PHILIPS

Monitorage
de patients

Améliorer le pronostic de la **cybersécurité des soins de santé**

Formation sur le monitorage de patients de Philips, gestion des risques et cybersécurité du réseau clinique

Les experts en informatique ne connaissent que trop bien les menaces de sécurité provenant des rançongiciels, de l'hameçonnage et du cybervol. Pourtant, la sécurisation des instruments médicaux réglementés nécessite un tout nouvel ensemble de processus, d'approbations et de collaboration.

Comprendre et appliquer les pratiques de gestion des risques

En adoptant les meilleures pratiques de gestion des risques, nous pouvons aider votre hôpital à éviter les cybermenaces potentielles et à atténuer les risques.

- **Appareils de monitorage de patients – un portail pour la cybercriminalité.** Les pirates informatiques sont attirés par les soins de santé, car le secteur tend à être à la traîne sur le plan de la cybersécurité. Selon Beazley – une compagnie mondiale d'assurance cybersécurité – 45 % de toutes les attaques de rançongiciels qu'elle a étudiées en 2017 visaient des établissements de soins de santé[1]. Sur le marché noir, les renseignements médicaux valent dix fois plus que les numéros de carte de crédit[2].

  L'un des moyens les plus simples pour les pirates d'accéder aux renseignements sur la santé protégés et sensibles des patients (ou au titre de l'HIPAA) est par l'intermédiaire des appareils de monitorage de patients. Étant donné que ces appareils sont connectés à des capteurs et des moniteurs, ils constituent également des points d'entrée pour les réseaux d'hôpitaux plus importants.

  Protection antivirus. Une validation est requise chaque fois que vous modifiez un instrument médical réglementé, ce qui comprend l'installation d'une application antivirus. À moins qu'ils ne soient revérifiés après l'installation, vos instruments médicaux ne sont pas considérés comme étant sûrs ou sécurisés.

- **Inclusion des bonnes parties prenantes.** La cybersécurité n'est pas seulement le domaine des experts en informatique, notamment lorsqu'il est question des soins de santé. Pour accroître la cybersécurité et l'efficacité de nos clients, nous encourageons le travail d'équipe et la collaboration. Pour ce faire, les parties prenantes aux niveaux clinique, biomédical et de la direction doivent également prendre part à l'exercice et donner des idées et des conseils. Prendre une décision en matière de cybersécurité qui peut avoir une incidence sur le personnel, les patients et l'avenir de votre hôpital est une étape importante et sérieuse. La figure 1 montre les principales parties prenantes recommandées.

- **Responsabilités des parties prenantes.** Nous vous recommandons de créer des accords (contrats) de responsabilités pour favoriser la responsabilisation et simplifier le flux de travail.

