THREATQUOTIENT™

ThreatQ™ pour le secteur de la santé

Vu les énormes volumes de données médicales et personnelles qu'ils conservent et traitent pour leurs patients, les établissements de santé sont devenus des cibles attrayantes pour les pirates informatiques. Les dossiers médicaux électroniques contiennent des données précieuses telles que le nom complet, la date de naissance, le numéro de sécurité sociale et les informations de facturation d'un patient, et constituent dès lors une véritable mine d'or numérique pour les escrocs, attirés par les perspectives lucratives associées à la vente d'informations personnelles sur le marché noir.

Les attaques par ransomware représentent 72 % des incidents liés à un logiciel malveillant dans le secteur de la santé. Généralement, ces campagnes ont recours au vol d'identifiants et infectent plusieurs machines avant d'être détectées, compromettant ainsi le fonctionnement du système de santé. Les attaques telles que WannaCry, qui a touché plus de 100 pays en mai 2017, tirent la sonnette d'alarme pour les prestataires de soins de santé et mettent en évidence la nécessité impérieuse de renforcer les défenses de cybersécurité au sein des systèmes de santé du monde entier.

PRINCIPAUX DÉFIS

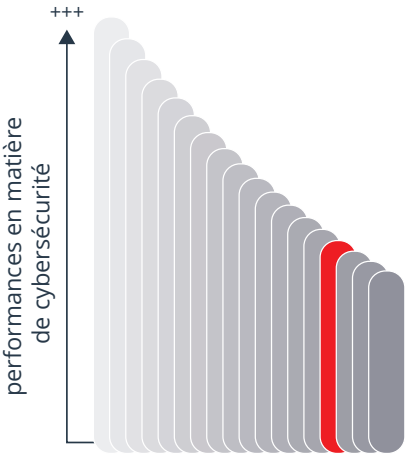
LA DISPONIBILITÉ DES DONNÉES

Un accès instantané et fiable aux données pertinentes des patients sauve des vies, et leurs dossiers doivent pouvoir être consultés sur demande par le personnel médical. L'attention portée au bien-être des patients et aux résultats cliniques l'emporte presque toujours sur la protection des données. Ceci explique le recours constant à des processus de partage des informations non sécurisés et des technologies de communication obsolètes. Or la vigilance est impérative. En effet, les données médicales confidentielles sont particulièrement vulnérables aux attaques par logiciel malveillant et par ransomware, et exigent par conséquent des contrôles de sécurité rigoureux. La Threat Intelligence peut fournir des informations inestimables sur les motivations des attaquants et leurs tactiques, techniques et procédures, et qui permettent de déterminer comment renforcer le plus efficacement les défenses.

DES SYSTÈMES ANCIENS

En général, les infrastructures et équipes médicales recourent à des systèmes et des appareils obsolètes, exécutant d'anciennes versions de logiciels et d'outils de sécurité qui sont extrêmement vulnérables aux compromissions. Le nécessité de pouvoir accéder aux informations des patients à tout moment et en tout lieu fait que les administrateurs et les professionnels de la santé sont souvent réfractaires à une mise à niveau des appareils, synonyme d'interruptions potentielles de la prestation des soins. Toutefois, il suffit parfois d'un système archaïque, non mis à jour ou compromis pour que l'établissement soit victime d'une violation de sécurité majeure.

Pour prioriser efficacement les mesures correctives à mettre en œuvre afin de protéger leurs ressources informatiques, à la fois les anciennes et les nouvelles, les systèmes de santé doivent corréler les données de Threat Intelligence et les failles de sécurité potentielles dans leur environnement. Les prestataires disposant de ressources



Dans le classement des performances en matière de cybersécurité des 18 principaux secteurs aux États-Unis, celui de la santé figure au 15e rang[1].

8 à 10 X

Un dossier médical se revend de 8 à 10 fois plus cher qu'une carte de crédit au marché noir[2].

Coût par dossier médical volé[3]

Coût moyen d'une compromission de données pour les établissements de santé au cours des deux dernières années[4]

de sécurité limitées peuvent ainsi se concentrer sur les vulnérabilités de l'infrastructure critique qui posent le plus haut risque pour l'établissement.

DES TECHNOLOGIES MODERNES

Ces technologies, telles que les applications de gestion de dossiers médicaux électroniques et les dispositifs médicaux connectés à l'Internet des objets (IoT), offrent une accessibilité, une connectivité et une évolutivité exceptionnelles, améliorant l'efficacité et les soins aux patients. Malheureusement, elles élargissent la surface d'attaque, de sorte que les données sensibles sont sans cesse exposées aux menaces conçues pour les dérober ou les exploiter à mauvais escient. Il reste difficile de trouver l'équilibre optimal entre technologies de numérisation avancées et stratégies de sécurité mises en œuvre pour protéger les ressources face à l'expansion de la surface d'attaque. Les réévaluations automatiques des menaces, scores, niveaux de risque et priorités en fonction des données de Threat Intelligence les plus récentes et de l'évolution de l'environnement interne permettent toutefois de rester concentré sur les stratégies de réduction des risques les plus judicieuses.

