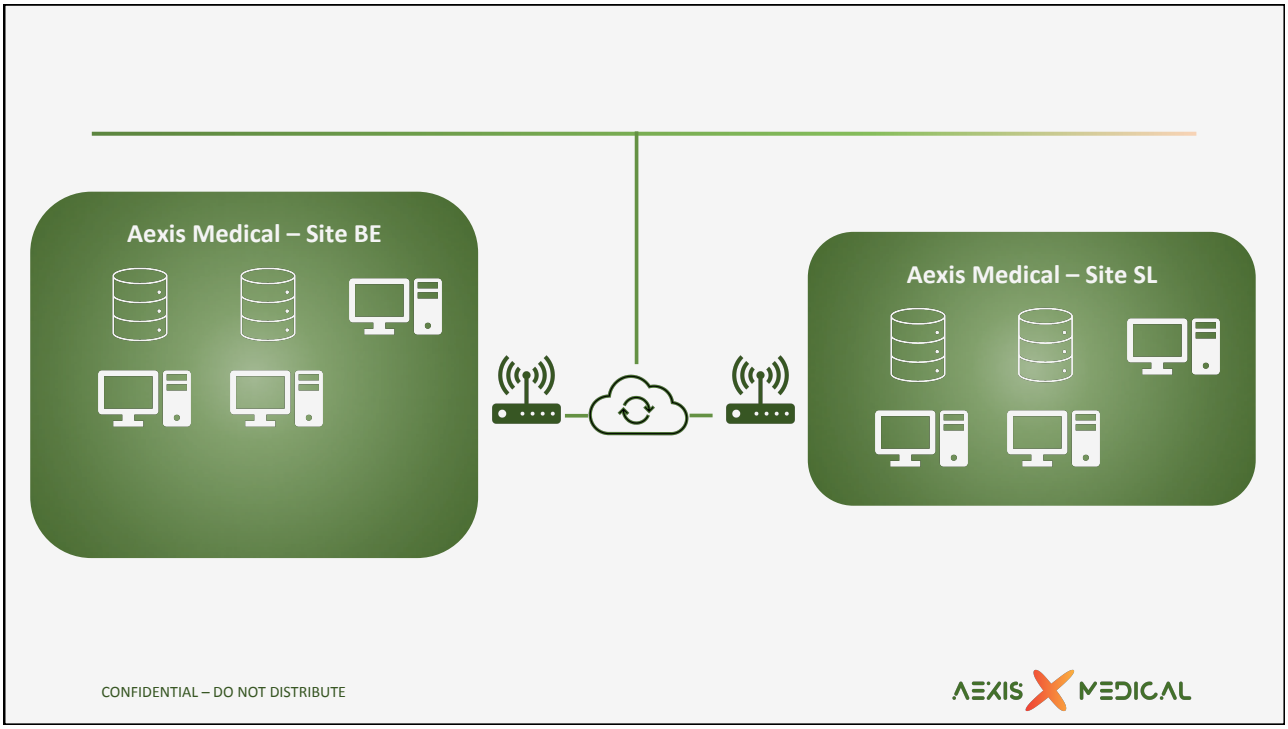
Mesures prises chez Aexis Medical

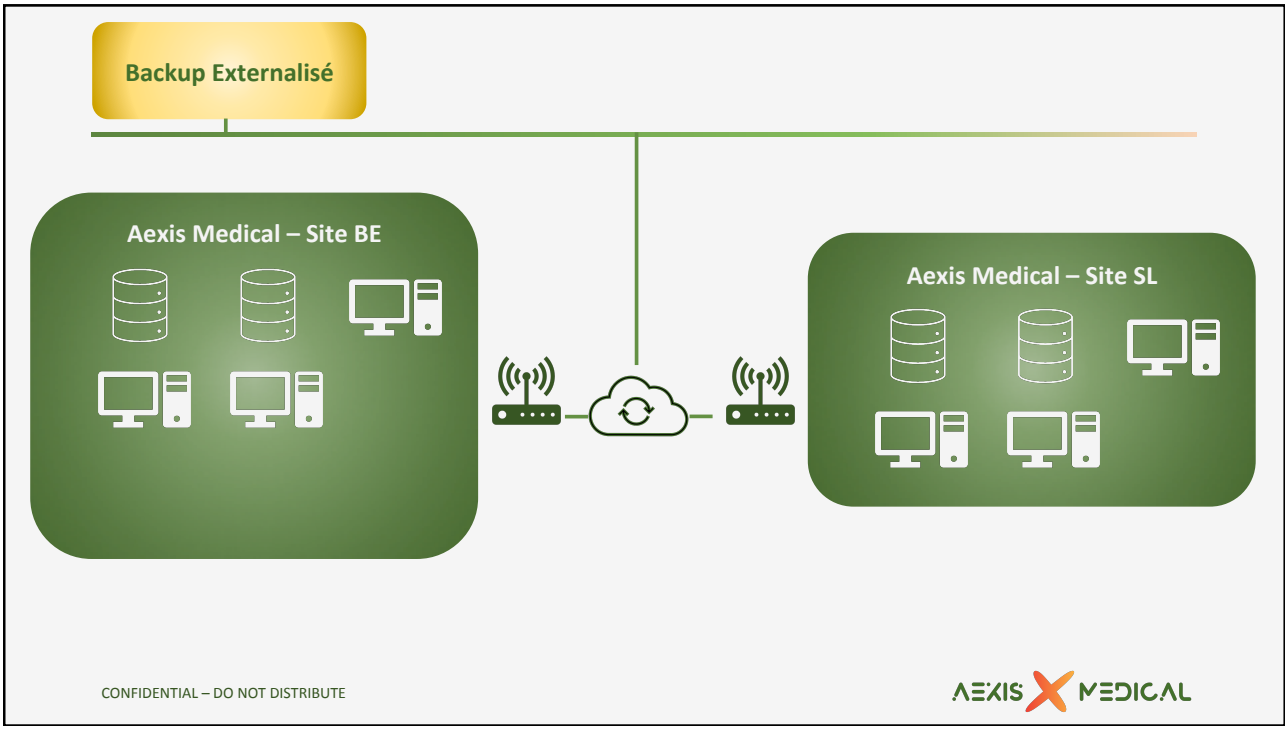
- Sécurisation de l’infrastructure (Pare-feux, mots de passe, anti-virus)
- Contrats de service avec des entreprises spécialisées

