PÔLE D'EXCELLENCE CYBER

Biotech & Santé BRETAGNE

CYBERLAB

CATALOGUE DE SERVICES ET DE PRESTATAIRES CYBER APPLIQUÉS AU DOMAINE DE LA SANTÉ

V1

NOVEMBRE 2021

UNION EUROPÉENNE
UNANIEZH EUROPA
L'Europe s'engage en Bretagne / Avec le Fonds européen de développement régional

Région BRETAGNE

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Remerciements

Le Pôle d'Excellence Cyber et Biotech Santé Bretagne tiennent à remercier les personnes suivantes qui ont contribué à la préparation et à l'élaboration de ce référentiel en fournissant soutien, expertise et conseils clés :

Patrick Erard
Délégué général adjoint
du Pôle d'excellence cyber
Responsable Axe formation

Coralie Borniambuc
Chargée de projets Technologies
et Handicap au sein de
Biotech Santé Bretagne

Arnaud Meunier
Responsable de la sécurité des
systèmes d'information territoriaux
Etablissements membres parties au
Groupement Hospitalier de Cornouaille
de l'Union Hospitalière de Cornouaille

Thomas Guyet
Enseignant – chercheur à l'IRISA

Nicolas Jolivet
Responsable Protection des Données
et Cybersécurité au sein du SIB

Gouenou Coatrieux
Professeur à IMT Atlantique et
Co-fondateur de Watoo

Sommaire

Édito

La menace CYBER a atteint un niveau d'intensité qui n'avait jamais été constaté jusqu'ici. Loin de s'améliorer, la situation continue à se dégrader.

Par ailleurs, la crise sanitaire que le monde connait depuis le début de l'année 2020 ne fait que tendre la situation et augmenter la criticité des risques CYBER que connait le monde de la santé.

Dans ce contexte, il importe d'être tous pleinement conscients des enjeux, les menaces CYBER sont à considérer avec le plus grand sérieux.

Face à la situation explosive que nous constatons, il existe fort heureusement des solutions pour former, prévenir, protéger, détecter et réagir face aux menaces CYBER.

En éditant ce «catalogue de services et de prestataires cyber appliqués au domaine de la santé», le Pôle d'excellence cyber joue pleinement son rôle de leader dans la communauté CYBER française. Dans la continuité de ses actions visant à valoriser l'offre CYBER française, le Pôle d'excellence cyber contribue à aider les acteurs du monde de la santé qui sont à la recherche des prestataires et des services les plus pertinents et les plus conformes à l'état de l'art.

Ce catalogue, élaboré par une équipe composée des meilleurs spécialistes de la CYBER en France, donne les clefs permettant à un acteur du monde de la santé de mieux choisir pour mieux se protéger. Il saura également assister un acteur du monde de la CYBER désireux d'adapter son offre au domaine de la santé.

Eclairer et informer, proposer et accompagner, tels sont les objectifs de ce catalogue.

Bonne lecture !

Jean-Luc Gibernon

Vice-président développement économique et industriel
Pôle d'excellence cyber

Les nouvelles technologies ont connu ces dernières années un essor important. La multiplication des objets connectés en santé est synonyme d'explosion de menaces pouvant entraîner des conséquences dévastatrices.

La modernisation des outils de santé passe par l'intégration massive du numérique et du tout connecté : numérisation des dossiers patients, robotique médicale et gestion des bâtiments de plus en plus connectées, accroissement des métadonnées de santé (big data, data lakes), déploiement de l'intelligence augmentée ou artificielle. Le monde médical est donc de plus en plus dépendant des machines.

Les vulnérabilités des systèmes et des réseaux sont nombreuses. Il est donc important de définir un cadre commun, de donner les moyens aux acteurs du SI de participer à la mise en œuvre de politiques de sécurité et de référentiels concernant les bons usages. Si les principales cibles des attaquants dans le domaine de la santé sont les données des patients, le vol d'informations sensibles et personnelles, le risque de perturber le bon fonctionnement d'appareils et de services médicaux pourrait, dans certains cas, entraîner des biais dans les diagnostics ou, pire, provoquer le décès du patient. De plus, les médecins, les soignants, les RSSI, les éditeurs de solutions sont aussi concernés par la sécurité de ces nombreux objets connectés, sachant que l'attaquant passe toujours par le maillon le plus faible. Il est donc essentiel de sécuriser les produits et les services.

En 2020, l'ANSSI a recensé 27 centres hospitaliers ciblés par des cyberattaques, tandis qu'en 2021, 1 attaque a lieu toutes les semaines. La cybersécurité dans le secteur de la santé et du médico-social est une priorité nationale pour réussir la transformation numérique : elle est stratégique pour notre société. De nombreux référentiels voient le jour au moment où l'Etat français a annoncé un plan de financement pour renforcer la cybersécurité des hôpitaux et des centres hospitaliers français dans le cadre du Ségur de la Santé. En ce qui concerne les établissements de santé, le Ministère des Solidarités et de la Santé s'engage dans la lutte contre les cyberattaques et met en place un dispositif de traitement des signalements.

S'il n'existe actuellement pas de réglementation européenne concernant la sécurité des objets connectés, les éditeurs ont tout de même un certain nombre d'obligations concernant la sécurité de leurs développements et projets IoT.

Plusieurs exigences peuvent impacter le système de sécurité selon la typologie du projet, du traitement de données, des informations traitées et de la cible utilisateur (patient ou établissement). Afin d'identifier et d'être accompagné dans la mise en place des référentiels applicables, le CyberLab Santé intègre une présentation générale de la cybersécurité appliquée au monde de la santé et référence différents prestataires nationaux pouvant intervenir pour sensibiliser ou former, identifier des cadres réglementaires, accompagner leurs mises en place ainsi que permettre la certification.

Coralie Borniambuc & Patrick Erard

CYBERSÉCURITÉ ET SANTÉ NUMÉRIQUE _

1. Présentation de la cybersécurité

La cybersécurité appliquée aux dispositifs et aux systèmes d'informations permet de réduire les risques et limiter les impacts des attaques extérieures pouvant compromettre leur fonctionnement. Un ensemble de mesures techniques et/ou organisationnelles sont à mettre en place pour répondre aux critères **DICP** de la cybersécurité :

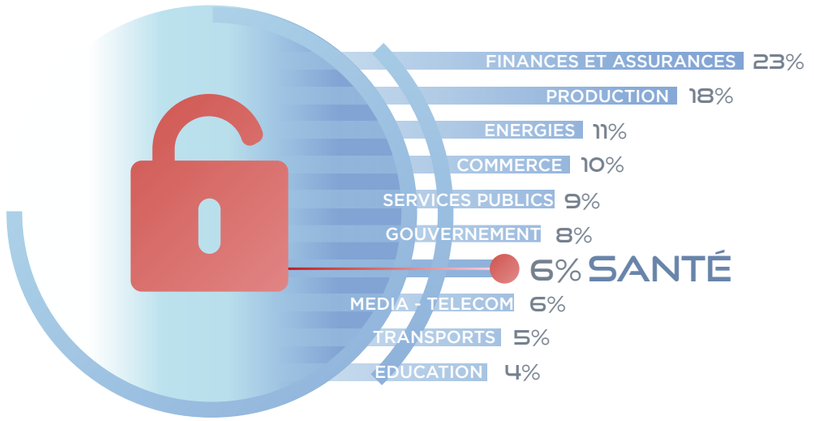
- **Disponibilité** : Capacité à accéder aux applications et aux données qui s'y trouvent au moment voulu par les personnes autorisées ;
- **Intégrité** : Assurer la complétude et l'exactitude des données, s'assurer que la donnée n'est pas altérée ;
- **Confidentialité** : Assurer que seules les personnes autorisées accèdent aux données ;
- **Preuve** : Assurer la traçabilité, l'authentification et l'imputabilité.

Ces critères de classification de l'information (DICP) permettent de définir le niveau de sécurité d'un bien ou d'un service, d'évaluer si celui-ci est correctement sécurisé.

2. Un défi majeur en santé

D'après IBM Security X-Force, c'est l'Europe qui a subi le plus de cyber attaques (tout secteur confondu) au cours de l'année 2020, 31% des attaques contre 27% pour l'Amérique. Le domaine de la santé représenterait 6% des attaques, avec une hausse de 3% depuis l'année 2019.

Répartition des cyber attaques mondiales en 2020



Source : IBM Security – X-Force Threat Intelligence Index

Le secteur de la santé utilise massivement les technologies numériques et de communication. « On évalue entre 95 et 99 % la dépendance au numérique dans un hôpital selon les services », affirme Vincent Trély, président de l'Association pour la sécurité des systèmes d'information de santé (APSSIS). Il ajoute que l'hôpital est particulièrement attaqué car jugé techniquement plus vulnérable par les pirates.

Trois facteurs expliquent la cible du secteur de la santé en termes de cyber attaques, d'après le « *Cyber Peace Institute* » :

- Les hôpitaux représentent une cible idéale pour l'extorsion des données numériques car la santé des patients en dépend.
- Les établissements de santé possèdent énormément d'informations personnelles particulièrement visées par le vol et le cyber-espionnage. En effet, un dossier médical peut être vendu 250$ sur le darknet, d'après Trustwave. La pandémie de la Covid-19 a également mis en exergue que les informations médicales ne se limitent pas seulement au dossier médical du patient, mais comprennent également des données relatives aux activités de santé publique, de recherche et de la propriété intellectuelle.
- La santé se retrouve également au centre de rivalités stratégiques qui conduisent à des activités malveillantes.

