Evidence Packet

Measured using synthetic test data

Curated from an existing schema-2 Developer Evaluation export containing four retained decisions recorded October 27-29, 2026. This is not a new execution run.

Source export: 2026-11-07T06:58:36.404Z

Public curation: 2026-11-07T07:36:13.000Z

Read the records, with their boundaries

Four recorded requests, one exact policy version. Complete refers to four retained records out of four lifetime records in the supplied snapshot; it is not suite coverage, regulatory compliance, accuracy or production readiness.

Evaluation, user, tenant, application, receipt, request, decision-event and grant identifiers are replaced with deterministic public aliases, including correlated references and navigation paths. The private mapping is not distributed.

Historical fingerprints are preserved exactly as recorded. Original input and output bodies are not included, so those fingerprints cannot be independently recomputed here and do not authenticate the remapped identifiers or this packet. The manifest separately hashes the downloadable file bytes.

No external provider or customer production activity is represented. Final release authorization is not proof of delivery. The historical build version and original payload bodies were not included in the source export.

The following pages reuse the existing Evaluation PDF renderer. All four request records are included. The manifest and verify.mjs check packet file bytes, not authenticity, regulatory compliance or historical body fingerprints.

EVIDENCE FOR YOUR ENGINEERING DECISION

Evaluation evidence brief

Recorded decisions. Observed controls. A clear next step.

GENERATED 2026-11-07 06:58:36.404Z | STATUS ACTIVE

Workspace: 10000000-0000-4000-8000-000000000001

RETAINED REQUESTS

4

4 lifetime decisions

RETAINED WINDOW (UTC)

From: 2026-10-27 18:46:48.707Z

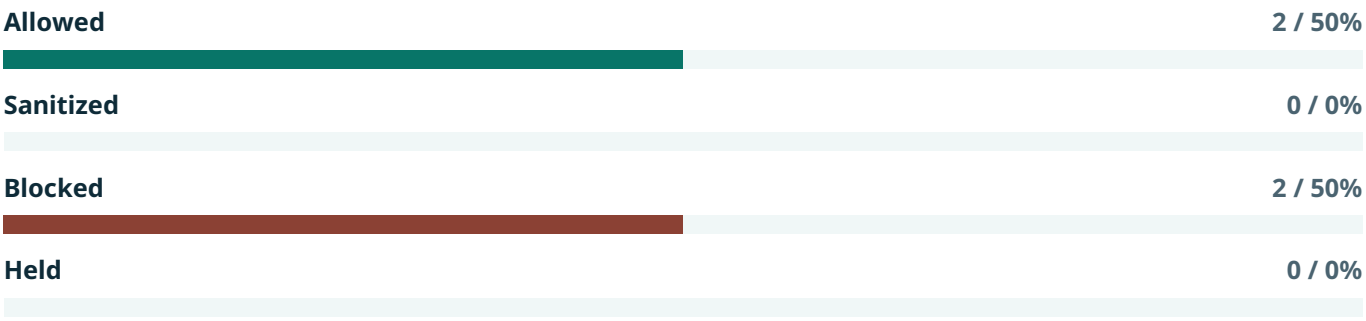
To: 2026-10-29 18:40:14.411Z

Organization-scoped evaluation snapshot

LSAS Platform recorded 4 governed requests across 1 policy version: 2 final outputs authorized unchanged, 0 final outputs sanitized before release authorization, and 2 withheld. These counts describe final outcomes; an earlier ingress transformation is recorded separately in scenario evidence. They do not establish application-wide detection accuracy.

Final request outcomes

Common scale: 0 to 4 retained requests. Labels show count / share.



One final outcome per recorded request. Percentages use the full retained total, not the appendix; rounded values may not sum to 100%.

COMPLETE RETAINED DECISION HISTORY

4 retained records / 4 lifetime decisions. Outcome and policy totals use the full retained history, not the appendix excerpt.

BOUNDARY CONTROLS & INTERPRETATION

Where controls were observed

Content controls at ingress and egress. These are matching recorded requests, separate from the final-outcome distribution.