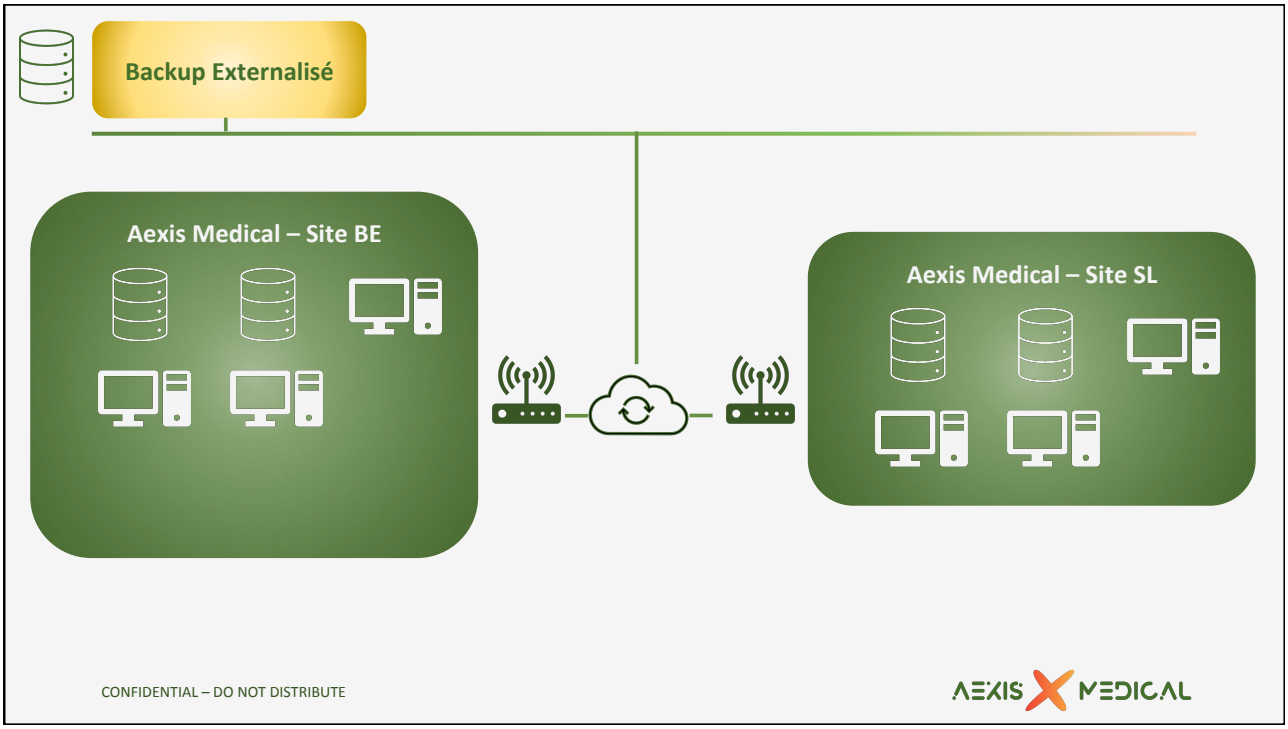
- Mix d’outils “On premise” et “Cloud/External based”
- Réplication des données entre les serveurs Belges et Sri Lankais
- Stockage de backups en dehors de l’infrastructure (réseau et physique) de l’entreprise