Ensuite, la multiplication des échanges d'information et de données entre les professionnels de santé, l'interconnexion entre les centres de soins, la sécurité sociale, les mutuelles et autres entités publiques, offrent un terrain propice à la cyber-malveillance.

Enfin, l'hétérogénéité des systèmes d'informations, applications métiers et autres équipements connectés rend ce secteur plus vulnérable que d'autres aux cyber-attaques.

Les conséquences de cyber-attaques dans le secteur de la santé peuvent être d'une extrême gravité et peuvent avoir des répercussions sur divers acteurs : les établissements de santé ainsi que les patients. De nombreux exemples et faits divers sont là pour nous rappeler l'importance du sujet :

Rappelons la terrible attaque en mars 2017 du logiciel de rançon WannaCry qui a paralysé le système de santé britannique NHS. Des milliers de consultations, examens et interventions chirurgicales ont dû être annulés dans plus de 40 établissements en raison du blocage des terminaux.

En septembre 2020, aux Etats-Unis, *Universal Health Services* a subi une rançon logicielle, le contraignant à déconnecter et couper ses réseaux pour éviter la propagation d'un virus sur 250 autres sites de soins et hôpitaux.

En 2020, au Royaume-Uni, l'institut de recherche biomédicale Hammersmith Medicines Research a subi un blocage du système informatique et de mail pendant un jour avec une fuite de données médicales de 2300 anciens patients, un vol.

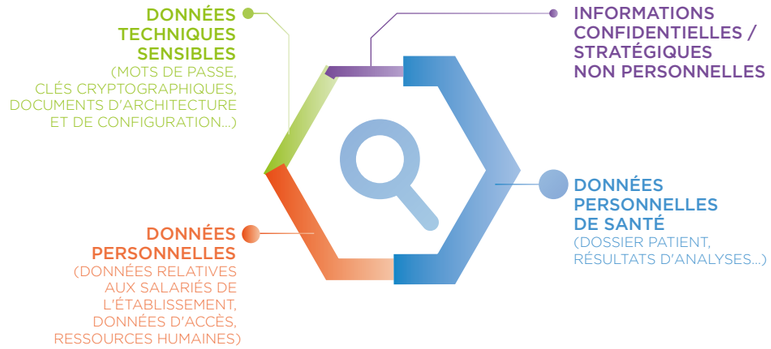
Également, en septembre 2020 a eu lieu le premier décès européen dans une clinique de Düsseldorf à la suite d'une attaque informatique. Le fonctionnement de l'établissement a été paralysé 2 jours par un rançongiciel et a empêché les soignants de prodiguer les soins nécessaires.

Plus récemment, en février 2021, le centre hospitalier de Dax a fait l'objet d'une attaque informatique qui a mis hors service le système d'information de l'hôpital. Les dossiers patients ainsi que certains équipements médicaux n'étaient alors plus accessibles.

En mai 2021, l'organisation publique de la santé en Irlande a subi une attaque informatique, plus de 40 établissements de santé ont été impactés. Le groupe de hackers a publié un échantillon de données de santé sur le darknet et réclame maintenant une rançon de 20 millions de dollars.

D'après l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur de la santé, publié par l'Agence Nationale de santé, en 2020, 250 établissements de santé ont déclaré 369 incidents. La part d'origine malveillante est en constante augmentation depuis trois ans (60% en 2020 contre 41% en 2018), et pour la moitié des incidents déclarés, tout ou partie des données présentes sur le SI de la structure étaient impactées.

Répartition selon les types de données impactées – en France



Source : Rapport observatoire des signalements d'incidents de sécurité des SI

A chaque fois le constat est le même, les hôpitaux ou organismes de santé qui ont subi des attaques ont implémenté des solutions ou utilisent des processus métier non suffisamment cyber-protégés et ils n'ont pas non plus intégré des mécanismes de défense ou de résilience aux cyber-attaques.

Les attaques cyber ne visent et n'impactent pas seulement les établissements de santé, en effet, les DM connectés, les équipements de mesure ou les big pharma peuvent aussi en être la cible.

Prenons l'exemple des équipements médicaux de *GE Healthcare*. La FDA[1] a alerté en janvier 2020 d'une faille de sécurité qui pourrait permettre à un tiers d'altérer les appareils de surveillance des patients.

Citons également les attaques en cascade qu'ont subi les laboratoires développant des vaccins dans le cadre de la crise Covid, la biotech Moderna visée par des cyberattaques chinoises en juillet 2020, suivie du laboratoire AstraZeneca en novembre.

1 FDA : Food, Drug and Administration indication

3. Evolution des règlementations en santé numérique

La feuille de route du numérique en santé présentée en 2019 impose la mise en place d'un cadre réglementaire opposable afin d'échanger, partager et sécuriser les données de santé. Pour cela, depuis deux ans, est publiée la « *Doctrine technique du numérique en santé* », permettant de matérialiser l'« *Engagement collectif vers une e-Santé au service des usagers* ». Ce document permet de fixer le cadre du numérique en santé, d'engager les acteurs privés et publics à développer des services respectant les valeurs et le cadre définis par le ministère.

Un certain nombre des référentiels et services ont été développés (ou sont en cours de développement) afin de sécuriser les données sensibles que sont les données de santé. Nombre d'entre eux sont opposables[2]. Nous pouvons ainsi citer l'Identité Nationale de Santé (INS) permettant l'utilisation par l'ensemble des acteurs d'une identité unique et pérenne pour chaque usager ; des services de messagerie sécurisée particulièrement adaptés à l'échange de données de santé (MSSanté) ; la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), des référentiels permettant de répondre aux problèmes d'interopérabilité des systèmes et services de santé, etc. Il existe de nombreux référentiels centrés sur la cybersécurité des Systèmes d'Information de Santé et/ou des dispositifs médicaux connectés. Une prise de connaissance de l'ensemble est nécessaire afin d'optimiser les développements et assurer la sécurité du service proposé.

Le règlement européen *Cybersecurity Act* paru le 7 juin 2019 marque une avancée pour l'autonomie stratégique européenne. Il poursuit un double objectif, d'une part l'adoption d'un mandat permanent pour l'ENISA[3], valorisant et développant son rôle de facilitateur des échanges entre les Etats membres ; d'autre part, la définition d'un cadre européen de certification de cybersécurité pour harmoniser à l'échelle européenne les méthodes d'évaluation.

Information importante : Ces informations réglementaires sont applicables au marché français, il est donc nécessaire de se tenir informé du cadre normatif des autres pays si la stratégie de l'entreprise se dirige vers l'international.

2 Opposable : terme juridique ayant pour signification l'obligation d'application

3 ENISA : European Network and Information Security Agency – L'agence de l'union européenne de cybersécurité

4. La cybersécurité des systèmes de santé

Les établissements de santé publics comme privés ont pour mission d'assurer la production des soins pour le compte des patients de leur bassin géographique en continu (24h/24 – 7j/7 – 365j/an). La forte dépendance au numérique de la production des soins impose aux établissements de santé de mettre en place, opérationnellement et réglementairement, des procédures et des produits de cybersécurité visant à assurer la continuité de leurs services informatiques.

Forte dépendance des établissements de santé à l'outil numérique pour assurer le cœur de son activité : la production des soins

Réglementairement, les établissements de santé peuvent être soumis à une vaste réglementation dont notamment l'instruction 309[4], la PGSSIS-S[5] et la certification hébergeur de données de santé (certification HDS). Cette dernière repose principalement sur la mise en œuvre de deux standards internationaux, l'un portant sur le management de la sécurité de l'information (ISO 27001), l'autre sur la protection des données de santé, données dites à caractère sensible (ISO 27018).

Pour faciliter la mise en œuvre de mesures de sécurité au sein des établissements, les instances nationales de la santé, le ministère de la Santé et des Solidarités (MSS) et la Direction Générale de l'Offre de Soins (DGOS), travaillent sur un dispositif de certification des SI, dit MATURIN-H, qui comprend un volet SSI. Il devrait voir le jour au 1er trimestre 2023 à la suite d'une phase pilote en qui aura lieu en 2022. A la différence de la certification HDS, ce dispositif de labellisation vise à être plus incitatif, via l'octroi de financement IFAQ (Incitation Financière à l'Assurance Qualité), et à fédérer l'ensemble de la réglementation SSI. Il aura aussi pour particularité d'intégrer la réglementation européenne de la directive NIS (Network and Information System Security). Or, depuis les cyber-attaques médiatiques du CHU de Rouen en 2019, des CH de Dax et de Villefranche-sur-Saône en février 2021, le Premier ministre a désigné Opérateurs de Services Essentiels (OSE) les établissements supports des 135 Groupements Hospitaliers de Territoire, et donc par contrecoup impose à ces 135 établissements de santé de respecter la directive NIS.

Un poids réglementaire SSI très élevé pour les établissements de santé et des impacts pour les éditeurs

Par ailleurs, un grand nombre d'établissements de santé sont engagés dans les programmes nationaux de développement de la maturité des SI hospitaliers (HOPEN et SEGUR USAGE NUMERIQUE (SUN)) qui comprennent la mise en œuvre de nombreuses exigences de sécurité. Pour ce qui est de SUN, les premiers travaux envisagent une labellisation SSI pour les applications des éditeurs. L'Agence du Numérique en Santé réfléchit également à rendre opposable aux établissements de santé et aux éditeurs la politique générale de la sécurité des systèmes d'informations.

