EXTERNAL ATTACK SURFACE · IN PREPARATION

Digital Discovery

Give us the domains, IP ranges and subsidiaries you know about. We look for internet-facing assets your list misses, with evidence for you to confirm, and profile who targets organisations like yours.

Passive-first
PUBLIC SOURCES FIRST

You confirm
BEFORE ANY TEST

Evidenced
DATED, WITH CONFIDENCE

Threat profile
SOURCED & DATED

What we assess

Companies, domains & networks
Subsidiaries from company registers and filings, then domains, certificates, DNS, registration data and IP ranges in records you share.

Cloud, code & apps
Cloud-hosted services found through DNS and provider address ranges, plus public code repositories and app-store listings tied to you.

Threat profile
Attacker types that dated public reports link to organisations like yours. Dark-web checks start only when Dark Web Monitoring opens.

What you get

- ✓ Assets you did not list, each with its dated evidence
- ✓ A confidence level on every candidate, for you to confirm
- ✓ Third-party assets reported to you, never tested
- ✓ Dangling DNS records flagged as takeover candidates
- ✓ A threat profile with sources, dates and confidence labels
- ✓ Email, TLS and header fixes for assets you confirm
- ✓ Confirmed assets to authorise for Vulnerability Scanning

How it works

1. Agree the seed list and which data services may see it
2. Search public sources and agreed services; log evidence
3. You confirm ownership; third-party assets are set aside
4. Report assets, threat profile and what we could not see

A good fit if

- ✓ Your estate grew through acquisitions, subsidiaries or teams buying their own domains and cloud.
- ✓ You are planning a scan or penetration test and want its scope to include what your list missed.
- ✓ You keep an asset inventory for NIS2, DORA Art 8 or NCSC CAF A3 and want it checked from outside.
- ✓ You want to know who targets organisations like yours, and the assets they would most likely go for.

Probably not, if

- × You need a targeted threat intelligence report for DORA TLPT, TIBER-EU or CBEST — we do not provide one.
- × You want vulnerabilities found or exploited — discovery is not a vulnerability scan or penetration test.
- × You want an inventory certified complete — our report is test evidence an auditor or assessor can review.

How we engage

Fixed scope, repeatable
A fixed-scope report you can repeat when you choose; each repeat shows what has changed.

Senior-led
The practitioner who scopes the work does the work and writes the report.

You confirm first
Until you confirm and authorise in writing, we touch an asset only as any visitor would.

In preparation
We are not yet taking on Digital Discovery clients. Ask us when it opens.

Security that locks down risk, not your business. · © 2026 verrou