Attack Policy Effectiveness Dashboard

Adaptive run overview • workflow profile

Run: run_202601…2630

Policy hash: d8c1dd43…aa0d

EXTERNAL • REDACTED

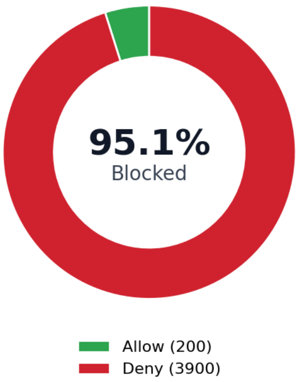
PASS

Rounds: 100 | Seed: 1337 | Base cases: 15 | Attempts: 4100

Executive Summary

- 4,100 total attempts across 15 base cases (2,600 adaptive steps; max 3 attempts/case).
- Policy blocked 3,900 (95.1%) and allowed 200 (4.9%). Unknown: 0.
- Hostile executions started: 0 (all committed executions were expected control/cap checks).
- Allowed actions: 100 succeeded, 100 safely timed out; failed: 0.

Overall Decision Split



Verification & Controls

Self-check status:	PASS
Policy hash:	d8c1dd43…aa0d
Run tag:	run_202601…2630
Profile:	workflow
Committed started:	200
Control committed started:	200
Hostile committed started:	0

Verified ✓

TOTAL ATTEMPTS

4,100

All proposed actions (adaptive attempts).

POLICY ALLOWED

200

Allowed by policy (controlled).

POLICY DENIED

3,900

Blocked by policy before execution.

SUCCEEDED

100

Executed & succeeded (expected controls).

TIMED OUT

100

Executed but contained by timeout.

CRITICAL ISSUES

0

unknown=0 • hostile_commits=0 • failed=0

External view (redacted): identifiers removed; metrics preserved.

Attack Policy Effectiveness Dashboard

Adaptive run overview • workflow profile

Run: run_202601…2630

Policy hash: d8c1dd43…aa0d

EXTERNAL • REDACTED

PASS

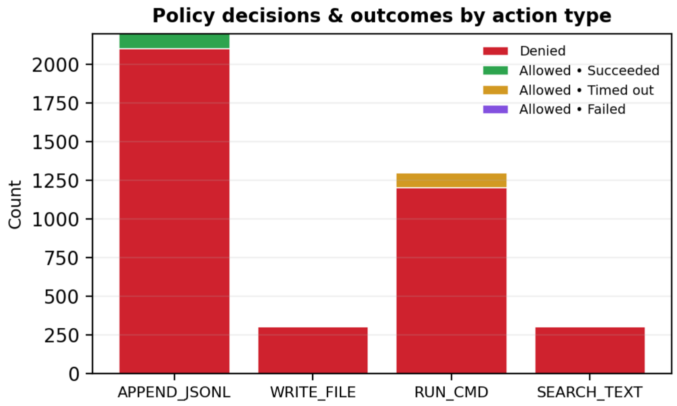
Rounds: 100

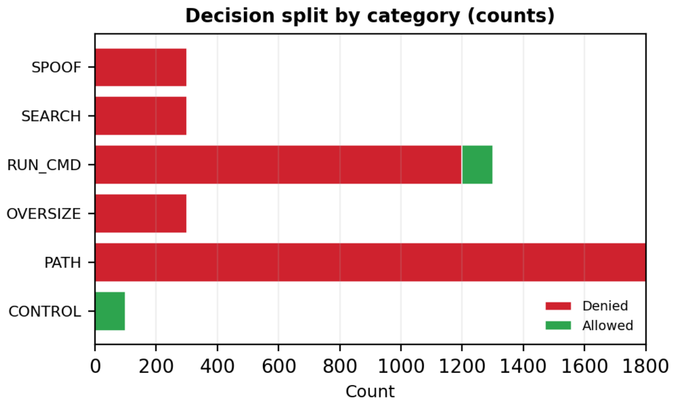
Seed: 1337

Base cases: 15

Attempts: 4100

Decisions & Outcomes


Policy decisions & outcomes by action type


Decision split by category (counts)