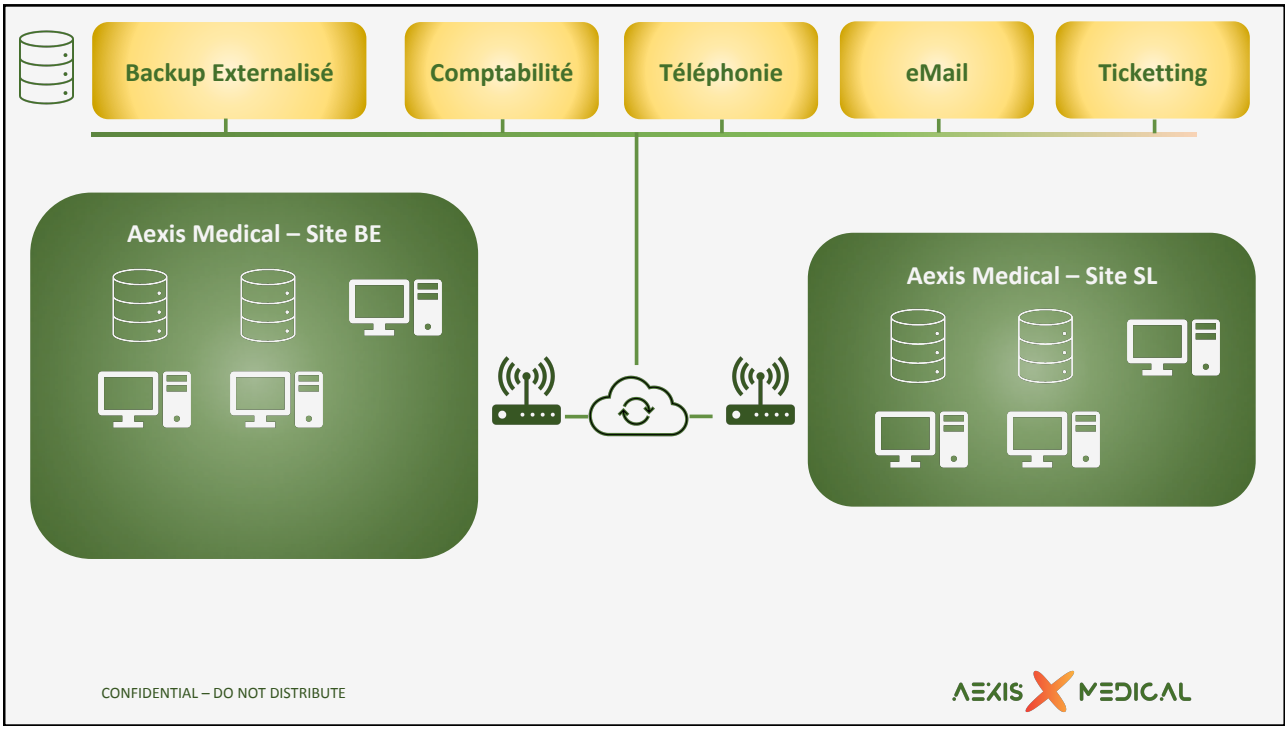
- Pas de connexion permanente chez nos clients (Tunnel VPN)
- Individualisation des instances utilisées pour le support des hôpitaux

