Protection des dispositifs médicaux

Plateforme pour la détection et la protection des dispositifs médicaux en réseau

Les dispositifs médicaux, du perfuseur au moniteur du patient en passant par le TRM, sont de plus en plus souvent connectés au réseau informatique – on parle alors d'IoMT (Internet of Medical Things). Cependant, de nombreux organismes de santé ne disposent souvent pas d'un inventaire complet des dispositifs IoMT en réseau, sans parler de la connaissance détaillée de leurs logiciels et de leur état de sécurité. En tant qu'entreprise spécialisée, Medigate, lauréate de nombreux prix et créée en 2017 par des experts de longue date en matière de cybersécurité, s'attaque à ce problème avec sa solution du même nom. Medigate fonctionne sur la base d'un senseur qui filtre les informations pertinentes pour l'IoMT dans le trafic réseau et les transmet pour analyse. Cela permet d'automatiser une stratégie de sécurité globale pour les équipements de technologie médicale, souvent mal protégés et rarement mis à jour. En outre, grâce à ses propres recherches, Medigate a accumulé d'énormes connaissances sur les différents types d'appareils, jusqu'aux protocoles propriétaires et les versions de micrologiciels. Les connaissances ainsi acquises sur les dispositifs médicaux interconnectés sont présentées sous forme textuelle et graphique sur une console web claire. Medigate est conçu comme une plateforme ouverte, est compatible avec les dispositifs existants et fonctionne avec d'autres solutions de cybersécurité et services d'annuaire.

- Crée un inventaire exact de tous les dispositifs médicaux
- Détecte les anomalies dans l'utilisation et le trafic des appareils
- Soutient l'application de la politique de sécurité
- Empêche, avec des solutions de pare-feu, la fuite de données
- Fournit des informations directement exploitables sur l'utilisation des appareils et d'autres informations de gestion
- Interfaces avec divers fabricants de NACS, Firewalls, Asset Management, Vulnerability Management, SIEM, IT Monitoring, EMR, IPAM

MEDIGATE by Claroty

Dépliant du fabricant
Medigate

Une visibilité et une sécurité totales des équipements médicaux

Visibilité

- Détecte et identifie chaque dispositif médical connecté dans le réseau clinique
- Fonctionne avec une base de données de signatures complète qui comprend les «empreintes» de tous les types de dispositifs grâce à l'inspection approfondie des paquets
- Détecte les versions obsolètes des microprogrammes et les vulnérabilités
- Informe sur l'utilisation des appareils
- Présente l'essentiel en un coup d'œil via la console web
- Fournit un Drill-down sur les propriétés de chaque appareil

Sécurité

- Analyse le flux de données pertinent pour l'IoMT
- Connaît les protocoles de communication des appareils, à la fois les plus courants comme DICOM et les propriétaires
- Identifie en temps réel un trafic de données non habituel, les comportements anormaux des utilisateurs et les cybermenaces
- Empêche le transfert illicite de données et protège contre le vol d'informations relatives aux patients (PHI Theft)
- Permet la micro-segmentation du réseau clinique et des politiques de sécurité adaptées

Intégration

- Fonctionne avec les solutions de pare-feu existantes
- Prend en charge les services d'annuaire comme Active Directory
- S'intègre aux plateformes de systèmes de gestion de la maintenance (CMMS) et SIEM (Security Information and Event Management)

Composantes de la plateforme

- Senseur pour la surveillance du trafic sur le réseau
- Service cloud ou serveur on-premise pour l'analyse des données
- Console web pour une présentation claire et compréhensible des résultats

BOLL Engineering SA . En Budron H15 / CH-1052 Le Mont-sur-Lausanne / Telefon +41 21 533 01 60 / contact@boll.ch
BOLL Engineering AG . Jurastrasse 58 / CH-5430 Wettingen / Telefon +41 56 437 60 60 / info@boll.ch / www.boll.ch
BOLL Europe GmbH . Ringstrasse 3 / DE-89081 Ulm / Telefon +49 731 85074823 / jwa@boll-europe.com / www.boll-europe.com

BOLL IT Security Distribution