

ÉTUDE DE CAS

Protection contre les vulnérabilités de réseau d'un opérateur d'importance vitale (OIV)

LES BESOINS

-  Protéger le savoir et la R&D
-  Garantir la confidentialité des données échangées (GED, messagerie, espaces collaboratifs avec les sous-traitants), ainsi que des propositions commerciales et des négociations
-  Garantir la disponibilité de la chaîne de production

LA SOLUTION ITRUST

Mise en place de la solution **IKare** afin de scanner les vulnérabilités de façon automatisée et d'avoir, grâce aux tableaux de bord, une **vision globale** et actualisée du réseau. IKare permet, en accélérant la détection, puis la correction des failles, de diminuer considérablement les points d'entrée pour les attaquants. Le choix par le client du mode SAAS dédié permet d'effectuer des **scans à la demande** en faisant appel aux infrastructures d'ITrust.

LES RÉSULTATS

Correction préventive des faiblesses identifiées sur le réseau, telles que :

- ✓ La non mise à jour de certains équipements, dont les failles connues et documentées sont susceptible d'être exploitées.
- ✓ Le durcissement incomplet des machines
- ✓ Les protocoles de communication vulnérables (chiffrement insuffisant ou inexistant)

CONTEXTE ET ENJEUX

Groupe international, partenaire de premier rang des grands avionneurs mondiaux, ce client maîtrise la production et la conception de produits industriels, ainsi que des systèmes d'interconnexion des équipements embarqués. Reconnu par l'état français comme un Opérateur d'Importance Vitale (OIV), sa sécurité informatique s'intègre ainsi dans un dispositif interministériel et est soumise à l'application de règles strictes.

5000

Employés

10

Sites à l'international

600 M

D'€ de CA en 2015

La solution IKare, par son interface intuitive et son système de notes, permet de corriger rapidement et préventivement les failles de sécurité.