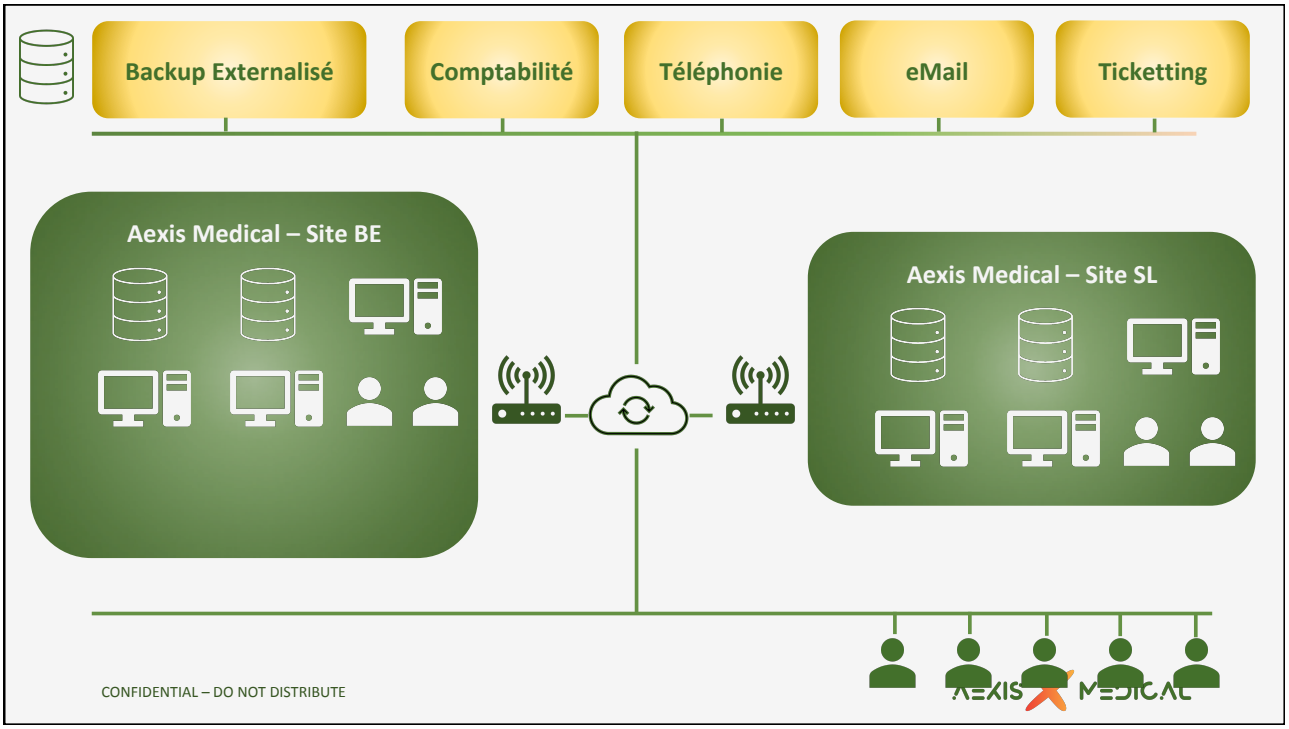
- Assurance et accès aux experts

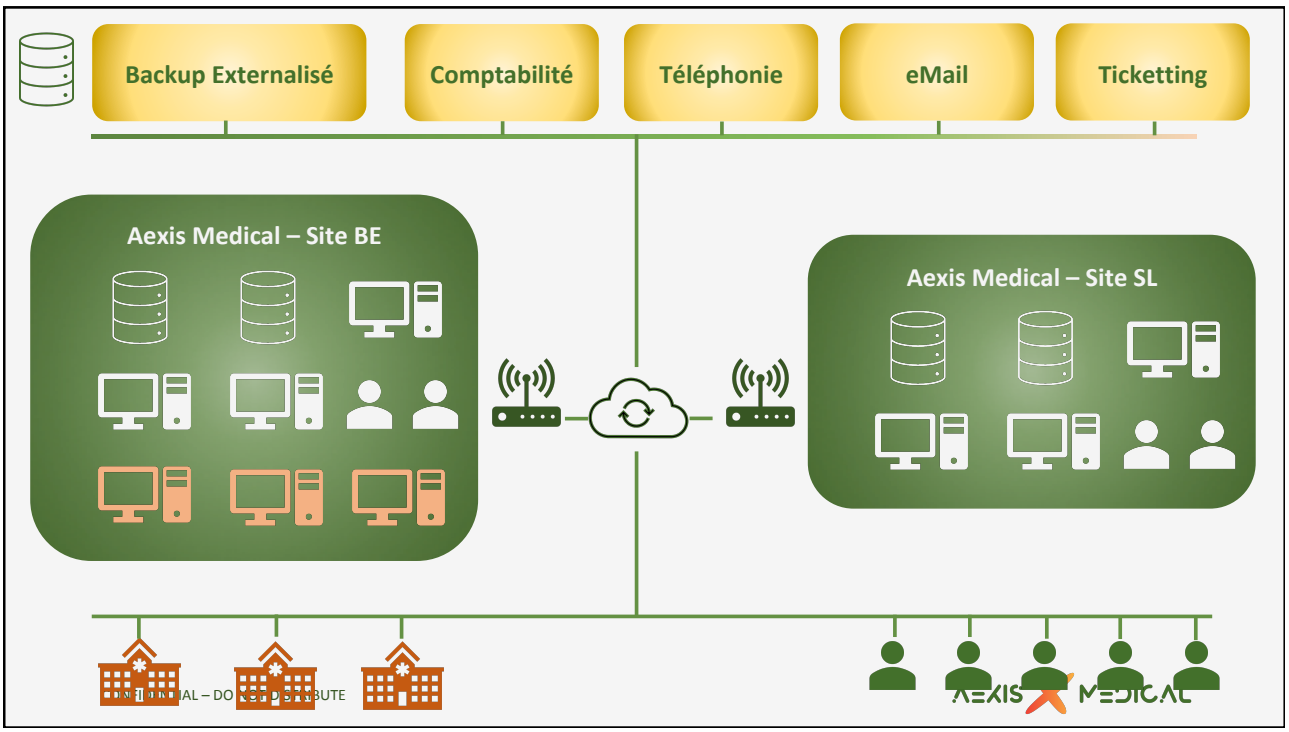

Aexis Medical – Site BE
Aexis Medical – Site SL
CONFIDENTIAL – DO NOT DISTRIBUTE
AEXIS MEDICAL


Backup Externalisé
Aexis Medical – Site BE
Aexis Medical – Site SL
CONFIDENTIAL – DO NOT DISTRIBUTE
AEXIS MEDICAL


Backup Externalisé
Aexis Medical – Site BE
Aexis Medical – Site SL
CONFIDENTIAL – DO NOT DISTRIBUTE
AEXIS MEDICAL


Backup Externalisé
Comptabilité
Téléphonie
eMail
Ticketting
Aexis Medical – Site BE
Aexis Medical – Site SL
CONFIDENTIAL – DO NOT DISTRIBUTE
AEXIS MEDICAL


Backup Externalisé
Comptabilité
Téléphonie
eMail
Ticketting
Aexis Medical – Site BE
Aexis Medical – Site SL
CONFIDENTIAL – DO NOT DISTRIBUTE


Backup Externalisé
Comptabilité
Téléphonie
eMail
Ticketting
Aexis Medical – Site BE
Aexis Medical – Site SL

Services proposés aux hôpitaux

