FORMATION TECH

CASE STUDY · EXTERNAL PENETRATION TEST

Validating Security Posture

A well-established UK retailer operating across multiple sites, with a significant online presence and millions of customers. Like many large consumer-facing brands, it operates in one of the UK's most heavily targeted sectors, where attacks on household names (M&S among them) are an increasingly familiar headline.

IN THIS STORY

Formation Tech were engaged to deliver external penetration testing for a major UK retailer, initially to satisfy insurance requirements. The engagement uncovered a previously unidentified vulnerability and has since grown into a monthly testing programme, giving the business ongoing visibility, operational confidence, and stronger insurance positioning.

01

CHALLENGES

A High-Risk Sector Under Insurer Scrutiny

Retail is one of the most consistently attacked sectors in the UK. Recent high-profile incidents at well-known **high-street brands have brought home the damage that follows a breach**, and insurers have responded: robust penetration testing has shifted from best-practice recommendation to contractual obligation.

For this organisation, the immediate driver was insurance. The customer's insurer had mandated penetration testing as a condition of cover. Validating the external network was no longer optional, it was a requirement to maintain the business's insurance position.

Beyond insurance, there was a wider concern: the business needed **independent assurance that its external-facing infrastructure was genuinely secure**, and that nothing had been overlooked in the day-to-day running of a complex retail network.

02

SOLUTION

A Targeted External Penetration Test

Formation Tech carried out external penetration testing across the retailer's network, beginning with an **initial scope of ten IP addresses**, a rigorous, independent assessment of the external attack surface, built to satisfy the insurer's specific requirements.

During the engagement, we identified an issue with a port that had not previously been picked up. In isolation it might have appeared minor, but alongside other vulnerabilities in the environment it represented a meaningful risk that **could have been exploited as part of a broader attack chain**, exactly the kind of finding routine internal checks miss, and what an independent external test is designed to surface.

The issue was reported, validated and remediated, closing down an exposure the business had been unknowingly carrying.

03

OUTCOMES

Ongoing Visibility and Operational Peace of Mind

Following the initial engagement, the customer expanded the scope of testing to gain broader visibility across the network. What began as a compliance-driven exercise has evolved into a continuous security programme, with the retailer now **receiving monthly penetration testing at a highly competitive rate.**

Commercially, the engagement has delivered on its brief: the business is well-positioned with its insurer and can demonstrate active, ongoing validation of its security posture. **Operationally, the benefits run deeper**, the previously unidentified vulnerability is resolved, and a regular testing cadence surfaces new exposures quickly rather than after the fact.

It shows how external penetration testing, delivered as an ongoing service rather than a point-in-time exercise**, becomes a core component of a mature security strategy.**

> For the customer, it has translated into both peace of mind and a measurably stronger security posture, supporting the business as it continues to operate in one of the UK's most heavily targeted sectors.

RESULTS AT A GLANCE

10 →

Initial IP scope, expanded for broader visibility across the network

×12

Times more testing than previously carried out

50%

Savings against the allocated budget

100%

Insurance requirement satisfied