Dans ce contexte, la cybersécurité prend une importance accrue, elle devient majeure pour les établissements de santé et pour les éditeurs. La nécessité pour les éditeurs d'intégrer la sécurité dès la phase de conception logicielle deviendra donc vraisemblablement un prérequis à la commercialisation de ses produits, si nos Grandes Écoles et Universités arrivent à former ces rares profils aujourd'hui de DevSecOps.

4 Instruction 309 : relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information

5 PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé

Nécessité pour les éditeurs d'intégrer la sécurité dans leurs produits pour assurer leur commercialisation

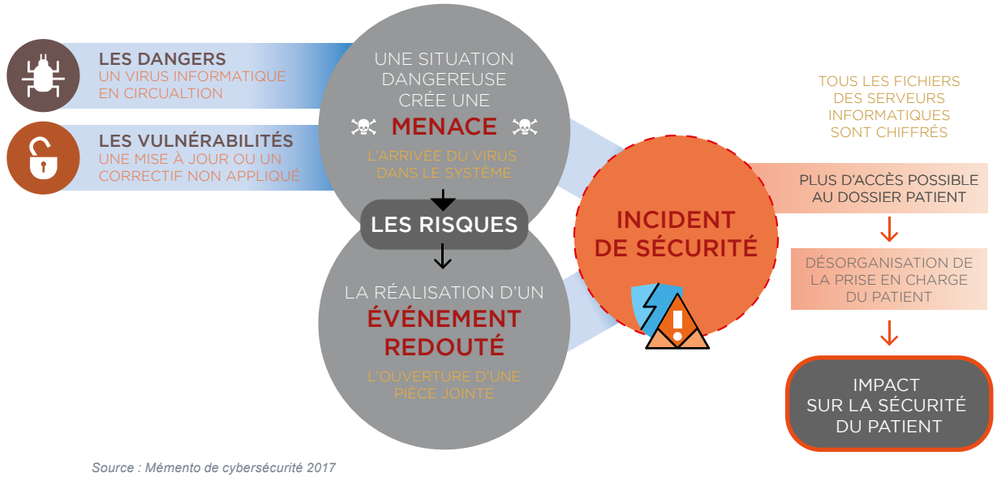
Tout projet de système d'information doit, avant sa mise en service, bénéficier d'une analyse formalisée des risques pesant sur sa sécurité. La gestion des risques vise à renforcer la confiance des utilisateurs dans les outils numériques et favorise donc le bon usage de ces systèmes d'information.

L'analyse des risques numériques est un élément central de la méthodologie SSI. Plus largement, elle rentre dans le périmètre réglementaire de l'homologation de sécurité (obligation s'appliquant aux établissements de santé dans le cadre de l'Instruction 309 du ministère des affaires sociales et de la santé). Elle permet à un responsable, en s'appuyant sur l'avis des experts, de s'informer et d'attester aux utilisateurs d'un système d'information que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés.

Une **analyse de risque** est une combinaison entre :

- Ses **vulnérabilités** du système :
  - Organisationnelle (chaîne fonctionnelle de responsabilité) ;
  - Réglementaire (Lois, PSSI, procédures et chartes) ;
  - Environnementale (infrastructure, protections physiques) ;
  - Informatique (architecture, configuration, virus, etc.) ;
  - Humaine (formation, comportement, motivation).
- Des **menaces** réelles sur ce système (dangers dûs à des vulnérabilités qui affectent un individu, un bien, un service, une organisation) ;
- Il en découle des **événements redoutés** (mode opératoire d'une menace qui exploite une vulnérabilité) dont on va juger le **risque** selon :
  - Sa **gravité** (les impacts possibles) : **x** sur une échelle de 1 à 4 (négligeable, limitée, importante, critique) ;
  - Sa **vraisemblance** (la possibilité qu'il se réalise) : **y** sur une échelle de 1 à 4 (minime, significative, forte, maximale) ;
- les 2 valeurs se multiplient (**xy**), et l'**analyse de risque traitera en priorité** les risques graves et vraisemblables (fort coefficient de multiplication, xy), et **ne traitera pas** (choix à opérer donc pour chaque organisation) les risques peu graves et/ou peu vraisemblables (faible coefficient xy).

Illustration graphique



Source : Mémento de cybersécurité 2017

La démarche de gestion des risques au cœur de l'activité SSI

Les risques numériques sont de quatre ordres :

- Risque **d'indisponibilité** du matériel ou de l'application, donc de l'accès aux données ;
- Risque de perte **d'intégrité** des données : impact sur la complétude et l'exactitude des données ;
- Risque de **rupture de la confidentialité** : accès à des données par une personne alors qu'elle ne dispose pas du niveau d'habilitation délivré par l'organisation, espionnage, fuite ;
- Risque de **modification des traces informatiques** compromettant l'imputabilité des actions sur le système d'information, la preuve.

La démarche de gestion de risque vise à traiter ces risques, c'est-à-dire à les réduire, éviter ceux qui sont critiques, partager ou accepter les autres, parce qu'on est pleinement conscient des vulnérabilités de notre système et qu'ont a apprécié l'impact d'un potentiel incident de sécurité.

Une politique globale de cybersécurité, qui comprend une fine évaluation des risques et de leurs conséquences, doit être mise en place, et cela pour chacune des phases du cycle de vie du produit. On pourra par exemple s'appuyer sur le « *framework* » de cybersécurité des infrastructures critiques défini par l'institut Américain des normes et technologies (NIST) pour définir une analyse de risques et une politique de cybersécurité pour chaque étape du cycle de vie.

Cycle de vie et cybersécurité

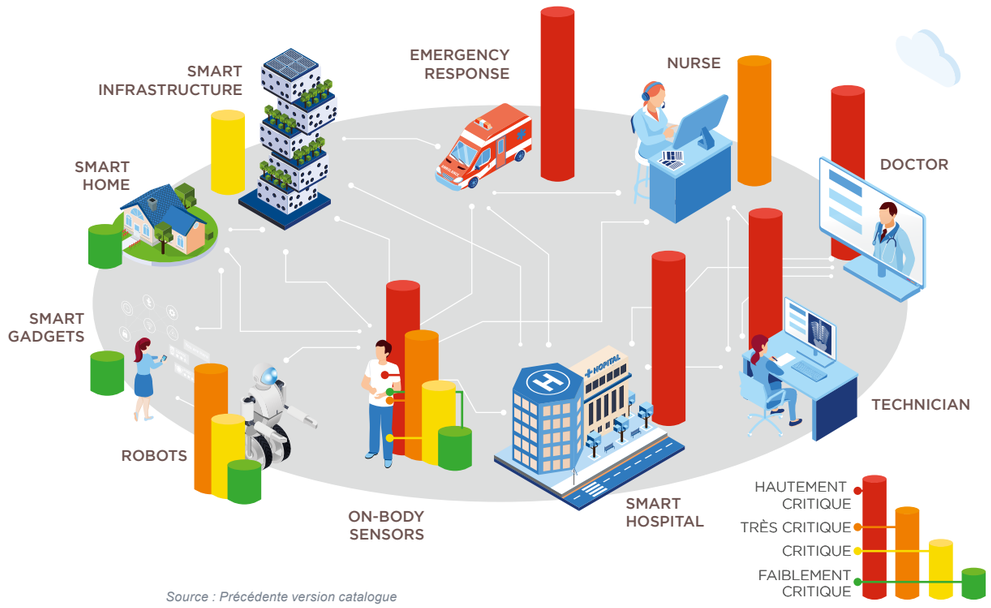
L'Institut national Américain des normes et de la technologies (NIST), « Framework IPDRR »

Cybersécurité et santé – niveaux de criticité

Il est aussi important de déterminer le niveau de criticité d'un appareil ou d'une application afin d'être en mesure d'adapter sa stratégie de cybersécurité.

Le graphique ci-dessous ne couvre pas tous les cas d'usages mais il nous aide à évaluer un niveau de criticité d'une application.

Niveaux de cyber-criticité et secteur de la santé



Source : Précédente version catalogue

Toute solution ou produit destiné à contribuer au parcours de santé, à la délivrance des soins, aux interventions d'urgence, au bien-être quotidien du patient ou au diagnostic par des professionnels de santé peuvent être considérés comme hautement critiques du point de vue de la cybersécurité.

Concernant les capteurs et autres équipements de mesure, le niveau de criticité dépendra des cas d'usages pour une pathologie donnée. Un capteur de monitoring cardiaque est bien entendu hautement critique alors qu'un simple podomètre peut être considéré comme faiblement critique.

De même pour une prothèse bionique ou un robot d'assistance. Un appareil d'assistance respiratoire ou un pacemaker est hautement critique par rapport à une prothèse de jambe connectée, qui elle-même est plus critique qu'une simple prothèse auditive, par exemple.

Le niveau de criticité des échanges de données peut varier en fonction de la nature des données et de leur destination. Une simple information d'horaire de rendez-vous pour une consultation est bien entendu moins critique qu'une information sur l'identité (INS – Identité Nationale de Santé) ou le diagnostic d'un patient. Il est impératif de s'assurer de la conformité à la nouvelle réglementation sur la protection des données (RGPD) ainsi que des règles qui régissent le numérique en santé.

Les cyber vulnérabilités (potentielles) des systèmes de santé

Les vulnérabilités potentielles sont nombreuses et les différents domaines d'activités sont concernés. Les cyber-vulnérabilités sont des failles de sécurité, et par conséquent, de potentielles portes d'entrées pour les attaques cyber. La figure ci-dessous résume ces vulnérabilités.