- Prestations spécifiques au service informatique inclues dans l'implémentation
  - Formation sur l'architecture applicative
  - Aide à la mise en place du dispositif de sauvegarde
  - Validation de sauvegarde
  - Mise en place de systèmes redondants (test / backup)

- Prestations spécifiques au service informatique supplémentaires
  - Tests de redondance
  - Tests de restauration

Fonctionnalités proposées aux hôpitaux

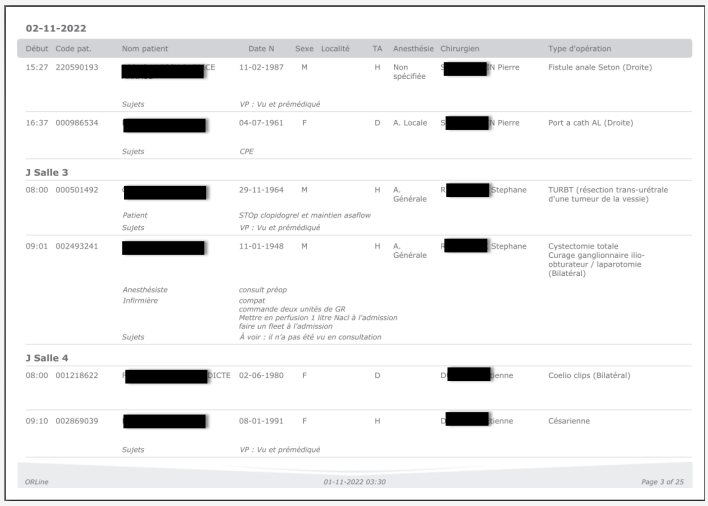
- Export automatisé et régulier de données opérationnelles
  - Inventaire et Contenu des boîtes
  - Inventaire des instruments (datamatrix)
  - Inventaire et état des Endoscopes
  - Profils opératoires (Liste de matériel à préparer)
  - Planning opératoire
  - Planning endoscopie

- Déploiement et distribution des données sur une liste de PC "stratégiques"

  Volume et fréquence de données exportées !!

