JOURNEE REGIONALE MATERIOVIGILANCE 2024

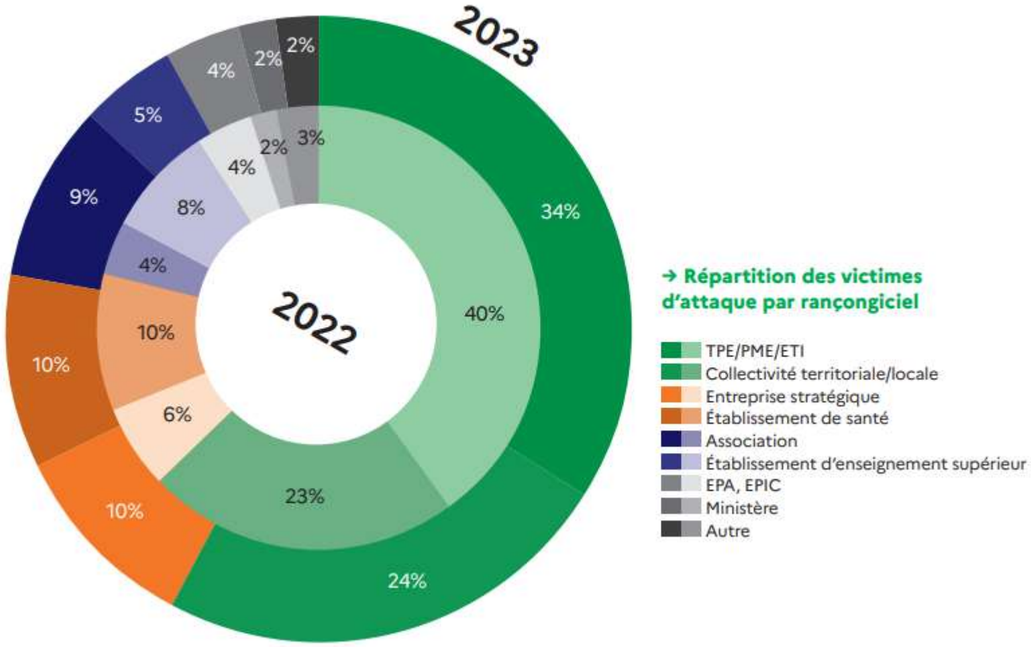
DMI et Cybersécurité

Thomas AUBIN

RSSI GHT Hôpitaux Publics Grand Lille

Agence Régionale de Santé Hauts-de-France
RRéVA HAUTS-DE-FRANCE
ansm Agence nationale de sécurité du médicament et des produits de santé
Matériovigilance Réactovigilance Hauts-de-France
OMéDIT Hauts-de-France
CHU LILLE
LE DISPOSITIF MÉDICAL snitem Pour faire avancer la santé

Etat de la menace



→ **Répartition des victimes d'attaque par rançongiciel**

- TPE/PME/ETI
- Collectivité territoriale/locale
- Entreprise stratégique
- Établissement de santé
- Association
- Établissement d'enseignement supérieur
- EPA, EPIC
- Ministère
- Autre

[Attaques cybersécurité auprès d'organismes publics - uMap (openstreetmap.fr)]

DMI, DMIL, DMI connecté

DMI

- Dispositif médical implantable
- Pas d'informatique embarqué = pas de risque IT !

DMIL

- Dispositif médical intégrant du logiciel
- Un risque inhérent au bon fonctionnement de la partie logiciel (garantir le maintien en condition opérationnel)

DMI connecté

- L'avenir …déjà là ! (pacemaker, prothèse connectée, ..)
- Le même risque cyber que le tout objet IoT connecté !

