

PROOFLABS / PUBLIC SYNTHETIC SAMPLE

Evidence Assurance Review.

From security signal to reviewable evidence.

DOSSIER	PD-EAR-DEMO-2026-001
RELEASE STATE	PUBLIC_SYNTHETIC_SAMPLE
SCOPE	STATIC / PASSIVE / NO REAL TARGET
DATE	28 AUGUST 2026

THIS IS NOT A PENTEST. NO REAL SYSTEM OR CUSTOMER DATA WAS USED.

A complete assurance route, demonstrated without a real target.

This dossier shows the form and evidence discipline of a ProofLabs Evidence Assurance Review. All assets, observations and hashes are synthetic demonstration material.

5	3	2	0
FINDINGS	FIXED + RETESTED	OPEN DECISIONS	ACTIVE TESTS

Decision in one line

The synthetic review is complete and traceable. Three findings reached CLOSED_FIXED after passive retest; two owner decisions remain visible and were not converted into false closure.

Management conclusion

The value is not an automated severity score. The value is the chain from authorized scope to evidence, independent review, remediation, retest and a bounded closure decision. The sample deliberately preserves open questions instead of claiming general system safety.

What a customer can rely on

- Every released observation has a source, evidence ID, hash, confidence statement and reviewer state.
- Severity and confidence are recorded separately.
- No active exploitation, network interaction, credentials or production mutation occurred.
- DPIA material is technical input; the controller and DPO retain the legal decision.
- Closure names remaining risks and data-handling limits instead of implying certification.

RELEASE DECISION: REVIEWABLE SAMPLE / NOT CERTIFIED / NOT A SAFETY GUARANTEE

The review starts with boundaries, not tools.

A real engagement cannot begin until the customer owner, reviewer, data route and exact scope are named. This sample substitutes synthetic roles and lab assets only.

Control	Sample record	Decision
Engagement	PD-EAR-DEMO-2026-001	PUBLIC_SYNTHETIC_SAMPLE
Authorizer	ProofLabs Demo Owner role	Synthetic demonstration authority only
Review lead	Evidence Review Lead role	No real target authority
Independent review	Separate Quality Reviewer role	Required before release
Time window	25-27 August 2026, Europe/Amsterdam	Closed
Data class	PUBLIC_SYNTHETIC_ONLY	No customer or personal data

Included - green lane	Excluded - hard boundary
Synthetic policy, threat model, source snippets, configuration, dependency manifest, finding triage, remediation evidence and passive retest.	Network scanning, real domains, credentials, exploitation, denial-of-service, social engineering, persistence, exfiltration and production mutation.

Stop conditions

- Unexpected personal data, secrets or credentials.
- Any target, technique or effect outside the approved register.
- Missing human reviewer or unclear customer decision authority.
- Any need for active validation that was not separately authorized.
- Loss of evidence integrity, time source or audit trail.

FIRST-REASON-WINS: UNCERTAINTY PRODUCES PAUSE OR STOP, NEVER SILENT SCOPE EXPANSION

One finding, five controlled transitions.

The workflow prevents raw scanner or model output from becoming a customer claim without traceable evidence and human review.

01	REGISTER	Source, rights, date, hash
02	HYPOTHESIS	Observation without overclaiming
03	REVIEW	Severity and confidence separated
04	REMEDiate	Owner, change and deadline
05	RETEST	Evidence and closure decision

Required evidence unit

Field	Required content
Identity	Engagement ID, finding ID, source ID and release state
Provenance	Origin, collection date, method/tool version and input hash
Integrity	SHA-256, version, timestamp and redaction status
Meaning	Observation, interpretation, recommendation and limitation kept separate
Review	Named operator role, independent reviewer role and decision rationale
Privacy	Data classification, minimization decision, retention and deletion trigger

Fail-closed design rule

No source, no released claim. No independent review, no customer finding. No retest evidence, no CLOSED_FIXED. No customer risk decision, no accepted residual risk.