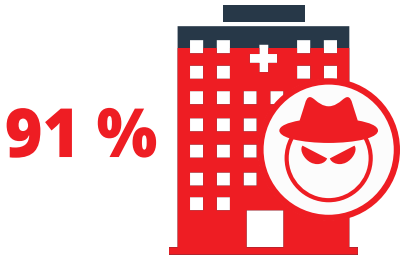
RATIONALISATION DES OPÉRATIONS DE SÉCURITÉ DANS LE SECTEUR DE LA SANTÉ

Une plate-forme de Threat Intelligence robuste fournit aux prestataires de soins le contexte, la personnalisation et la priorisation dont ils ont besoin pour prendre des décisions plus avisées, accélérer la détection et la réponse à incidents, et favoriser la collaboration entre équipes. Dans la mesure où tous les outils et technologies s'intègrent et fonctionnent en toute transparence avec l'architecture ouverte de ThreatQ, il n'est pas nécessaire de modifier l'infrastructure ou les workflows de sécurité existants.

PRINCIPAUX ATOUTS DE THREATQ :

- **CONSOLIDATION** au sein d'un référentiel central de toutes les sources de données de Threat Intelligence et sur les vulnérabilités, tant les sources externes (p. ex. NH-ISAC) qu'internes (p. ex. SIEM)
- **ÉLIMINATION** des nombreuses données parasites, pour mieux cibler les renseignements sur les menaces pertinents et se concentrer sur les ressources et les vulnérabilités critiques
- **PRIORISATION** des mesures et ressources primordiales pour l'environnement du système de santé
- Intégration des indicateurs pertinents uniquement dans les stratégies de sécurité liées à la loi HIPAA
- **TRAQUE PROACTIVE** des activités malveillantes susceptibles de porter gravement atteinte aux dossiers des patients et aux établissements de santé
- **PRIORISATION** des vulnérabilités de sécurité connues et exploitées de manière active, risquant d'affecter la conformité réglementaire
- **ANALYSE ACCÉLÉRÉE** permettant de contrer plus rapidement les attaques visant plusieurs cibles, y compris les dispositifs médicaux connectés au réseau
- **DIFFUSION AUTOMATIQUE** des données de Threat Intelligence vers les outils de détection et de réponse à incidents

Rendez-vous sur threatq.com/demo pour demander une démonstration en direct de la plate-forme ThreatQ et de ThreatQ Investigations.



des établissements de santé signalent avoir subi au moins une compromission de données au cours des deux dernières années[2].

Le nombre de comptes médicaux compromis est passé de 26,4 à 33,7 millions en 2017[5].

Au cours des deux dernières années, le nombre de cas de piratage connus a été multiplié par 2,6 dans le secteur de la santé[6].

[1] SecurityScorecard, 2018 Healthcare Cybersecurity Report (Rapport de cybersécurité 2018 pour le secteur de la santé)

[2] Cisco, Cybersecurity Strategies for Healthcare (Stratégies de cybersécurité pour le secteur de la santé)

[3] Ponemon Institute LLC, Ponemon Institute Research Report – 2017 Cost of Data Breach Study (Rapport du Ponemon Institute – Étude 2017 sur le coût des compromissions de données)

[4] Ponemon Institute LLC, Ponemon Institute Research Report, Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data (Rapport du Ponemon Institute – 6e étude de référence annuelle sur la confidentialité et la sécurité des données médicales)

[5] Gemalto, 2017 Breach Level Index (Indice 2017 du niveau de compromission)

[6] HIPAA Journal, Largest Healthcare Data Breaches of 2017 (Les plus graves divulgations de données médicales de 2017)

À PROPOS DE THREATQUOTIENT™

ThreatQuotient™ sait parfaitement qu'une sécurité axée sur les renseignements repose essentiellement sur les ressources humaines. ThreatQ™, notre plate-forme de Threat Intelligence ouverte et extensible, et ThreatQ Investigations, notre solution de gestion des situations de crise, fournissent aux équipes de sécurité le contexte, la personnalisation et la priorisation dont elles ont besoin pour prendre des décisions éclairées, accélérer la détection et la réponse à incidents, et favoriser la collaboration entre équipes. Adoptées par de nombreuses entreprises de premier plan à travers le monde, les solutions de ThreatQuotient sont au cœur même de leur système de gestion des menaces et de leurs opérations de sécurité.

Pour plus d'informations, consultez le site threatq.com.

TQ_ThreatQ-for-Healthcare_Rev1

THREATQUOTIENT™
11400 Commerce Park Drive, Suite 200, Reston, VA 20191, États-Unis • ThreatQ.com
Sales@ThreatQ.com • Demandes de renseignements généraux et commerciaux : +1 703 574-9885