Livre blanc sur la cybersécurité des produits Mindray

Novembre 2024

mindray

Table des matières

Résumé exécutif

Dans le paysage en constante évolution des soins de santé et des dispositifs médicaux, on ne saurait trop insister sur la nécessité de mettre en place des mesures de cybersécurité solides. Alors que le secteur continue d'adopter les avancées technologiques et la numérisation, la nécessité de disposer de services de soins de santé et de dispositifs médicaux sécurisés, résilients et dignes de confiance devient primordiale. Ce livre blanc détaille l'approche globale de Mindray en matière de cybersécurité, en présentant les principes, les valeurs et les pratiques qui guident nos efforts pour garantir la sécurité des patients, protéger les données des clients et assurer la résilience et la continuité du fonctionnement de nos appareils.

Les principes et les valeurs qui sous-tendent les initiatives de Mindray en matière de cybersécurité mettent l'accent sur **la transparence, la responsabilité et l'amélioration continue**. Nous pensons que permettre à nos parties prenantes de prendre des décisions éclairées grâce à un partage transparent des mesures de sécurité mises en œuvre dans nos appareils, des considérations de risque pertinentes et des procédures de traitement des données sensibles est la clé pour établir **la confiance** en Mindray. En intégrant la protection de la confidentialité et la cybersécurité à chaque étape du cycle de développement de nos produits, Mindray fournit de manière responsable des produits et services à la fois innovants et résilients.

Chez Mindray, un cadre de **sécurité de l'information d'entreprise** solide est indispensable pour fournir **des dispositifs et des services** médicaux à la fois sûrs et fiables. Cette fondation repose sur l'expertise et la vision unifiée de nos **travailleurs** bien formés, dont l'engagement en faveur de la cybersécurité est le moteur de notre capacité à innover en toute sécurité.

L'engagement de Mindray en matière de cybersécurité dépasse largement la simple **conformité** aux normes et réglementations internationales. Il s'agit de cultiver une culture de la sécurité qui imprègne tous les aspects de notre organisation. De la phase de conception initiale à la surveillance après la mise sur le marché, Mindray intègre des considérations de cybersécurité à chaque étape du cycle de vie du produit. **L'obtention des certifications** par Mindray illustre notre engagement à atteindre les plus hauts niveaux de sécurité et de confidentialité. Ces certifications ne sont pas de simples gratifications symboliques. Elles témoignent de notre quête incessante de l'excellence et de notre engagement à préserver le bien-être des patients et leurs données sensibles confiées à nos appareils.

Dans le contexte de **la responsabilité partagée**, Mindray reconnaît que la cybersécurité dans les soins de santé est un effort de collaboration. Nous coopérons activement avec les prestataires de soins de santé, les autorités de réglementation et les autres parties prenantes, afin de créer un environnement sûr pour les soins aux patients. Cette collaboration est essentielle pour identifier les vulnérabilités potentielles, répondre aux incidents et améliorer la sécurité de l'environnement mondial des soins de santé. En encourageant une communication et une coopération ouvertes, nous visons à mettre en place une défense redoutable face aux cybermenaces.

Les piliers du **modèle de cybersécurité des produits Mindray** (gouvernance et gestion des risques, conception et développement sécurisés, et protection des données) reflètent une stratégie holistique qui tient compte des multiples facettes de la cybersécurité.

Chaque pilier représente un élément essentiel de notre cadre de sécurité global, garantissant que nos appareils sont non seulement conformes aux normes actuelles, mais aussi résistants aux menaces futures.

Nous savons que la confiance qui nous est accordée, à nous et à nos appareils, est une responsabilité que nous devons assumer avec un dévouement inébranlable. Alors que nous naviguons dans les complexités de l'ère numérique, Mindray continuera à mener avec intégrité, innovation et un dévouement inébranlable à la protection de la communauté des soins de santé.

Naviguer dans la numérisation des soins de santé : Une voie vers l'innovation sûre

Le secteur de la santé et des dispositifs médicaux a connu une mutation significative au cours des dernières décennies, sous l'effet des progrès technologiques rapides et de la numérisation. Des innovations telles que la télémédecine, les dispositifs portables de surveillance de la santé et les outils de diagnostic à distance ont révolutionné les soins apportés aux patients, les rendant plus efficaces, plus précis et plus accessibles. Les patients bénéficient désormais de plans de traitement personnalisés, d'un suivi de leur état de santé en temps réel et de procédures peu invasives, ce qui améliore considérablement leur état de santé et leur qualité de vie en général.

Néanmoins, alors que la dépendance du secteur aux technologies numériques interconnectées s'accroît, des risques accrus en matière de cybersécurité sont également à prendre en compte. L'intégration des dispositifs médicaux aux réseaux hospitaliers et aux plateformes cloud a créé de nouvelles vulnérabilités qui soulignent le besoin critique de mesures de sécurité robustes pour garantir la fiabilité des dispositifs et protéger les données sensibles des patients.

À l'instar de l'incident WannaCry, de nombreuses violations importantes de la cybersécurité ont touché le secteur de la santé ces dernières années. Par exemple, le ransomware[1] du Springhill Medical Center a mis hors service les systèmes de l'hôpital, contribuant à la mort d'un nourrisson après que les systèmes de surveillance critiques sont tombés en panne pendant l'accouchement. L'attaque par ransomware en 2020 contre le réseau de santé de l'université du Vermont[2] a provoqué d'importantes perturbations opérationnelles, retardant les soins aux patients et obligeant les hôpitaux à revenir aux dossiers papier. Les attaques Medjack[3], qui visaient des appareils médicaux tels que des pompes à perfusion et des appareils d'IRM, ont exploité des logiciels obsolètes et des mesures inadéquates pour prendre le contrôle et pénétrer dans des réseaux hospitaliers plus vastes. Le ransomware NotPetya[4] a gravement affecté les opérations de santé mondiales en employant les exploits EternalBlue[5] et en chiffrant les données critiques et en perturbant les services. Tous ces incidents soulignent les graves conséquences que les cyberattaques peuvent avoir sur les systèmes de santé, en compromettant la confidentialité des patients et en perturbant les services médicaux essentiels.

À la lumière de ces défis, Mindray vise à emprunter cette voie de l'innovation, tout en atteignant un équilibre entre l'exploitation des avancées technologiques et la garantie d'une sécurité solide dans nos dispositifs médicaux.
En établissant des normes strictes, en se conformant aux exigences internationales et en promouvant la transparence et le partage des responsabilités, Mindray vise à assurer que les avantages permis par les innovations sont réalisés de manière sûre et fiable, ce qui permet d'améliorer les soins aux patients sans sacrifier la sécurité.

[1] https://www.healthcareitnews.com/news/hospital-ransomware-attack -led-infants-death-lawsuit-alleges
[2] https://coverlink.com/case-study/uvm-health-network-ransomware-attack/
[3] https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf
[4] https://www.cloudflare.com/learning/security/ransomware/petya-notpetya-ransomware/
[5] https://www.avast.com/c-eternalblue

Position en matière de cybersécurité de Mindray

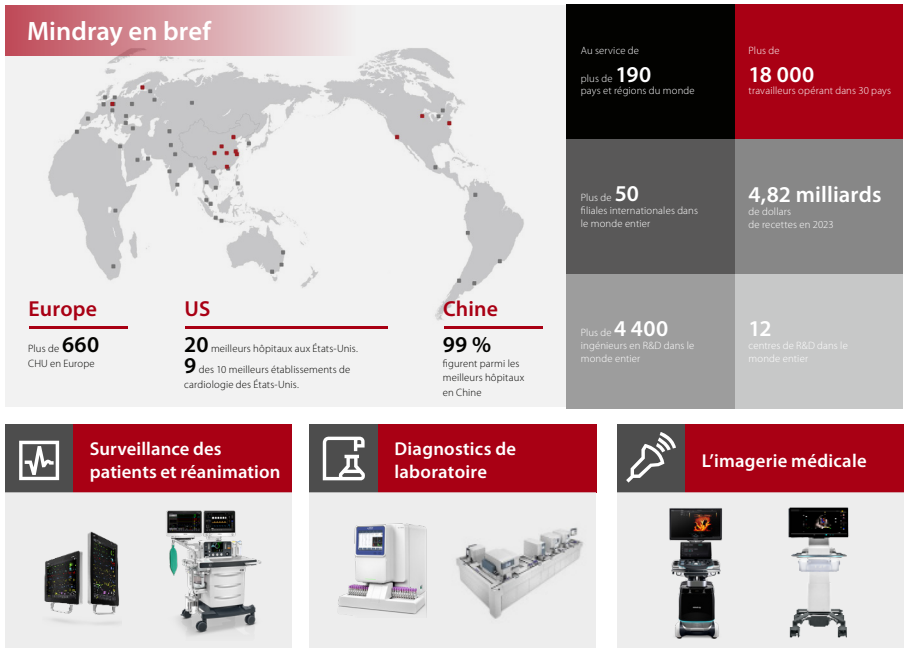
Conscient du risque croissant des menaces de cybersécurité, Mindray s'engage à améliorer continuellement ses processus et ses systèmes, afin d'intégrer la cybersécurité et la protection de la vie privée à tous les niveaux.

