

CONTINUOUS THREAT EXPOSURE MANAGEMENT · VALIDATION

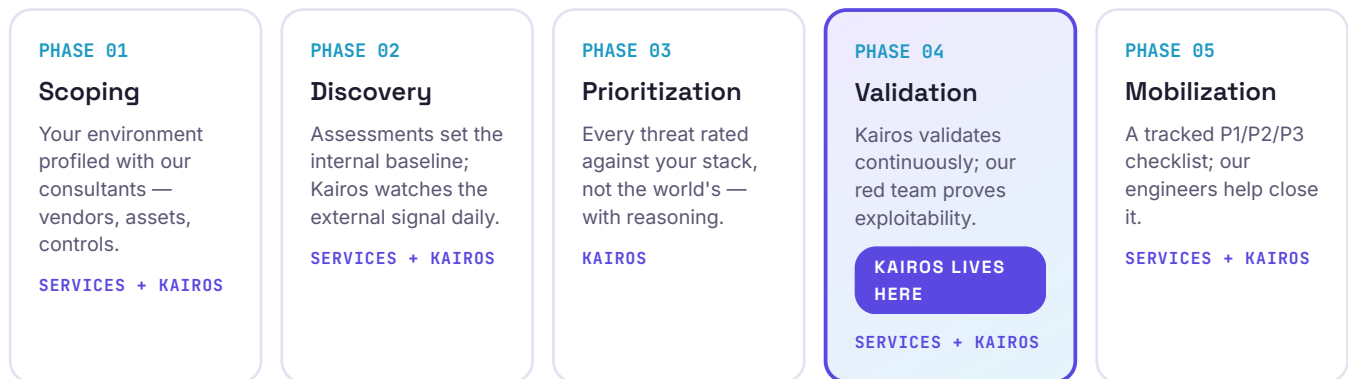
Kairos — continuous threat validation

The oracle for your CTEM cycle.

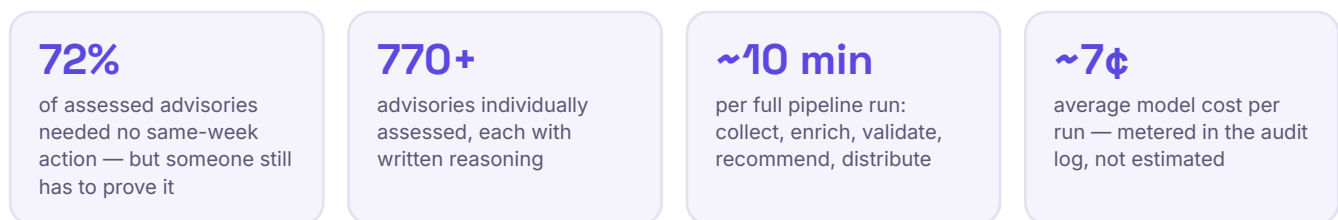
Scanners and feeds tell you what could be exposed — against the world's stack, not yours. Kairos validates every emerging advisory, KEV entry and PSIRT bulletin against **your actual environment**, every day, and turns the result into the **two or three actions that matter this week**. Privacy-defensible by construction.

01 The gap in every CTEM program

Continuous Threat Exposure Management runs in five phases. Most vendors sell you one of them. The Vulnium program covers the cycle end to end — specialists and Kairos divide the work — and the phase most programs still run by hand, **Validation**, is automated and evidenced daily.