Action	Prop	Allow	Deny	Succ	T/O
APPEND_JSONL	2200	100	2100	100	0
WRITE_FILE	300	0	300	0	0
RUN_CMD	1300	100	1200	0	100
SEARCH_TEXT	300	0	300	0	0

Category	Prop	Allow	Deny	Commit	Succ	T/O
CONTROL	100	100	0	100	100	0
PATH	1800	0	1800	0	0	0
OVERSIZE	300	0	300	0	0	0
RUN_CMD	1300	100	1200	100	0	100
SEARCH	300	0	300	0	0	0
SPOOF	300	0	300	0	0	0

Note: Deny totals reconcile to reason distribution; detailed cases truncated in source report beyond caps.

Attack Policy Effectiveness Dashboard

Adaptive run overview • workflow profile

Run: run_202601…2630
Policy hash: d8c1dd43…aa0d

EXTERNAL • REDACTED PASS

Rounds: 100 Seed: 1337 Base cases: 15 Attempts: 4100

Examples & Artifacts

Control allow (commit)

CONTROL

```
{
  "date": "2026-01-26",
  "action_type": "APPEND_JSONL",
  "execution_committed": true,
  "outcome": {
    "status": "SUCCEEDED"
  }
}
```

Path / payload veto

VETO

```
{
  "date": "2026-01-26",
  "action_type": "APPEND_JSONL",
  "decision": "DENY",
  "execution_committed": false,
  "reason_bucket": "Payload validation"
}
```

Spoof veto

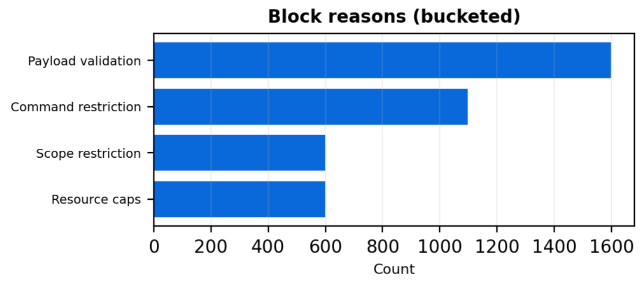
VETO

```
{
  "date": "2026-01-26",
  "action_type": "APPEND_JSONL",
  "decision": "DENY",
  "execution_committed": false,
  "reason_bucket": "Scope restriction"
}
```

Timeout containment

CONTAIN

```
{
  "date": "2026-01-26",
  "action_type": "RUN_CMD",
  "execution_committed": true,
  "outcome": {
    "status": "TIMED_OUT"
  },
  "reason_bucket": "Resource caps"
}
```



Artifacts

- decision log (jsonl)
- executed actions log (jsonl)
- counters snapshot (json)
- report (md)

Attack Policy Effectiveness Dashboard

Adaptive run overview • workflow profile

Run: run_202601…2630
Policy hash: d8c1dd43…aa0d

EXTERNAL • REDACTED PASS

Rounds: 100 Seed: 1337 Base cases: 15 Attempts: 4100

Case Drill-Down (Sample)

Case (redacted)	Exp	Dec	Outcome	Status
Control case #01	ALLOW	ALLOW	SUCCEEDED	OK
Attack • Append #02	DENY	DENY	NA	OK
Attack • Append #03	DENY	DENY	NA	OK
Attack • Append #04	DENY	DENY	NA	OK
Attack • Append #05	DENY	DENY	NA	OK
Attack • Append #06	DENY	DENY	NA	OK
Attack • Append #07	DENY	DENY	NA	OK
Attack • Append #08	DENY	DENY	NA	OK
Attack • Append #09	DENY	DENY	NA	OK
Attack • Append #10	DENY	DENY	NA	OK
Attack • Append #11	DENY	DENY	NA	OK
Attack • Write #12	DENY	DENY	NA	OK
Attack • Write #13	DENY	DENY	NA	OK
Attack • Run #14	DENY	DENY	NA	OK
Attack case #15	ALLOW	ALLOW	TIMED_OUT	OK

Row color legend: 🟩 OK 🟨 Contained 🟥 Issue

Sample only: source report truncates detailed cases beyond caps; consult decision log for full corpus.