Cyber vulnérabilités des systèmes de santé

- Télémédecine
- Téléconsultation
- Télédiagnostic
- Déports d'écran
- Hospitalisation à domicile
- Big data
- Dossier patient informatisé
- Dossier médical partagé
- Fichiers de personnels
- Fichiers de patient
- Agendas partagés
- Mon Espace Santé
- MSSanté
- ApCV
- eCPS
- Pro Santé Connect
- Réseaux télécom
- Capteurs, sondes, IOT
- Implants, télémétrie
- Prothèses bioniques
- Équipement de mesure
- Équipement d'analyse
- Véhicules connectés

- Bâtiments intelligents
- BMS/BAS - HVAC
- Gestion d'énergie
- Contrôle d'accès
- Alarmes, CCTV
- Systèmes de localisation
- Systèmes d'informations
- Cloud (SaaS)
- Stockage de données
- Workflow
- ICS/SCADA
- Facturation
- Gestion de paie
- Gestion du personnel
- Gestion des stocks
- Postes administratifs
- Messagerie
- Tous Anti-Covid
- TAC Verif
- ...

Par exemple, les centres de soins, les hôpitaux et autres institutions de santé utilisent des bâtiments de plus en plus intelligents et connectés. Ces bâtiments possèdent de nombreuses vulnérabilités potentielles. En effet ils sont gérés par des systèmes de Gestion Technique du Bâtiment (GTB), connectés sur l'Internet au travers de passerelles (*Gateway*) pour permettre à des applications *BMS* (*Building Management System*) ou *BAS* (*Building Automation System*) de contrôler à distance le chauffage, l'air conditionné, *HVAC* (*Heating, Ventilation Air Conditioning*), l'éclairage, les détecteurs, les alarmes incendie et autres, les systèmes de contrôle d'accès, les caméras de vidéo protection *CCTV* (*Closed-Circuit Television*), les ascenseurs, la production autonome d'énergie, le stockage de cette énergie, etc.

Le milieu médical utilise déjà massivement les réseaux de communications très haut débit, IP ou radio (DECT, WiFi, 3G, 4G, 5G, NB-IoT, Lora, Sigfox…), pour communiquer et partager les dossiers patients, les imageries médicales, les résultats d'analyses et autres informations médicales. Les réseaux hospitaliers transportent ces informations et données patients et peuvent donc être la cible des cyber-attaques.

La médecine d'aujourd'hui utilise également de plus en plus de capteurs, de sondes ainsi que d'autres objets connectés : implants connectés, télémétrie, prothèses bioniques connectées sont une préoccupation majeure. Déjà aujourd'hui les équipements de mesure, d'analyses et autres matériels médicaux (scanner, IRM, etc.), les boîtiers de monitoring, les alarmes des patients, sont connectés sur l'Internet et sont des cibles de choix pour les cyber-attaquants.

La crise sanitaire liée à la Covid-19 a accéléré le déploiement des services et outils de télésanté et des dérogations ont dû être octroyées au cours de la pandémie. Ces nouvelles opportunités d'accès au soin à domicile (développement de l'Hospitalisation À Domicile, téléconsultation…) représentent un nouveau moyen de captation de données de santé et peuvent représenter une nouvelle cible d'attaque pour les hackers. *« La diversité de l'offre numérique doit se structurer afin de répondre aux enjeux de sécurité, d'interopérabilité, de confiance et de qualité »*, Doctrine technique du numérique en santé.

Toutes les données médicales, dossiers des patients, fichiers des personnels, bases de données, agendas informatisés et autres big data sont des informations confidentielles très recherchées par les cyber-attaquants. Le ministère de la santé encourage le développement et la mise en conformité d'outils, de réglementations, de référentiels afin d'*« intensifier l'éthique, la sécurité, l'interopérabilité des systèmes d'information de santé »*. Les données de santé sont soumises à la nouvelle réglementation sur la protection des données (RGPD, Loi Informatique et Libertés avant), qui nécessite, entre autres, la désignation d'un DPO (Délégué à la Protection des Données), la nécessité d'informer sur les finalités de traitement et les moyens de traitement, etc. Le traitement de données de santé nécessite également une utilisation de l'Identité Nationale de Santé (INS), le recourt à un Hébergeur de Données de Santé certifié (HDS), des contraintes d'authentification de plus en plus contraignantes, une conformité des services de messageries sécurisées, etc.

Afin de protéger les droits des usagers et la confidentialité des échanges entre l'usager et le praticien, le cadre réglementaire lié au numérique en santé est en pleine évolution, de nouveaux outils et référentiels apparaissent. Nous pouvons ainsi citer le déploiement en cours de *« Mon espace Santé »*, un espace personnel où les usagers vont pouvoir gérer leurs données de santé, aussi la *« Messagerie Sécurisée de Santé » (MSSanté)*, un système national de messageries sécurisées de santé, ou encore *« Pro Santé Connect »*, prochainement déployé, fédérateur de fournisseurs d'identité pour les professionnels de santé. Tous ces outils vont permettre de cadrer les données personnelles, mais peuvent également à la source de cyberattaques.

Pour un diagnostic meilleur et plus rapide, de nouveaux outils et méthodes de travail collaboratif entre professionnels de santé (Télémédecine, téléexpertise,…) ont été massivement déployés. Ces ouvertures sur les SI de santé peuvent constituer des failles de sécurité dans les processus métiers ou dans les parcours de santé.

Les systèmes d'information (SI) des hôpitaux et centres médicaux, les centres de calculs ou *clouds* privés, publics ou semi-publics, les applications de « *workflow* » métiers *ERP (Enterprise Resource Planning, PRM - Patient Relation Management)*, facturations, *SCADA (Supervisory Control and Data Acquisition)*, gestion des stocks, etc., les postes de travail ainsi que les systèmes de messageries sont très sensibles, et doivent, impérativement, faire l'objet de mesures des sécurité numériques et physiques adaptées aux risques.

Les cyber-menaces (réelles) et les cyber-risques (possibles) sur les systèmes de santé

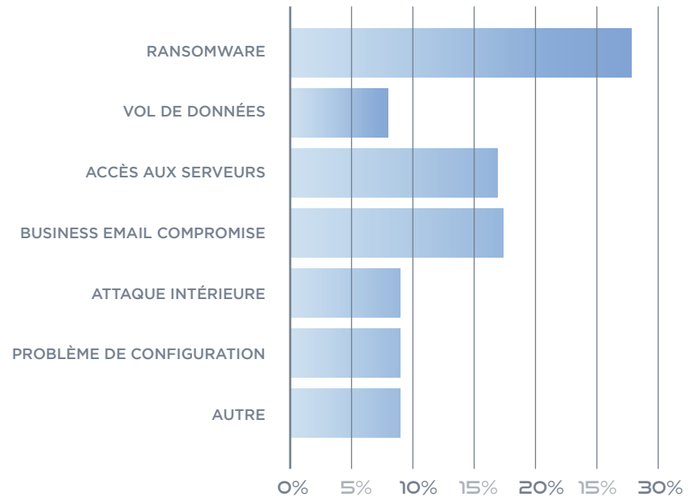
Si les vulnérabilités sont éventuelles, les menaces sont par contre bien réelles et multiples.

Les attaques utilisent la plupart du temps une combinaison des techniques d'attaques pour maximiser le taux de réussite.

Il convient aussi de noter que l'on voit maintenant apparaitre des cyber-attaques sur les infrastructures, serveurs ou applications, combinées et synchronisées avec des sabotages physiques sur les sites et infrastructures.

Ci-dessous, une représentation des différents types d'attaques qu'a subi le secteur de la santé au cours de l'année 2020.

Types de cyberattaques dans le domaine de la santé en 2020



Source : IBM Security X-Force

Toutes les menaces font courir des risques importants pour les acteurs du secteur. Elles peuvent causer de graves dommages aux centres médicaux et hôpitaux et potentiellement mettre la vie de patients et personnels en danger. Elles peuvent aussi générer de graves préjudices moraux ou financiers aux acteurs du secteur si des informations sont volées, compromises ou détruites.

Le schéma ci-dessous illustre les différents niveaux d'une cyberattaque :

Les tenants et aboutissants d'une cyber-attaque

BUT VISÉ	▸ **Confrontations étatiques** : stratégie d'ingérence/contre-ingérence, renseignement, positionnement stratégique ▸ **Financier** : cyber-crime, concurrence ▸ **Pouvoir** : clients, fournisseurs, fabricants produits de substitution, dont ▸ **Idéologie** : conviction personnelle, recrutement, utopies, etc. ▸ **Ego, Personnel** : vengeance d'un ancien employé/associé/adminsitrateur, etc.
EFFET	▸ **Vol** : brevets, dessins et modèles, savoir-faire, fichiers clients/ fournisseurs, données commerciales, comptables & personnelles ▸ **Chantage, Contrainte, Atteinte à la vie publique/privée** d'un employé/chef d'entreprise/médecin ▸ **Espionnage** : accès à la PI, aux données, aux partenaires, données patients ▸ **Sabotage** : action sur les appareils de santé, modification de leur programmation, données, destruction, mise en danger des personnes ▸ pouvant aller jusqu'à la **Destruction** : de la réputation, de l'image de marque, de la confiance patient, des matériels, logiciels, données
MODE OPÉRATOIRE	▸ **Attaque physique** interne ou externe : **Compromission**, stagiaire passé à la concurrence, clé USB, vol téléphone/tablette/PC, BYOD, etc. ▸ **Social engineering/Web** : attaque de point d'eau, Nmap, Code/SQL injection, Cross Site Scripting (XSS), remote file inclusion, brute force, etc. ▸ **DoS/DDoS**, flood. **Scripting** : buffer/heap overflow ▸ **Phishing**, spear phishing, sniffing, spoofing, attaque par sondage ▸ **Attaque par faute & canaux auxiliaires**, glitch attack, retro-engineering ▸ **MITM, TEMPEST** : signaux compromettants, interceptions ▸ **Hoax, Fake news**
CHARGE ACTIVE OU MALWARE	▸ **Action humaine ou matériel** : pince pour section des cables GTB, déclenchement d'alarmes (incendie, par exemple), erreur, etc. ▸ **Laser, ondes électromagnétiques** ▸ **ZeroDay/Virus** : cryptolocker, bombe de décompression, blastware, etc. ▸ **Backdoor/Keylogger/Ver**, botnet, wabbit, nuker, dropper, etc. ▸ **Cheval de Troie** : spyware, adware, anonyware, nagware, hijacker, parasiteware, scumware, rootkit, RAT, sniffer, dialer, etc.

