> Vertical brochure

Répondre aux enjeux de *cybersécurité* des établissements de santé

GATEWATCHER

CONTEXTUALISATION_

Cinquième secteur d'activité le plus ciblé[1] à l'échelle européenne, la santé fait face à des cyberattaques toujours plus fréquentes et plus sophistiquées, qui visent les systèmes d'information hospitaliers (SIH).

Les établissements de santé sont des organisations vulnérables et ne peuvent être considérés comme des structures comme les autres. La multitude d'utilisateurs se connectant au système IT des établissements de santé en augmente leur surface d'exposition et leur vulnérabilité. La diversité des professions - corps médical, chercheurs, sous-traitants - et l'usage de la télémédecine sont autant de facteurs de risque.

Cette pluralité de métiers et la complexité de l'écosystème IT implique une interconnexion des postes de travail habituels (laptop/PC/imprimante) avec des infrastructures IT complexes tels que les équipements médicaux ou encore les réseaux de caméra de surveillance.

Une seule compromission peut induire l'immobilisation complète du fonctionnement de toutes ces infrastructures en même temps. Dans ce contexte, quelles solutions peuvent être mises en œuvre pour répondre aux vulnérabilités spécifiques des structures dans le secteur de la santé ?

> **Le dysfonctionnement d'un élément peut entraîner l'arrêt complet des soins et mettre en danger la vie d'un patient.**
>
> RSSI établissement de santé

En **2022**[2]

+33 % d'établissements déclarent au moins 1 incident de sécurité

432 établissements de santé couverts par le CERT Santé

62 structures impactées par au moins 2 incidents dans l'année

1 : Health Threat Landscape, European Union Agency for Cybersecurity (ENISA), Juillet 2023.

2 : source: esante.gouv.fr

ENJEUX ET RISQUES MAJEURS_

PRINCIPAUX ENJEUX POUR LES ÉTABLISSEMENTS DE SANTÉ

- Se prémunir des arrêts de services de soins qui mettent en danger la vie des patients.
- Se protéger contre l'accès illicite, l'indisponibilité et l'exfiltration de données sensibles de santé des patients.
- Sensibiliser et accompagner les équipes à identifier et qualifier les menaces pour y faire face.
- Renforcer la visibilité sur les usages et les équipements présents au sein du parc informatique hospitalier.

RISQUES MAJEURS, CONTRAINTES SECTORIELLES ET CRITICITÉ DES ÉTABLISSEMENTS

- Diversité des professions médicales et non médicales.
- Évolution du mode de soin et de la télémédecine : intervention de médecins libéraux en centre hospitalier et multiplication de « tiers » (plateforme de télémédecine et de prise de rendez-vous).
- Hétérogénéité des outils et des équipements médicaux à couvrir.
- Multiplicité des structures et des organisations (CHU, CHP, GHT et organisations en groupement, ARS, ou EHPAD).
- Disparité des capacités budgétaires et des ressources humaines, expertes ou moins expérimentées (nécessitant des solutions easy to use, opérée via un service managé ou par l'établissement directement).
- Variété et sensibilité des données traitées (informations médicales ou de recherche).

PRINCIPAUX OBJECTIFS DE L'OFFRE GATEWATCHER SPÉCIALEMENT CONÇUE POUR LES HÔPITAUX

- Détecter les menaces au plus tôt mais aussi les menaces induites par les actifs en mouvement, potentiellement compromis à l'extérieur.
- Détecter les menaces directement au niveau du réseau informatique, dès les premiers signaux faibles, grâce à un processus de détection et de réaction automatisé permettant de réagir beaucoup plus rapidement aux menaces potentielles.
- Remonter les menaces au prestataire de service cyber santé en place pour une action proactive.
- Offrir des solutions intégrables au sein d'un SOC (Security Operations Center) managé.
- Tout cela à moindre coût et sans impacter les métiers médicaux de l'établissement.

CAS D'USAGE OBSERVÉS_

De la théorie à la pratique, Gatewatcher accompagne ses clients à mieux maîtriser le risque cyber et à répondre à des actes malveillants ayant exploité les risques majeurs susmentionnés.

CAS D'USAGE N°1 : WORKSTATION INFECTÉE

Lors d'une implémentation de la solution de NDR, les équipes de Gatewatcher ont détecté l'infection du PC du personnel administratif par un implant EMOTET. Gatewatcher a identifié les communications récurrentes, correspondant à une « pattern » entre la machine infectée et le serveur de contrôle. En corrélant l'ensemble des alertes disponibles dans la solution NDR (Network Detection and Response), les équipes ont établi avec certitude l'existence de cette intrusion et ont pu la relier à EMOTET, grâce à la connaissance des menaces fournie par la solution.

L'infection étant déjà présente, les équipes n'ont pu établir la méthode d'intrusion utilisée, mais elles ont pu imaginer quelques-unes d'entre elles comme le phishing, fichier incluant un exécutable, ou une quelconque activité sur un site internet malveillant à l'encontre de l'utilisateur.

L'intrusion identifiée par les équipes a permis d'y remédier avant le déclenchement complet de l'arsenal de l'assaillant (chiffrement, exfiltration d'informations, etc.).

