ARMIS®

BURKE
REHABILITATION
MONTEFIORE HEALTH SYSTEM

ÉTUDE DE CAS

L'hôpital De Rééducation Burke Explore Le Vaste Potentiel Des Solutions Armis

Armis est spécialisée dans les appareils connectés en réseau sur des sites informatiques et cliniques et assure la surveillance du trafic des données pour mieux protéger les informations des patients

Profil client

Établissement de soins médicaux de rééducation pour patients hospitalisés ou en ambulatoire dans l'État de New York.

Industrie

Services de santé

Environnement IT

L'hôpital de rééducation Burke dispose d'un site principal et de 10 antennes dans la région. Les 1 100 employés de la structure utilisent des appareils gérés par l'entreprise, y compris du matériel médical, des serveurs et des périphériques en réseau.

Introduction

L'hôpital de rééducation Burke est l'un des principaux établissements de soins de réadaptation pour patients hospitalisés ou en ambulatoire dans l'État de New York. L'équipe chargée de la sécurité était consciente de la nécessité d'améliorer la sécurité du réseau. Après le déploiement d'Armis, elle a pu améliorer la visibilité sur les appareils connectés au réseau, suivre l'utilisation des appareils au sein de l'organisation et voir le trafic, chiffré ou non chiffré, pour détecter et prévenir les piratages des données de patients. L'hôpital Burke continue d'appliquer Armis à de nouveaux cas d'utilisation, renforçant la sécurité et tirant des insights opérationnels à l'échelle de l'organisation.

L'hôpital de rééducation Burke à White Plains dans l'État de New York, fait partie du réseau Montefiore Health System et fait figure de leader dans le secteur des soins de rééducation. Ce prestataire de soins en activité depuis plus d'un siècle offre aux patients un service d'hospitalisation avec 150 lits disponibles dans son unité de soins de courte durée pour adultes, ainsi que des soins ambulatoires grâce à un large réseau d'établissements dans la région. L'hôpital Burke propose des soins de rééducation pour les troubles neurologiques, musculosquelettiques, cardiaques et pulmonaires résultant de maladies, de blessures ou d'opérations.

L'équipe sécurité se tourne vers Armis pour mettre à niveau la sécurité du réseau

Brian Schultz, directeur des opérations et de la sécurité du réseau depuis 10 ans à l'hôpital Burke, est toujours à l'affût de solutions innovantes et robustes pour renforcer la sécurité de l'organisation. C'est un leader actif, sur le terrain, à la tête d'une équipe de 14 professionnels de l'informatique et de la sécurité. Après avoir suivi une formation au SANS Institute sur l'étude du trafic réseau et la prévention des intrusions, il a entendu parler d'Armis et des nombreuses possibilités offertes par cette solution par le biais d'un revendeur. Cet échange a donné lieu à la mise en place un test technique avant la phase de déploiement.
« Ce qui nous a motivés à essayer Armis, c'est que nous étions à la traîne en matière de sécurité réseau. Nous n'avions pas de solution de contrôle d'accès réseau (NAC). Or, une telle mise en oeuvre aurait demandé des efforts considérables et nous n'avions aucune visibilité sur ce qui se passait sur le réseau. Armis nous a semblé être une bonne alternative pour nous, car cette solution nous a immédiatement fourni une visibilité sur les appareils qui se connectaient au réseau », explique M. Schultz.

Pourquoi l'inspection des paquets est capitale

M. Schultz a comparé Armis avec une solution concurrente. Il a constaté que le produit concurrent fournissait seulement des données réseau sous forme de fichiers log et non une inspection des paquets de trafic réseau. L'appliance Armis, en revanche, est administrée hors bande et utilise des ports SPAN (Switch Port Analyzer) pour surveiller le trafic réseau de manière passive, sans impacter les performances du réseau. Elle permet une inspection approfondie des paquets, fournit des informations sur le type de trafic acheminé sur le réseau, y compris les anomalies, et identifie à la fois le trafic chiffré et non chiffré. C'est d'une importance capitale dans le secteur de la santé qui est soumis aux exigences strictes de la loi HIPAA (Health Insurance Portability and Accountability Act) et d'autres organismes en matière de confidentialité des données des patients. Par exemple, Armis est capable de détecter

Défis

- Pas de visibilité sur les appareils connectés au réseau
- Multiplication des appareils, avec de nombreux appareils médicaux sous-utilisés
- Impossibilité de détecter un trafic suspect ou risqué, menant à un faible niveau de sécurité des données et du réseau

un appareil qui envoie des images médicales non chiffrées. La solution envoie ensuite une alerte aux équipes de sécurité pour qu'elles puissent prendre des mesures pour faire face au risque.

« Si vous pouvez voir les paquets, c'est le summum. Regarder uniquement des fichiers log n'est pas pertinent », remarque M. Schultz. « Armis nous permet de mieux comprendre notre réseau. Nous obtenons de nombreuses informations avec peu d'efforts de notre part. Avant l'adoption d'Armis, les efforts à déployer pour recueillir ces données dépassaient nos capacités. »

Armis expose les appareils médicaux et informatiques peu utilisés

Autre initiative majeure de M. Schultz : limiter la prolifération des serveurs. Son équipe et lui exploitent Armis pour voir le trafic réseau sur tous les serveurs de l'organisation afin de déterminer leur niveau d'utilisation. Grâce à ces informations, ils peuvent retirer les serveurs devenus inutiles. Il constate qu'avant Armis, lancer des analyses sur l'utilisation des serveurs prenait un temps considérable avec leurs systèmes hérités.

