

Répondre aux enjeux de *cybersécurité* des établissements de santé

 GATEWATCHER



CONTEXTUALISATION

Cinquième secteur d'activité le plus ciblé 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.

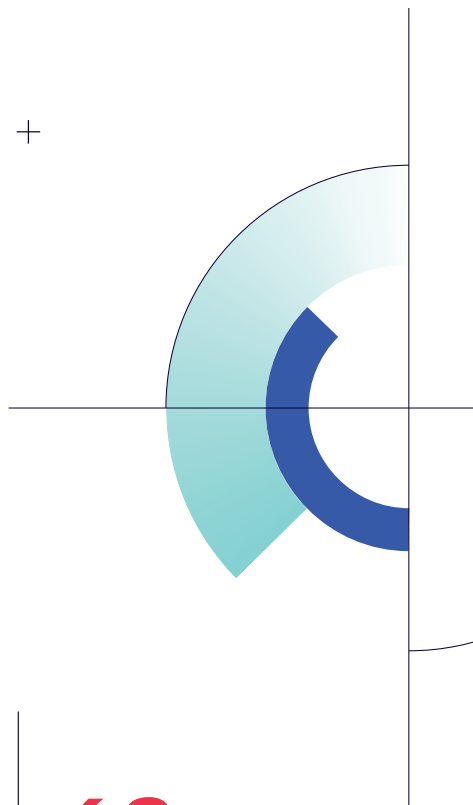
Cette pluralité de métiers et la complexité de l'écosystème IT implique une interconnexion des postes de travail habituels (laptop/PC/imprimante) avec des infrastructures IT complexes tels que les équipements médicaux ou encore les réseaux de caméra de surveillance.

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
2022²

432

établissements de
santé couverts par le
CERT Santé

+ 33 %

d'établissement
déclarent au moins
1 incident de sécurité

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

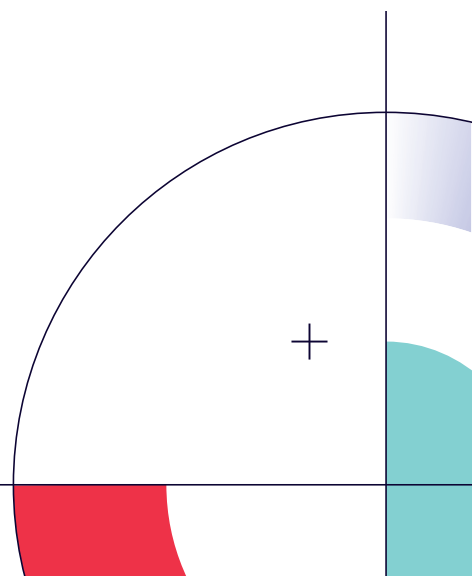
- ▶ Se prémunir des arrêts de services de soins qui mettent en danger la vie des patients.
- ▶ Se protéger contre l'accès illicite, l'indisponibilité et l'exfiltration de données sensibles de santé des patients.
- ▶ Sensibiliser et accompagner les équipes à identifier et qualifier les menaces pour y 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.



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, intégré au sein d'un SOC (Security Operations Center).

Nous contacter

www.gatewatcher.com

contact@gatewatcher.com