La protection, la défense et la résilience des organismes et systèmes de santé aux cyber-attaques deviennent donc des enjeux majeurs de la filière.

5. IA & Cyber sécurité

L'utilisation d'outil à base d'intelligence artificielle (IA) est amenée à se déployer dans les années à venir. Les secteurs de la cybersécurité et de la santé en sont particulièrement concernés. Le développement des méthodes d'IA constitue de nouvelles menaces et opportunités pour tous les niveaux des systèmes informatiques (données, logiciels et systèmes).

L'utilisation de méthodes d'IA augmente les capacités d'analyse des systèmes par les attaquants. D'une part, ces techniques vont leur permettre d'identifier les vulnérabilités d'un système de manière beaucoup plus automatique et massive, d'autre part, l'arrivée potentielle d'attaques elles-mêmes construites au moyen d'IA (par exemple, en apprentissage par renforcement) pourrait déjouer les systèmes de protection usuellement mis en place, voire s'y adapter dynamiquement (*zero-day attacks*). De plus, l'expertise requise pour l'élaboration d'une attaque devient moindre et le potentiel de cyberattaquant s'accroît.

Le développement des IA offre également des opportunités importantes pour la protection des systèmes informatiques. Ainsi, l'utilisation de nouveaux outils offre la possibilité aux analystes d'explorer plus efficacement une plus grande quantité de logs, pour mieux identifier et répondre plus rapidement aux attaques. L'IA améliore l'aide à la décision dans les systèmes automatiques de détection d'intrusion des infrastructures à protéger.

De manière plus marginale, l'utilisation d'outils à base d'IA au sein d'un système informatique peut aussi générer des vulnérabilités, en particulier les systèmes basés sur l'apprentissage automatique[6]. La faible robustesse de ces outils les rend particulièrement vulnérables aux attaques (sur les données d'entrée, sur les modèles, sur les architectures de calcul). Les systèmes à base d'IA appliqués à la santé sont considérés à haut risque, leur déploiement fait donc l'objet d'une attention toute particulière et celui-ci est encore marginal. Le recours à des moyens de certification devra répondre à ces risques majeurs.

6 https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

CYBERLAB : UN CATALOGUE DE SERVICES _

Le **Pôle d'excellence cyber** et **Biotech Santé Bretagne** proposent un catalogue de services et de prestataires de cybersécurité pour aider les sociétés développant des produits et des services à destination du secteur de la santé à bien prendre en compte et intégrer la cybersécurité dès la conception, le démarrage de leurs projets.

Ce catalogue de services est constitué de 5 familles de prestations : formation, conseil, audit, certification et test :

FORMATION	CONSEIL	AUDIT	CERTIFICATION	TEST
Sensibilisation aux menaces sur les systèmes de santé	Analyse de risques	Audit préliminaire	Support à l'auto-certification	Tests préliminaires de sécurité
Management de la cybersécurité dans les projets	Politique de cybersécurité	Audit et tests de sécurité	Pré Audit CSPN[7]	Tests fonctionnels
Gestion de crises et continuité de services	Groupe de travail cyber	Audit de code source	Évaluation/ Certification 1er niveau (CSPN)	Tests d'interopérabilité
Ingénierie de solutions de sécurité	Gestion de crise	Audit de configuration	Évaluation/ Certification (CC – EAL 1 à 7)	
Sécurité des applications mobiles et objets connectés	Plan de tests	Audit d'architecture	Qualification	
Programmation sécurisée pour les développeurs	Architecture de sécurité	Audit organisationnel et physique		

7 CSPN : Certification de Sécurité de Premier Niveau

La liste des prestations de services du catalogue CyberLab n'est pas exhaustive et pourra évoluer en fonction des besoins de chaque organisation, projet.

Les prestations de services sont délivrées par des sociétés ou des laboratoires académiques qui sont référencés dans ce catalogue. Leur référencement a été fait au travers d'un processus d'appel à manifestation d'intérêt qui a eu lieu au cours de l'année 2021.

Les prestations de **formation** (avec une sensibilisation de tous les personnels d'abord) sont principalement destinées aux chefs de projets, développeurs, architectes et administrateurs des projets ainsi qu'aux exploitants (direction des hôpitaux) et aux usagers des solutions ou des services.

Les prestations de **conseil** sont destinées aux projets des sociétés ou organismes utilisateurs des solutions ou services.

Les prestations d'**audit** sont proposées par des prestataires labélisés par **l'ANSSI (PASSI, Prestataire d'Audit de la Sécurité des Systèmes d'Information[8])**. Elles s'adressent aux projets et concernent les solutions, produits, applications et services développés dans ces projets. Elles peuvent également concerner les exploitants pour les aspects d'organisation et de sécurité physique.

De même la **certification** des équipes projet, des projets, solutions, applications et produits se fait par des prestataires agréés ou certifiés ANSSI, qui sont des **Centres d'Evaluation de la Sécurité des Technologies d'Information (CESTI)**. Deux catégories de certification sont possibles : la **CSPN (Certification de Sécurité de Premier Niveau)**, qui permet d'obtenir un premier niveau de confiance en la sécurité d'un produit, et l'**ISO 15408-CC** autrement appelée **Critères Communs**, un standard internationalement reconnu qui comprend plusieurs niveaux d'assurance de sécurité (**EAL** pour **Evaluation Assurance Level**).

Enfin, les tests fonctionnels ou d'interopérabilité concernent les solutions, produits et applications.

8 https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/

CATALOGUE CYBERLAB
LES PRESTATAIRES DE SERVICES _

Un appel à manifestation d'intérêt a été émis par le Pôle d'excellence cyber fin 2021 pour référencer ces prestataires.

1. Les prestataires de services cyber et leurs cordonnées

Le tableau ci-dessous liste les prestataires de services qui ont répondu à l'appel à manifestation d'intérêt.