DM intégrant du logiciel

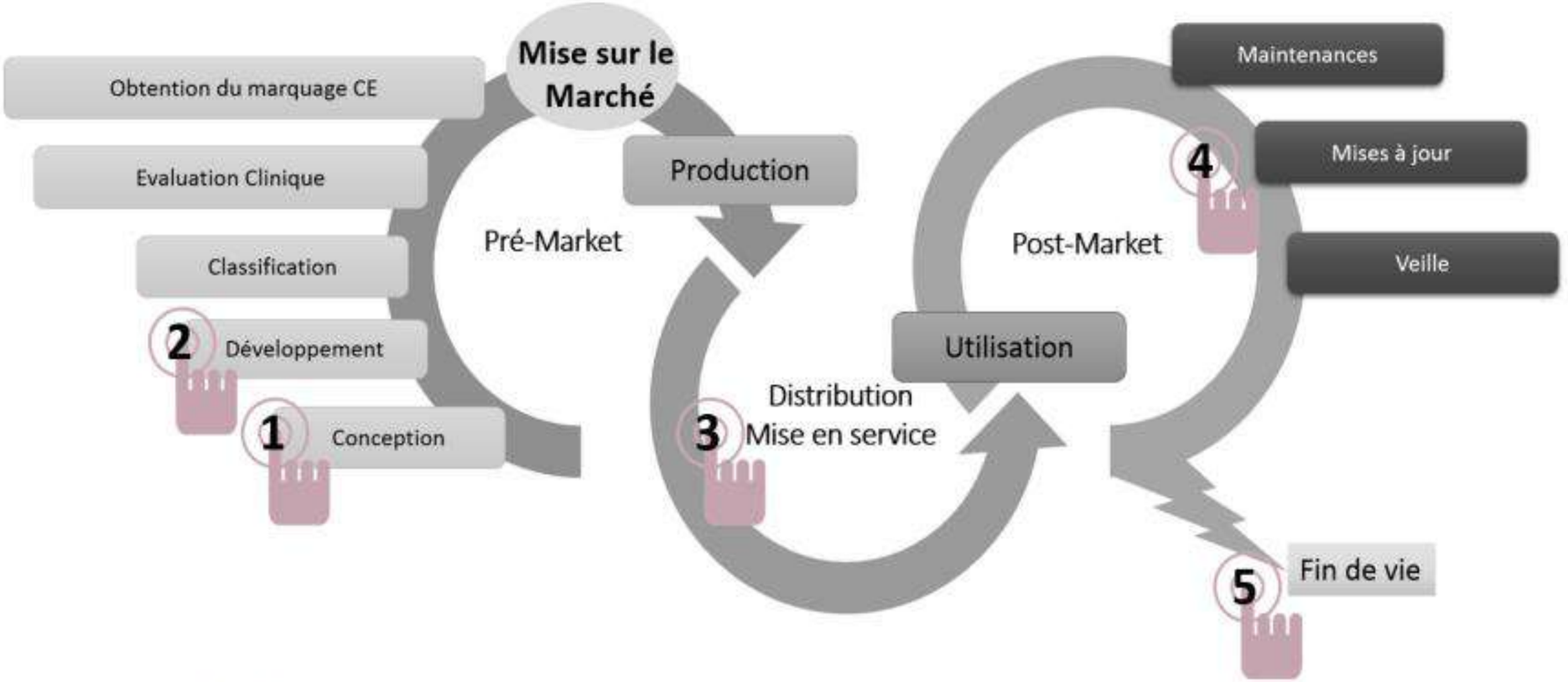


Figure 6 : Cycle de vie du logiciel

Cybersécurité des Dispositifs Médicaux Intégrant du Logiciel aux cours de leur cycle de vie ANSM (sante.fr)

DMI connecté

Enjeux :

- **Sécuriser le fonctionnement du dispositif (MCO, MCS)**
- **Sécuriser son intégration dans un écosystème**
- **Sécuriser les communications - les accès distants**

Risques :

