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.

PHASE 01
### Scoping
Your environment profiled with our consultants — vendors, assets, controls.
SERVICES + KAIROS

PHASE 02
### Discovery
Assessments set the internal baseline; Kairos watches the external signal daily.
SERVICES + KAIROS

PHASE 03
### Prioritization
Every threat rated against your stack, not the world's — with reasoning.
KAIROS

PHASE 04
### Validation
Kairos validates continuously; our red team proves exploitability.
KAIROS LIVES HERE
SERVICES + KAIROS

PHASE 05
### Mobilization
A tracked P1/P2/P3 checklist; our engineers help close it.
SERVICES + KAIROS

## 02 Why validation is the bottleneck

**72%**
of assessed advisories needed no same-week action — but someone still has to prove it

**770+**
advisories individually assessed, each with written reasoning

**~10 min**
per full pipeline run: collect, enrich, validate, recommend, distribute

**~7¢**
average model cost per run — metered in the audit log, not estimated

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.

### Adversarial validation VULNIUM SERVICES

Our pentesters and red team prove exploitability by hand: point-in-time engagements that confirm an attacker can actually reach and abuse an exposure — and that your detection fires. OSCP/OSWE/OSWP-certified, OWASP/OSSTMM/PTES/NIST SP 800-115 methodologies.

```
// deep · human · definitive
```

### Threat validation KAIROS

Between engagements, Kairos validates the external threat axis daily: is this new CVE exploited in the wild, does it hit a vendor you actually run, do your stated controls already blunt it? Each verdict carries reasoning and the exact assets affected.

```
// continuous · company-aware · always current
```

## 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.