- Mener avec impact
- Sécuriser par la transparence et la confiance
- Fournir une base solide pour la sécurité de l'entreprise
- Respecter et faire respecter les normes
- Protéger dans le partenariat : Responsabilité partagée

Position en matière de cybersécurité de Mindray

Mener avec impact

Mindray est l'un des principaux concepteurs, développeurs et fabricants mondiaux de dispositifs et de solutions médicales, dont l'objectif est de rendre les soins de santé plus accessibles à l'humanité. Depuis sa création en 1991, Mindray s'est focalisé sur l'établissement de trois gammes de produits principales : la surveillance des patients et réanimation (PMLS), l'imagerie médicale (MIS) et les diagnostics de laboratoire (IVD). Mindray compte environ 7500 employés dans le monde entier, répartis entre le siège social situé à Shenzen, en Chine, et 42 filiales internationales avec des bureaux dans 32 pays, qui soutiennent divers prestataires de soins de santé générateurs de valeur pour la société. L'engagement de l'entreprise envers l'innovation est démontré par ses 12 centres mondiaux de R&D et un investissement leader de 10 % du chiffre d'affaires annuel dans la recherche et le développement, qui en fait un leader de son secteur.



Sécuriser par la transparence et la confiance

Chez Mindray, nos principes et valeurs de sécurité reposent sur un engagement ferme à préserver la sécurité des patients, à renforcer l'intégrité de nos dispositifs médicaux et à protéger les données sensibles.

Guidés par les normes internationales les plus strictes et les meilleures pratiques, nous aspirons à la transparence, la responsabilisation et l'amélioration continue. Nos efforts visent à créer un paysage de santé plus sûr et plus fiable, où les technologies de pointe et une sécurité sans compromis s'allient pour protéger et accompagner ceux que nous servons.

"La confiance repose non seulement sur notre volonté de révéler ce que nous faisons, mais également comment nous procédons. L'approche transparente de Mindray en matière de cybersécurité donne à nos clients une visibilité totale sur nos pratiques de sécurité. En veillant à ce que nos pratiques de cybersécurité soient claires et transparentes, nous offrons à nos clients la confiance dont ils ont besoin."

Cheng Minghe
Vice Chairman, Membre du Comité de conformité de Mindray

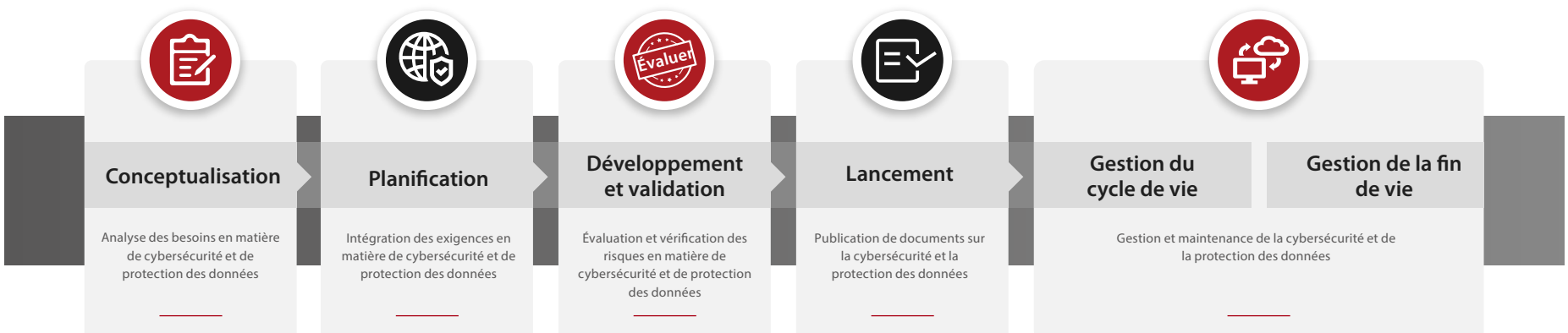
"Chez Mindray, la sécurité fait partie intégrante de l'ADN de chaque appareil que nous créons, garantissant résilience et fiabilité même dans les environnements de santé les plus critiques. La cybersécurité n'est pas qu'une simple fonctionnalité : c'est un principe fondamental à la base de la conception, du développement et du déploiement de chacun de nos dispositifs médicaux."

Li Zaiwen
Senior Vice President, Membre du Comité de conformité de Mindray

En tant que fabricant de dispositifs médicaux dans le secteur des soins de santé, la notion de "transparence" est au cœur de nos principes et de nos valeurs. Notre vision dépasse largement la simple conformité. Elle incarne notre engagement et notre profonde responsabilité pour donner la priorité à la prise de décisions éclairées par nos utilisateurs. La FDA[6] préconise une communication claire et ouverte sur les caractéristiques de cybersécurité des dispositifs et les risques potentiels, afin d'instaurer la confiance avec les prestataires de soins de santé, les régulateurs et les patients. Grâce à diverses formes de partage d'informations, notamment des livres blancs, des manuels d'utilisation et des documentations techniques, Mindray s'efforce d'améliorer sans relâche son engagement à maintenir la transparence sur les mesures de sécurité mises en œuvre, les considérations de risque et nos méthodes de protection des patients et de traitement des données sensibles.

En intégrant la sécurité et la confidentialité dès la conception dans le cycle de développement de nos produits, nous nous efforçons de garantir que la cybersécurité et la confidentialité sont intégrées dans la structure même de nos dispositifs médicaux dès la conception, afin d'assurer une continuité sans entrave des services médicaux essentiels et de préserver le caractère fondamental de la confidentialité des données. Notre cadre méticuleux de gestion des risques évalue et atténue sans relâche les menaces potentielles pour la sécurité, garantissant ainsi que nos appareils sont non seulement sûrs, mais aussi résistants et fiables. Grâce à une collaboration étroite avec les prestataires de soins de santé, les régulateurs et les partenaires industriels, nous visons à promouvoir une culture de la sécurité qui renforce la confiance dans l'écosystème mondial des soins de santé.

Sécurité et confidentialité dès la conception



[6] https://www.fda.gov/media/119933/download

Fournir une base solide pour la sécurité de l'entreprise

Chez Mindray, notre approche de la cybersécurité imprègne l'ensemble de notre éthique organisationnelle, ce qui se traduit par des produits et des services individuels. Nous comprenons qu'une sécurité robuste des informations de **l'entreprise** est fondamentale pour développer et maintenir la confiance en nous et en nos appareils. Une base aussi solide ne peut être établie que par des **personnes** bien informées et rigoureusement formées, qui conçoivent et fournissent des services et **des produits** sûrs et fiables. Cette stratégie de sécurité exhaustive de l'UE, qui renforce cycliquement les pratiques de sécurité de notre entreprise, l'expertise de notre personnel et nos innovations en matière de produits illustre la relation symbiotique nécessaire pour garantir que les opérations de notre entreprise et nos produits sont protégés contre les cybermenaces, ce qui donne des assurances à nos clients et parties prenantes.

Culture de sécurité unifiée : La culture d'entreprise de Mindray repose sur la sensibilisation à la sécurité et sur les meilleures pratiques. Nous encourageons tous les travailleurs, de la direction aux laboratoires de développement, à adopter un état d'esprit axé sur la sécurité. Cette culture de la vigilance se forme grâce à des programmes de formation réguliers qui englobent non seulement les principes de sécurité et de respect de la vie privée dès la conception, mais aussi la sécurité de l'information et la protection de la vie privée au sens large. Ce solide cadre de formation permet d'intégrer des fonctionnalités avancées de sécurité et de confidentialité dans les opérations quotidiennes et la conception des produits, renforçant ainsi la fiabilité et la conformité de notre entreprise et de nos appareils.

Infrastructure résiliente : L'infrastructure de sécurité de notre entreprise est conçue pour garantir la stabilité opérationnelle et la confidentialité des données, qui sont essentielles à la continuité et à la fiabilité de nos activités commerciales et de notre support client.
En protégeant nos centres de données, nos réseaux et nos architectures logicielles contre les perturbations et les violations, nous nous assurons que les systèmes qui soutiennent nos services de développement et de maintenance de produits sont toujours disponibles et sûrs.

Réponse proactive aux incidents et amélioration continue : Les capacités dynamiques de Mindray en matière de réponse aux incidents et les évaluations continues de la sécurité garantissent que nous pouvons rapidement faire face aux cyberattaques et vulnérabilités potentielles, tant au niveau de l'entreprise que du produit. Cette attitude proactive permet non seulement de limiter les risques, mais aussi d'améliorer en permanence les fonctions de sécurité de notre entreprise et de nos produits, sur la base de données réelles et des menaces émergentes.

