Attack Simulation Dashboard

Policy enforcement + execution containment run summary

Run: 2026-01-26 09:23:06Z | Rounds: 500 | Profile: workflow | Policy: d8c1dd4354f6…

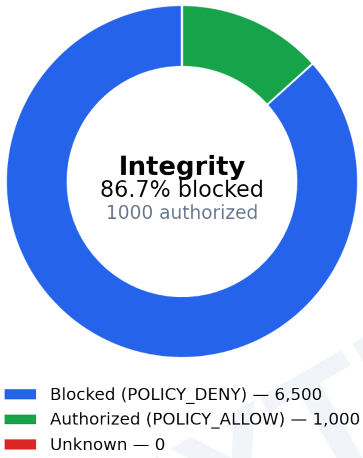
EXTERNAL

PASS

Executive Summary

- Blocked unsafe proposals: 6,500 / 7,500 (86.7%).
- Authorized proposals: 1,000 / 7,500 (13.3%).
- Execution integrity: committed_started == policy_allow (1,000 == 1,000).
- Authorized outcomes: 500 succeeded, 500 contained (timed out), 0 failed.

Notes: POLICY_ALLOW is an authorization decision. Timeouts indicate cap/containment enforcement, not necessarily failure.



Verification: PASS

Aggregate invariants (from counters)

✓ No unknown decisions
policy_unknown = 0

✓ No commit without allow
committed_started = 1,000; policy_allow = 1,000

✓ No failed executions
outcome_failed = 0

✓ Outcomes sum to commits
succeeded + timed_out + failed = 1,000

TOTAL PROPOSED
7,500
All proposed cases across rounds

BLOCKED BY POLICY
6,500
Denied at authorization time

AUTHORIZED
1,000
Allowed to proceed to irreversible sinks

SUCCEEDED
500
Completed execution successfully

CONTAINED (TIMED OUT)
500
Stopped by resource/time caps

CRITICAL ISSUES
0
Unknown decisions + failed executions

Definitions: POLICY_* are authorization-time decisions. committed_started indicates irreversible execution began. Outcomes: SUCCEEDED / TIMED_OUT / FAILED.

Attack Simulation Dashboard

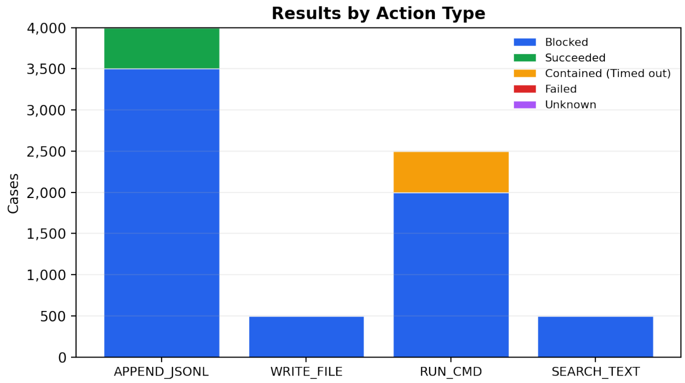
Policy enforcement + execution containment run summary

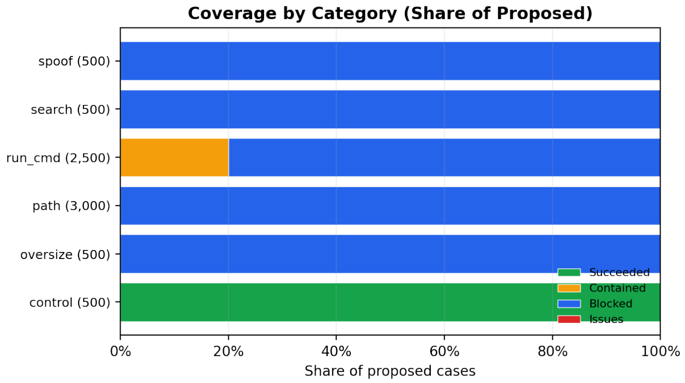
Run: 2026-01-26 09:23:06Z | Rounds: 500 | Profile: workflow | Policy: d8c1dd4354f6…

EXTERNAL

PASS

Evidence (Redacted)





Aggregates by Action Type

Action	Proposed	Allow	Deny	Started	Succ	Timed out	Fail	Unknown
APPEND_JSONL	4,000	500	3,500	500	500	0	0	0
WRITE_FILE	500	0	500	0	0	0	0	0
RUN_CMD	2,500	500	2,000	500	0	500	0	0
SEARCH_TEXT	500	0	500	0	0	0	0	0
TOTAL	7,500	1,000	6,500	1,000	500	500	0	0

Redacted Examples

Policy veto example

VETO

```
{
  "ts_utc": "2026-01-26T09:23:06Z",
  "action_type": "APPEND_JSONL",
  "decision": "INVALID",
  "policy_decision": "POLICY_DENY",
  "execution_committed": false,
  "reason_codes": [
    "SCOPE_PATH_NOT_ALLOWED"
  ],
  "attack_class": "Path scope escape"
```

Containment example

CONTAIN

```
{
  "ts_utc": "2026-01-26T09:23:08Z",
  "action_type": "RUN_CMD",
  "execution_committed": true,
  "outcome_status": "TIMED_OUT",
  "reason_codes": [
    "CAP_RUN_CMD_TIMEOUT_EXCEEDED"
  ],
  "attack_class": "Resource exhaustion (cap enforced)"
}
```

Artifacts

- decision_log_attack.jsonl
- executed_actions_attack.jsonl

Full logs available on request for independent verification.
Redactions: internal IDs and harness names removed.