

Public-source n8n starter-kit change review

n8n AI workflow release evidence pack

DELIVERY STATUS DRAFT	POLICY RESULT Human review required Static evidence is available, but no passing staging receipt is bound to this exact candidate.
---	---

DELIVERED TO n8n-io/self-hosted-ai-starter-kit · public commits	REVIEW ID wcr-0d10a827199c-733b3cbe
GENERATED 2026-08-22T06:32:11.976Z	Staging evidence not-run

Change summary

BLOCKERS 0	TO REVIEW 1	IMPROVEMENTS 0	OPEN FINDINGS 2
Baseline Demo workflow · 3	Candidate Demo workflow · 3		

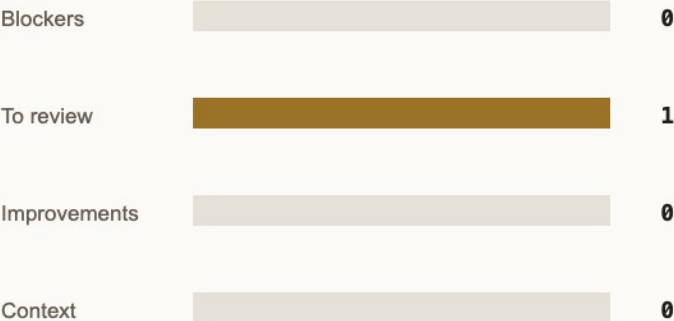
Change summary

Every value is calculated from the selected workflow files.

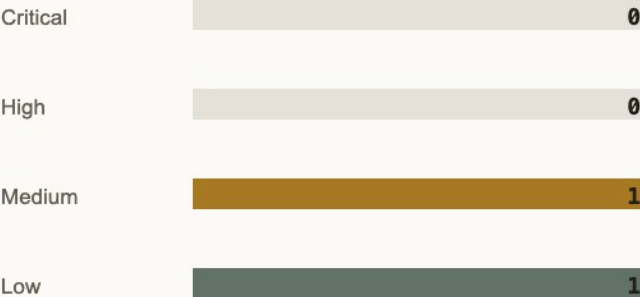
Workflow size



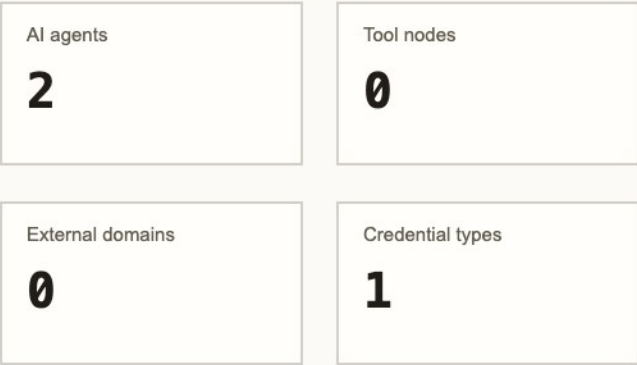
Review disposition



Open findings



Candidate access surface



Connection delta

0 added, 0 removed

Staging evidence

NOT-RUN · 0/0

Human validation

Retest evidence NOT-SUPPLIED	No prior ReleaseGuard receipt was supplied for retest comparison.
NO LONGER OPEN —	STILL OPEN —
	NEW IN CORRECTED CANDIDATE —

Recorded statuses

AA-005-01 · NEEDS-ENVIRONMENT-EVIDENCE Codex-assisted public-source review pending human sign-off The public export has no structured output parser. Downstream consumption and the required output contract were not runtime-verified.
AA-010-02 · CONFIRMED Codex-assisted public-source review pending human sign-off The candidate export has no errorWorkflow setting or explicit failure-handling node.

Change register

1-1 / 1

CR-001 · REVIEW

Security-relevant configuration changed: Basic LLM Chain

The node behaviour changed outside layout-only fields. Review the candidate configuration and the attached staging evidence.

Open findings

MEDIUM · AA-005

No structured model-output validation was detected

LOW · AA-010

No workflow-level failure route was detected

Evidence boundaries

- This receipt compares exported JSON and a supplied staging record. It does not inspect production credential scope or external service authorization.
- Runtime evidence is accepted only when its canonical workflow fingerprint matches the candidate in this receipt.
- Local runtime receipts are reproducible evidence records, not cryptographically signed third-party attestations.
- A passing receipt records evidence for the tested policy and contract. It is not a penetration test, compliance certificate or security guarantee.
- Node names, node types, public domains and credential types can appear in the receipt. Prompt text, parameter values and credential values are omitted.
- Automatic findings remain review signals until a person records a manual review status. A score or clean static result is not a vulnerability verdict.
- Instance configuration, published-workflow identity, installed package versions and production permissions require separate environment evidence.

Production evidence

Production checks that cannot be seen in the workflow export.

n8n-version · NOT-VERIFIED
Environment review pending · —
—
credential-permissions · NOT-VERIFIED
Environment review pending · —
—
rbac · NOT-VERIFIED
Environment review pending · —
—
webhook-access · NOT-VERIFIED
Environment review pending · —
—
community-nodes · NOT-VERIFIED
Environment review pending · —
—
network-egress · NOT-VERIFIED
Environment review pending · —
—
backup · NOT-VERIFIED
Environment review pending · —
—
logging · NOT-VERIFIED
Environment review pending · —
—
published-workflow · NOT-VERIFIED
Environment review pending · —
—

Customer acceptance

STATUS	RECORDED WITH
NOT-RECORDED	Customer acceptance pending
—	