Common scale: 0 to 2 matching requests.

Ingress / Sanitize before the provider	**0 requests**
Ingress / Block before provider dispatch	**2 requests**
Ingress / Hold before provider dispatch	**0 requests**
Egress / Sanitize output before release	**0 requests**
Egress / Block at the output boundary	**0 requests**
Egress / Hold at the output boundary	**0 requests**

Matching recorded requests; controls can overlap and must not be added into a request total. Zero means not observed in this evidence, not a failed or unavailable control.

4 records inspected from the retained snapshot.

Read the outcomes and boundaries

FINAL OUTCOMES

Allowed / Released

Final checked output authorized unchanged. An earlier input may already have been sanitized.

Sanitized / Transformed

Final output changed, checked again, and authorized for return.

Blocked

Protected output withheld because a control denied release. The boundary shows where enforcement occurred.

Held

Output withheld because release conditions were unmet. A hold does not establish completed human review or approval. ESCALATE_HITL requests human-in-the-loop review; it does not prove a handoff.

ENFORCEMENT STAGES

Ingress

Checks before provider or action dispatch. A recorded block with zero invocations demonstrates that execution was prevented.

Egress

Checks before output is returned. Execution may already have occurred; withholding output does not establish that execution was prevented.

Action permission

Permission to invoke a registered action is separate from authorization to release its output.

OBSERVED CONTROLS

Observed controls & evidence gaps

A control is observed only when the retained request evidence demonstrates it. These counts are not a score or a pass rate.

CONTROL / RECORDED BEHAVIOR	STATE / REQUESTS
Authorize unchanged output The final content boundary authorized output without a transformation.	OBSERVED 1 request
Sanitize before the provider Ingress was transformed before the synthetic provider was invoked.	NOT OBSERVED 0 requests
Block before provider dispatch Ingress was blocked and the synthetic provider received zero calls.	OBSERVED 2 requests
Hold before provider dispatch Ingress was held and the synthetic provider received zero calls.	NOT OBSERVED 0 requests
Release with a warning The final content decision retained a warning while authorizing release.	NOT OBSERVED 0 requests
Sanitize output before release The output boundary transformed and revalidated the content before authorizing release.	NOT OBSERVED 0 requests
Block at the output boundary A payload or synthetic-provider response was blocked at egress.	NOT OBSERVED 0 requests
Hold at the output boundary A payload or synthetic-provider response was withheld at egress.	NOT OBSERVED 0 requests
Authorize the registered action The kernel authorized the fixed synthetic reader and recorded one invocation.	OBSERVED 1 request
Deny an unauthorized action The kernel denied the fixed action attempt and recorded zero invocations.	NOT OBSERVED 0 requests

Counts are matching recorded requests, not distinct test cases, detection accuracy, or a suite pass rate. A missing observation means this retained evidence does not demonstrate that control; it does not establish that the control failed or is unavailable. Local suite assertions and application handler behavior are not persisted here.

Snapshot: 2026-11-07 06:58:36.404Z. 4 retained records inspected. The complete recorded history is present.

CONTROL EVIDENCE REFERENCES

Trace the observed controls

These references come from the full retained history. A matching request can be older than the 25-record appendix; use the full export to inspect it.

Authorize unchanged output / 1 matching request

Exact policy: developer-data-guard@1.0.0

Example request: 30000000-0000-4000-8000-000000000004

Block before provider dispatch / 2 matching requests

Exact policy: developer-data-guard@1.0.0

Example request: 30000000-0000-4000-8000-000000000001

Authorize the registered action / 1 matching request

Exact policy: developer-data-guard@1.0.0

Example request: 30000000-0000-4000-8000-000000000003

Inspect the full retained evidence (HTML)

POLICIES & MEASUREMENT

Policies actually tested

Exact recorded versions define the configured checks. A selected policy, or a policy's configured coverage, is not proof that every control was exercised.

Developer Data Guard / 4 decisions

developer-data-guard@1.0.0

Deterministic JSON data-boundary evaluation for supported personal-data, credential and prompt-injection patterns. Not a compliance certification.