Engagement et transparence des parties prenantes : Chez Mindray, nous nous efforçons de maintenir un dialogue ouvert sur nos processus et développements en matière de sécurité. En faisant preuve de transparence quant à nos stratégies de sécurité pour l'entreprise et les produits, nous visons à instaurer une plus grande confiance avec nos clients, en les assurant de notre engagement en faveur de normes de sécurité élevées, de la sécurité des patients et de la protection de leurs informations sensibles.

Entreprise : une défense stratégique

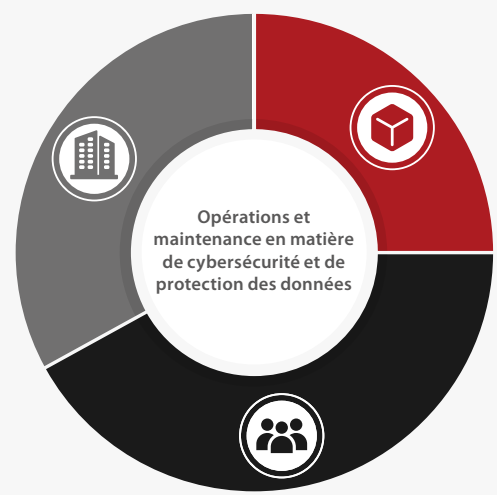
Maintenir une sécurité d'entreprise robuste avec des plans de réponse aux incidents complets et une infrastructure résiliente, ce qui garantit la stabilité opérationnelle et l'amélioration continue de la protection des systèmes internes etdes données.

Collaborateurs : des protecteurs habilités

Grâce à une formation approfondie aux pratiques de sécurité et aux normes de confidentialité, notre personnel maintient et fait progresser notre culture axée sur la sécurité.

Produit : une innovation sécurisée

Intégration de fonctionnalités de sécurité avancées dans chaque dispositif médical, de la conception au développement, favorisant la confiance et la fiabilité auprès de nos clients.



Respecter et faire respecter les normes

Chez Mindray, nous reconnaissons et respectons l'importance et la valeur de l'adhésion aux normes et certifications internationales pour garantir les plus hauts niveaux de qualité, de sécurité et de cybersécurité des produits. Notre engagement à respecter ces normes n'a pas pour seul but de respecter la législation ou d'obtenir des certifications, mais de donner à nos clients et utilisateurs un profond sentiment de confiance et d'assurance. Il rassure nos parties prenantes en leur montrant que nous travaillons avec la plus grande intégrité, en veillant à ce que nos produits répondent à des critères stricts de qualité et de sécurité. Ce sentiment de confiance est crucial dans le secteur des soins de santé, où la fiabilité et la sécurité des dispositifs médicaux ont un impact direct sur les soins comme sur les résultats des patients. Ces normes et certifications témoignent donc de notre engagement à garantir la sécurité de notre entreprise et de nos produits, ainsi que de nos efforts de croissance et d'amélioration continues, qui nous poussent à améliorer sans cesse nos pratiques.

Les normes et exigences pertinentes auxquelles Mindray se conforme comprennent, sans s'y limiter, TIR57, ISO 14971, ISO 31000, IEC/TR 80001-2-2, les exigences et directives pré et post-commercialisation de la FDA, MDCG 2019-16, les principes et pratiques de l'IMDRF, le Règlement Général sur la Protection des Données (RGPD) européen, la loi américaine sur la portabilité et la responsabilité de l'assurance maladie (HIPAA), ou la loi chinoise sur la protection des informations personnelles (PIPL). Ces normes guident nos processus, de la gestion des risques et de la cybersécurité au développement global des produits et à la gestion de leur cycle de vie. En adhérant à ces normes, nous nous assurons que nos risques organisationnels sont gérés et que nos produits sont conçus, développés et entretenus avec les plus hauts niveaux de sûreté et de sécurité.

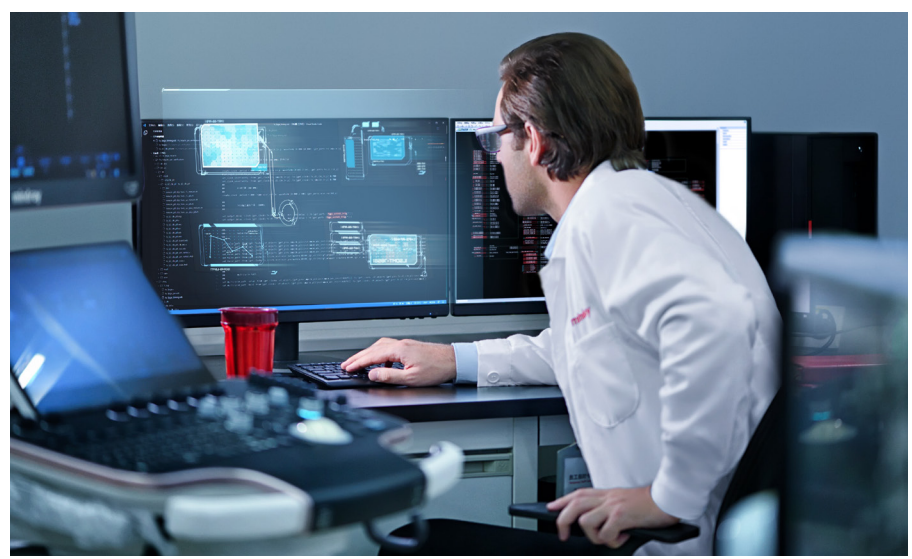
En termes de certifications, Mindray a obtenu plusieurs reconnaissances prestigieuses, notamment ISO/IEC 27001:2022 pour la gestion de la sécurité des informations et ISO/IEC 27701:2019 pour la gestion des informations relatives à la protection de la confidentialité. Ces certifications couvrent différents aspects de nos activités, tels que la R&D, les ventes, le service, l'informatique et bien d'autres, garantissant une approche globale de la conformité et de la sécurité. Parmi les autres certifications, citons la NEN7510 pour la sécurité des informations sur les soins de santé, l'UL2900-2-1 pour les dispositifs connectables au réseau, etc.

UL Solutions

L'applicabilité de certaines normes et certifications dépend du produit spécifique et des régions commercialisées. Par exemple, les exigences applicables de la FDA sont respectées pour les dispositifs conformément aux voies réglementaires et aux orientations, telles que la notification préalable à la mise sur le marché 510(k). Grâce à des recherches et des contrôles approfondis, nous nous assurons que nos produits répondent aux exigences réglementaires pertinentes en fonction des marchés et des utilisations auxquels ils sont destinés.

En atteignant et en maintenant ces normes et certifications, Mindray s'efforce de démontrer son engagement inébranlable en faveur de l'excellence, d'améliorer sa crédibilité et de nous motiver à innover et à nous améliorer en permanence, en veillant à ce que nous fournissions constamment des dispositifs médicaux et des services sûrs, sécurisés et fiables aux prestataires de soins de santé et aux patients dans le monde entier.

> Notre engagement à respecter ces normes n'a pas pour seul but de respecter la législation ou d'obtenir des certifications, mais de donner à nos clients et utilisateurs un profond sentiment de confiance et d'assurance.