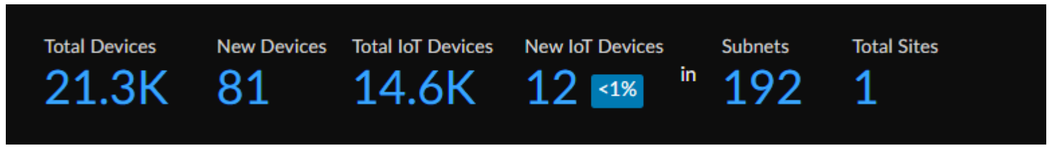
- **Marquage CE = cadre rigide qui limite**
- **« Exotisme » des technologies embarqués**
- **Méconnaissance des attentes de l'acheteur par le vendeur**

Un levier = le Security By Design

Les solutions

Pour les DMI connectés en place :

- **Un référentiel partagé (Une sonde …?)**



- **Une maitrise des fournisseurs**
- **Une identification des flux**
- **Un durcissement des accès**

- **Une analyse de risque, et une réponse associée**

Considérer le DMI connecté comme tout autre ioT connecté !

Les solutions

Le security by design – Une réponse de l'AFIB :

- **une liste de 32 objectifs de sécurité**. Ce document reprend la déclination des objectifs de sécurité applicables aux dispositifs médicaux et propose aux établissements des mesures compensatoires si le niveau de sécurité requis n'est pas atteint.
- **D'un questionnaire d'évaluation de la sécurité du système d'information des dispositifs biomédicaux.** Rempli par le fournisseur pour chaque modèle d'équipement, il permet d'évaluer le niveau de sécurité et de recueillir les documents nécessaires à l'installation et à l'intégration informatique de l'équipement.
- D'un guide fournisseur qui apporte des précisions sur certains aspects du questionnaire.
- D'un outil de dépouillement des réponses des fournisseurs. A destination des ingénieurs biomédicaux, il permet de comparer et noter les fournisseurs. Il permet également d'attribuer un poids supplémentaire à certaines questions.
- D'un guide qui apporte des précisions sur l'outil de dépouillement.

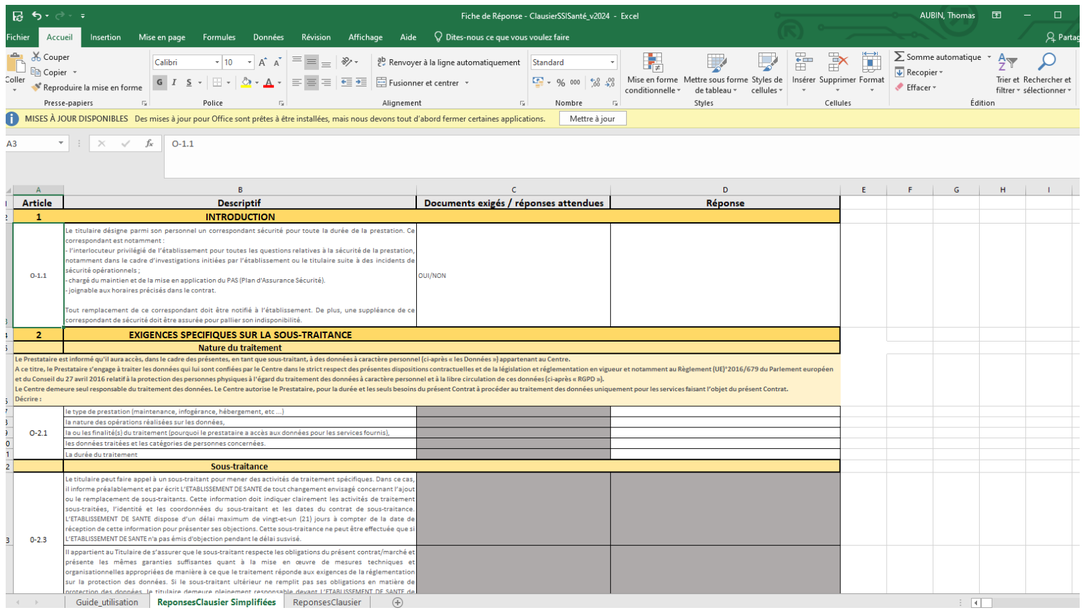
https://afib.asso.fr/details/articles/questionnaire-commun-pour-evaluer-la-securite-numerique-des-equipements-bio