  (Disaster – Recovery)

Fonctionnalités proposées aux hôpitaux



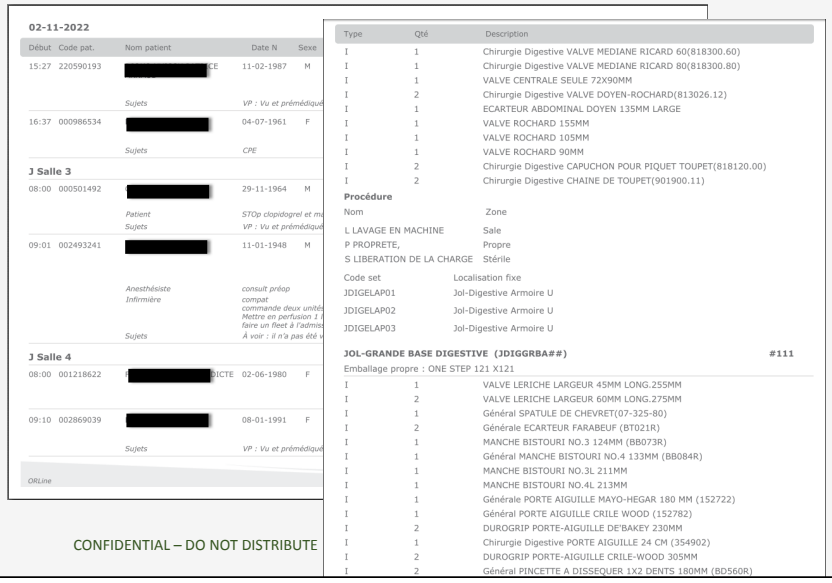
02-11-2022

Début	Code pat.	Nom patient	Date N	Sexe	Localité	TA	Anesthésie	Chirurgien	Type d'opération
15:27	220590193	[redacted]	11-02-1987	M		H	Non spécifiée	[redacted] Pierre	Fistule anale Seton (Droite)
		Sujets	*VP : Vu et prémédiqué*						
16:37	000986534	[redacted]	04-07-1961	F		D	A. Locale	[redacted] Pierre	Port a cath AL (Droite)
		Sujets	*CPE*						
J Salle 3									
08:00	000501492	[redacted]	29-11-1964	M		H	A. Générale	[redacted] Stephane	TURBT (résection trans-urétrale d'une tumeur de la vessie)
		Patient	*STOp clopidogrel et maintien asaflow*						
		Sujets	*VP : Vu et prémédiqué*						
09:01	002493241	[redacted]	11-01-1948	M		H	A. Générale	[redacted] Stephane	Cystectomie totale Curage ganglionnaire ilio-obturateur / laparotomie (Bilatéral)
		Anesthésiste *Infirmière*	*consult préop* *compat* *commande deux unités de GR* *Mettre en perfusion 1 litre Nacl à l'admission* *faire un fleet à l'admission*						
		Sujets	*À voir : il n'a pas été vu en consultation*						
J Salle 4									
08:00	001218622	[redacted]	02-06-1980	F		D		[redacted] Jienne	Coelio clips (Bilatéral)
09:10	002869039	[redacted]	08-01-1991	F		H		[redacted] Jienne	Césarienne
		Sujets	*VP : Vu et prémédiqué*						

ORLine *01-11-2022 03:30* *Page 3 of 25*

AEXIS MEDICAL

Fonctionnalités proposées aux hôpitaux



02-11-2022

Début	Code pat.	Nom patient	Date N	Sexe
15:27	220590193	[redacted]	11-02-1987	M
		Sujets	*VP : Vu et prémédiqué*	
16:37	000986534	[redacted]	04-07-1961	F
		Sujets	*CPE*	
J Salle 3				
08:00	000501492	[redacted]	29-11-1964	M
		Patient	*STOp clopidogrel et ma*	
		Sujets	*VP : Vu et prémédiqué*	
09:01	002493241	[redacted]	11-01-1948	M
		Anesthésiste *Infirmière*	*consult préop* *compat* *commande deux unités* *Mettre en perfusion 1 l* *faire un fleet à l'admiss*	
		Sujets	*À voir : il n'a pas été v*	
J Salle 4				
08:00	001218622	[redacted]	02-06-1980	F
09:10	002869039	[redacted]	08-01-1991	F
		Sujets	*VP : Vu et prémédiqué*	

ORLine

Type	Qté	Description
I	1	Chirurgie Digestive VALVE MEDIANE RICARD 60(818300.60)
I	1	Chirurgie Digestive VALVE MEDIANE RICARD 80(818300.80)
I	1	VALVE CENTRALE SEULE 72X90MM
I	2	Chirurgie Digestive VALVE DOYEN-ROCHARD(813026.12)
I	1	ECARTEUR ABDOMINAL DOYEN 135MM LARGE
I	1	VALVE ROCHARD 155MM
I	1	VALVE ROCHARD 105MM
I	1	VALVE ROCHARD 90MM
I	2	Chirurgie Digestive CAPUCHON POUR PIQUET TOUPET(818120.00)
I	2	Chirurgie Digestive CHAINE DE TOUPET(901900.11)