Five synthetic signals, with certainty kept visible.

The table is the review index. Detailed evidence remains in controlled appendices; no exploit code, credentials or sensitive raw data belongs in the management dossier.

ID	Finding	Severity	Confidence	Evidence state	Closure
F-001	Outbound webhook allowlist absent	Medium	High	SUPPORTED	CLOSED_FIXED
F-002	Dependency range permits unreviewed minor updates	Low	High	SUPPORTED	CLOSED_FIXED
F-003	Secret-rotation response time not defined	Medium	High	SUPPORTED	PARTIAL
F-004	Provider retention evidence not attached	Medium	Medium	NEEDS_EVIDENCE	OWNER_DECISION
F-005	Debug logging retains synthetic identifiers	Low	High	SUPPORTED	CLOSED_FIXED

Reading the register

- Severity estimates potential impact if the finding is true and reachable.
- Confidence describes the strength of the available evidence.
- SUPPORTED means passive evidence supports the observation; it does not mean exploitability was tested.
- NEEDS_EVIDENCE remains open. It is not quietly downgraded or presented as resolved.
- CLOSED_FIXED requires a scoped retest against the agreed correction.

0 CRITICAL / 0 ACTIVE EXPLOITS / 0 REAL TARGET INTERACTIONS

Why an open decision is healthy

F-004 remains visible because the sample lacks external provider evidence. A polished dossier is not one where every row is green; it is one where unknowns cannot disappear.

05 / FINDINGS IN CONTEXT

Observation, impact and limitation stay separate.

F-001 / CLOSED_FIXED

Outbound webhook allowlist absent

Observation: the synthetic configuration accepted an arbitrary destination string. Evidence: EVD-003. Potential impact: unintended outbound data routing if similar logic existed in a real system. Limitation: no host was contacted and reachability was not tested.

Fix: explicit hostname allowlist, redirect deny and egress policy. Retest: static configuration review supports the fix at sample commit DEMO-FIX-01.

F-002 / CLOSED_FIXED

Dependency range permits unreviewed minor updates

Observation: one synthetic dependency used a permissive range without a locked artifact review. Evidence: EVD-004. Potential impact: uncontrolled supply-chain change. Limitation: no vulnerability or malicious package was claimed.

Fix: lockfile pin, integrity validation and review rule. Retest: manifest and lockfile evidence are consistent.

F-003 / PARTIAL

Secret-rotation response time not defined

Observation: the synthetic incident policy required rotation but had no owner or service-level target. Evidence: EVD-001. Potential impact: delayed containment after exposure. Limitation: no secret was received or tested.

Partial fix: Security Owner role and four-hour target proposed. Open: management must approve staffing and escalation coverage.

Fix evidence is part of the dossier, not a follow-up email.

F-004 / OWNER_DECISION - Provider retention evidence not attached

The synthetic data-flow register names an external analysis provider but the sample does not contain a current contract, retention setting or regional processing receipt. Confidence remains Medium because absence in this sample is not proof of absence in a real organization.

Required owner decision

Attach current DPA/order-form evidence and document retention, training use, region and subprocessors - or remove the provider from the approved route. Counsel and the DPO decide adequacy.

F-005 / CLOSED_FIXED - Debug logging retains synthetic identifiers

Static review found synthetic subject identifiers in a debug output example. The correction replaces identifiers with bounded event codes and shortens diagnostic retention. The passive retest confirms the sample configuration and code no longer emit the identifier field.

Finding	Retest basis	Result	Reviewer state
F-001	Config diff + policy EVD-006	FIXED	REVIEWED
F-002	Manifest + lock integrity EVD-007	FIXED	REVIEWED
F-003	Draft response control EVD-008	PARTIAL	OWNER APPROVAL OPEN
F-004	No new provider receipt	INCONCLUSIVE	OWNER DECISION OPEN
F-005	Code/config diff EVD-009	FIXED	REVIEWED

RETEST SCOPE: ONLY THE ORIGINAL OBSERVATION AND THE AGREED FIX

Technical input for the controller and DPO - not a compliance verdict.