CAS D'USAGE N°2 : MISE À JOUR DE LOGICIEL À RISQUE

Certains équipements médicaux nécessitent des mises à jour régulières afin d'en améliorer leur efficacité. Lors d'une implémentation, Gatewatcher a identifié des méthodes mises en œuvre par certains éditeurs, ne répondant pas aux bonnes pratiques en la matière. La solution AIonIQ de Gatewatcher permet l'analyse du contenu des échanges et l'identification des signatures de contenus suspicieux. Les équipes intervenantes ont ainsi identifié des mises à jour de logiciels contenant des sections de code très similaires à ce qu'utiliserait un assaillant. Une analyse complète a été engagée afin de :

- **Lever les doutes d'une possible infection par supply chain.**
- **Informer les sous-traitants sur la légitimité de ses pratiques afin d'en élever le niveau de sécurité.**

L'anticipation et l'analyse multivectorielle délivrée par la solution NDR de Gatewatcher a apporté un haut niveau de visibilité et de connaissance sur les usages par rapport à d'autres solutions de détection sur le marché.

CAS D'USAGE N°3 : DÉTECTION D'ÉQUIPEMENTS OU D'USAGES NON BANALISÉS

Les établissements de santé accueillent en leur sein une population d'acteurs plus ou moins sensibilisée aux enjeux de cybersécurité. Les équipes de Gatewatcher ont notamment pu révéler et signaler l'usage de PC / laptops qui étaient jusqu'alors hors de visibilité des équipes IT d'un établissement de santé. Cette mise en évidence leur a permis de prévenir une partie de leur pratique peu sécuritaire tout en partageant les perspectives et risques associés. Après une révision régulière et quotidienne, Gatewatcher a procédé à une déconnexion de certaine(s) salle(s) car des menaces types adware ou des activités de téléchargement non sécurisées y étaient régulièrement observées malgré les avertissements.

Grâce à la solution NDR de Gatewatcher, la surface d'exposition aux menaces a été limitée, et la technologie du produit a fourni les éléments nécessaires à une prise de décision rapide et globale.

SOLUTION_

La solution GATEWATCHER NDR® permet de :

- Paramétrer simplement et de se déployer sur l'ensemble de l'hôpital, en des points uniques et bien identifiés du réseau de l'établissement de santé, sans impacter directement les SIH ni perturber le travail des équipes médicales.
- Identifier l'ensemble des appareils connectés au réseau informatique de l'hôpital : postes de travail, machines médicales, smartphones, objets connectés, etc... pouvant échapper au contrôle des équipes IT des établissements de santé.
- Offrir une haute visibilité et une surveillance sur l'ensemble de ces appareils, même non référencés par la direction informatique.
- Prévenir dès les premiers signaux faibles en amont d'une cyberattaque en identifiant tout comportement anormal d'un utilisateur connecté au réseau, réduisant ainsi les impacts métier et les répercussions sur les patients, quotidiennement.
- Éviter tout disfonctionnement : compromission d'accès initial, propagation d'un ransomware ou exfiltration de données.

Avantages de la solution GATEWATCHER NDR® :

- Visibilité à 360° du niveau de risque cyber.
- Solution agnostique et interopérable, capable de s'intégrer rapidement et harmonieusement dans la plupart des stacks de sécurité existants au sein d'un écosystème technologique hétérogène.
- Implémentation passive, sans impact sur l'activité médicale et sans agent.
- Capacités « Plug and Detect » dès les premiers flux réseaux collectés pour une rapidité d'action dans des situations de crise et une efficacité améliorée des modèles de Machine Learning utilisés.
- Détection et identification des menaces connues et inconnues de façon fine et hyper contextualisée grâce à une approche multivectorielle ainsi qu'à l'association de l'IA et du Machine Learning.
- Maîtrise des données : les informations restent sous propriété des CHU ou CHP. Possibilité de contrat de confiance avec des tiers impliqués sur des recherches bio médicales.

CONCLUSION & BÉNÉFICES

Dans cet **environnement complexe**, les établissements de santé sont une cible idéale. L'obligation d'ouverture de leur systèmes IT, induite par l'activité quotidienne et de recherche, les innovations technologiques et l'évolution de la télémédecine implique de pouvoir compter sur un réseau **robuste et sécurisé**.

Il leur est donc indispensable de mettre en place des solutions de détection qui permettront une **maîtrise complète des usages** pour un minimum d'impact et de complexité d'implémentation. Le NDR devient très rapidement un support d'investigation efficace et d'amélioration continue, afin de réduire au **maximum la surface d'exposition aux risques cyber**.

NOS RÉFÉRENCEMENTS, PARTENAIRES ET CERTIFICATIONS

Gatewatcher entretient des partenariats de confiance avec des acteurs clés de la cybersécurité et de la santé dont l'Union des Groupements d'Achats Publics (UGAP), le Resah et différents marchés de la C.A.I.H. Gatewatcher fait partie des cinq acteurs et éditeurs dont les solutions, portées par Advens, constituent le nouveau marché de SOC Managé 100% souverain de la C.A.I.H.

Les solutions Gatewatcher sont éligibles au plan « France Relance », permettant aux établissements de santé de bénéficier d'un parcours de cybersécurité proposé et financé par l'ANSSI.

Depuis sa création, Gatewatcher a obtenu plusieurs distinctions et labellisations : certification ANSSI, French Tech 2030, Cyber Task Force, France Cyber Security. L'entreprise est membre d'Hexatrust et membre fondateur du Campus Cyber, projet porté par le Gouvernement dans le renforcement de l'écosystème cyber souverain.

À PROPOS DE GATEWATCHER

Leader technologique dans la détection des cybermenaces, Gatewatcher protège depuis 2015 les réseaux critiques des grandes entreprises et des institutions publiques.
Nos solutions associent des techniques d'analyse dynamique combinée à de l'IA pour offrir une vision à 360°en temps réel des cybermenaces sur l'ensemble du réseau, dans le cloud et on premise. Gatewatcher est présent sur plusieurs plateformes de marché et sa technologie NDR est disponible en mode service managé, intégréeau sein d'un SOC (Security Operations Center).

Nous contacter

www.gatewatcher.com
contact@gatewatcher.com