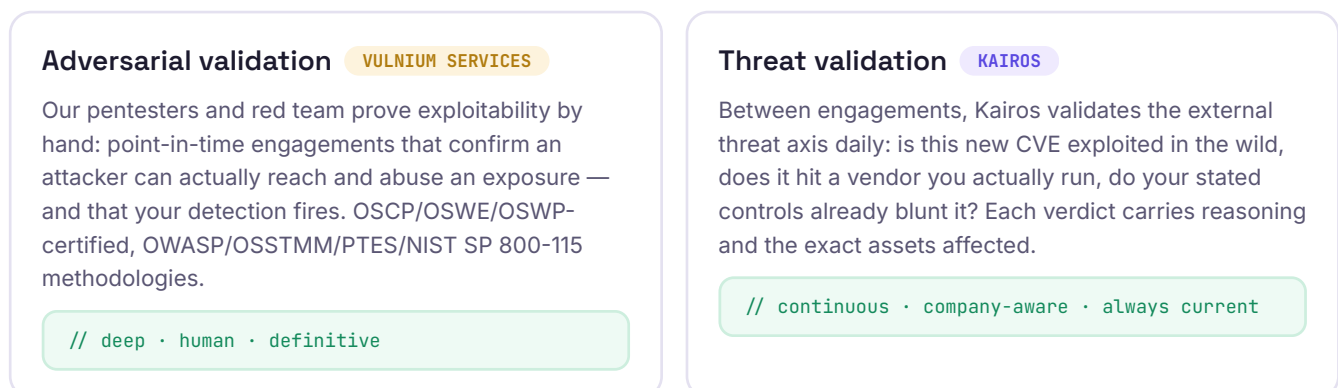
02 Why validation is the bottleneck



Figures from a 32-run pilot deployment, April–June 2026.

03 Validation has two layers — the program runs both

Proving a threat is real takes both continuous analysis and human adversaries. Point tools offer one; the Vulnium program runs both.



04 How a run works

Five steps, the same every run, each one leaving a record. **Kairos deploys inside your perimeter** — public sources come in, nothing about your environment goes out.

STAGE		WHAT IT DOES
Collect	EVERY 24H	CISA KEV & Alerts, vendor PSIRT feeds, OTX, abuse.ch, MITRE ATT&CK, research blogs and social aggregators.
Enrich	AUTOMATED	Each item summarized and tagged: CVEs, ATT&CK techniques, threat actors and the products affected.
Validate	YOUR ENVIRONMENT	Every item rated High / Medium / Low / N-A for your environment specifically, with written reasoning and the exact assets affected.
Recommend	PRIORITIZED	Validated High/Medium items become a P1/P2/P3 action checklist with concrete steps and source links.
Distribute	YOUR CHANNELS	Microsoft Teams card, leadership dashboard, printable briefing pack — and structured output your GRC or ticketing platform can ingest.

05 Your data stays yours — verifiably

Runs where your data lives

Public advisories flow in; verdicts and briefings go to your own channels. Your environment profile — vendors, assets, controls — is stored and processed under your control, and is never uploaded to us or to anyone else.

✓ Your environment profile never leaves your infrastructure

A paper trail your auditors will like

Every run is logged end to end — what was collected, how each item was rated, what it cost, and what was sent where. When a security review or an auditor asks how your threat intelligence is handled, the answer is a report, not a promise.

✓ Every run reviewable: sources, verdicts, costs, destinations

06 What your team gets

◆ Executive home

Today's validated High/Medium items, KPI cards and run status — ready when leadership opens the laptop.

◆ Grounded verdicts

Every rating tied to a public source and a specific profile match. No "where did this come from?"

◆ Plain-English Q&A

"Does CVE-X affect us?" answered in seconds, with citations, from the validated corpus.

◆ Action checklist

P1/P2/P3 with concrete steps, live status tracking, and a printable board briefing pack.

◆ Careful about sources

Authoritative sources are evidence; everything else is treated as untrusted input and handled accordingly.

◆ Supply-chain watch

Your supplier watchlist monitored daily: which suppliers' technology is being exploited right now — and does it touch us?

The Vulnium CTEM Program — how engagements start

One owner for the whole cycle: Kairos validates continuously, Vulnium specialists prove and close — evidence at every phase.

STEP 1 Profile & deploy

We model your environment (vendors, assets, controls) and deploy Kairos on your infrastructure — data stays on your box.

STEP 2 Continuous validation

Daily runs validate the landscape against your profile; leadership gets the checklist, analysts get their week back.

STEP 3 Adversarial proof

Scheduled Vulnium pentest / red-team engagements prove exploitability on what Kairos surfaces — loop closed.