OBTENIR UNE VISIBILITÉ PERMANENTE SUR LE PÉRIMÈTRE RÉEL D'EXPOSITION

Prioriser et accélérer les corrections

Brest MÉTROPOLE

Contexte client

Établissement public de coopération intercommunale (EPCI)

Regroupe 8 communes où vivent 400 000 habitants

Équipe cyber réduite donc besoin d'une solution pour l'aider face aux menaces de plus en plus importantes

Utilisait des tests d'intrusions annuels

Difficultés client

Périmètre vaste qui devient complexe à maîtriser pour les équipes cybersécurité

Complexification et intensification des menaces qui augmentent la surface d'attaque à un rythme devenu très intense

Livrables

Plus de 1000 actifs répertoriés

Découverte chaque semaine 2 ou 3 actifs exposés et liés à leurs systèmes

Cartographie actualisée en temps réel des actifs vulnérables

Identification du niveau de sévérité des vulnérabilités détectées

Indicateurs

Hiérarchisation de ses interventions selon le niveau de sévérité des vulnérabilités détectées

Gain de temps

Réactivité dans l'approche offensive

Suivi mensuel et écoute – demandes d'évolutions formulées et prises en compte

> « L'implémentation de votre test relatif à la vulnérabilité SharePoint (CVE 2025 53770) s'est avérée pleinement opérationnelle : notre Blue Team a été immédiatement alertée. Nous avons reçu la notification préventive concernant le nouveau test Patrowl à 15 h 57 et, dès 16 h 36, une alerte était déclenchée au sein de Brest Métropole. Nous vous remercions pour la qualité de votre surveillance active et la fiabilité de votre accompagnement. »

Patrowl