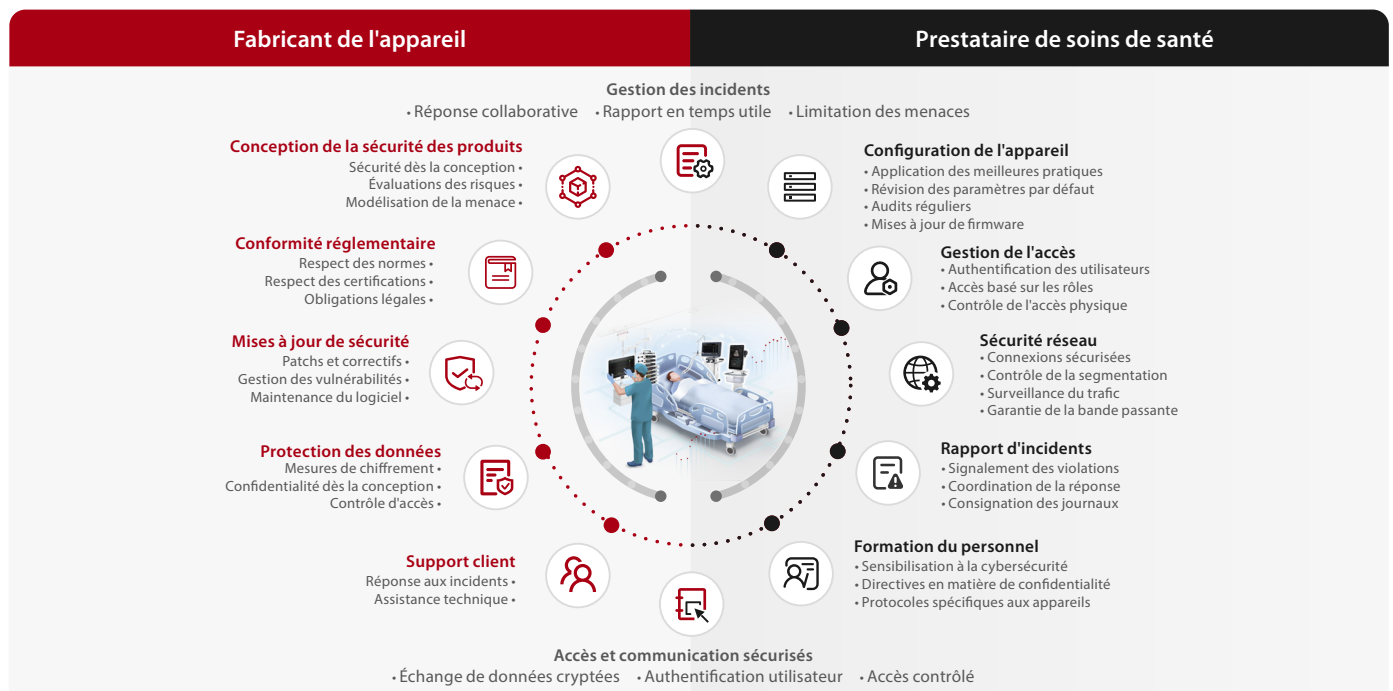


Protéger dans le partenariat : Responsabilité partagée

Mindray pense que la cybersécurité dans le secteur de la santé et des dispositifs médicaux est une responsabilité partagée. La nature interconnectée des dispositifs médicaux nécessite une collaboration entre les fabricants et les prestataires de soins de santé afin de garantir des pratiques de cybersécurité solides. Les fabricants d'appareils ont la responsabilité de concevoir des produits sûrs en respectant les réglementations industrielles, en intégrant des fonctions de sécurité robustes lors de la conception et du développement, en effectuant des tests rigoureux et en fournissant des mises à jour logicielles et des correctifs en temps voulu pour répondre aux vulnérabilités. Ils doivent également proposer des directives claires sur l'utilisation sécurisée des appareils et en assurer la maintenance. D'autre part, les prestataires de soins de santé jouent un rôle crucial dans la gestion de la sécurité dès lors que le dispositif est déployé dans leurs systèmes. Il s'agit notamment de mettre en œuvre des configurations de réseau appropriées, de contrôler l'accès physique aux appareils et d'effectuer une surveillance constante à la recherche de menaces potentielles. Les organismes de santé doivent également veiller à ce que leur personnel soit correctement formé aux meilleures pratiques en matière de sécurité, qu'il ait une meilleure compréhension des caractéristiques techniques et qu'il suive des protocoles pour protéger les appareils et les données sensibles qu'ils manipulent. Grâce à cette collaboration, les fabricants et les prestataires de soins de santé contribuent à un écosystème sûr, en conciliant l'innovation avec la sécurité des patients et la protection des données.

Ce principe n'est pas seulement défendu par Mindray, il est également soutenu par de nombreux instituts de recherche, universités et pairs du secteur. Selon l'International Medical Device Regulators Forum (IMDRF)[7], la cybersécurité des dispositifs médicaux nécessite une collaboration étroite entre les fabricants de dispositifs et les prestataires de soins de santé, ce qui souligne l'importance de l'applicabilité d'une responsabilité partagée tout au long du cycle de vie du dispositif. Cette approche assure que les parties impliquées dans l'utilisation et la gestion des dispositifs médicaux sont équipées pour prévenir les menaces de cybersécurité, améliorant ainsi la résilience globale. La FDA[8] souligne en outre que la protection contre les cyberintrusions et la réaction à celles-ci sont une responsabilité partagée par l'ensemble de l'écosystème des dispositifs médicaux, y compris les établissements de santé, les patients, les fournisseurs et les fabricants de dispositifs. Cette collaboration permet d'identifier et d'atténuer plus efficacement les risques, et d'assurer une réponse et une récupération après accident plus rapide.

En promouvant cette notion de responsabilité partagée, Mindray s'efforce de collaborer étroitement avec toutes les parties prenantes concernées, en particulier les prestataires de soins de santé, afin de bien équiper toutes les parties en matière de mesures préventives et réactives contre les défis de la cybersécurité, et de préserver en fin de compte la santé et la sécurité des patients.



[7] https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf
[8] https://www.fda.gov/media/119933/download

Modèle de cybersécurité des produits Mindray

Mindray met en œuvre un cadre solide, développé en interne, pour assurer une protection complète des dispositifs médicaux, en guidant et en alignant les efforts de cybersécurité au sein des diverses équipes et divisions de Mindray.

- Gouvernance et gestion des risques
- Conception et développement sécurisés
- Contrôles et mesures de protection
- Maintenance et gestion du cycle de vie
- Gestion des incidents
- Protection des données.

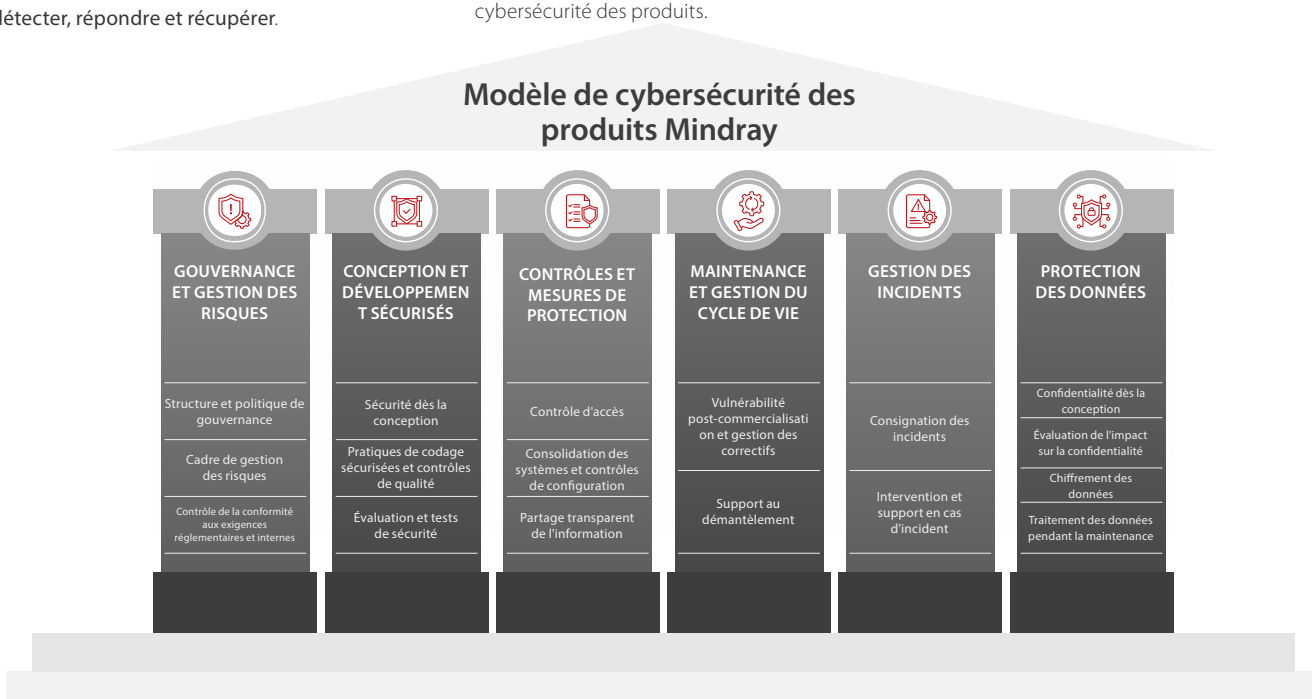
Modèle de cybersécurité des produits Mindray

La cybersécurité des produits Mindray est régie par le Modèle de cybersécurité des produits Mindray, un cadre robuste développé en interne pour assurer la protection complète de nos dispositifs médicaux, guider et aligner les efforts de cybersécurité à travers les différentes équipes et divisions de Mindray. Notre modèle est fondé sur les principes du cadre de cybersécurité NIST (CSF)[9], qui met l'accent sur six éléments fondamentaux : **gouverner, identifier, protéger, détecter, répondre et récupérer**.

En nous appuyant sur cette base reconnue, nous avons adapté notre modèle pour répondre aux défis et aux exigences de l'industrie des dispositifs médicaux.

Le modèle comprend six piliers et dix-sept éléments. Chaque pilier intègre et s'aligne sur les normes internationales et les exigences réglementaires pour garantir une couverture complète de tous les aspects critiques de la cybersécurité des produits.