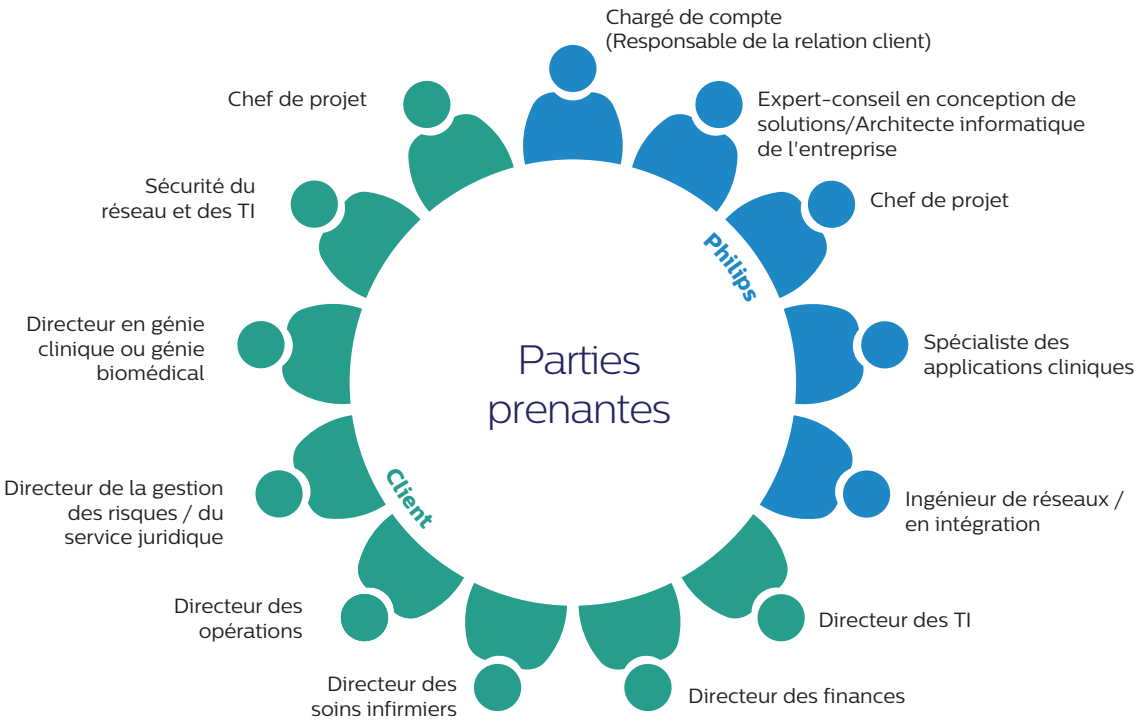


Figure 1 : Parties prenantes clés recommandées.

Exigences cliniques et informatiques

Le monitorage des patients et les réseaux cliniques doivent travailler ensemble pour soutenir les normes de sécurité et les efforts en matière de cybersécurité. La solution intégrée de monitorage de patients de Philips doit s'interfacer avec de nombreux appareils de soins aux patients et systèmes hospitaliers.

Le schéma d'architecture de référence (figure 2), illustre comment les exigences cliniques et informatiques de l'hôpital convergent pour soutenir les clients et leurs besoins en matière de soins.