En tant que technicien chevronné, très impliqué dans le backend des opérations, M. Shultz sait qu'Armis peut fournir des informations utiles sur l'utilisation des appareils, pouvant générer des économies. Par exemple, l'équipe Armis a créé une requête pour permettre à M. Schultz et son équipe de savoir quels moniteurs de signes vitaux étaient utilisés par l'équipe médicale. Les moniteurs de signes vitaux sont des appareils numériques, portables et connectés au réseau qui permettent à l'équipe médicale de recueillir des données de santé comme la tension ou la fréquence respiratoire. En général, ces moniteurs sont équipés d'écrans, de scanners et d'imprimantes.

« Armis nous a permis de voir si certains moniteurs qui semblaient prendre la poussière dans un coin étaient réellement utilisés », explique-t-il.

L'hôpital Burke partage un modèle de service avec le réseau de l'hôpital Montefiore et se connecte au réseau de l'organisation mère pour utiliser son système de dossiers médicaux électroniques. Dans ce contexte, Armis apporte une valeur ajoutée en identifiant l'efficacité de l'utilisation des appareils partagés entre eux, ainsi que les coûts.

« Armis nous permet de mieux comprendre notre réseau. Nous obtenons de nombreuses informations avec peu d'efforts de notre part. Avant l'adoption d'Armis, les efforts à déployer pour recueillir ces données dépassaient nos capacités. »

Brian Schultz
Directeur des opérations et de la sécurité du réseau
Hôpital de rééducation Burke

Une sécurité renforcée grâce à la détection des failles et à l'intégration d'outils de diagnostic

Armis a également détecté une faille de grande ampleur dans les frameworks de journalisation Java de l'utilitaire Apache Log4j. Cette vulnérabilité permet aux hackers d'exécuter un code à distance sur un appareil ciblé. Autrement dit, les pirates peuvent voler des données, installer des logiciels malveillants et prendre le contrôle de l'appareil. Les attaques Apache Log4j sont particulièrement répandues sur les dispositifs médicaux. Cette vulnérabilité a même contraint la FDA américaine à soulever ce problème auprès des fabricants de produits médicaux.

M. Schultz s'implique également dans les investigations d'incident de sécurité de base. Pour cela, il utilise CrowdStrike. Bien que CrowdStrike soit installé sur tous les appareils basés sur des agents, il reste des angles morts avec les appareils sans agents. L'intégration de CrowdStrike à Armis a permis de gagner en visibilité et d'approfondir les investigations sur un plus grand nombre d'appareils.

Armis ouvre la voie à de nouveaux cas d'utilisation

Bien que M. Schultz et son équipe n'en soient qu'au début de leur exploration d'Armis, ils ont pu constater que les cas d'utilisation d'Armis sont pratiquement illimités. Pour le moment, ils se concentrent sur l'identification du trafic réseau et du matériel hérité qui n'est plus utilisé à sa capacité maximale. Ils sont également enthousiastes et impatients de découvrir d'autres applications de la solution. Par exemple, M. Schultz a pour projet d'utiliser Armis prochainement pour gérer les performances du réseau en analysant les écarts dans les protocoles réseau, qui peuvent être d'importants indicateurs d'exfiltration de données.

Résultats d'Armis

- Visibilité étendue sur les dispositifs médicaux et de l'Internet des objets (IoT), qui se connectent au réseau, qu'ils soient indésirables ou nouveaux
- Meilleure compréhension de l'utilisation des appareils, qu'il s'agisse des serveurs, des périphériques ou des dispositifs médicaux, pour déterminer lesquels apportent réellement une valeur ajoutée et lesquels peuvent être éliminés
- Intégration de Crowdstrike qui permet d'approfondir les investigations lors d'incidents suspects
- Détection du trafic réseau chiffré et non chiffré pour une meilleure protection des données de santé et d'autres informations réglementées relatives aux soins de santé
- Gain important par rapport aux efforts nécessaires pour déployer et gérer Armis

Armis est la principale plateforme unifiée de visibilité et de sécurité des actifs conçue pour répondre au nouveau paysage de menaces que créent les appareils connectés.

Les sociétés classées au Fortune 1000 font confiance à notre protection continue et en temps réel pour voir avec le contexte complet tous les appareils gérés, non gérés et IoT, y compris les appareils médicaux (IoMT), les technologies opérationnelles (OT) et les systèmes de contrôle industriel (ICS).

Armis offre une gestion passive inégalée des actifs de cybersécurité, la gestion des risques et la mise en application automatisée.

Armis est une société privée dont le siège social est situé à Palo Alto, en Californie.

1.888.452.4011

Website
Platform
Industries
Solutions
Resources
Blog

Try Armis
Demo
Free Trial