Configured coverage: Email, phone and supported identifier patterns; Structured credentials and known secret patterns; Known prompt-injection patterns

Limits: Pattern-based checks can miss sensitive data. No model call, destination delivery or full security assessment.

Recorded engine timing

Median 190.5 ms | P95 1877.7 ms | 4 samples

Recorded engine timing varies by route: payload requests measure the initial validator pass; synthetic-provider scenarios span ingress, the local adapter (including its pre-dispatch authority check), and egress up to the last policy evaluation. Final transformation checks can fall outside that interval. Action tests include content checks, local kernel execution, intermediate authority reads, and kernel audit writes, before final publication checks. Excludes network, authentication, final database commit, and work performed by your application. Mixed-route summaries are not comparable latency benchmarks.

A recorded zero reflects timer precision, not zero end-to-end latency. This is not a load benchmark.

INTERPRETATION & NEXT STEPS

Turn the evidence into a next step

Use this snapshot as an engineering review input. It grants no approval, override or deployment authority.

Evidence still to establish

3 synthetic-provider requests; 1 synthetic reader invocation; 0 action denials with zero invocations.

7 of 10 listed controls are not observed in this retained set. Run the missing cases relevant to your application's purpose, then review their exact outcomes. An absent observation is not a failed control.

01 Keep an application contract suite

Declare expectations for representative synthetic cases, run the reusable test kit in CI, and reconcile its local results with these committed request records. Local assertions and receiver behavior remain separate evidence.

Open the application contract suite

02 Connect the evidence to Discovery

Use the observed controls and evidence gaps to identify which application data surfaces need a scoped Discovery Scan. The evaluation does not establish estate-wide coverage.

Discuss scope with LSAS Platform

03 Prepare your application for a pilot

Bring the local brief's application purpose, integration point, open questions, and these exact policy references into organization onboarding and alignment review. A tenant pilot establishes the permitted runtime boundary; this evaluation grants no approval or deployment authority.

Discuss scope with LSAS Platform

Scope & limitations

These are deterministic checks on the recorded requests, not a certification or a guarantee that every sensitive value or harmful instruction is detected.

Persisted evidence proves the release decision committed. It does not prove that a downstream application received or correctly used the returned content.

Payload requests use deterministic checks; provider scenarios and the action lab use fixed in-process synthetic adapters. No external model provider, external connector, arbitrary tool, or production workflow is exercised.

Observed control counts describe committed requests. They do not verify a local contract suite's assertions, establish detection accuracy, or grant application deployment or review authority.

Payload bodies are not retained in this report. Compare request IDs with your local terminal or the transient console scenario result to inspect actual returned content.

These results do not establish general detection accuracy, compliance or production readiness.

REQUEST EVIDENCE APPENDIX

Request evidence appendix

This brief includes 4 of 4 retained request records, limited to the most recent 25. The full-history summary is not limited.

Workspace: 10000000-0000-4000-8000-000000000001

How to read the record

Allowed means authorized for return. Sanitized means changed and revalidated before release authorization. Blocked and held mean protected content was withheld. A commit is not a downstream delivery acknowledgement.

Released artifact fingerprints are SHA-256 of JSON.stringify of the authorized returned data, preserving serialization order. Withheld content has no released artifact fingerprint. Hashes are not anonymization guarantees.

Grant details describe the recorded execution and are not reusable authority. A computed execution receipt alone does not authorize release; inspect the final recorded outcome.
These fixed-policy evaluation receipts do not establish organizational baseline approval, an accountable approver or completed human review.

Open the full retained evidence (HTML)

Download full retained metadata and fingerprints (JSON)

01 BLOCKED / Release denied

Input blocked before provider dispatch. Input rule details were not retained for this request. The provider was not invoked; no provider output was evaluated.

Request: 30000000-0000-4000-8000-000000000001

Recorded: 2026-10-29 18:40:14.411Z | Engine time: 0 ms (rounded)

Exact policy: developer-data-guard@1.0.0

Final decision: BLOCKED | Outcome: BLOCKED | Boundary: ingress

Rules in this decision: PROMPT_INJECTION_HEURISTIC

Synthetic scenario: block-input (original example)

Ingress: BLOCKED / BLOCKED | Actual recording-provider calls: 0

Input remediation details were not retained.