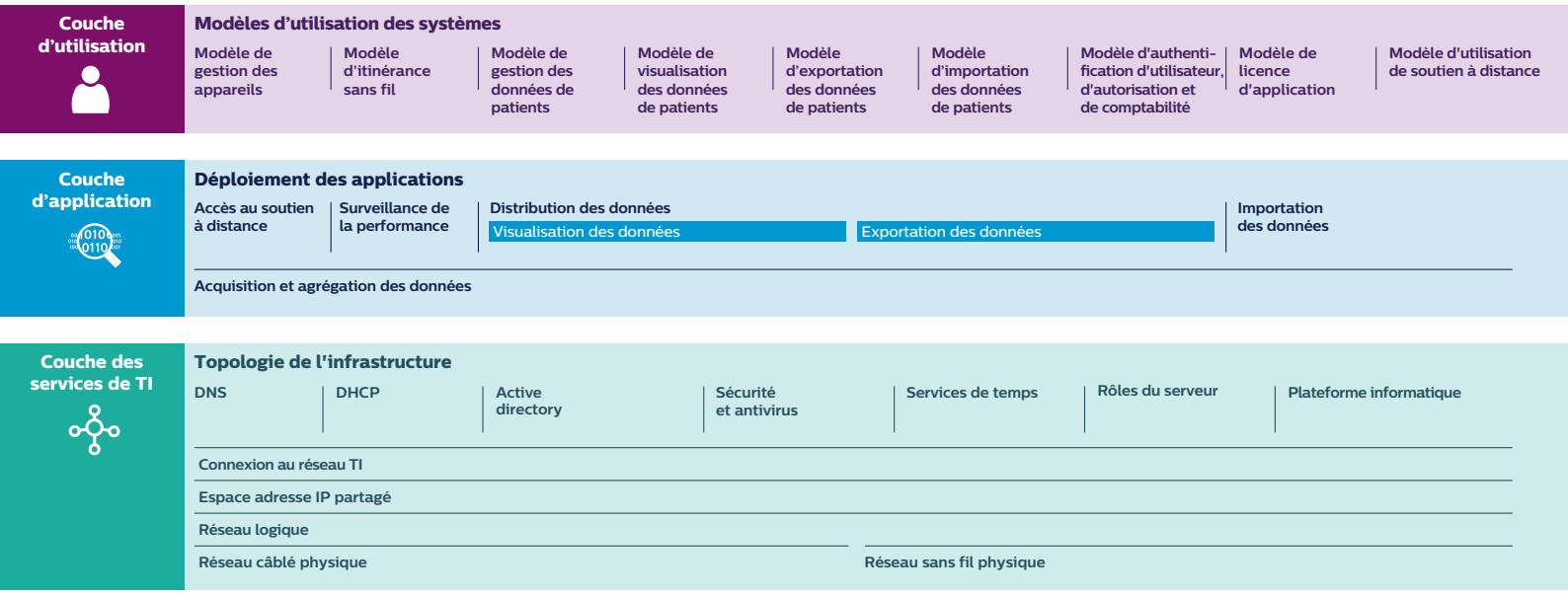


Figure 2 : Architecture de référence de monitorage de patients.

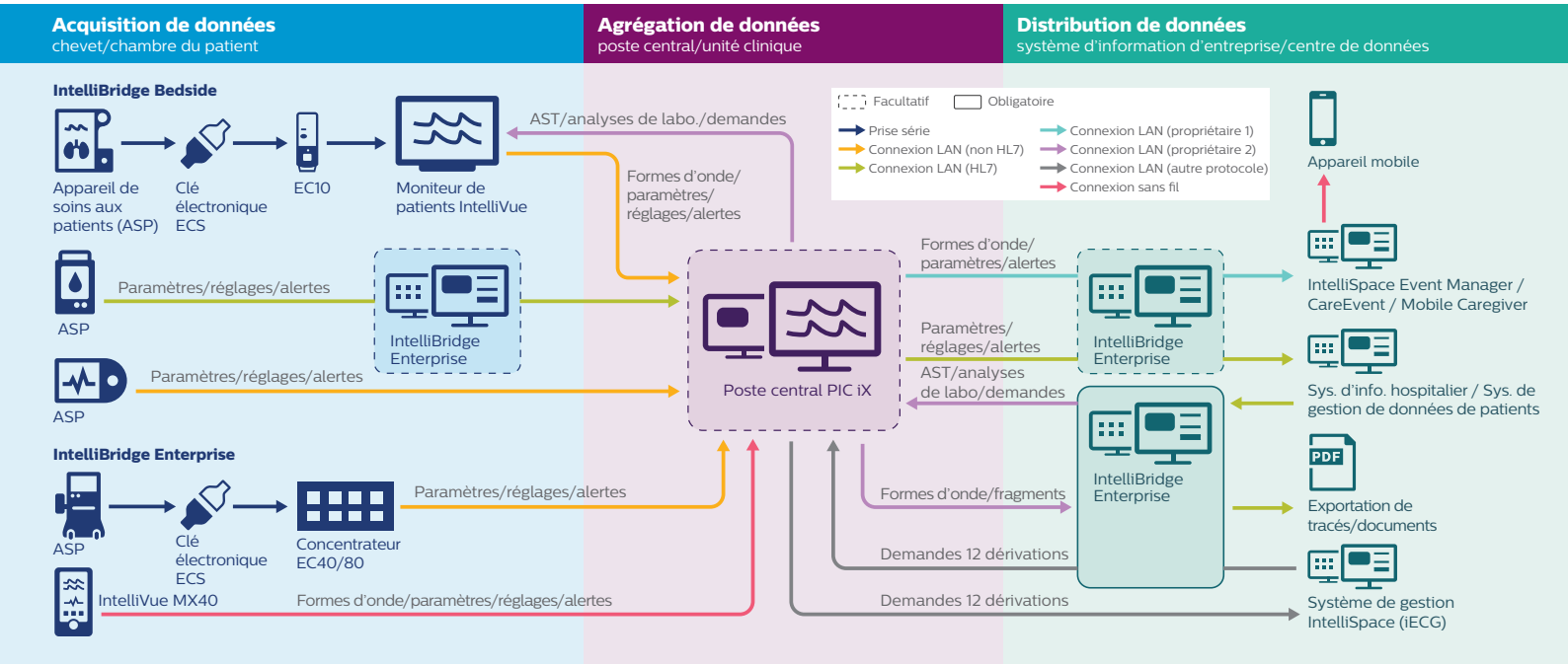
Connaître l'écosystème de monitorage des patients est essentiel pour comprendre la cybersécurité des soins de santé

