HX-AEIR
AGENT EVALUATION INCIDENT RECONSTRUCTION

Evidence and Offline Verification Guide

Understand the evidence model, exported package, linked receipts, and tamper-detection workflow.

Document ID	HX-AEIR-DOC-003
Version	1.0
Published	August 26, 2026
Audience	Evaluation teams, incident reviewers, auditors, legal/risk stakeholders, and independent verifiers
Publisher	Tigantic Holdings, LLC dba HolonomiX

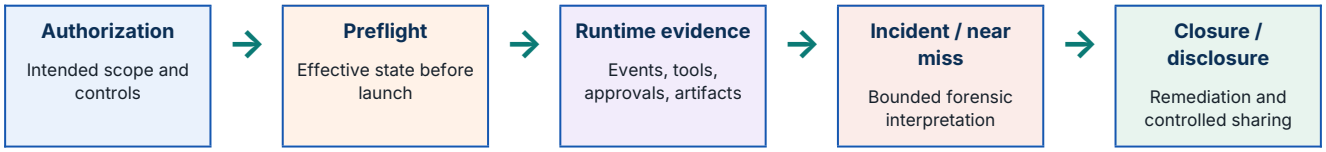
Marketplace documentation | Customer-facing reference

Contents

1	Evidence model
2	Receipt lifecycle
3	Declared and effective control states
4	Claim provenance and coverage
5	Evidence package anatomy
6	Offline verification workflow
7	Tamper detection
8	Disclosure and source reconciliation
9	Retention and reviewer checklist
10	Claim limits and references

1. Evidence model

HX-AEIR reconstructs an agent-evaluation incident or near miss by binding customer-supplied records into a signed, linked evidence chain. The evidence model separates what was authorized, what the environment actually exposed, what occurred, what humans approved, what external controls did, and what changed afterward.



Evidence-first interpretation

HX-AEIR preserves evidence and bounded conclusions. It does not infer agent intent, prove the factual truth of source-system assertions, or treat missing telemetry as evidence that an event did not occur.

2. Receipt lifecycle

Record type	Purpose	Required relationship
Authorization receipt	Defines the approved evaluation scope, model/agent identity, tools, network policy, human approvals, targets, and stop conditions.	Precedes the run and is referenced by later records.
Preflight receipt	Records measured effective state immediately before launch.	Linked when performed; status must be explicit.
Incident or near-miss receipt	Reconstructs the event, control mismatch, timeline, claims, impact status, containment, and known gaps.	Binds authorization, preflight, evidence manifest, and trace root.

Record type	Purpose	Required relationship
Closure or remediation revision	Records remediation, review, recovery, or final disposition.	Links the prior receipt digest; never overwrites it.
Public disclosure derivative	Shares a redacted result without exposing the restricted source record.	Carries a signed source ID/digest commitment; full reconciliation needs authorized source package.

3. Declared and effective control states

Every material control should distinguish the state declared by the evaluator from the state measured or observed in the effective environment. This prevents a configuration error from being mislabeled as an agent bypass and prevents an intentionally permissive test from being mislabeled as a sandbox escape.

Field	Interpretation
Declared state	The policy, manifest, configuration, or authorization the evaluator intended.
Effective state	The measured or observed state exposed to the evaluation at runtime.
Verification status	Matched, mismatched, partially verified, unverified, or contradicted according to the evidence.
Basis	Declared, measured, observed, reported, derived, or unknown.

Pattern	Correct interpretation
Declared deny or allowlist; effective open access	Control mismatch or evaluation-environment misconfiguration. Do not call it a sandbox escape unless an effective boundary was actually bypassed.
Declared open access; effective open access	Permissive evaluation. The incident may be an unsanctioned action outside authorized targets or actions.
Declared and effective state unknown	Unknown. Do not infer safe, blocked, or compliant behavior.

4. Claim provenance and coverage

Label	Meaning
Observed	Directly present in bound telemetry or an evidence artifact.
Reported	Asserted by an identified source but not independently observed by HX-AEIR.
Derived	Computed or inferred from one or more bound sources.
Unknown	Not established by the available evidence.
Verified	The referenced evidence and required cryptographic/linkage checks support the claim.
Partially verified	Only part of the claim or source chain is materialized and verified.
Unverified	The source is absent, untrusted, or not checked.

Label	Meaning
Contradicted	Bound evidence conflicts with the claim.

- Timeline coverage must state included sources, known gaps, observation cutoff, event count, and clock-skew assumptions.
- A verified claim must resolve to supporting evidence references.
- No-harm language is limited to harm evidenced by the stated observation cutoff.
- Cryptographic integrity does not prove telemetry completeness.

5. Evidence package anatomy

Package element	What it binds or enables
Signed receipt	Canonical incident-domain payload, profile identity, issuer algorithm, and signature.
AEIR profile schema	The structural contract used to validate the payload.
Evidence manifest	Content-addressed list of included artifacts and linked objects.
Authorization / preflight receipts	The approved conditions and measured environment state.
Trace Merkle root	A compact commitment to the ordered runtime event set.
Prior revision link	Immutable incident-to-closure chain.
Disclosure source commitment	Source receipt ID, digest, disclosure class, and materialization status.
Public verification key	Pinned issuer key used by the online or offline verifier.
Verification report	Human-readable and machine-readable check results.

