GAIN CONTINUOUS VISIBILITY INTO THE ACTUAL EXPOSURE SCOPE

Prioritize and accelerate remediation efforts

Brest MÉTROPOLE

Customer context

Public inter-municipal cooperation establishment (EPCI)

Comprises 8 municipalities with a total population of 400,000 residents

Small cybersecurity team, therefore in need of a solution to help address increasingly significant threats

Previously relied on annual penetration testing

Customer pains

A broad scope that has become increasingly complex for cybersecurity teams to manage

The growing sophistication and intensification of threats, increasing the attack surface at a very rapid pace

Patrowl's deliverables

Over 1,000 assets identified

Discovery of 2 to 3 exposed assets linked to their systems each week

Real-time mapping of vulnerable assets

Identification of the severity level of detected vulnerabilities

Key indicators

Prioritization of remediation actions based on the severity level of detected vulnerabilities

Time savings

Increased responsiveness in the offensive security approach

Monthly follow-up and attentive support – enhancement requests submitted and taken into account

> “The implementation of your test related to the SharePoint vulnerability (CVE-2025-53770) proved to be fully operational: our Blue Team was immediately alerted. We received the preventive notification regarding the new Patrowl test at 3:57 p.m., and by 4:36 p.m., an alert had been triggered within Brest Métropole. We thank you for the quality of your active monitoring and the reliability of your support.”

Patrowl