Le pilier **Gouvernance et gestion des risques** garantit une approche structurée de la gestion des risques liés à la cybersécurité, conformément aux normes du secteur et aux exigences réglementaires. **La conception et le développement sécurisés** intègrent les pratiques de sécurité dans le cycle de vie du produit dès le départ, en s'appuyant sur les meilleures pratiques telles que le codage sécurisé et les tests rigoureux. **Les mesures de protection et les contrôles** mettent en œuvre des garanties techniques telles que les contrôles d'accès et le renforcement des systèmes pour se protéger contre les accès non autorisés et les cybermenaces. **La maintenance et la gestion du cycle de vie** se concentrent sur la gestion continue de la sécurité des appareils, grâce à une gestion efficace des vulnérabilités et à une mise au rebut sécurisée. Le pilier **Gestion des incidents** établit des processus de détection, de réponse et d'analyse des incidents de cybersécurité, en mettant l'accent sur la responsabilité partagée entre Mindray et les prestataires de soins de santé. Enfin, le pilier de **la protection des données** assure la confidentialité, l'intégrité et la disponibilité des données des patients grâce à la prise en compte du respect de la confidentialité dès la conception, à l'évaluation de l'impact sur la confidentialité, au cryptage et à des contrôles rigoureux du traitement des données.



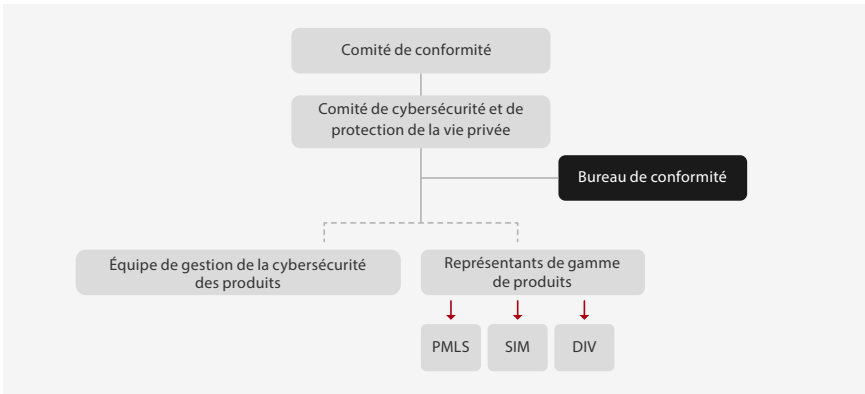
[9] https://www.nist.gov/cyberframework

Gouvernance et gestion des risques

La cybersécurité des produits Mindray repose sur les bases solides de politiques de gouvernance structurées, de cadres de gestion des risques et de méthodologies de contrôle de la conformité.

Structure et politique de gouvernance

En rationalisant le processus de prise de décision stratégique et de mise en œuvre des politiques, nous avons établi des canaux de responsabilité et de communication clairs.



Le comité de conformité, composé des plus hauts responsables de l'entreprise, guide et supervise la cybersécurité chez Mindray. Ce comité supervise différents domaines, notamment les stratégies et les plans de conformité en matière de cybersécurité et de protection de la confidentialité. Le comité dirige les initiatives globales de l'entreprise ainsi que la conformité pertinente et prend des décisions sur la feuille de route principale.

Le comité de cybersécurité et de protection de la confidentialité formule les principes et les objectifs de l'entreprise en matière de cybersécurité et de protection de la production. Ce comité dirige et passe en revue les cadres internes pertinents et gère et supervise la mise en œuvre complète dans les unités opérationnelles à travers les régions.

Le Bureau de conformité soutient les activités quotidiennes des comités, tient l'équipe informée des diverses lois et réglementations et coordonne la formulation des politiques et des cadres. Ce bureau assiste les comités dans la supervision et l'audit de la bonne mise en œuvre des mesures de cybersécurité et de protection de la confidentialité, en prenant l'initiative de veiller à l'adaptation effective des politiques par les unités opérationnelles et les départements dans toutes les régions.

L'Équipe de gestion de la cybersécurité des produits joue un rôle crucial en soutenant le comité et le bureau de conformité en s'occupant des aspects techniques de la cybersécurité des dispositifs. Cette équipe est chargée d'établir des exigences et des normes internes en matière de cybersécurité. Les principales responsabilités consistent à identifier, promouvoir et appliquer les technologies essentielles de cybersécurité et les méthodes de test, à surveiller et évaluer les vulnérabilités et à fournir un soutien technique à la recherche dans des domaines critiques tels que la réponse aux vulnérabilités et le développement de logiciels sécurisés.

Les représentants des gammes de produits, en tant qu'entité de première ligne pour le développement des produits, sont chargés de mettre en œuvre les exigences et les normes formulées par le comité, le bureau et l'équipe de gestion de la cybersécurité des produits tout au long du cycle de vie des produits, tels que le développement, la production, la maintenance, etc. Ils veillent à ce que les mesures de cybersécurité établies soient intégrées dans chaque produit. Ils fournissent également un retour d'information en temps utile à la direction concernant les besoins et les problèmes liés à la cybersécurité, et coopèrent à l'amélioration des capacités globales de gestion de la cybersécurité des produits du groupe.

Cadre de gestion des risques

Un cadre solide de gestion des risques constitue la pierre angulaire de la stratégie de cybersécurité de Mindray, nous permettant d'identifier, d'évaluer et d'atténuer les vulnérabilités potentielles en matière de cybersécurité de manière systématique tout au long du cycle de vie du produit.

Notre cadre de gestion des risques commence par des évaluations détaillées des menaces à l'aide du cadre de modélisation des menaces STRIDE, qui identifie catégoriquement les menaces potentielles liées à l'usurpation, à la falsification, à la répudiation, à la divulgation d'informations, au déni de service et à l'élévation de privilèges. Ce processus nous permet de comprendre les formes possibles de menaces et d'évaluer leur impact potentiel sur la sécurité des dispositifs.

Nos efforts en matière de gestion des risques comprennent l'établissement d'un plan détaillé de gestion des risques, d'une nomenclature des logiciels, d'une évaluation des risques liés aux vulnérabilités connues et de rapports sur les tests de pénétration et d'analyse. Ces documents donnent un aperçu complet des mesures de sécurité déployées et témoignent de notre engagement en faveur de la sécurité des produits. Les résultats de ces analyses nous permettent de mieux concevoir nos contrôles des risques, qui sont intégrés dans des exigences Notre analyse des risques de cybersécurité n'est pas un effort ponctuel mais une démarche qui s'ancre dans un processus continu étendu tout le cycle de vie du produit, garantissant ainsi que les menaces potentielles sont identifiées et atténuées de manière précoce et rapide. Ainsi, la probabilité de failles de sécurité après le déploiement s'en trouve amoindrie.

Contrôle de la conformité aux exigences réglementaires et internes

Chez Mindray, la surveillance de la conformité réglementaire est une composante essentielle de notre stratégie de cybersécurité, garantissant que les normes internes s'alignent sur les exigences réglementaires et les attentes du secteur. Le comité de cybersécurité et de protection de la confidentialité s'assure que les exigences réglementaires sont évaluées en permanence et que tout changement pertinent est rapidement intégré dans les normes et exigences de développement des produits. Pour aller au delà de la conformité minimale, Mindray mène des recherches et des analyses comparatives continues par rapport aux meilleures pratiques du secteur. Cette approche proactive permet aux mesures de sécurité de l'entreprise d'être robustes et à jour, reflétant les dernières avancées et tendances en matière de cybersécurité.

Pour s'assurer que les normes de sécurité conçues sont mises en œuvre comme prévu, Mindray utilise également une "matrice de cybersécurité et de conformité des données" systématique pour vérifier que les pratiques de développement et de fabrication sont conformes aux lignes directrices et aux exigences établies. Cette matrice sert de liste de contrôle pour les audits internes et garantit le contrôle de la qualité.

Conception et développement sécurisés

Sécurité dès la conception

Comme illustré précédemment, la sécurité dès la conception est l'idéologie fondamentale de Mindray. Cette notion intègre les principes et les exigences de sécurité dès le départ et à chaque étape du développement du produit. Ce concept fondamental est intégré et se reflète dans nos systèmes robustes et nos politiques rigoureuses, qui garantissent que les spécifications de sécurité sont prises en compte dès le départ et ancrées dans la culture de conception des produits. Les activités comprises dans le cycle de développement de la sécurité (SDL) sont profondément intégrées à notre processus global de développement de produits, ce qui nous permet d'adopter les meilleures pratiques en matière de développement de la cybersécurité des produits.

Le principe de **la défense en profondeur** est un aspect clé de notre approche de la sécurité dès la conception, qui est à la base de tous nos produits. Cette stratégie de défense multicouche garantit que même si une mesure de sécurité s'avère inefficace, d'autres couches de protection demeurent en place pour sécuriser l'appareil et ses données.

Pratiques de codage sécurisées et contrôles de qualité

En nous appuyant sur les principes de la sécurité dès la conception, nous avons établi des **normes complètes et systématiques** basées sur les normes de la Commission électrotechnique internationale (CEI), les meilleures pratiques du secteur et notre vaste expérience en développement logiciel. Nos normes de codage sécurisé couvrent divers aspects critiques du codage, **notamment la validation des entrées, la gestion des erreurs et l'authentification**.
Ces principes permettent de remédier aux failles de sécurité potentielles lors de la phase de codage, ce qui réduit considérablement le risque d'introduire des vulnérabilités dans nos produits finaux.

