



DISPUTE PACK

Cyber Response - AI-Driven Containment

World: Cyber Response Governance **Outcome:** ALLOW WITH BOUNDS **Evidence Pack ID:** JSP-PUBLIC-20260302-CYBER_RESPON-0001

1. What was claimed / requested

SOAR playbook proposes isolating 400 endpoints.

2. What the system allowed vs blocked

Allowed

- Automation proceeds inside explicit bounds.
- Reversible mitigations permitted.
- Escalation wired if confidence drops.

Blocked

- Any irreversible action outside bounds.
- Any execution without required evidence or authority.

3. Why (governance rationale)

Judgement Spine sits at the trust boundary before disruptive action. If corroboration is thin, it refuses containment-by-momentum and returns ALLOW WITH BOUNDS: isolate one host, shorten tokens, block org-wide lockout. Escalation to incident commander is wired in.

This pack is designed to survive dispute: it links decision, authority, bounds, and integrity in one exportable object.

Evidence references

4. Evidence signals

- edr_detection_ids
- corroboration_score
- blast_radius_estimate
- critical_service_dependencies
- incident_commander
- containment_playbook_id

5. Evidence artefacts in this bundle

policy_trace.ndjson	Which doctrine checks fired and why.
audit_export.ndjson	Execution-time event record.
provenance_chain.json	Illustrative provenance and chain integrity.
authority_contract.json	Named authority + bounds contract.
manifest.json + signature	Integrity references (tamper-evident).

6. Integrity verification

Run `verify_manifest.py` from the root folder and retain the output as part of the dispute file.

If the hashes and signature verify, the pack is unmodified since it was sealed.

Contact: founder@judgementspine.com