Recorded validator versions: pii-phi@1.1.1, prompt-injection@1.2.0, security-secrets@1.1.0

Released artifact SHA-256: none - protected output withheld.

02 BLOCKED / Release denied

Input blocked before provider dispatch. Input rule details were not retained for this request. The provider was not invoked; no provider output was evaluated.

Request: 30000000-0000-4000-8000-000000000002

Recorded: 2026-10-29 18:06:55.808Z | Engine time: 1 ms

Exact policy: developer-data-guard@1.0.0

Final decision: BLOCKED | Outcome: BLOCKED | Boundary: ingress

Rules in this decision: PROMPT_INJECTION_HEURISTIC

Synthetic scenario: block-input (original example)

Ingress: BLOCKED / BLOCKED | Actual recording-provider calls: 0

Input remediation details were not retained.

Recorded validator versions: pii-phi@1.1.1, prompt-injection@1.2.0, security-secrets@1.1.0

Released artifact SHA-256: none - protected output withheld.

03 ALLOWED / Registered synthetic read authorized

1 recorded synthetic reader invocation. The final outcome governs whether its output was authorized for return.

Request: 30000000-0000-4000-8000-000000000003

Recorded: 2026-10-27 18:47:17.044Z | Engine time: 2142 ms

Exact policy: developer-data-guard@1.0.0

Final decision: ALLOW | Outcome: RELEASED | Boundary: egress

Rules in this decision: None recorded

Synthetic action: allowed-read | AUTHORIZED | Actual synthetic reader invocations: 1

Content decision: ALLOW | Requested skill: lsas.evaluation.records.read

Destination: lsas-evaluation://records/approved

Manifest: lsas.evaluation.records.read@1.0.0

Manifest SHA-256: 48e7ea84c5d0bc7e9c6674d6c13e58113785407b4b6070323450fb473e4a4e02

Recorded grant: 50000000-0000-4000-8000-000000000003 | Expires: 2026-10-27 18:47:24.312Z

Input SHA-256: 57917c57c9ced57600eef5fa07b6aaeb8ae2f5a6f50517ac5b3e824c953f6088

Action SHA-256: b4ab0a61ba3051382b6028522386cfb23555d1728aec910d87f58bd0b750a0c3

Authority SHA-256: 99ef788ca86d0fb2dde030cca50ef0b83a756afe45c9e81340cfe7d58d939ee7

Execution receipt: computed-unreleased

Reader output SHA-256: e7b496a2f19ad8397da7867d92d20fd4f2971c89e841727372d10b5f109e4df9

Recorded validator versions: pii-phi@1.1.1, prompt-injection@1.2.0, security-secrets@1.1.0

Released artifact SHA-256: e7b496a2f19ad8397da7867d92d20fd4f2971c89e841727372d10b5f109e4df9

04 ALLOWED / Output authorized unchanged

Input authorized for provider dispatch. Input rule details were not retained for this request. No rule matches were recorded at the final output boundary. This does not establish that all risks were absent.

Request: 30000000-0000-4000-8000-000000000004

Recorded: 2026-10-27 18:46:48.707Z | Engine time: 380 ms

Exact policy: developer-data-guard@1.0.0

Final decision: ALLOW | Outcome: RELEASED | Boundary: egress

Rules in this decision: None recorded

Synthetic scenario: safe-release (original example)

Ingress: ALLOW / RELEASED | Actual recording-provider calls: 1

Input remediation details were not retained.

Ingress artifact SHA-256: 7b1dc83bdc9c0dc68817dc653d99ef285b4e88cff992207c13cb19eb3b1d2bb2

Recorded validator versions: pii-phi@1.1.1, prompt-injection@1.2.0, security-secrets@1.1.0

Released artifact SHA-256: 1abae86b19980619984798c8944885dc062380ff03cf811cce82d8cf938141cb