STORMSHIELD

TÉMOIGNAGE CLIENT

Comment un groupe hospitalier s'organise pour renforcer sa cybersécurité

SANTÉ

Premier acteur hospitalier de sa région, avec 100 000 professionnels et 8 millions de patients par an, le groupement fait face à des enjeux vitaux en matière de cybersécurité. Ce secteur, en proie aux attaques de plus en plus fréquentes et virulentes, se structure pour mieux protéger ses systèmes d'information. Explications.

100 000
Professionnels de santé

39
Hôpitaux en France

8 millions
De patients par an

Conscient des défis à relever, le groupement hospitalier que nous accompagnons a orchestré de nombreux changements pour garantir sa sécurité et harmoniser les systèmes d'information des six Groupes Hospitalo-Universitaires.

Se concentrer sur les infrastructures réseau

En effet, l'ensemble des équipements connectés de chacun des hôpitaux, qu'ils soient industriels et biomédicaux (ex : radio, IRM, robot pharmaceutique...), étaient sur le même réseau, avec peu ou pas de sécurité. Une partie de ces dispositifs était pilotée par des postes de contrôle sous Windows XP, Windows 2000 ou Windows 7. Une source de vulnérabilités certaine puisque les systèmes d'exploitation Windows 2000 et XP ne sont plus supportés par l'éditeur depuis juillet 2010. Ces postes de contrôle devenus obsolètes contenaient ainsi de fortes vulnérabilités, mettant indirectement en péril les automates qu'ils contrôlaient.

« Nous devions cloisonner les flux, protéger les postes de commande et sécuriser les machines afin qu'elles n'acceptent que des communications légitimes et autorisées. »

Les objectifs à atteindre

Pour mettre en place une politique de sécurité proactive et réduire les risques d'impact de cyberattaques, le choix s'est porté sur les pare-feux Stormshield Network Security. Les raisons ? La combinaison d'un haut niveau de qualification auprès de l'ANSSI et des fonctionnalités répondant en tout point au cahier des charges attendu.

Les solutions proposées par Stormshield offrent notamment :

- Une résilience des pare-feu à des conditions hors datacenter (présence d'humidité et de poussière, rayonnement électromagnétique, plage de température étendue...)
- Une administration centralisée ergonomique et simple d'utilisation
- Une capacité à surveiller et à protéger les automates programmables industriels (Programmable Logic Controller, PLC) en supervisant certains systèmes (dont le système de contrôle et d'acquisition de données en temps réel SCADA)
- Une supervision et une analyse des protocoles IT classiques
- Une continuité de service en cas de panne du pare-feu via l'utilisation du mode bypass.



En un an, une augmentation des cyberattaques de 500% contre les établissements de santé dans le monde.

Cybersécurité : les hôpitaux en première ligne

Plus 500% en un an : c'est l'augmentation des cyberattaques dans le monde visant des établissements de santé (Cabinet PwC). Ce chiffre est évocateur. Pendant longtemps, le secteur de la santé a été épargné par les cybercriminels, plus occupés à viser les particuliers et les entreprises. Cette vérité commence à changer en novembre 2019, avec l'attaque du CHU de Rouen. Et se confirme avec la crise du Covid en 2020.

Dans un premier temps, cinq pare-feux SNi40 ont été déployés sur trois sites. L'objectif de cette installation : cloisonner les flux, protéger les postes de contrôle commande et sécuriser les automates afin qu'ils n'acceptent que des communications légitimes venant d'équipements autorisés.

« Avec le pare-feu SNi40, nous apprécions la rupture technologique du bypass et la supervision des protocoles industriels. »

Par ailleurs, pour assurer une administration unique à la fois des réseaux IT et OT, la plateforme Stormshield Management Center (SMC) a été déployée. Au travers de cette solution, tous les hôpitaux du groupement sont interconnectés en central et par GHU. Chaque DSI peut accéder à la gestion des règles liées à son périmètre, sans risque de modification sur ceux des autres établissements.

Test des équipes

Pour mener à bien ce projet, les équipes techniques de Stormshield ont réalisé différents tests, qui se sont avérés rapidement positifs. Cela a conduit à la mise en production des solutions sur les différents sites.



LES SOLUTIONS MOBILISÉES

PARE-FEU INDUSTRIEL

→ SNI40

PLATEFORME DE SUPERVISION

→ Stormshield Management Center

Les prochaines étapes

01

INSTALLER TRENTE SNI40 SUPPLÉMENTAIRES

Installer trente SNi40 supplémentaires afin d'assurer la protection des environnements mono-automate biomédicaux (radio, IRM, robot pharmaceutique...).

02

ÉTENDRE LES DÉPLOIEMENTS

Étendre les déploiements à l'ensemble des hôpitaux regroupés dans les différents GHU.

03

SÉCURISER LES ÉQUIPEMENTS

Sécuriser les équipements liés à la gestion technique des bâtiments (automates de ventilation, climatisation, éclairage, chauffage, alarme incendie, système de vidéoprotection...).

STORMSHIELD

Version 1.0 - Copyright Stormshield 2021