Procédure

Nom	Zone
L LAVAGE EN MACHINE	Sale
P PROPRETE,	Propre
S LIBERATION DE LA CHARGE	Stérile

Code set	Localisation fixe
JDIGELAP01	Jol-Digestive Armoire U
JDIGELAP02	Jol-Digestive Armoire U
JDIGELAP03	Jol-Digestive Armoire U

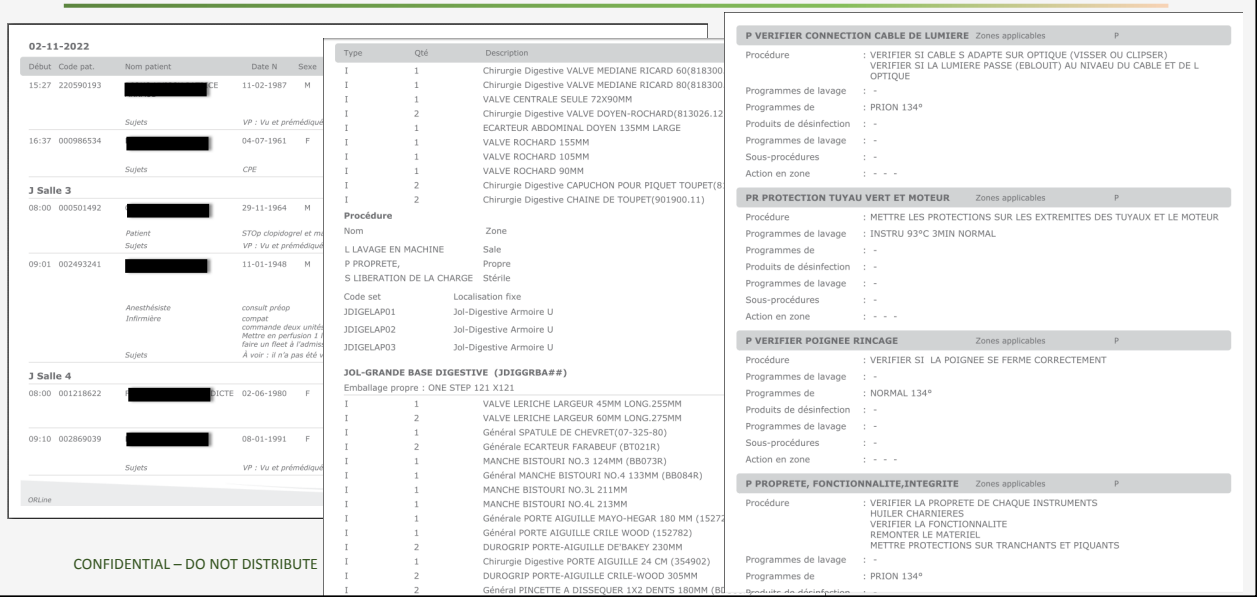
JOL-GRANDE BASE DIGESTIVE (JDIGGRBA##) **#111**

Emballage propre : ONE STEP 121 X121

I	1	VALVE LERICHE LARGEUR 45MM LONG.255MM
I	2	VALVE LERICHE LARGEUR 60MM LONG.275MM
I	1	Général SPATULE DE CHEVRET(07-325-80)
I	2	Générale ECARTEUR FARABEUF (BT021R)
I	1	MANCHE BISTOURI NO.3 124MM (BB073R)
I	1	Général MANCHE BISTOURI NO.4 133MM (BB084R)
I	1	MANCHE BISTOURI NO.3L 211MM
I	1	MANCHE BISTOURI NO.4L 213MM
I	1	Générale PORTE AIGUILLE MAYO-HEGAR 180 MM (152722)
I	1	Général PORTE AIGUILLE CRILE WOOD (152782)
I	2	DUROGRIP PORTE-AIGUILLE DE'BAKEY 230MM
I	1	Chirurgie Digestive PORTE AIGUILLE 24 CM (354902)
I	2	DUROGRIP PORTE-AIGUILLE CRILE-WOOD 305MM
I	2	Général PINCETTE A DISSEQUER 1X2 DENTS 180MM (BD560R)

AEXIS MEDICAL

Fonctionnalités proposées aux hôpitaux



CONFIDENTIAL – DO NOT DISTRIBUTE

Quelques réflexions…

- Un bon backup…
  - Accessible (Attention à l'encryption !)
  - Restaurable
  - Assez récent
  - Complet

→ Copie sur stockage décentralisé (pas sur le serveur de production!)
→ Test de restauration
→ Fréquence de copie
→ Comprenant les différents éléments nécessaires au bon fonctionnement

