

SAMPLE EXPOSURE REPORT

AI-agent identity exposure, made reviewable.

PermitGraph turns supplied identity metadata into an owner-to-credential-to-resource graph, prioritizes consequential access paths, and seals the result with a reproducible evidence digest.

ORGANIZATION Acme Robotics		EXPOSURE SCORE 85 / 100	REPORT ID PG-39F6D8659AD2
3 IDENTITIES	3 CREDENTIALS	3 ACCESS PATHS	9 FINDINGS

Executive readout

- 3 critical paths require immediate human review before production use continues.
- 2 identities lack an accountable owner, weakening approval and incident-response routing.
- 2 credentials never expire, extending access beyond a single agent task or deployment window.

Priority exposure map

SEV	FINDING	SUBJECT	NEXT CONTROL
CRIT	Agent has administrative access to a critical resource	agent:invoice-reconciler -> res:vendor-master	Remove admin scope and grant only the exact task-level actions.
CRIT	Critical write path lacks human approval	agent:invoice-reconciler	Require human approval or reduce the action set to read-only.
CRIT	Identity has no accountable owner	agent:invoice-reconciler	Assign an owner and review access before the next execution.
HIGH	Dormant identity still has access	workload:legacy-sync	Disable the identity or document a current operational need.
HIGH	Identity has no accountable owner	workload:legacy-sync	Assign an owner and review access before the next execution.

EVIDENCE DETAILS

What the report proves - and what it does not.

This sample analyzes a supplied metadata snapshot. It demonstrates graph normalization, deterministic risk rules, a non-enforcing authorization boundary, prioritized remediation, and evidence integrity. It does not prove discovery completeness, enforce access, or certify compliance.

Integrity envelope

ALGORITHM	SHA-256
DIGEST	39f6d8659ad20229f5ebcceb4e55856f0f9a7ddfb29badbc72bb9acdb761f67
COVERS	normalized graph, findings, and advisory authorization boundary
COLLECTION	Metadata only; secret material rejected; no hosted-demo persistence.

Advisory authorization boundary

Normalized from supplied metadata. PermitGraph did not grant, revoke, or modify access.

PATH	ALLOWED ACTIONS	CREDENTIAL / EXPIRY	APPROVAL / REVIEW
agent:invoice-reconciler -> res:vendor-master	admin, read, write	cred:finance-key Expiry not recorded	NOT RECORDED CONTROL GAP accountable owner not recorded; credential expiry not recorded; human approval not recorded for consequential action
spn:deploy-prod -> res:prod-cluster	deploy	cred:oidc-prod 2026-08-16T18:00:00Z	RECORDED BOUNDED AS SUPPLIED No boundary gap produced from supplied fields.
workload:legacy-sync -> res:artifact-store	read, write	cred:legacy-shared Expiry not recorded	NOT RECORDED CONTROL GAP accountable owner not recorded; credential expiry not recorded

Complete prioritized register

SEV	RULE / SUBJECT	WHY IT MATTERS	RECOMMENDED ACTION
CRIT	critical-admin-path agent:invoice-reconciler -> res:vendor-master	agent:invoice-reconciler reaches vendor-master with admin scope.	Remove admin scope and grant only the exact task-level actions.
CRIT	critical-write-no-approval agent:invoice-reconciler	invoice-reconciler can change a critical resource without a recorded approval threshold.	Require human approval or reduce the action set to read-only.
CRIT	missing-owner agent:invoice-reconciler	invoice-reconciler can act without a named business or technical owner.	Assign an owner and review access before the next execution.

SEV	RULE / SUBJECT	WHY IT MATTERS	RECOMMENDED ACTION
HIGH	dormant-identity workload:legacy-sync	legacy-sync has not been observed for 258 days.	Disable the identity or document a current operational need.
HIGH	missing-owner workload:legacy-sync	legacy-sync can act without a named business or technical owner.	Assign an owner and review access before the next execution.
HIGH	non-expiring-credential cred:finance-key	cred:finance-key grants standing access beyond any single agent task.	Replace it with a short-lived, workload-bound credential.
HIGH	non-expiring-credential cred:legacy-shared	cred:legacy-shared grants standing access beyond any single agent task.	Replace it with a short-lived, workload-bound credential.
HIGH	stale-credential cred:legacy-shared	cred:legacy-shared was last rotated 918 days ago.	Rotate or revoke the credential and record its owner.
MED	stale-credential cred:finance-key	cred:finance-key was last rotated 318 days ago.	Rotate or revoke the credential and record its owner.

FOUNDING DESIGN-PARTNER PILOT

\$4,000 fixed / 60 days

Up to three metadata sources, two scan cycles, an ownership workshop, prioritized findings, and an executive evidence package.

NEXT STEP

pithstrategies@gmail.com

permitgraph-agent-security.andrew7carlin.c
hatgpt.site