This public sample uses no personal data. The screening outcome below applies only to the synthetic demonstration and cannot be copied into a customer DPIA without a new assessment.

Question	Synthetic sample answer	Evidence / decision owner
Personal data processed?	No. Synthetic identifiers and generated records only.	EVD-002 / ProofLabs Demo Owner
Real people evaluated or scored?	No.	Scope register
Systematic monitoring?	No.	Scope register
Special or criminal data?	No.	Data inventory
External model data egress?	No.	Execution receipt
Full DPIA triggered?	No for this synthetic sample only.	Controller decision required for real work

Risks a real engagement must assess

- Credential or secret exposure during code or configuration review.
- False positive or overstated finding affecting people or business decisions.
- Scope escape, wrong target or use of evidence beyond the instructed purpose.
- Excessive retention, unauthorized access or incomplete deletion.
- Model/provider logging, training use or regional processing outside the approved route.
- Disclosure of vulnerability details to an unauthorized recipient.

Decision boundary

ProofLabs supplies technical risks, controls, evidence and open questions. The customer as controller decides legal basis, necessity, proportionality, DPIA outcome and residual risk with its DPO/counsel.

Minimal data, short retention, provable closure.

Class	Sample treatment	Real engagement default
PUBLIC	May appear with source attribution	Retain to closure plus agreed period
CUSTOMER_INTERNAL	Not used	Tenant-separated, encrypted, named access
SECURITY_RESTRICTED	Synthetic finding detail only	Restricted evidence, no open export
PERSONAL_DATA	Not used	Redact/pseudonymize; shortest necessary retention
SPECIAL / CRIMINAL	Not used	NO-GO without separate legal basis and DPIA
SECRET	Not used	Never intentionally collect; stop and rotate on exposure

Sample data-flow receipt

Stage	Location	Data	Result
Authoring	Local controlled workspace	Synthetic records	COMPLETE
Analysis	Local static review	Synthetic source snippets	COMPLETE
Model egress	None	None	NOT PERFORMED
Public release	This PDF only	Reviewed synthetic summary	APPROVED SAMPLE
Closure	Local evidence manifest	Hashes and release record	COMPLETE

NO CREDENTIALS / NO CUSTOMER CODE / NO PERSONAL DATA / NO EXTERNAL MODEL REQUEST

Closed with two visible owner decisions.

A review may close operationally while residual decisions remain assigned. The closure state must not erase open risk or imply general safety.

Closure item	Status	Evidence
Approved scope completed	YES	Scope register + review log
Prohibited methods performed	NO	Execution receipt
Real customer data received	NO	Data inventory
Findings fixed and retested	3 OF 5	EVD-006 to EVD-009
Open decisions assigned	YES	F-003 and F-004
Access to revoke	NONE	Synthetic local workflow
Deletion exceptions	NONE	No customer dataset
Incident open	NO	Stop/incident register

Residual decision register

ID	Decision	Owner	Review trigger
F-003	Approve rotation SLA, named coverage and escalation path	Security Service Owner	Before first paid green-lane pilot
F-004	Approve provider route based on DPA, retention and region evidence	DPO + Counsel + Contract Owner	Before any private customer data

Closure state

CLOSED_WITH_OPEN_OWNER_DECISIONS. The synthetic review activity is complete. F-003 and F-004 remain open governance decisions and cannot be represented as fixed, compliant or certified.

What ProofLabs may sell now - and what remains blocked.

