INDUSTRIE

GROUPE INDUSTRIEL ET TECHNOLOGIQUE FRANÇAIS

UNE VISIBILITÉ GLOBALE DES SYSTÈMES D'INFORMATION POUR AMÉLIORER LA CYBERSÉCURITÉ

+ de 84 000
COLLABORATEURS

+ 1 300
EXPERTS AU SERVICE DE LA STRATÉGIE D'INNOVATION

+300
ÉTABLISSEMENTS PARTOUT DANS LE MONDE

Les défis cyber de l'usine 4.0

Analyse des données fournies par des capteurs, automatisation de la logistique, personnalisation des produits... L'industrie migre progressivement vers la « smart factory » pour augmenter la productivité, anticiper la maintenance prédictive et améliorer l'expérience client.

Mais les connexions de plus en plus multiples avec l'univers IT via des réseaux IP et des communications « machine to machine » génère de nouveaux risques de cybersécurité et augmente les surfaces d'attaque. Or, les systèmes de contrôle industriels (ICS - Industrial Control Systems) sont des éléments complexes qui nécessitent une politique de sécurité adaptée à leurs contraintes particulières.

Les défis sont multiples. Il faut assurer l'intégrité des données envoyées aux différents équipements, éviter les attaques par rebond et sécuriser les communications entre les différents systèmes d'information. Cette visibilité exhaustive est indispensable afin d'assurer la pérennité et la résilience de l'activité industrielle.

Le contexte

La transformation numérique au service de l'industrie du futur nécessite pour les industriels une véritable vision à 360° de leur activité. Et en particulier, des données relatives à la qualité de la production, aux taux d'utilisation des machines, aux temps d'arrêt et aux fréquences de maintenance. Ce recueil d'informations en temps réel implique donc une connexion permanente entre les systèmes d'information IT et OT.

Assurer cette interconnexion IT/OT est donc la préoccupation première d'un grand groupe industriel français dans le domaine de l'aéronautique. Dans un premier temps, cet industriel a souhaité interconnecter trois usines en France, comprenant pour chacune plus d'une centaine d'équipements. En tenant compte, bien entendu, de la dimension sécurité pour éviter les cyberattaques de plus en plus variées et sophistiquées que subissent les industriels – et leurs conséquences : infection par un logiciel malveillant, prise de contrôle d'une machine, vol de données critiques, espionnage économique…

Ce groupe industriel souhaitait également garantir un accès aux servitudes techniques (annuaires de l'entreprise, serveurs de temps, serveurs DNS…) et d'exploitation (administration, sauvegarde et télémaintenance) pour les collaborateurs opérant au sein des usines.

La solution retenue

Pour assurer la sécurité de ses systèmes d'information, le client a retenu la solution Stormshield Network Security et mis en place un cluster de SN2100 sur chacun des trois sites afin de protéger l'ensemble des points d'entrées et interconnexions entre les différents réseaux.

Grâce à sa modularité inégalée, ce pare-feu « Next Generation » optimise la segmentation et la séparation des réseaux OT de chaque site du reste du système d'information (IT), où sont remontées et centralisées toutes les données industrielles liées à l'exploitation.

Spécifiquement conçus pour protéger les « Automates Programmables Industriels » (API), une dizaine de pare-feux Stormshield SNi40 ont également été déployés pour assurer une sécurisation rapprochée de chacun des équipements.

Ces boîtiers permettant également une uniformisation des plans d'adressage IP via la fonctionnalité « Network Address Translation » (NAT). Notamment pour les îlots de machines dites « homologuées », fournies par des équipementiers externes et disposant de leurs propres adresses IP non modifiables pour des raisons de garantie constructeur. Les pare-feux SNi40 offrent ainsi la possibilité de réaliser une traduction de l'adresse de l'équipement au niveau de la passerelle de connexion à Internet, entre l'adresse interne de la machine et l'adresse IP de la passerelle, ce qui permet d'intégrer un API de façon transparente dans le plan d'adressage du client.

En déployant les équipements Stormshield, le client a également pu améliorer la visibilité de son système d'information industriel grâce au mécanisme « Intrusion Detection System » (IDS), qui permet de détecter un trafic malicieux et de lever une alarme.

Par ailleurs, le choix de Stormshield a été motivé par plusieurs autres facteurs déterminants :

- une technologie basée sur des plugins applicatifs pour une protection maximale contre les menaces connues et les attaques de type « Zero Day » ;
- des capacités d'inspection protocolaires permettant de durcir les protocoles industriels pour éviter les attaques et les erreurs humaines ;
- une faible empreinte des équipements sur la latence dans le réseau industriel ;
- une installation facile grâce à une procédure simple de configuration ;
- un logiciel unique pour un processus d'administration en une étape, quel que soit le domaine de protection (OT ou IT).

Le client est aujourd'hui pleinement satisfait par l'interconnexion de ces réseaux IT et OT, qui lui permet d'exploiter pleinement l'ensemble des données industrielles et d'améliorer ainsi son efficacité, tout en apportant une meilleure offre de services aux opérationnels.

À suivre...

Ce grand groupe industriel continue d'accorder sa confiance à Stormshield, reconnue pour son expérience et sa connaissance des contraintes et défis spécifiques aux milieux industriels, afin d'équiper l'ensemble de ces sites européens dans les prochains mois et à plus long terme, l'ensemble de ces sites à l'échelle mondiale.

L'intégration de nouveaux plugins protocolaires est également prévue, et en cours d'étude au sein de la R&D Stormshield, afin de répondre à des besoins opérationnels futurs.

STORMSHIELD

Partout dans le monde, les entreprises, les institutions gouvernementales et les organismes de défense ont besoin d'assurer la cybersécurité de leurs infrastructures critiques, de leurs données sensibles et de leurs environnements opérationnels. Les technologies Stormshield, certifiées et qualifiées au plus haut niveau européen, répondent aux enjeux de l'IT et de l'OT afin de protéger leurs activités. Notre mission : cyber-séréniser nos clients pour qu'ils puissent se concentrer sur leur cœur de métier, si cruciale pour la bonne marche de nos institutions, de notre économie et des services rendus aux populations. Choisir Stormshield, c'est privilégier une cybersécurité européenne de confiance. Pour en savoir plus : www.stormshield.com

Version 1.0 - Copyright Stormshield 2020