Le contrôle des processus et **les normes d'assurance qualité** figurent également parmi les éléments clés du codage sécurisé. Grâce à notre **procédure de vérification du code en trois étapes**, qui comprend l'évaluation de la liste de contrôle à l'aide des normes de base établies, l'examen du code statique à l'aide d'outils avancés et la validation humaine manuelle, Mindray s'assure que tous les ingénieurs en développement de logiciels respectent les normes de codage sécurisées, et ce tout au long du processus de développement.

En outre, Mindray met l'accent sur l'amélioration continue et le partage des connaissances entre les développeurs. Tous les développeurs suivent des formations régulières sur les techniques de codage sécurisées et se tiennent au courant des derniers exploits en matière de sécurité et des méthodes d'atténuation. Cette approche proactive garantit que nos ingénieurs sont bien équipés pour faire face aux risques émergents.

Évaluation et tests de sécurité

Parallèlement aux pratiques de codage sécurisé, Mindray mène des évaluations et des tests de sécurité rigoureux pour s'assurer que les vulnérabilités potentielles sont identifiées et atténuées, et que les mesures de sécurité mises en œuvre sont testées et validées.

- **Analyse de vulnérabilité :**
  Des outils avancés sont utilisés pour analyser régulièrement nos produits et nos systèmes afin de détecter les vulnérabilités potentielles, d'identifier les risques de manière proactive et efficace et d'appliquer rapidement les correctifs nécessaires.
- **Tests de pénétration :**
  Des cyberattaques globales simulées sont menées pour tester la résilience des appareils dans des circonstances réelles.
- **Évaluation de sécurité par un tiers :**
  Des organisations tierces autonomes sont engagées pour des évaluations de sécurité, fournissant un niveau supplémentaire de validation et d'assurance, et garantissant que nos produits répondent aux normes industrielles et réglementaires.

En intégrant des pratiques rigoureuses d'évaluation et de test de la sécurité à ses principes de conception, Mindray s'efforce de garantir que ses dispositifs médicaux sont sécurisés dès leur conception et résilients face aux cybermenaces potentielles. Cette approche globale illustre notre engagement à fournir des dispositifs médicaux sûrs, fiables et conformes, afin de donner confiance à nos utilisateurs dans le paysage en constante évolution de la cybersécurité.

Contrôles et mesures de protection

Conformément au principe de responsabilité partagée, la mise en place des fonctions et moyens de sécurité nécessaires dans les configurations des dispositifs médicaux est de la responsabilité essentielle de Mindray en tant que fabricant de dispositifs.

Contrôle d'accès

Le contrôle d'accès, qui comprend des mécanismes tels que **l'authentification, l'autorisation et la comptabilité**, est un élément de sécurité essentiel pour les dispositifs médicaux, car il garantit que seules les personnes autorisées peuvent accéder aux informations sensibles et aux fonctionnalités du système. Les dispositifs médicaux de Mindray sont équipés d'une fonctionnalité de **contrôle d'accès basé sur les rôles** (RBAC), qui attribue les autorisations d'accès en fonction des rôles des utilisateurs individuels au sein de l'organisation. Cela permet aux organisations de n'accorder que l'accès minimum aux utilisateurs en fonction de leurs besoins opérationnels, réduisant ainsi le risque d'accès non autorisé aux fichiers ou de modifications arbitraires de la configuration.

Les appareils Mindray, s'ils peuvent varier en fonction du modèle, comportent plusieurs mesures de protection supplémentaires pour améliorer encore la sécurité d'accès. Ces mesures incluent notamment, mais sans s'y limiter, les éléments suivants :

Mécanisme de verrouillage	Après un certain nombre de tentatives de connexion infructueuses, l'appareil est verrouillé, ce qui empêche tout accès non autorisé via des attaques par force brute.
Déconnexion automatique	Pour éviter tout accès non autorisé lorsqu'un appareil est laissé sans surveillance, les sessions sont interrompues après une période d'inactivité.
Gestion des mots de passe	Les appareils Mindray permettent de personnaliser les politiques de mot de passe. Nous conseillons également aux utilisateurs de changer régulièrement de mot de passe.
Authentification centralisée et sécurisée	Mindray s'appuie sur des systèmes avancés et sécurisés pour stocker les informations d'identification et procéder à l'authentification. Ces systèmes adoptent une technologie de chiffrement pour protéger les données d'identification et gérer les privilèges, garantissant ainsi une authentification sécurisée et réduisant le risque de vol ou d'utilisation abusive des données d'identification.
Changements majeurs de configuration contrôlés	Les changements majeurs, tels que la mise à niveau du système d'exploitation, sont contrôlés par des contrôles d'accès stricts, permettant uniquement au personnel autorisé d'effectuer les mises à niveau.

Consolidation des systèmes et contrôles de configuration

La consolidation des systèmes est une autre étape cruciale pour renforcer nos appareils en minimisant la surface d'attaque.

Les éléments clés des pratiques de renforcement du système de Mindray, qui peuvent varier selon le modèle, sont les suivants :

Directives de renforcement du système d'exploitation (OS)	Un ensemble détaillé de méthodes et d'exigences de configuration est défini pour les différentes fonctions du système d'exploitation. Ces exigences garantissent que le système d'exploitation est configuré de manière sécurisée et unifiée par toutes les équipes de développement, ce qui permet de mettre en œuvre les exigences de manière structurée.
Liste blanche des processus et applications	Seuls les applications et processus approuvés sont autorisés à fonctionner sur les appareils, ce qui empêche les logiciels ou activités non autorisés de s'exécuter et de compromettre potentiellement le système.
Programmes anti-virus et anti-malware	Les appareils Mindray sont conçus pour fonctionner de manière transparente avec les programmes de protection contre les virus et les logiciels malveillants, garantissant ainsi une protection continue contre ces logiciels malveillants.
Pare-feu	Les appareils Mindray basés sur Microsoft Windows utilisent le pare-feu intégré pour restreindre l'accès externe et contrôler les applications exécutées dans l'appareil.
Désactivation des vecteurs de risque inutiles	En fonction des besoins et des circonstances de l'entreprise, les services, les ports et les fonctions inutiles, tels que la connexion à distance et l'exécution automatique de l'USB, sont désactivés afin de minimiser l'exposition à des attaques potentielles.
Mode kiosque	Les appareils dotés du mode kiosque réduisent considérablement la surface d'attaque en limitant l'accès des utilisateurs aux seules fonctions essentielles, en empêchant les activités non autorisées et en minimisant l'accès aux informations sensibles sur les patients.
Mises à jour contrôlées du système d'exploitation et des logiciels	La mise à niveau du système d'exploitation et du logiciel de l'appareil ne peut être effectuée que par le biais de packages de mise à niveau contrôlés, vérifiés et publiés par Mindray. Seul le personnel agréé peut effectuer des mises à niveau et les mises à niveau automatiques du système d'exploitation sont désactivées afin d'éviter les changements non autorisés.

Partage transparent de l'information

Mindray s'efforce d'améliorer sans relâche son engagement à maintenir la transparence sur les mesures de sécurité mises en œuvre dans ses dispositifs. Nos principaux efforts visant à promouvoir la transparence comprennent notamment :

Livres blancs sur la cybersécurité

Nous fournissons des livres blancs complets sur la cybersécurité pour chaque gamme de produits, détaillant nos mesures, contrôles et pratiques de sécurité, et offrant aux parties prenantes une compréhension claire de nos efforts en matière de cybersécurité. Veuillez contacter Mindray pour obtenir le livre blanc spécifique à votre produit.

Manuels d'utilisation des produits

Nos manuels d'utilisation contiennent des descriptions détaillées et des recommandations concernant les fonctions de cybersécurité de nos produits, ce qui permet aux utilisateurs de comprendre les mécanismes de sécurité mis en place et la manière de les utiliser efficacement.

Déclaration du fabricant sur la sécurité des dispositifs médicaux (MDS2)

Mindray fournit la MDS2 sur demande, afin d'aider les prestataires de soins de santé à évaluer les risques de cybersécurité et les mesures d'atténuation associées à nos dispositifs. Ce document décrit les capacités de sécurité de nos dispositifs médicaux, offrant une transparence sur la façon dont nos produits sont conformes aux exigences de sécurité nécessaires et aux normes opérationnelles.

Nomenclature des logiciels (SBOM)

Pour les appareils concernés, nous proposons également la nomenclature des logiciels (SBOM) sur demande. La SBOM fournit une liste détaillée des composants logiciels utilisés dans nos dispositifs médicaux, ce qui permet aux parties prenantes d'identifier toutes les bibliothèques ou dépendances tierces susceptibles de présenter des risques. Cette transparence est essentielle pour comprendre les vulnérabilités potentielles et maintenir l'intégrité de l'architecture logicielle de l'appareil.