… faire le pont avec les RSSI …

Les solutions

Le security by design – Une autre réponse Club RSSI Santé / Club DPO / AFIB :

- **Un clausier unique traitant des aspects de Conformité Numérique (SSI / RGPD), travaillé par des groupes issus des trois associations**
- **Un fichier de réponse (Onglet simplifié, onglet « précisions »)**
-



Article	Descriptif	Documents exigés / réponses attendues	Réponse
1	INTRODUCTION		
O-1.1	Le titulaire désigne parmi son personnel un correspondant sécurité pour toute la durée de la prestation. Ce correspondant est notamment : - l'interlocuteur privilégié de l'établissement pour toutes les questions relatives à la sécurité de la prestation, notamment dans le cadre d'investigations initiées par l'établissement ou le titulaire suite à des incidents de sécurité opérationnels ; - chargé du maintien et de la mise en application du PAS (Plan d'Assurance Sécurité). - joignable aux horaires précisés dans le contrat. Tout remplacement de ce correspondant doit être notifié à l'établissement. De plus, une suppléance de ce correspondant de sécurité doit être assurée pour pallier son indisponibilité.	OUI/NON	
2	EXIGENCES SPECIFIQUES SUR LA SOUS-TRAITANCE		
	Nature du traitement		
	Le Prestataire est informé qu'il aura accès, dans le cadre des présentes, en tant que sous-traitant, à des données à caractère personnel [ci-après « les Données »] appartenant au Centre. A ce titre, le Prestataire s'engage à traiter les données qui lui sont confiées par le Centre dans le strict respect des présentes dispositions contractuelles et de la législation et réglementation en vigueur et notamment au Règlement (UE)°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [ci-après « RGPD »]. Le Centre demeure seul responsable du traitement des données. Le Centre autorise le Prestataire, pour la durée et les seuls besoins du présent Contrat à procéder au traitement des données uniquement pour les services faisant l'objet du présent Contrat. Décrire :		
O-2.1	le type de prestation (maintenance, infogérance, hébergement, etc ...) la nature des opérations réalisées sur les données, la ou les finalité(s) du traitement (pourquoi le prestataire a accès aux données pour les services fournis), les données traitées et les catégories de personnes concernées. La durée du traitement		
	Sous-traitance		
O-2.3	Le titulaire peut faire appel à un sous-traitant pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit L'ETABLISSEMENT DE SANTE de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. L'ETABLISSEMENT DE SANTE dispose d'un délai maximum de vingt-et-un (21) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si L'ETABLISSEMENT DE SANTE n'a pas émis d'objection pendant le délai susvisé. Il appartient au Titulaire de s'assurer que le sous-traitant respecte les obligations du présent contrat/marché et présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences de la réglementation sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de		

CLAUSIER SÉCURITÉ 2024

club_rssi_sante_clausier_web_20240530.pdf (rssi-sante.fr)

Les solutions

Le security by design – Une mise en application au Chu de Lille:

- **La mise en œuvre d'une commission sécurité,**
- **L'intégration des clausiers sécurité dans les procédures achats**
- **Un rythme de réunion important pour répondre à la demande**
- **Un an d'existence « efficace » = 80 dossiers traités**

Avantages :

- **Une commission pour traiter de tous les sujets CHU – toutes directions**
- **Une commission pour traiter les sujets du GHT – être capable de répondre d'une seule voix qu'elle que soit l'établissement !**

Pour aller plus loin :

- **L'union fait la force : si baser sur un référentiel unique fait sens auprès des fournisseurs**