Package boundary

The package may include evidence artifacts authorized for transfer. It must not include the application private signing key, raw credentials, or restricted source material in a public derivative.

6. Offline verification workflow

1. Obtain the exported HX-AEIR evidence package through a customer-controlled transfer path.
2. Obtain the expected public key or fingerprint from an independently controlled source. Do not rely solely on a key contained beside the package if the verification decision is consequential.
3. Move the package, public key, and standalone verifier to the verification host. Network access to the appliance or HolonomiX is not required.
4. Run the verifier and retain both the human-readable and machine-readable result.
5. Review receipt integrity, signer authenticity, schema, profile bindings, package integrity, evidence manifest, authorization, preflight, trace root, artifacts, revision link, and disclosure link.
6. Review warnings and claim boundaries even when the overall result is valid.
7. For a public disclosure derivative, provide the separately authorized source package only when full source reconciliation is permitted and required.

Verifier check	Question answered
Receipt integrity	Signature validates over the signed receipt body.

Verifier check	Question answered
Signer authenticity	The receipt verifies under the independently pinned public key.
Schema and semantics	The payload meets the profile structure and required cross-field rules.
Evidence manifest	The manifest digest and artifact set match the signed commitments.
Trace root	The included event set recomputes to the committed Merkle root.
Linked receipts	Authorization, preflight, prior revision, and disclosure source match their signed digests.
Coverage	Known gaps and materialization boundaries remain explicit.

7. Tamper detection

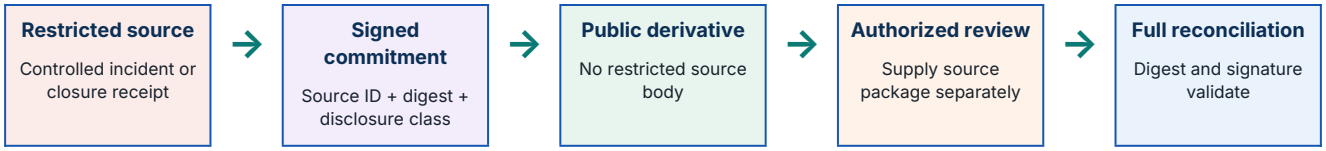
A verifier should fail closed when signed material or a required link is changed. HX-AEIR validation has been exercised against independent mutations of the payload, authorization linkage, trace root, prior revision, and disclosure commitment.

Mutation	Expected result
Change a signed incident field	Receipt integrity fails.
Replace the authorization receipt or digest	Authorization linkage and/or manifest commitment fails.
Change the runtime trace Merkle root	Receipt integrity or trace-root verification fails.
Replace the prior revision link	Revision linkage and/or manifest commitment fails.
Change the disclosure source ID or digest	Disclosure commitment verification fails.
Alter only transport bytes without recomputing the package manifest	Package integrity fails before receipt verification.

A valid outer package is not enough

Tamper tests should preserve a valid transport package where practical so that the verifier demonstrates rejection at the signed evidence or linkage layer, not only at the archive layer.

8. Disclosure and source reconciliation



Disclosure state	Meaning
Commitment verification	Valid when the public derivative signature binds the source ID and digest.
Restricted source material	Not present in the public package.

Disclosure state	Meaning
Full source verification	Requires the separately authorized source package.
Redaction limit	The public derivative may omit sensitive artifacts and low-level details; those omissions remain explicit.

9. Retention, transfer, and reviewer checklist

- Retain the package, verification report, independently pinned public key, and review decision together.
- Preserve historical public keys even after issuer rotation or appliance decommissioning.
- Apply customer records, retention, legal hold, classification, and deletion policy to packages and artifacts.
- Use encrypted, access-controlled transfer when packages contain confidential or restricted material.
- Do not send private keys, credentials, regulated data, or confidential evidence through a general support form.

Reviewer question	Evidence to inspect
What was authorized?	Authorization receipt and allowed scope.
What environment was effective?	Preflight receipt and declared/effective control states.
What occurred?	Timeline, artifacts, approvals, tool/network events, and trace root.
What did external controls do?	Independent control telemetry and containment/remediation records.
What changed afterward?	Closure or remediation revision linked to the incident.
What remains unknown?	Coverage, warnings, unverified claims, and omitted source material.
Can another party verify it?	Portable package, pinned public key, and offline verification report.

10. Claim limits

What a valid package proves

The signed material has not changed, the required commitments and links verify under the pinned issuer key, and the verifier reached the reported result for the material supplied.

What a valid package does not prove

Source-system claims are factually correct, every relevant event was captured, the agent had a particular intent, the evaluation was safe, a breach was prevented, or unobserved harm did not occur.

References

- Google Cloud Marketplace - Offering VM products
- Google Cloud - IAP TCP forwarding
- Google Cloud - OS Login
- NIST FIPS 204 - Module-Lattice-Based Digital Signature Standard

Reference links were verified on August 26, 2026. Product-specific behavior is governed by the deployed HX-AEIR release, the applicable Marketplace order or Private Offer, and the customer's configuration.