Aide aux plans de déploiement

Nous aidons les prestataires de soins de santé à élaborer des plans de déploiement, en veillant à ce que les fonctions de sécurité de nos dispositifs soient correctement intégrées dans l'environnement déployé et gérées efficacement. Ce support comprend des conseils sur l'installation, la configuration et la maintenance continue.

Maintenance et gestion du cycle de vie

La maintenance post-commercialisation illustre la responsabilité de Mindray dans la protection des patients, de leurs données et des opérations de soins de santé, du déploiement à la mise hors service.

Vulnérabilité post-commercialisation et gestion des correctifs

Les produits Mindray utilisent des systèmes d'exploitation tiers, tels que Microsoft Windows et Linux. Pour garantir que l'utilisation de ces systèmes d'exploitation ne présente aucun risque, nous avons développé **une stratégie complète de gestion des correctifs** pour surveiller en permanence les vulnérabilités pertinentes, évaluer leur impact sur nos dispositifs et déployer des correctifs pour résoudre ces problèmes.

Pour les produits fonctionnant sous Microsoft Windows, l'évaluation de l'impact des correctifs de sécurité et des hotfixes nouvellement publiés commence généralement dans les 48 heures suivant la prise de connaissance par Mindray du nouveau correctif de sécurité. Nous évaluons l'impact des correctifs afin de déterminer s'ils doivent être appliqués immédiatement ou s'ils peuvent être intégrés dans des mises à jour programmées. Pour les correctifs critiques nécessitant une attention immédiate, nous fournissons **des instructions détaillées pour une mise à jour rapide**. Cela permet de s'assurer que les vulnérabilités urgentes sont traitées rapidement et en toute sécurité. Dans d'autres cas, les correctifs sont publiés en l'espace de quelques semaines et notifiés aux utilisateurs de l'appareil, ce qui garantit que les utilisateurs sont tenus informés et que nos appareils restent protégés. Pour nos produits basés sur Linux, nous effectuons une analyse tous les six mois. Étant donné que les plateformes Linux des dispositifs médicaux sont généralement personnalisées pour des usages spécifiques, la publication des correctifs se fait généralement sous la forme d'une mise à jour complète du logiciel. Si la menace ne peut être résolue par la seule installation des correctifs du système d'exploitation, une mise à jour du logiciel du système peut être effectuée.

Les packages de mise à niveau font l'objet **d'une validation de checksum** avant leur installation. Cette approche garantit l'intégrité et l'authenticité du package de mise à niveau, empêchant ainsi toute modification non autorisée. En outre, notre processus de mise à niveau est rigoureusement contrôlé, car seul le personnel autorisé peut effectuer des mises à niveau à l'aide d'un outil développé par Mindray et protégé par un mot de passe. Les mises à jour automatiques du système d'exploitation sont désactivées afin d'éviter toute modification non autorisée.

Support fin de vie et déclassement

S'il existe des variations entre les différents marchés, nous fournissons à nos clients de manière proactive **des lettres détaillées de fin de vie (EOL)** lorsqu'un produit arrive en fin de vie utile. Ces lettres contiennent des informations cruciales sur l'interruption des services de réparation, la disponibilité des pièces et les délais de l'assistance technique, ce qui laisse aux clients suffisamment de temps pour planifier des remplacements ou des mises à niveau.
Cette approche transparente garantit que les clients sont bien informés et peuvent assurer une continuité opérationnelle tout en abandonnant les anciens modèles, ce qui renforce l'engagement de Mindray en faveur d'un service et d'un support clients de grande qualité.

Pour les appareils qui doivent être mis au rebut, il est essentiel de gérer le processus de manière sûre et responsable, en empêchant tout accès non autorisé aux informations sensibles et en veillant à ce que les appareils ne présentent aucun risque après leur mise hors service. Mindray assiste et permet aux prestataires de soins de santé de désaffecter leurs appareils en toute sécurité, et nous conseillons également les prestataires de soins de santé afin qu'ils se conforment aux réglementations locales ainsi qu'aux directives internationales, y compris celles de la FDA et du NIST, concernant la mise au rebut des dispositifs électroniques, en veillant à ce que les dispositifs mis hors service soient éliminés d'une manière sûre et conforme à la loi.

GESTION DES INCIDENTS

Dans le contexte du secteur des soins de santé et des dispositifs médicaux, la gestion des incidents est reconnue comme une responsabilité partagée. Seule une collaboration entre les prestataires de soins de santé et les fabricants de dispositifs médicaux peut permettre une prévention et une réaction efficaces aux cyberattaques. Grâce aux approches détaillées plus avant, Mindray vise à encourager une démarche coopérative en matière de cybersécurité, en veillant à ce que Mindray et que les prestataires de soins de santé soient bien équipés pour répondre aux menaces potentielles en matière de sécurité et les atténuer.

Consignation des incidents

La consignation efficace des incidents est un élément crucial que les fabricants de dispositifs médicaux peuvent proposer. Les dispositifs médicaux de Mindray sont équipés de journaux dédiés à la consignation des opérations liées à la sécurité, fournissant une trace complète des activités qui peut s'avérer cruciale pour l'analyse et la réponse aux incidents. Nous travaillons en étroite collaboration avec les prestataires de soins de santé dans le processus d'exportation, de gestion et d'analyse des journaux de sécurité dans leurs environnements et besoins spécifiques.

Nos appareils sont également conçus avec divers mécanismes de sauvegarde et de récupération des données afin de garantir que les informations critiques en matière de sécurité sont préservées et peuvent être restaurées en cas de défaillance ou d'incident du système. Cette résilience permet de maintenir l'intégrité et la disponibilité des journaux de sécurité et de soutenir les efforts continus en matière de sécurité.

Intervention et support en cas d'incident

Mindray a mis en place des équipes dédiées pour superviser le processus de réponse aux incidents, et surveiller et étudier en continu les incidents émergents susceptibles d'affecter nos appareils. En cas d'incidents de sécurité détectés ou signalés, les équipes, en collaboration avec les unités opérationnelles, évaluent les risques, élaborent des plans d'intervention et mettent en œuvre des mesures correctives. Les directives relatives à la réponse aux incidents de cybersécurité ont été établies pour permettre une approche normalisée et unifiée entre les différentes parties prenantes. Dans le cas du reporting réglementaire obligatoire, nous travaillons en étroite collaboration avec les autorités compétentes pour assurer une communication précise et opportune. Tout au long du processus, nous maintenons une communication étroite avec nos clients en travaillant ensemble pour évaluer rapidement la situation et mettre en œuvre les mesures correctives nécessaires afin de minimiser l'impact et maintenir la sécurité des appareils.

En ce qui concerne les fonctionnalités de support supplémentaires, les dispositifs médicaux de Mindray sont dotés de fonctions qui assurent la continuité des activités, même en cas d'incidents liés à la cybersécurité. En fonction de leur capacité, certains dispositifs utilisent des mécanismes tels que le backfill et la synchronisation des données pour garantir qu'aucune information critique sur les patients n'est perdue pendant les pannes de réseau. Certains appareils sont également dotés d'un réseau à plusieurs niveaux qui permet d'isoler les risques entre l'appareil et le réseau de l'hôpital. En outre, le fait de fonctionner dans un environnement de réseau à la fois câblé et sans fil assure que, même si l'un des dispositifs du réseau tombe en panne, les dispositifs peuvent continuer à fonctionner normalement.

En aidant les prestataires de soins de santé avec des mesures systématiques de réponse aux incidents et de support technique, Mindray s'efforce de permettre à ses partenaires de gérer et d'atténuer efficacement les incidents de cybersécurité tout en améliorant la résilience opérationnelle.

PROTECTION DES DONNÉES

Confidentialité dès la conception

Du point de vue de l'entreprise, Mindray s'appuie sur les normes internationales et les meilleures pratiques du secteur pour mettre en place un système de gestion de la sécurité de l'information et de protection de la confidentialité axé sur les risques. Ce système gère l'ensemble du cycle de vie des données, y compris la collecte, la transmission, l'utilisation, le partage, le stockage et la suppression, en adhérant aux principes de légalité, d'équité, d'honnêteté, d'ouverture et de transparence, dans le but de protéger **la confidentialité, l'intégrité et l'exactitude** de toutes les données personnelles traitées par Mindray. Grâce à son système de gestion robuste, Mindray a obtenu les certifications ISO/IEC 27001 et ISO/IEC 27701 et affine en permanence ses exigences en matière de protection de la confidentialité.

S'appuyant sur une telle culture d'entreprise et une telle sensibilisation à la protection de la vie privée, et avec l'engagement de protéger et de respecter la vie privée et les données de nos clients et patients, Mindray a intégré les principes fondamentaux de "**Confidentialité dès la conception**" et de "**Confidentialité par défaut**" dans le processus de développement des produits (voir la figure à la page 6).

Mindray s'efforce d'intégrer la protection de la confidentialité en tant que valeur fondamentale dans tous les aspects de son processus de développement de produits.

