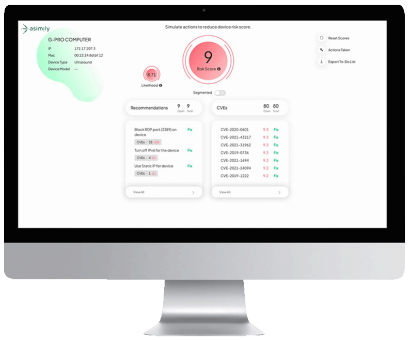
Sécurité pour l'IoMT et l'IoT



Plateforme pour la sécurité des appareils IoMT et IoT

Les hôpitaux équipés d'appareils médicaux en réseau (IoMT), mais aussi d'autres environnements fortement influencés par l'IoT tels que la production et le transport, ont des exigences complexes en matière de gestion des risques. De telles organisations doivent savoir quels sont les appareils critiques et ceux qui ne le sont pas, afin d'éviter tout travail inutile pour remédier aux risques. En cas de points faibles, elles doivent être en mesure d'identifier et de résoudre les problèmes le plus rapidement possible. Une visibilité complète, jusque dans les moindres détails de chaque appareil, en est la base.

Plateforme complète de gestion de la cybersécurité

Avec sa plateforme Insight, le fabricant américain Asimily fournit l'outil parfait pour la gestion de la cybersécurité pour l'IoT et les appareils médicaux.

La plateforme fournit en continu des connaissances pilotées par les données et des recommandations réalisables pour protéger les actifs et réagir aux vulnérabilités et aux anomalies. Elle utilise pour cela des sources de données spécifiques au secteur de la santé, telles que les indications MDS2 et les SBOM des fabricants. Asimily contribue ainsi à la réduction des risques et à la réaction aux incidents, et permet de garantir la disponibilité des appareils.

Asimily, dont le siège principal se trouve à Sunnyvale, en Californie, a été fondée en 2017 et s'est établie depuis comme leader de la sécurité IoT/IoMT dans les domaines de la santé, de l'industrie de production et du secteur public. Asimily emploie une centaine de personnes et est l'une des entreprises à la croissance la plus rapide dans le domaine de la sécurité IoT.

Asimily: les points forts

- Plateforme complète de gestion de la cybersécurité IoT/IoMT
- Permet de dresser un inventaire, de réduire les risques, de réagir aux incidents et de garantir la disponibilité des appareils
- Identifie et priorise les risques de chaque appareil en fonction de sources de données spécifiques et de la configuration de l'appareil
- Offre une correction automatisée des vulnérabilités via le bouton «Fix»
- Fonctionne avec des scanners de vulnérabilité comme Tenable et des systèmes NAC comme Cisco ISE ou Aruba Clearpass, ainsi qu'avec les pare-feu de Palo Alto, Fortinet ou Checkpoint
- Utilisable comme solution sur site ou en cloud
- Sans agent, c'est-à-dire qu'aucune installation de logiciel n'est nécessaire sur les appareils

Asimily: sécurité maximale pour l'IoMT et l'IoT

La plateforme Asimily Insight, cliniquement validée, combine un inventaire précis de tous les appareils IoMT et IoT en collectant de manière sécurisée les données des appareils et de l'activité sur place, avec une gestion efficace des vulnérabilités, y compris la priorisation des risques spécifiques à l'appareil et des recommandations pour y remédier. Asimily favorise également une réponse réactive aux incidents grâce à une vérification continue des violations de politiques basée sur le comportement.

L'utilisation d'appareils médicaux en réseau, également appelés appareils IoMT (internet of medical things), ainsi que l'utilisation d'appareils IoT en général, comporte des risques qui sont difficiles à mesurer et à éliminer – notamment parce que les appareils ne peuvent souvent pas être patchés du tout, parce que les fabricants ne fournissent que rarement des mises à jour et parce que le risque pour un appareil spécifique peut être soit critique, soit insignifiant. De plus, de nombreuses entreprises ne disposent pas d'une vue d'ensemble de leurs appareils.
Les solutions courantes de gestion des vulnérabilités n'apportent qu'une aide limitée : elles ne connaissent pas les protocoles et les risques spécifiques aux domaines médical et industriel et se limitent parfois à la simple identification des vulnérabilités, sans fournir de recommandations immédiatement utilisables pour y remédier, ni même fermer ou contourner les failles de sécurité en appuyant sur un bouton.

La plateforme Insight d'Asimily collecte toutes les informations disponibles sur les appareils en temps réel et présente les résultats sur un tableau de bord clair. Les points faibles découverts sont classés par ordre de priorité en fonction de critères médicaux ou industriels. En arrière-plan, Asimily utilise des informations spécifiques telles que les données des formulaires MDS2 des fabricants d'appareils et tient compte du type d'appareil. Ainsi, les appareils qui traitent des informations médicales protégées présentent un risque nettement plus élevé que les autres. L'évaluation CVSS des vulnérabilités, généralement utilisée par les solutions de gestion des vulnérabilités, ne tient pas compte de ces facteurs. Asimily dispose en revanche de la plus grande collection d'informations sur les fabricants de MDS2 et couvre ainsi largement plus de 1000 appareils.

Pour remédier aux problèmes et réduire les risques, Asimily travaille selon une procédure en trois étapes:

- S'il est faisable et économique de corriger une vulnérabilité → appliquer les patches.
- Si le vecteur d'attaque peut être désamorcé → appliquer le désamorçage
- Si rien de tout cela n'aboutit → segmenter/microsegmenter

Étant donné qu'Asimily donne la priorité aux problèmes à forte probabilité et à fort impact, l'effort nécessaire à leur résolution est considérablement réduit. La pratique montre qu'avec Asimily, il est possible de réduire jusqu'à 90 % l'effort manuel des analystes en gestion des vulnérabilités.

BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Téléphone +41 (0)21 533 01 60 / vente@boll.ch / www.boll.ch
BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Téléphone +41 (0)56 437 60 60 / sales@boll.ch / www.boll.ch
BOLL Europe GmbH . Ringstrasse 3 / D-89081 Ulm / Téléphone +49 (0)731 85 07 48 23 / info@boll-europe.com / www.boll-europe.com
BOLL Europe GmbH . Wienerbergstrasse 3–5 / A-1100 Wien / Téléphone +43 (0)664 46 48 580 / info@boll-europe.at / www.boll-europe.at

BOLL