

Test your own estate. On purpose.

Real active reconnaissance — admin-gated, consent-based, and deliberately kept out of your posture score.

Shipped August 2026. Two things sit side by side: the platform's **active web application scan** (OWASP ZAP-based, with its own per-domain Request → Authorise → Start approval flow) and a **validation-tool list** covering DNS, IP and application-layer reconnaissance, using a shared consent flow — a tickbox per tool and one "Start validation session" action.



Why it is gated

Active scanning touches live systems. Every action — authorising a scan, viewing raw output — is restricted to administrators, and every session requires explicit consent. Visible to every role; actionable by very few.

Why it is not scored

A test you chose to run at a moment you chose is not the same evidence as continuous monitoring. Blending the two would make the posture score look better and mean less. A persistent "use with care" banner says so in the product.

LIVE TODAY

- **Active web application scan** (ZAP-based), per-domain Request → Authorise → Start flow
- **DNS, IP and application-layer reconnaissance** tool list with a shared per-session consent flow
- Admin-gated throughout; visible to every role, actionable by administrators only
- Amber treatment, not red — this is information, not an alarm
- Time-boxed at 60 minutes per scan — larger or more dynamic sites may be truncated, not exhaustively covered
- Results shown as validation coverage, validated findings and test recency
- A persistent "why is this not scored?" explainer in-product
- Baseline passive web scanning runs separately and does feed posture

The distinction we will not blur

Continuous Threat Exposure Management (CTEM) as an industry framework includes an active-validation stage — breach-and-attack simulation and exploit testing. Our always-on CTEM claim covers **discovery, prioritisation and mobilisation only**. Testing & Validation is genuine active-validation capability and we name it as such — but the two are never described in the same sentence, because they are genuinely different things: continuous and automatic versus deliberate and opt-in.

WHAT IT DELIBERATELY IS NOT

- Not breach-and-attack simulation in the CTEM industry-framework sense
- Not a penetration test — it does not replace one
- Not exhaustive on large or highly dynamic sites, because of the time box
- Not included in any automatic posture score

HOW TEAMS USE IT

- Validate that a remediation actually closed the finding
- Check external exposure before a customer security review
- Evidence an active-testing control requirement, with the consent record attached
- Sanity-check the passive scan's picture of a web estate