

KONVU VS CODEX SECURITY

Codex validates when possible. Konvu reproduces by default.

Run Codex Security to find vulnerabilities in your own code. OpenAI's docs say it validates issues when possible, and findings that fail stay in the results as unvalidated. Add Konvu when each finding needs a decision before engineering time goes in: Konvu reproduces every vulnerability report by default against its own deployed copy of your app.

Konvu is not a scanner. **Codex Security exports come in as reports.**

AT A GLANCE

	CODEX SECURITY	KONVU
Finds vulnerabilities	Yes, in first-party code: cloud, desktop app, CLI or CI	No. Konvu decides on findings from scanners, researchers and AI tools
Dependencies	No SCA shipped. An open PR adds a scan that does not establish exploitability	Four-precondition exploitability check on scanner findings
Verification	When possible, in a sandbox. Unvalidated findings stay listed	An exploit attempt on every report, by default
Runs against	The checked-out repo in a container, or your machine or CI	Konvu's deployed copy of your app, attacked from a separate host
Fixes	Patch with a fail-then-pass test, draft PR after review	Draft PRs or a Codex fix prompt, then the exploit re-run on the fix
Write-back	Jira and Linear unchanged unless you ask. SARIF upload	Dismissals to Snyk, Semgrep, Dependabot. Jira and ServiceNow on Enterprise
Pricing	Cloud scans on tokens since Oct 1, 2026. \$500 in credits	Business: \$2,000/month for 400 confident verdicts

Where Codex Security is stronger

- New vulnerabilities in your code, with CVEs credited by OpenAI.
- Apache-2.0 CLI and SDK, with recipes for four CI systems.
- Deep scans: up to 40 across parallel workers, for up to 96 hours.
- Diff scans, a pre-commit hook and PR review before merge.

Where Konvu fits

- One decision record for Codex Security, scanners and bug bounty.
- An exploit attempt on every report, against a running copy.
- Dependency findings, where Codex Security has no scanner.
- Fixes shipped, then re-tested against the exploit.

RUNNING BOTH

Codex Security finds. Konvu decides what to fix.

01

Export the findings

findings.json or SARIF from Cloud, the plugin or CI.

02

Konvu reproduces

Each report is triaged, deduplicated and attacked in an isolated lab.

03

The fix goes back

Copy fix prompts Codex with the proof. Konvu re-tests the fix.

Detection is solved. **The decision is not.**

Full comparison with every source: konvu.com/compare/konvu-vs-codex-security

Konvu docs: docs.konvu.com

Sources checked October 13, 2026: learn.chatgpt.com/docs/security (FAQ, CLI, triage backlog, fix findings), help.openai.com, github.com/openai/codex-security, openai.com/index (research preview, Patch the Planet), docs.konvu.com, konvu.com/pricing.