SOCIÉTÉ	CONTACT	COURRIEL	TÉLÉPHONE	ADRESSE	WEB
ACCEIS	Christophe BEUCHARD	christophe@acceis.fr	06 64 59 15 50	2 rue Micheline Ostermeyer 35000 Rennes	www.acceis.fr
Airbus CyberSecurity	Nicolas RAZI	contact.cybersecurity@aibrus.com	01 61 38 50 00	Metapole, 1 bd Jean Moulin Elancourt, Yvelines 78990	airbus-cyber-security.com
ALGODONE	Christophe BALLAN	christophe@algodone.com	04 67 13 00 82	Cap Omega, Rond-Point Benjamin Franklin CS 39521 34960 Montpellier	www.algodone.com
ALL4TEC	Laurent COSSON	lac@all4tec.net	06 73 41 04 55	Parc CERES, 21 Rue Ferdinand BUISSON 53810 Changé	www.all4tec.com
AMOSSYS	Vattana VONG	contact@amossys.fr	06 98 76 63 79	Immeuble Le Ouessant Bâtiment B 11 rue Maurice Fabre 35000 Rennes	www.amossys.fr
AVOXA	Jean-Nicolas ROBIN	jnrobin@avoxa.fr	02 23 48 46 00	5 allée Ermengarde d'Anjou 35 000 Rennes	avoxa.fr
AxBx	Gregory SNAUWAERT	gsnauwaert@axbx.com	06 15 05 09 35	53 rue Albert Samain 59650 Villeneuve d'Ascq	www.axbx.com
BEIJAFLORE FRANCE	Armel CONGAR	acongar370@beijaflore.com	06 50 69 36 03	11-13 avenue du Recteur Poincaré PARIS, 75016	www.beijaflore.com/fr
BLOO CONSEIL	Aurélien MAGNIEZ	aurelien.magniez@bloo-conseil.fr	06 78 07 03 21	9 rue Pierre-Marie Pautonnier 35520 La Chapelle des Fougeretz	www.bloo-conseil.fr
CARDELYA	Typhaine VANNIER	typhaine.vannier@cardelya.fr	02 99 00 30 83	4 rue Paul Langevin ZAC de la Goulgatière 35520 Châteaubourg	www.cardelya.fr
CoESSI	Hervé DAUSSIN	herve.daussin@coessi.fr	01 47 84 02 31	18 rue d'Arras Bâtiment D2 92000 Nanterre	www.coessi.com
CONSCIO TECHNOLOGIES	Michel GERARD	michel.gerard@conscio-technologies.com	06 07 04 92 57	12 rue Vivienne 75002 Paris	ww.conscio-technologies.com
DIATEAM	Joris DHUICQUE	sales@diateam.net	02 98 05 00 50	31 rue Yves Collet 29200 Brest	www.diateam.net
eShard	Georges GAGNEROT	georges.gagnerot@eshard.com	06 03 05 02 39	11 avenue de canteranne 33600 Pessac	eshard.com
FORMIND	Mathieu MEYNIER	mathieu.meynier@formind.fr	06 13 03 40 53	13 rue Claude Chappe 35510 Cesson-Sévigné	www.formind.fr/fr
GATEWATCHER	Aubin de BELLEROCHE	aubin.debelleroche@gatewatcher.com	06 87 10 84 99	75 Boulevard Haussmann 75008 Paris	www.gatewatcher.com/fr
GIP SIB	Nicolas JOLIVET	nicolas.jolivet@sib.fr	06 88 70 58 50	4 rue du professeur Jean Pecker 35700 Rennes	www.sib.fr
GROUPE PRORISK	Pascal LE CLAIRE	pascal.leclaire@groupe-prorisk.com	06 21 24 51 53	7 rue du Commandant Malbert 29200 Brest	www.prorisk-cyber.com
KALIS CONSULTING	Nathan BOUKOBZA	nathan.boukobza@kalis-consulting.fr	06 21 01 03 27	101 avenue François Arago 92 000 Nanterre	www.kalis-consulting.fr
KEOPASS	Hervé-François LE DEVEHAT	contact@keopass.com	02 97 58 00 95	18 rue Du Gréo, 56870 Baden	keopass.com
KEREVAL	Vincent ALLIOT	vincent.alliot@kereval.com	02 23 20 36 64	4 rue Hélène Boucher 35235 Thorigné Fouillard	www.kereval.com
LEXFO	Rodolphe ARNOUX	r.arnoux@lexfo.fr		5 rue Drouot 75009 Paris	www.lexfo.fr
LOCKSELF	Pierre RANGDET	p.rangdet@lockself.com	07 80 90 43 06	6 rue des Bateliers 92110 Clichy	www.lockself.com
OPPIDA	Eric DEHAIS	contact@oppida.fr	01 30 14 19 00	4-6, avenue du Vieil Etang 78180 Montigny le Bretonneux	www.oppida.fr
PRADEO	Romain CHASSERE	romain.chassere@pradeo.com		71B Place Vauban 34000 Montpellier	pradeo.com
QUARKSLAB	Marion VIDEAU	mvideau@quarkslab.com	01 58 30 82 51	12 avenue Henri Fréville 35200 Rennes	quarkslab.com
Rubycat	Cathy LESAGE	cathy.lesage@rubycat.eu	02 99 30 21 11	1137 avenue des champs blancs Digital Square 35510 Cesson Sévigné	www.rubycat.eu
SCASSI	Julien CHAPPUY	julien.chappuy@scassi.com	07 63 79 43 34	209 rue Jean Bart 31670 Labège	www.scassi.com
SEC-IT SOLUTIONS	Pascal MONTEL	pascal.montel@sec-it.fr		48 rue de Bray 35510 Cesson-Sévigné	www.sec-it.fr
Secure-IC	Ismail GUEDIRA	sales-emea@secure-ic.com		15 rue Claude Chappe 35510 Cesson-Sévigné	www.secure-ic.com
SEELA	Arthur BATAILLE	arthur@seela.io	06 16 61 30 82	125 Boulevard Jean Jaures 92100 Boulogne-Billancourt	seela.io
SERMA SAFETY AND SECURITY	Nathalie MONEY	contact-s3@serma.com	05 57 26 08 88	4 rue Galilée - CS 10071 33608 Pessac	www.serma-safety-security.com
SOPRA STERIA	Jean-Luc GIBERNON	jean-luc.gibernon@soprasteria.com	06 81 27 86 52	Parc de la Conterie 2 12 rue Léo Lagrange 35131 Chartres-de-Bretagne	www.soprasteria.fr
SOURCITEC	Coralie CEGALERBA	coralie.cegalerba@sourcitec.com	06 71 18 09 56	6 rue de Porstrein 29200 Brest	www.sourcitec.com
SYNACKTIV	Benoît LAMIRE	benoit.lamire@synacktiv.com	07 87 10 61 54	5 boulevard Montmartre 75002 Paris	www.synacktiv.com
SYSDREAM	Hortense AMPHIMAQUE	hortense.amphimaque@hubone.fr	06 08 54 98 67	14 place Marie-Jeanne Bassot 92300, Levallois-Perret	sysdream.com
THALES SIX GTS FRANCE SAS	Claude-Luce IMBAUD	claude-luce.imbaud@thalesgroup.com	06 77 02 21 89	4 avenue des Louvresses 92230 Gennevilliers	www.thalesgroup.com
TRANSFERTPRO	Jérémy VERNET	j.vernet@transfertpro.com	06 77 52 52 53	32 boulevard de Courcelles 75017 Paris	www.transfertpro.com
TRIALOG	Antonio KUNG	Antonio.kung@trialog.com	01 44 70 61 00	25 rue du Général Foy 75008 Paris	www.trialog.com/fr/accueil
YESWEHACK	Rodolphe HARAND	r.harand@yeswehack.com	06 33 45 23 62	14 rue Charles V 75004 Paris	www.yeswehack.com/fr
Watoo	Javier Franco Contreras	contact@watoo.tech		115 rue Claude Chappe, 29280, Plouzané	watoo.tech
ZIWIT	Elsa JONQUET	montpellier@ziwit.com		40 avenue Theroigne de Mericourt 34000 Montpellier	www.ziwit.com

2. Autres services d'accompagnement à la mise sur le marché

Des outils nationaux et régionaux sont également à disposition des acteurs afin de comprendre les réglementations applicables et d'obtenir des conseils d'accès au marché.

Pôle d'excellence cyber : Il répond à trois enjeux majeurs. Disposer des compétences nécessaires pour répondre aux besoins de développement d'un filière souveraine et européenne en cybersécurité; disposer d'une offre de formation et de recherche en adéquation avec les besoins du ministère et des industriels; disposer de produits et de services de confiance.

Biotech Santé Bretagne : Centre d'innovation Technologique en Santé et Biotechnologies en Bretagne qui accompagne les porteurs de projets innovants : conseils, mises en relation, ingénierie de projets, identification de financements, veilles réglementaire scientifique et technologique, etc.

GCS e-santé Bretagne : Le Groupement de Coopération Sanitaire e-Santé Bretagne promeut, pilote et coordonne les projets mutualisés permettant les échanges numériques entre tous les professionnels de santé.

GIP SIB : La direction de l'innovation identifie des projets d'innovation puis pilote leur mise en œuvre en collaboration avec des établissements de santé et les startups. La BU Protection des données et cybersécurité vient en support de ces projets pour intégrer le security et privacy by design.

ANS : L'Agence du Numérique en Santé accompagne la transformation numérique du système de santé français. Elle assure trois grandes missions :

- Définir les cadres et bonnes pratiques en termes de sécurité et d'interopérabilité afin de réguler la e-santé ;
- Conduire des projets d'intérêt national sous l'égide des pouvoirs publics ;
- Accompagner le déploiement national et territorial des outils et projets numériques en santé.

G_NIUS : Le Guichet National de l'Innovation et des Usages en e-Santé proposé par la Délégation Nationale de Santé, est une plateforme qui a pour objectif de stimuler les innovations du numérique en santé et ainsi faire gagner du temps aux entrepreneurs et d'accélérer la mise sur le marché des innovations. De nombreux services y sont proposés :

- Une analyse haut niveau de l'innovation permettant de comprendre le cadre réglementaire applicable au projet, accompagnée de différentes fiches techniques permettant de comprendre les différents principes applicables et leur mise en application
- Une identification des grands acteurs de l'écosystème, leur rôle et l'engagement qu'ils peuvent avoir au sein d'un projet en santé numérique
- Une identification des sources de financement Santé accessibles selon les différentes étapes de projet.

CNIL : La Commission Nationale de l'Informatique et des Libertés est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité. Les services proposés par la CNIL sont les suivants :

- Informer et protéger autour du droit du numérique, elle encadre l'utilisation des données ;
- Accompagner la conformité et conseiller les entreprises ;
- Anticiper et innover en participant à la constitution d'un débat de société sur les enjeux éthiques des données. Elle constitue un point de contact avec les écosystèmes d'innovation du numérique ;
- Contrôler et sanctionner en cas de manquement constaté.

