STORMSHIELD

TÉMOIGNAGE CLIENT

Comment un grand stade français renforce la protection de son SI

SPORT ET ÉVÈNEMENT

Haut lieu de rencontres sportives et événementielles, notre client fait face à de forts enjeux de cybersécurité. Stormshield est intervenu pour aider la structure à renforcer sa sécurité informatique et donc, indirectement, la sécurité des millions de personnes qui le fréquentent chaque année.

30 millions
de personnes accueillies

350
événements

Plus de
100
employés

Ce projet a été mené pour le compte d'un des plus grands stades français. En plus d'accueillir chaque année des centaines d'événements sportifs et culturels, il propose la location d'espaces événementiels.

La structure dispose également de plusieurs bureaux administratifs distants et fait appel quotidiennement à de nombreux partenaires externes. Du fait de ses activités publiques, elle représente une cible privilégiée pour les cyberattaques, qui pourraient potentiellement bloquer son activité et occasionner des fuites de données.

Des accès réseau multiples

Ce stade présente deux particularités qui augmentent sa surface d'attaque et nécessitent de renforcer sa sécurité informatique, pour mieux contrôler les accès : un réseau Wi-Fi public sur lequel des dizaines de milliers de spectateurs se connectent à chaque événement et un service de location d'espaces.

Les équipes Stormshield ont mis tout en oeuvre pour améliorer la sécurité de son infrastructure réseau, en remplaçant ses anciens pare-feux (Netasq NG1000), par des solutions « Next-Generation ». Les équipes Stormshield ont également mis en place des politiques de sécurité applicative pour sécuriser dynamiquement les vulnérabilités potentielles sur le réseau, les applications internes et les serveurs.

Ce pare-feu évolutif (SN3100) lui a permis de segmenter les flux réseau et d'intégrer des zones étanches, pour diminuer les risques d'attaques par « rebond » et éviter de donner accès à toutes les ressources critiques en cas d'intrusion.

La réponse de Stormshield en trois étapes clés

01

Un pare-feu évolutif

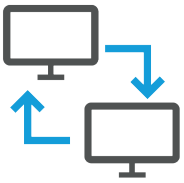
02

Une interface d'administration web rapide et intuitive (IHM)

03

De nombreux outils interactifs pour simplifier le travail des administrateurs

Par ailleurs, les accès distants ont également été sécurisés via une solution VPN IPSec qualifiée par l'ANSSI (Agence nationale de sécurité des systèmes d'information) pour protéger les informations sensibles échangées.



« Les outils interactifs se sont avérés très utiles pour les administrateurs : moteurs de recherche, assistants multiples, etc.»

DJAMEL SLAOUTI
Ingénieur Avant-Vente

Un module de management des vulnérabilités

Pour améliorer et compléter la sécurité de son parc informatique, le client s'est également équipé de la solution Stormshield Network Vulnerability Manager (SNVM). Cette solution garantit et étend la politique de sécurité du stade à toutes les machines. Résultat : les administrateurs gagnent un temps précieux au quotidien.

L'outil collecte, analyse et trie en temps réel des informations pour détecter des logiciels obsolètes ou interdits par la politique de sécurité, corriger des vulnérabilités ou encore informer immédiatement d'un risque d'attaque.

Robustesse éprouvée

Le client sollicite régulièrement des sociétés externes pour réaliser des audits et tests d'intrusion (pentests). Les résultats sont toujours très satisfaisants, grâce à la sécurité assurée par les solutions déployées. Celles-ci sont qualifiées au plus haut niveau de confiance auprès de l'ANSSI.

La collaboration, facteur clé de succès

Les équipes de Stormshield ont étroitement collaboré avec l'intégrateur retenu pour établir le dimensionnement et la qualification technique en amont du projet. Elles ont également assuré le déploiement et la formation. Cette collaboration entre le constructeur, l'intégrateur et le client a favorisé la réactivité et la bonne réussite du projet dans le respect des délais.

LES SOLUTIONS MOBILISÉES

UNE SOLUTION DE SÉCURITÉ DÉDIÉE

→ SN3100

UNE PLATEFORME DE SUPERVISION

→ Stormshield Network Vulnerability Manager

LA CREATION DE TUNNEL VPN

→ IPSec

Et demain ?

La grande modularité en termes de densité de ports, de débit et de connectiques du SN3100, organisé en cluster, répond aux besoins futurs du client : assurer la redondance escomptée d'un réseau dont les flux internet ne cessent d'augmenter.