La solution de monitorage de patients IntelliVue est un écosystème complexe d'appareils interconnectés qui fournissent de l'information vitale en temps réel et qui doivent fonctionner en continu jour et nuit, 365 jours par année. L'information vitale comprend notamment les données sur les signes vitaux du patient acquises auprès du patient et agrégées à partir de plusieurs sources, ce qui entraîne la distribution de formes d'onde, de tendances, d'alarmes et de chiffres à plusieurs systèmes, y compris le dossier médical électronique.

Une approche globale et à multiples facettes est essentielle pour gérer l'écosystème et maintenir les exigences de gérabilité, de facilité de service et de sécurité des appareils.

Bien que les établissements de santé soient particulièrement vulnérables – et la majorité des établissements interrogés dans le cadre d'une étude du Ponemon Institute menée en 2017 croyaient qu'ils feraient face à une attaque d'ici l'an prochain – seulement 53 % d'entre eux ont effectué des tests sur leurs appareils de monitorage de patients[4].

Schéma du flux d'information destinée au monitorage de patients de Philips



Philips vous aide à surmonter les obstacles pour sécuriser votre système de monitorage de patients

Des protocoles de sécurité et des évaluations des risques à une protection multicouche et à l'introduction de fonctions les plus novatrices, Philips adopte les meilleures pratiques pour vous offrir une tranquillité d'esprit supplémentaire.

Autosignalement

En tant que fabricant d'instruments médicaux, l'un des protocoles de sécurité que nous prenons le plus au sérieux est celui concernant l'autosignalement des vulnérabilités. Dans l'ensemble, le signalement des vulnérabilités – la pratique des fabricants d'instruments médicaux et des chercheurs indépendants divulguant les vulnérabilités en matière de cybersécurité – est en hausse de 400 % par trimestre depuis que la Food and Drug Administration a publié ses directives de cybersécurité en 2016, selon un rapport de MedCrypt[5].

C'est une bonne nouvelle pour vous. Chez Philips, nous prenons en charge les failles de sécurité et les signalons de manière proactive, en suivant ce processus relatif aux meilleures pratiques :

- Lorsque nous détectons une faille, nous la signalons à l'Industrial Control Systems Cyber Emergency Response Team ou ICS-CERT (équipe d'intervention en cas d'urgence informatique pour les systèmes de contrôle industriel), une division du département de la Sécurité intérieure des É.-U.
- Elle est ensuite signalée à la Food and Drug Administration (FDA).
- Nous disposons ensuite du temps nécessaire pour résoudre le problème.
- Nous signalons la faille de sécurité, et le correctif qui en découle, au public.
- Nous exerçons également une autosurveillance proactive chaque semaine pour rester au fait des problèmes connus et détecter les menaces possibles.

Une défense multicouche

Il n'y a pas qu'un seul moyen de garantir la cybersécurité de vos appareils de monitorage de patients. C'est pourquoi les experts recommandent une approche approfondie et multicouche. Conformément aux meilleures pratiques, chacune de ces couches de défense joue un rôle important en aidant à déjouer les pirates, à contrer les programmes malveillants et à empêcher les accès non autorisés aux instruments médicaux. Ces couches comprennent :

- Coupe-feu
  - Renforcement du système d'exploitation et des applications basé sur les guides techniques de mise en œuvre de la sécurité (STIG) du département américain de la Défense.
  - Authentification, autorisation et comptabilité
- Listes de contrôle
- Cryptage et authentification des nœuds

Stratégie de défense en profondeur de Philips

Meilleures pratiques relatives à la norme CEI 80001-1

Cette nouvelle norme internationale et volontaire décrit ce qu'il faut privilégier lorsque vous connectez des instruments médicaux à votre réseau TI afin de maintenir la sécurité, l'efficacité et la sécurité des données et des systèmes.