ORGANISME	SITE INTERNET	CONTACT (SI APPLICABLE)
Pôle d'excellence cyber	www.pole-excellence-cyber.org	contact@pole-excellence-cyber.org
Biotech Santé Bretagne	www.biotech-sante-bretagne.fr	contact@biotech-sante-bretagne.fr
GCS e-Santé	www.esante-bretagne.fr	N/A
GIP SIB	www.sib.fr	innovation@sib.fr
ANS	esante.gouv.fr	N/A
GNIUS	gnius.esante.gouv.fr	N/A
CNIL	www.cnil.fr/professionnel	N/A

3. Les prestataires et leurs services au sein du catalogue CyberLab

		ACCEIS	Airbus CyberSecurity	Algodone	ALL4TEC	AMOSSYS	Avoxa	AxBx	Beijaflore France	BLOO CONSEIL	Cardelya	CoESSI	Conscio Technologies	DIATEAM	eShard	Formind	GATEWATCHER	GIP SIB	GROUPE PRORISK	Kalis Consulting	KEOPASS	KEREVAL	LEXFO	LockSelf	Oppida	Pradeo	RUBYCAT (PAM/bastion)	Quarkslab	SCASSI	SEC-IT SOLUTIONS	Secure-IC	Seela	SERMA SAFETY AND SECURITY	SOPRA STERIA	SourcITEC	Synacktiv	SYSDREAM	Thales SIX GTS France SAS	TransfertPro	Trialog	Watoo	YesWeHack	ZIWIT
FORMATION	Menaces systèmes santé	X	X				X	X	X				X	X		X		X	X	X			X						X	X	X	X		X	X		X	X					X
	Mgt cyber dans projets	X				X	X	X	X	X						X				X									X	X	X			X	X			X		X			X
	Gestion de crises	X					X	X	X					X		X				X										X			X	X	X			X	X				X
	Ingénierie solutions	X	X			X	X	X	X	X						X	X			X										X	X			X	X				X	X			
	Sécurité applis et IoT	X				X									X	X				X								X	X		X			X	X	X		X		X			X
	Programmation sécurisée	X				X		X	X				X			X							X						X	X	X		X	X	X	X	X		X				
CONSEIL	Analyse de risques	X		X	X	X		X	X			X			X	X		X				X			X				X	X	X		X	X	X			X		X			X
	Politique de cyber	X		X		X		X	X			X				X		X				X			X				X	X	X		X	X	X			X					X
	GT cyber	X				X	X		X	X		X				X		X				X							X	X	X			X	X			X		X			X
	Gestion de crises						X	X	X							X		X											X	X			X	X	X			X	X				X
	Plan de tests	X				X			X	X					X	X						X			X				X		X			X	X	X				X			X
	Architecture de sécurité	X		X		X			X	X	X	X			X	X	X				X	X		X					X	X	X		X	X	X			X	X	X	X		X
AUDIT	Audit préliminaire	X				X		X	X			X			X	X		X				X			X				X	X			X	X	X	X	X	X					X
	Audit et tests d'intrusion	X				X		X	X			X			X	X	X	X				X			X				X	X			X	X	X	X	X	X					X
	Audit code source	X				X		X	X			X			X	X									X			X	X				X	X		X	X	X					X
	Audit configuration	X				X			X			X				X	X	X				X			X				X	X			X	X	X	X	X	X					X
	Audit architecture	X				X			X			X				X	X	X				X			X				X	X			X	X	X	X	X	X					X
	Audit orga & physique	X				X		X	X			X				X		X							X				X	X			X	X	X	X	X	X					X
CERTIFICATION	Auto certification	X				X																			X						X							X					
	Pré-audit CSPN	X				X																	X		X			X			X		X		X			X				X	
	CSPN	X				X																	X		X		X	X			X		X		X			X				X	
	CC - EAL 1-7					X																X			X					X		X		X				X					
	Qualification	X																				X	X		X								X					X					
TEST	Tests de sécurité					X		X							X							X	X		X	X			X		X		X						X				X
	Tests fonctionnels					X		X														X	X		X				X		X		X		X				X				X
	Tests d'interopérabilité					X																	X						X		X				X				X				

CATALOGUE CYBERLAB
DÉTAILS DES PRESTATIONS ET COÛTS APPROXIMATIFS _

Le catalogue de prestations liste une série de services qui ont été définis comme étant pertinents pour des projets relatifs au secteur de la santé. Cette liste n'est pas exhaustive et pourra évoluer en fonction des besoins des projets et des propositions que pourront faire les prestataires qui délivrent ces services.

Les coûts des prestations et leurs durées figurent dans les tableaux ci-après, ce sont des valeurs minimales, moyennées et maximales, issues de l'ensemble des réponses reçues des prestataires qui ont répondu à l'Appel à Manifestation d'Intérêt (AMI) de 2021.

Les coûts mentionnés (minimum, moyen et maximum) sont approximatifs, cela pour permettre aux équipes projets de pré-budgéter les prestations visées au moment du montage financier du projet, étant bien entendu que le prix réel de la prestation de service sera défini par le prestataire quand celui-ci sera sollicité par les équipes projets, sur la base d'un cahier des charges ou d'une demande de cotation précisée.

De même pour les durées des prestations (minimale, moyenne et maximale), celles-ci sont données à titre informatif, sachant que la durée réelle de la prestation sera définie par le prestataire quand celui-ci sera sollicité par les équipes projets lorsque la demande sera bien précisée.

1. Les prestations de formation

FORMATION - SENSIBILISATION								
Titre	Descriptif	Pour qui	Durée en nbr de jours*			Coût approx en K€ HT*		
			MIN	MOY	MAX	MIN	MOY	MAX
Sensibilisation aux menaces Cyber des systèmes de santé	Les organismes de santé font partie des Organismes d'Importance Vitale (OIV) ou de Services Essentiels (OSE). Les objectifs de cette formation sont : Comprendre et assimiler les enjeux et les risques des attaques cyber, les réglementations Françaises et Européennes et le règlement de la protection des données (RGPD), la politique générale de sécurité des systèmes d'information de la santé (PGSSI-S). Les réglementations ou directives HDS, HNUM, INS*	Chef de projet, développeur, architecte, exploitant, gestionnaire	0,5	1	5	1	5	31
Management de la cybersécurité dans les projets	Acquérir les fondamentaux du management de la cybersécurité dans les projets : analyse et gestion des risques ; modèles de sécurité ; politique de sécurité ; aspects juridiques ; respect des directives ; certifications et règlements (ISO,...).	Chef de projet	1	2	4	0,6	7	36
Gestion de crises et continuité de services	Comprendre et assimiler les différentes crises cyber et leurs impacts ; définir les réponses appropriées ; mettre en place les différentes phases des traitements ; élaborer un plan de communication de crise ; définir un plan de continuité opérationnel de services et de reprise d'activité.	Chef de projet, Exploitant, gestionnaire	1	2	4	0,7	10	36
Ingénierie de solutions de cybersécurité	Maîtrise de l'ingénierie des architectures, produits ou des solutions de sécurité basée sur des composants matériels, réseaux et logiciels sécurisés ; gestion de la sécurité du cycle de vie des composants, logiciels, produits et solutions.	Architecte, développeur, intégrateur	1	3	6	1	10	41
Sécurité des applications mobiles et objets connectés	Comprendre et assimiler les enjeux et les technologies pour sécuriser les objets connectés et leurs réseaux de communications ainsi que les applications mobiles (IOS, Android) associées.	Architecte, développeur	1	3	6	1	9	41
Programmation sécurisée pour les développeurs	Assimiler les bonnes pratiques de développement des firmware et logiciels afin de créer des applications avec le moins de failles possibles et plus résilientes aux attaques cyber.	Développeur	1	3	6	1	6	41

* Coûts et durées donnés à titre indicatif sans engagement contractuel.

2. Les prestations de conseil

CONSEIL								
Titre	**Descriptif**	**Pour qui/quoi**	**Durée** en nbr de jours*			**Coût** approx en K€ HT*		
			MIN	MOY	MAX	MIN	MOY	MAX
Analyse de risques	Identification, évaluation et hiérarchisation des cyber-risques et de leurs impacts.	Projets, organisations	1	17	60	2	17	70
Politique de cybersécurité	Définition et mise en place d'une politique de cybersécurité et élaboration de son plan d'investissement associé.	Projets, organisations	3	15	60	1	14	52
Groupe de travail cyber	Animation d'un groupe de travail sur la cybersécurité pour par exemple : sensibiliser une équipe, définir des objectifs ou un plan d'action...etc.	Projets, organisations	1	3	10	0,7	5	20
Gestion de crise	Que faire en cas de crise : mise en place d'une cellule de crise, définir les priorités, stratégies de communications, processus de gestion de la crise, plan de reprise d'activité (PRA).	Organisations	2	22	120	2	21	90
Plan de tests	Définition d'un plan de tests fonctionnels pour spécifier ce qui doit être testé et comment.	Produits, solutions, logiciels	1	13	50	1,5	11	30
Architecture de sécurité	Conception d'architecture sécurisée et structuration des choix techniques et technologiques.	Produits, solutions, logiciels	3	18	60	2,1	17	70

* Coûts et durées donnés à titre indicatif sans engagement contractuel.

3. Les prestations d'audit

Pour ces prestations d'audit, il conviendra aux clients de vérifier que le prestataire retenu dispose de la labélisation PASSI – Prestataire d'Audit de la Sécurité des Systèmes d'Information délivrée par l'ANSSI. Un audit est souvent suivi d'un accompagnement pour l'amélioration et la mise en œuvre ainsi que le transfert de compétences vers les équipes.

AUDIT								
Titre	**Descriptif**	**Pour qui/quoi**	**Durée** en nbr de jours*			**Coût** approx en K€ HT*		
			MIN	MOY	MAX	MIN	MOY	MAX
Audit préliminaire	Audit flash d'un système ou d'une solution pour un pré-diagnostique de vulnérabilité cyber potentielles.	Projets, produits, solutions, logiciels	1	5	20	0,7	6	20
Audit et tests d'intrusion	Evaluation des points forts et vulnérabilités potentielles au regard d'une analyse des risques et d'un référentiel. Recommandations pour supprimer les vulnérabilités.	Produits, solutions, logiciels	2	11	30	1,5	12	40
Audit de code source	Analyse exhaustive du code d'une application ou logiciel pour détecter d'éventuelles vulnérabilités. Rapport et proposition d'actions correctives.	Applications, logiciels	1	12	60	2	12,5	60
Audit de configuration	Vérification de la configuration des systèmes, solutions et applications au regard des règles de sécurité. Rapport et proposition d'actions correctives.	Solutions, systèmes, applications	1	7	20	0,8	7,5	20
Audit d'architecture	Vérification de la conception d'une architecture d'un système ou d'une solution au regard des règles de sécurité. Rapport et proposition d'actions correctives.	Systèmes, solutions	1	7	20	2	8,5	25
Audit organisationnel et physique	Identification des vulnérabilités de sécurité liées aux processus d'exploitation ou d'administration des systèmes/ solutions ainsi qu'aux accès physiques aux installations ou systèmes.	Systèmes, solutions, installations	1	10	20	2	10	28

* Coûts et durées donnés à titre indicatif sans engagement contractuel.