L'engagement de Mindray en faveur de la protection de la confidentialité dès la conception nous a permis d'établir une relation de confiance avec les prestataires de soins de santé et les patients. Nous pouvons ainsi traiter les données sensibles de nos utilisateurs selon les normes les plus strictes en matière de sécurité et de confidentialité.

Ces principes sont intégrés dès les premières phases de conception et de planification du développement du produit, en appliquant les lignes directrices de référence pour les autorisations, la journalisation, le chiffrement et la dépersonnalisation/anonymisation, etc. En intégrant la protection de la confidentialité dès la conception, nous nous assurons que les mesures de protection de la vie privée ne sont pas simplement une fioriture, mais font partie intégrante de l'architecture du produit, ce qui permet de répondre de manière proactive aux préoccupations en matière de protection de la vie privée, de renforcer la confiance de l'utilisateur et et de se conformer aux exigences réglementaires.

Évaluation de l'impact sur la confidentialité

Pour Mindray, le respect des réglementations en matière de protection des données et de la vie privée n'est pas simplement une obligation légale : il constitue une pierre angulaire qui nous aide à atténuer les risques associés aux violations de données et à renforcer la confiance de nos parties prenantes. Afin d'identifier de manière exhaustive les failles et les risques concernant le respect de la confidentialité et la protection des données, nous avons introduit l'évaluation de **l'impact sur la confidentialité (Privacy Impact Assessment ou PIA)** dans le processus de développement des produits afin de garantir la mise en oeuvre de mesures de contrôle efficaces conformément aux exigences réglementaires applicables. Le processus PIA implique une analyse rigoureuse des risques potentiels pour la vie privée, suivies de la mise en œuvre de stratégies d'atténuation appropriées. Une telle évaluation robuste et une telle mise en œuvre de contrôle permettent non seulement à Mindray mais aussi à nos clients de se conformer aux lois et réglementations pertinentes, telles que le **RGPD**, l'HIPAA ou le PIPL. Nous avons également publié un livre blanc **RGPD**[10] détaillé, qui explique comment Mindray se conforme à l'une des normes internationales les plus rigoureuses en matière de protection des données. Le livre blanc présente un aperçu de la gouvernance d'entreprise, des contrôles internes et des mécanismes de traitement des données personnelles de Mindray, en gage de notre engagement à maintenir des normes élevées en en matière de sécurité et confidentialité des données.

[10] https://www.mindray.com/content/dam/xpace/en/legal/GDPR.pdf

Chiffrement des données

S'appuyant sur les principes de confidentialité dès la conception, le chiffrement des données est la pierre angulaire de l'approche de Mindray en matière de protection des données.
Le chiffrement des données est un mécanisme de défense essentiel pour protéger les informations sensibles contre les accès non autorisés et les violations. Mindray utilise des méthodes de chiffrement complètes conçues pour sécuriser les données en transit et au repos. Chaque ligne de produits Mindray utilise les protocoles et les méthodes les plus adaptés à leur propre conception et à leurs besoins commerciaux spécifiques, garantissant ainsi une protection adéquate de toutes les données.

Données en transit

Les normes DICOM et HL7 sont adoptées lors de la transmission des données, qui prend en charge divers protocoles de cryptage, notamment TLS 1.2 avec le chiffrement AES-256. Pour les communications sans fil, les appareils Mindray prennent en charge la norme WPA/WPA2 Enterprise, qui assure un chiffrement solide des données transmises sur les réseaux Wi-Fi.

Données au repos

Bien que nous encouragions la minimisation de l'enregistrement et du stockage des données personnelles, dans les circonstances nécessaires, les appareils Mindray mettent en œuvre des algorithmes sécurisés, tels que AES-256, pour chiffrer les données au repos afin d'empêcher l'utilisation abusive des données en cas d'accès non autorisé.

Données affichées

Les informations personnelles identifiables (IPI) affichées à l'écran ou dans les rapports exportés peuvent être configurées pour être masquées. Cette flexibilité permet de mieux contrôler la gestion de l'accès aux informations confidentielles.

Export de données

Pour les sauvegardes sur USB, la compression 7z avec un chiffrement robuste est utilisée pour sauvegarder les données archivées, garantissant que les ensembles de données sont compressés et stockés en toute sécurité. Les appareils Mindray prennent également en charge les techniques d'anonymisation et de pseudonymisation lors de l'exportation ou de la sauvegarde de supports sensibles sur des disques durs.

En utilisant des technologies de chiffrement avancées et en maintenant des normes rigoureuses de protection des données, les appareils Mindray permettent aux utilisateurs de protéger les données de manière appropriée à tout moment, qu'elles soient transmises, stockées, affichées ou exportées.

Traitement des données pendant la maintenance

Lorsqu'une maintenance s'avère nécessaire, il se peut que notre personnel doive accéder aux appareils ou les envoyer à nos centres de réparation. Dans le cas où les données sur les appareils ne sont pas entièrement effacées, anonymisées ou désensibilisées, Mindray a établi des protocoles stricts et des réglementations internes solides pour le traitement des données pendant la maintenance, afin de garantir que les informations sensibles soient correctement protégées ou détruites pour empêcher tout accès non autorisé.

Mindray fournit des conseils complets aux prestataires de soins de santé sur la gestion sécurisée des données pendant la maintenance d'un dispositif. L'une des mesures clés concerne la capacité d'effacement sécurisé des données. Elle est fortement recommandée dans la mesure où elle permet de s'assurer qu'aucune information sensible ne reste sur les appareils entretenus.

Dans chaque région, les équipes locales constituent la première ligne d'évaluation et déterminent si les problèmes peuvent être résolus à leur niveau. Dans les régions où le retour des appareils et des journaux en Chine est interdit, tous les problèmes sont résolus localement. Dans les cas où le retour des appareils et des journaux en Chine à des fins de dépannage n'est pas interdit et s'avère inévitable, l'équipe locale procède à un examen approfondi pour confirmer que les données sensibles ont été correctement supprimées, ce qui garantit la conformité avec les réglementations internationales en matière de protection des données et de transferts transfrontaliers. Il est également possible d'appliquer des méthodes de désensibilisation des données, en modifiant les informations sensibles pour les rendre intraçables ou non identifiables, tout en conservant leur pertinence pour le diagnostic. Il peut s'agir de masquer ou de modifier des données personnelles identifiables, des tests d'anonymisation permettant de vérifier que les données restantes ne peuvent pas être reliées à des patients individuels.

Par ailleurs, notre personnel adopte **des mesures strictes de contrôle d'accès**, selon le principe du moindre privilège. Cette approche garantit que seules les personnes autorisées ont accès à l'appareil et aux données qu'il contient, et que leur accès est limité au strict nécessaire que leur rôle requiert. Tout le personnel interne ou tiers autorisé est soumis à des obligations de confidentialité, garantissant que les travailleurs traitent les données résiduelles avec le plus haut niveau de discrétion et de sécurité.

Dans les cas de maintenance à distance, Mindray utilise des outils sécurisés qui font l'objet d'une gestion stricte de la part de l'équipe de gestion des risques et des contrôles. L'autorisation du client est requise avant toute activité de maintenance à distance. En outre, conformément au principe de nécessité minimale, seules les données essentielles requises pour la maintenance sont accessibles afin de minimiser le risque d'exposition des données. Des procédures de contrôle et de clôture des sessions sont mises en place pour garantir que les sessions d'accès à distance sont gérées en toute sécurité et clôturées une fois les tâches de maintenance terminées.

Mindray s'engage à respecter les normes les plus strictes en matière de protection des données tout au long du cycle de vie de ses dispositifs médicaux. Cette approche permet non seulement de protéger les informations sensibles, mais aussi de procurer un sentiment de confiance aux utilisateurs de nos appareils, en accord avec l'engagement de Mindray à faire progresser la technologie médicale, tout en donnant la priorité à la sécurité de nos clients et de nos utilisateurs.

Remarque de fermeture

À mesure que nous évoluons, Mindray reste fidèle à sa mission de faire progresser les technologies médicales tout en garantissant les normes les plus élevées en matière de cybersécurité. Nous savons que la confiance qui nous est accordée, à nous et à nos appareils, est une responsabilité que nous devons assumer avec un dévouement inébranlable. En améliorant continuellement nos mesures de cybersécurité et en restant à l'affût des menaces émergentes, nous nous efforçons de fournir des solutions de soins de santé qui sont non seulement innovantes mais aussi sûres.

En conclusion, ce livre blanc démontre l'approche globale et proactive de Mindray en matière de cybersécurité. Il souligne notre engagement à protéger les données des patients, à garantir l'intégrité de nos dispositifs médicaux et à promouvoir une culture de la sécurité qui fait partie intégrante de notre mission. Alors que nous naviguons dans les complexités de l'ère numérique, Mindray continuera à mener avec intégrité, innovation et un dévouement inébranlable à la protection de la communauté des soins de santé.