→ Vérification systématique de bonne exécution et alerte en cas d'erreur

CONFIDENTIAL – DO NOT DISTRIBUTE

Quelques réflexions…

- Durée d'installation logicielle à prendre en compte
  - 1/2 à 1 jour nécessaire pour la base
  - Interfaçage avec logiciels externes
  - Intervention sur place
  - Outils de déploiement bridés
  - Equipe informatique débordée

→ Intérêt de la mise en place d'une instance "miroir"
→ Synchronisation des données
→ Segmentation

Quelques réflexions…

- Si je n'ai plus internet …
  - Accès aux données extérieures (Sharepoint, OneDrive, …)
  - Accès aux sites web de mes fournisseurs (Commandes, Factures, Procédures, Catalogues, …)
  - Communication vers l'extérieur (emails)

- Puis-je m'en passer ?
- Combien de temps ?

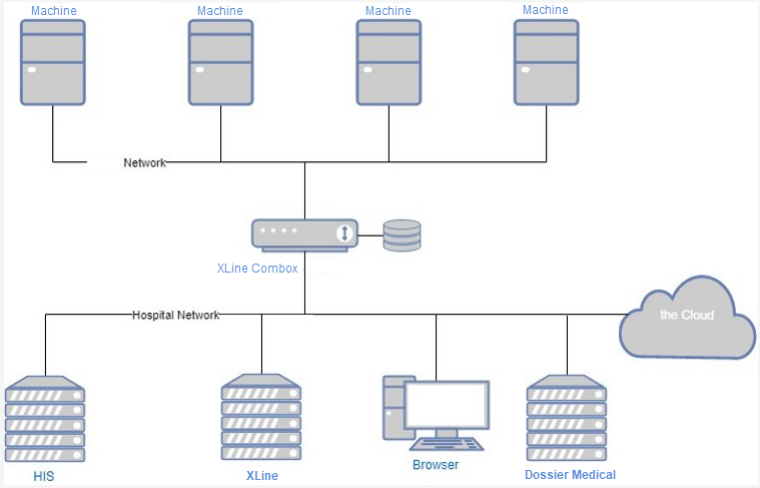
- Comment puis-je remplacer / compenser l'absence du service?

- Hébergement de la plateforme XLine dans le cloud (Azure, Amazon…) : Oui ! Mais…

Quelques réflexions…

- Fonctionnement des machines (lavage / stérilisateurs) – Pilotage par ordinateurs
- Système dépendant d'une base de données ? Centralisée ?
- Traçabilité informatique :
  - Temps réel
  - Synchronisation à postériori possible ?
  - Historique des données de cycle sauvegardées ?
- Conséquences d'une remise à zéro du logiciel de gestion de machine ?
  - Interface Machine / SteriLine
  - N° de lot ?
- Intervention du fournisseur nécessaire pour passer en mode "off-line" ?
- Intérêt d'isoler le réseau "machines" du réseau hospitalier

Quelques réflexions…



Quelques réflexions…

Et si XLine est inaccessible…

- Utilisation du disaster / recovery (Où ??)
- Traçabilité papier à mettre en oeuvre
  - Entrée du matériel en zone sale
  - Sortie du matériel stérile
  - Matériel inclus dans une charge machine à associer au n° de lot de la machine
  - Données techniques du cycle de machine
  - Identifier matériel et n° de lot de production stérile sur étiquette

- Lorsque XLine est à nouveau disponible
  - Encodage des données tracées papier
    → Difficilement réalisable en cas de longue interruption

Evolution envisagée…

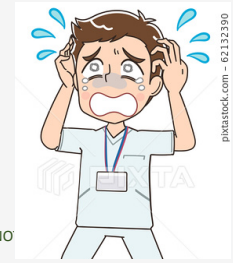
- Mise à disposition d'une application "standalone" permettant :
  - Impression d'étiquettes de production offline
  - Enregistrement de données minimales de production
  - Stockage local des données enregistrées
    → Fonctionnement sans réseau sur un PC autonome

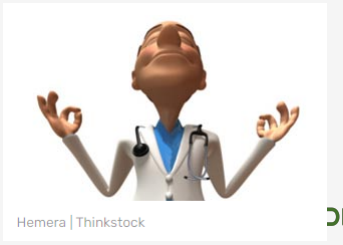
  - Réconciliation des données stockées localement avec XLine lors de la remise en route

Conclusion

- Sh!@# happens …

- La préparation et l'anticipation sont des facteurs clés
- Investir du temps maintenant pour limiter les conséquences néfastes
- Définir, Documenter et Informer sur la procédure à appliquer
- Mise en situation – Test de restauration – Oser tirer la prise !





Questions / Réponses