4. Les prestations de certification

Pour ces prestations de certification, il conviendra aux clients de vérifier que le prestataire retenu est agréé ou certifié par l'ANSSI (CESTI, Centre d'Evaluation de la Sécurité des Technologies d'Information, par exemple, ou CSPN, pour la Certification de Sécurité de Premier Niveau, ou ISO 15408-CC pour les Critères Communs).

CERTIFICATION									
Titre	**Descriptif**	**Pour qui/quoi**	**Durée** en nbr de jours*			**Coût** approx en K€ HT*			
			MIN	MOY	MAX	MIN	MOY	MAX	
Support à l'auto-certification	Support auprès de l'entreprise ou l'organisme pour définir et mettre en place des processus d'auto-évaluation de la conformité d'un système, produit, solution…aux règles de sécurité.	Équipe, Projets, produits, Solutions, applications	2	18	50	1	18	62,5	
Pré Audit CSPN	Evaluation préliminaire d'un produit en vue d'une future certification de 1er niveau de l'ANSSI : CSPN.	Produits	5	14	30	4	11	21	
Evaluation/ Certification 1er niveau (CSPN)	Evaluation et certification ANSSI de 1er niveau, CSPN d'un produit.	Produits	25	38	60	20	35	61	
Evaluation/ Certification CC – EAL 1 à 7)	Vérification et certification d'un produit à la norme ISO 15408.	Produits On retrouve une liste sur le site de l'ANSSI :	50	129	360	35	115	300	
	www.ssi.gouv.fr/entreprise/produits-certifies/cc/profils-de-protection/								
Qualification	Recommandation par l'État français de produits ou services de cybersécurité éprouvés et approuvés par l'ANSSI : conformité aux exigences règlementaires, techniques et de sécurité promues par l'ANSSI, garantie de robustesse du produit et de compétence du prestataire de service, et d'engagement du fournisseur de solutions à respecter des critères de confiance	Produits On retrouve une liste sur le site de l'ANSSI :							
	www.ssi.gouv.fr/liste-produits-et-services-qualifies/								

* Coûts et durées donnés à titre indicatif sans engagement contractuel.

5. Les prestations de test

TEST								
Titre	**Descriptif**	**Pour qui/quoi**	**Durée** en nbr de jours*			**Coût** approx en K€ HT*		
			MIN	MOY	MAX	MIN	MOY	MAX
Tests préliminaires de sécurité	Tests de sécurité conformément au plan de tests préalablement défini.	Solutions, produits, applications	1	9	40	1,5	10,5	100
Tests fonctionnels	Tests fonctionnels de sécurité conformément au plan de tests préalablement défini.	Solutions, produits, applications	1	12	45	2	12	100
Tests d'interopérabilité	Tests d'interopérabilité avec l'environnement dans lequel la solution ou le produit doit s'interfacer.	Solutions, produits, applications	1	12	40	2	13	100

* Coûts et durées donnés à titre indicatif sans engagement contractuel.

AVANTAGES DU CATALOGUE POUR LES PROJETS DE SANTÉ NUMÉRIQUE

L'introduction de la cybersécurité au sein des projets présente de nombreux avantages pour la filière santé :

- Une confiance numérique instaurée entre les clients, fournisseurs, utilisateurs et les sociétés qui commercialiseront les produits, solutions et applications issues de ces projets ;
- Un avantage compétitif pour ces mêmes sociétés, qui auront alors un élément de différenciation majeur face à leurs concurrents ;
- Une réduction des coûts. En cas de cyber attaque, les coûts de maintenance, de support, de gestion de crise et éventuellement les pénalités seront plus faibles, voire nulles pour des produits et services cyber-résilients ;
- Le développement d'une filière cyber & santé. Ce catalogue permettra la création de synergies et interactions entres les filières « santé » et « cybersécurité ».
- Un respect de la réglementation applicable au projet numérique, ainsi qu'une consolidation de la transformation numérique nationale en santé.

QUELLES PRESTATIONS CHOISIR EN FONCTION DU PROJET ?

La réponse à cette question peut paraître complexe, car elle est fonction de la taille de l'entreprise, de sa maturité cyber, du type de projet, du produit, de la solution ou de l'application développés dans ce projet et de son cycle de vie.

Dans le cadre du projet européen ***EDIH***[9] (***European Digital Innovation Hub***), les experts du Pôle d'excellence cyber, issus des mondes industriels, académiques et militaires, sont en cours de concertation pour produire un diagnostic de maturité pour les PME/PMI innovantes du domaine de la santé. Ce diagnostic orientera les responsables projets vers les services adaptés à leurs besoins, il sera accessible en ligne très bientôt sur le site du Pôle. Les PME/PMI pourront ainsi tester certains produits ou services des partenaires du catalogue Cyberlab Santé sur une plateforme servicielle disponible à distance afin de comparer leur usage et de sélectionner le plus approprié au projet.

Biotech Santé Bretagne structure et anime les filières régionales des Biotechnologies (Capbiotek) et de la Santé, il est le Centre de référence en matière d'innovation dans ces deux domaines pour 7 marchés identifiés : éco-industries, agro-industrie, alimentaire, cosmétique, biotech pharma, technologies médicales et e-santé.

Au cœur de l'écosystème régional d'innovation, nos expert·e·s thématiques en Santé et en Biotechnologies accompagnent les porteurs de projets innovants : conseils technologiques, mises en relation de partenaires industriels, académiques et cliniques, ingénierie de projets, études de faisabilité, identification de financements, veille réglementaire, scientifique et technologique, accompagnement à l'Europe, promotion des innovations, organisation de journées techniques et de rencontres networking, etc.

8 https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/

Cycle de vie et politique de cybersécurité

La politique globale de cybersécurité doit découler d'une analyse de risques rigoureuse, elle doit être mise en place à chacune des phases du cycle de vie du projet. La définition de la politique de cybersécurité doit être effectuée aussi en collaboration avec les prestataires de services.

Cybersécurité et sante – niveaux de criticité

Outre la politique de cybersécurité doit orienter les prestations à choisir pour le développement, la production, l'opération et la maintenance d'un produit ou d'un service.

Le choix de la prestation nécessaire selon la phase du cycle produit dépend de son positionnement et du lieu de son utilisation.

Le tableau ci-dessous résume les préconisations de prestations de services Audit et Certification en fonction du niveau de criticité de la solution, du produit ou du service devant faire l'objet d'une cyber-protection. Ce tableau est donné à titre d'information uniquement. Chaque projet devra faire l'objet d'une analyse de risque (prestation de Conseil) pour évaluer plus finement les prestations de services qui sont nécessaires.

Exemple de choix de prestations en fonction du niveau de criticité

AUDIT	Audit préliminaire		X	X	
	Audit & tests de sécurité	X	X		
	Audit orga & physique	X			
CERTIFICATION	Auto certification			X	
	Pré-audit CSPN		X		
	CSPN	X	X		
	CC - EAL 1-7	X			

CONCLUSIONS _

La cybersécurité est aujourd'hui une préoccupation majeure des acteurs de la santé. Suite à une première publication en 2018 d'un catalogue de services avec une liste de prestataires spécialisés en cybersécurité (le catalogue CyberLab Santé), le Pôle d'Excellence Cyber s'est associé à Biotech Santé Bretagne pour proposer une évolution du document. Pour cette mission, Biotech Santé Bretagne a mobilisé des spécialistes du domaine, issus du groupe de travail « Data, IA, Cyber en santé » animé en région, afin d'apporter une expertise complémentaire.

Ce catalogue permet de comprendre les fondamentaux de la cybersécurité des systèmes d'information de santé (relatifs aux établissements de santé, objets connectés et dispositifs médicaux connectés) et l'identification d'acteurs accompagnateurs dans l'appréhension optimale des sujets de sécurité.

Ce CyberLab Santé a pour objectif d'aider les entreprises et consortium développant des solutions pour les établissements de santé et les usagers à intégrer la cybersécurité nativement dans leurs projets, plus communément appelé le « security by design ».

Pour toute demande d'information ou toute suggestion, contactez le Pôle d'excellence cyber.

contact@pole-excellence-cyber.org

PUBLICATIONS RECOMMANDÉES _

- La Politique Générale de Sécurité des Systèmes d'Information de Santé – PGSSI-S
- Certification des hébergeurs de santé – HDS
- Les prérequis de l'hôpital numérique – HNUM
- Les enjeux de l'Identifiant National de Santé - INS
- Le Référentiel cyber - Pôle d'excellence cyber
- Le Guide de sécurité numérique pour les PME/ PMI, collectivités et petites organisations et les 15 vidéos associées sur la chaine YouTube du Pôle d'excellence cyber
- le chapitre 4 de la loi de programmation militaire de 2013 sur la protection des infrastructures vitales en France – section 22
- Directive Européenne Network & Information Security (NIS)
- Directive Européenne General Data Protection Regulation (GDPR) – RGPD article 25
- La sécurité des systèmes d'information - ANS
- Le diagnostic réglementaire GNIUS
- NIST Framework for Improving Critical Infrastructure Cybersecurity

PÔLE D'EXCELLENCE
CYBER

12 B rue du Patis Tatelin
35700 RENNES
France

www.pole-excellence-cyber.org