Bien que la norme 80001-1 soit volontaire, nous nous attendons à ce qu'elle devienne la norme à appliquer en matière de santé. Nous vous recommandons de commencer à appliquer les politiques et procédures nécessaires afin de réduire les risques pour les réseaux informatiques médicaux.

Les caractéristiques les plus novatrices

Vous offrir les caractéristiques dont vous avez besoin lorsque vous en avez besoin fait partie de notre engagement à vous aider à assurer la cybersécurité de votre hôpital. Voici certaines des caractéristiques qui distinguent Philips de la concurrence :

- Envoi de Microsoft Windows 10
- Prise en charge complète des mises à jour de sécurité validées du système d'exploitation
- Intégration dans votre domaine d'hôpital
- Cryptage
- SCCM

Regarder vers l'avenir et toujours essayer d'anticiper vos besoins

La technologie évolue rapidement. Nous gardons une longueur d'avance en innovant continuellement et en introduisant de nouvelles fonctionnalités.

Ensemble, nous pouvons maintenir un environnement sécurisé en restant vigilants et en définissant le paysage des cybermenaces en constante évolution. Nous nous engageons à répondre à vos besoins actuels et futurs.

Autres ressources utiles

Politique de divulgation des vulnérabilités du département de la Défense
https://hackerone.com/deptofdefense

Health Insurance Portability and Accountability Act (HIPAA)
Répertorie les exigences liées aux normes de sécurité et de respect de la vie privée, notamment la transmission électronique de renseignements sur la santé.
https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Application du management du risque aux réseaux des technologies de l'information contenant les dispositifs médicaux – Partie 2-2 (IEC 80001-2-2)
Donne des conseils pour la divulgation et la communication des besoins, des risques et des contrôles en matière de sécurité des instruments médicaux.
https://www.iso.org/standard/57939.html

Federal Information Processing Standard Publication 200 (FIPS PUB 200)
Fournit une liste complète des exigences à respecter par les entreprises.
https://csrc.nist.gov/publications/detail/fips/200/final

National Institute of Standards and Technology 800-53 (NIST 800-53)
Décrit les bases en matière de contrôles de sécurité comme point de départ du processus de sélection des contrôles de sécurité.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Sources

1. Becker's Health IT & CIO Report, « The 3 most important security statistics healthcare organizations need to know », 7 mars 2018, Mike Duffy; (https://www.beckershospitalreview.com/healthcare-information-technology/the-3-most-important-security-statistics-healthcare-organizations-need-to-know.html).
2. Reuters, « Your medical record is worth more to hackers than your credit card », 24 septembre 2014, Caroline Humer, Jim Finkle; (https://www. reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924).

3.-4. HIT Consultant, « Protecting Medical Device Security in the Age of Ransomware », 25 juin 2018, Kayla Matthews; (https://hitconsultant.net/2018/06/25/medical-device-ransomeware /).

5. Healthcare IT News, « Is FDA doing enough to support medical device security? », 15 août 2018, Jessica Davis; (https://www.healthcareitnews.com/news/fda-doing-enough-support-medical-device-security).

Ressources supplémentaires consultées :
Biomedical Instrumentation & Technology, « The Vital Role of Device Manufacturers as Cybercitizens », novembre/décembre 2015, William L. Holden; (http://www.aami-bit.org/doi/abs/10.2345/0899-8205-49.6.410).

Pour en savoir plus sur la solution de monitorage de patients IntelliVue de Philips, veuillez visiter le **www.philips.com/monitoring**

4522 991 51571 * Juillet 2019

www.philips.com