DECEPTION CHECK

DEPLOYMENT CHECK / ONE APPLICATION AND ONE RELEASE

What are we actually shipping?

Record references to evidence. Keep credentials and full sensitive response bodies in restricted storage.

01 / Identify the release

Application / business owner / technical owner

Artifact ID or digest / deployment date / evidence reference

02 / Check the boundary

Private tool files in scope / intentionally published configuration

Final artifact inspected by / result / excluded paths

03 / Verify the route

Web root / public route / CDN or cache owner

Approved test path / time / response evidence reference

A repository ignore rule is only one control. Inspect the built package and the actual serving behavior. A 200 status alone does not establish that a private file was returned.

DECEPTION CHECK

RESPONSE CHECK / REQUEST, RESPONSE, AND CREDENTIAL USE

What did the visitor get?

Record the strongest finding supported by the evidence. Assign a person, an action, and a retest.

Request observed

Preserve path, time, method, response metadata, and nearby requests. Review approved tests separately.

Unexpected file served

Preserve restricted evidence; correct packaging, access rules, and any cached copies.

Real secret exposed

Revoke or rotate through the provider, investigate use, and fix the deployment path.

04 / Name the next action

Action / owner / due date / evidence location

Provider revocation or rotation reference, if needed

Retest result / reviewer / next release check

TOOLS AND FIELD NOTE

Use standard web-access rules and the local staged-path checker alongside the deployment review. A path match is a triage lead; inspect the contents and intended audience.

deceptioncheck.ai/research