

Artifact: evidence.jsonl — Replay Capsules for Intrusion Nullifier

Each line is a JSON object representing a simulated breach attempt. These are synthetic, timestamped, and federation-safe.

jsonl

```
{"timestamp": "2025-10-25T16:01:00Z", "adversary": "Insider Drift", "action": "Accessed patient_records without justification", "asset": "EHR:patient_records", "severity": "medium", "replayable": true}
{"timestamp": "2025-10-25T16:03:12Z", "adversary": "Credential Thrashers", "action": "Brute-forced login endpoint", "asset": "auth:tokens_and_sessions", "severity": "high", "replayable": true}
{"timestamp": "2025-10-25T16:05:47Z", "adversary": "Lateral Escalators", "action": "Escalated via misconfigured IAM role", "asset": "audit:logs_and_ledgers", "severity": "high", "replayable": true}
{"timestamp": "2025-10-25T16:08:22Z", "adversary": "Supply-chain Compromisers", "action": "Injected malicious code via vendor SDK", "asset": "backups:object_store", "severity": "critical", "replayable": true}
{"timestamp": "2025-10-25T16:10:59Z", "adversary": "APT", "action": "Established covert command channel", "asset": "kms:keys", "severity": "critical", "replayable": true}
```