



Pattern A - Webhook Adapter (Fast Path)

Use when you can intercept via events/webhooks and enforce via API calls.

Implementation steps

1. Identify the tool event emitted before commit (e.g., SOAR action run, quote send, data export).
2. Create an adapter that receives the event payload and normalises it into a Judgement Spine trigger (intent + context).
3. Call the Judgement Engine and receive outcome + bounds + escalation instructions.
4. Enforce outcome back into the tool via its API (pause, hold, constrain, route approvals, or safe-degrade).
5. Mint an evidence pack and attach IDs/links (ticket, rollback plan, telemetry).

Minimal adapter contract (illustrative)

```
{
  "intent": { "action": "isolate_endpoints", "scope": "400" },
  "world": "Cyber Response Governance",
  "context": { "corroboration_score": 0.41, "blast_radius": "high" }
}
```

Outputs you should produce

- Runtime outcome returned (ALLOW / BOUNDS / ESCALATE / BLOCK / SAFE DEGRADE)
- Enforcement applied in the target system
- Evidence pack minted (intent, authority, bounds, doctrine version, rationale, integrity refs)

Contact: founder@judgementspine.com