Lane	Offer	Current state
GREEN	Policy, threat model, code/config/dependency review, DPIA-ready evidence, remediation and passive retest	CONDITIONAL PILOT
YELLOW	Limited real-target validation under separate authorization and qualified partner responsibility	BLOCKED UNTIL ALL GATES
RED	DoS, social engineering, credential attacks, persistence, lateral movement, exfiltration or production mutation	NOT OFFERED

Commercial launch gates still open

- Counsel and DPO approval of claims, contracts, data route and DPIA templates.
- Professional and cyber liability coverage for the exact service scope.
- Named service owner, qualified independent reviewer and tested incident/closure process.
- Tenant-isolated evidence platform with RBAC, audit, retention and deletion evidence.
- Written approval for the intended OpenAI business/downstream route when applicable.
- Qualified partner, external identity/signing and isolated runner before any real-target lane.

PUBLIC WEBSITE: EVIDENCE ASSURANCE REVIEW / NOT PENTEST / NOT DPIA-COMPLIANT

Safe customer promise

We make the security evidence reviewable: what was in scope, what supports each finding, who reviewed it, what was fixed, how it was retested and what remains unresolved.

Every released item has provenance and integrity context.

These hashes are deterministic over labelled synthetic sample records. They do not attest to any external system or customer artifact.

Evidence ID	Description	Class	SHA-256
EVD-001	Synthetic security policy	PUBLIC_SYNTHETIC	6d14e7d0b91d5b44...
EVD-002	Synthetic data-flow and pre-DPIA register	PUBLIC_SYNTHETIC	1b2e25e2d8c8d581...
EVD-003	Synthetic webhook configuration	PUBLIC_SYNTHETIC	4afa823cef1e5bc8...
EVD-004	Synthetic dependency manifest	PUBLIC_SYNTHETIC	93cbe2d92f82650b...
EVD-005	Synthetic threat model	PUBLIC_SYNTHETIC	8be1e6fb43bab4bf...
EVD-006	Webhook remediation diff	PUBLIC_SYNTHETIC	11308026e4e9f927...
EVD-007	Dependency lock remediation evidence	PUBLIC_SYNTHETIC	c575799e3c490c85...
EVD-008	Draft incident response control	PUBLIC_SYNTHETIC	5faabc0c3f55560b...
EVD-009	Logging minimization diff	PUBLIC_SYNTHETIC	f57a12d6f591f992...

Review record

Control	Sample state
Source provenance	COMPLETE for synthetic sample
Hash verification	COMPLETE
Severity/confidence separation	COMPLETE
Independent human review	DEMONSTRATED AS ROLE BOUNDARY; assign named person before customer use
Customer/controller decision	NOT APPLICABLE to public sample
External timestamp/signature	NOT ESTABLISHED; commercial launch gate

EVIDENCE INTEGRITY IS NOT THE SAME AS TRUTH, AUTHORITY OR CERTIFICATION

A controlled first engagement starts small.

Recommended green-lane pilot

Phase	Customer input	ProofLabs output
1. Qualify	One decision question and named owner	Lane, data class and stop decision
2. Bound	Exact repo/artifact and exclusions	Scope, roles, privacy and review criteria
3. Review	Approved code/config/policy evidence	Hypotheses and source-bound finding register
4. Decide	Business context and control owners	Human triage, priorities and remediation plan
5. Close	Fix evidence and risk decisions	Passive retest, residual risk and closure receipt

Reference framework

- NIST SP 800-115 - planning, Rules of Engagement, execution and reporting structure.
- NCSC Netherlands - explicit authorization, secure handling, disclosure and retest considerations.
- GDPR Articles 28, 32, 35 and 36 - processor controls, security, DPIA and prior consultation boundaries.
- ProofLabs EvidenceOps - source, finding, reviewer, remediation, retest and closure discipline.

Start safely

Share only the decision question, expected source types and intended reviewer by ordinary email. Do not send code, credentials, logs or sensitive dossier material until scope, contract and secure channel are agreed.

PROOFLABS.NL / INFO@PROOFLABS.NL / EVIDENCE ASSURANCE REVIEW

Document state: PUBLIC_SYNTHETIC_SAMPLE. No real target was accessed. No private data was processed. No model or external provider was invoked to analyze customer data. This document is not legal advice, a pentest report, a certificate or a compliance guarantee.