

DWP Security Solutions / Digital Warfare Productions

Role Sheet: MI Ops

ML-Ops - Forensics & Artifact Control

Role ID: ml_ops

Responsibilities

- Verify dataset hashes and model signatures
- Reproduce training runs in isolated environment
- Provide Last Known Good (LKG) artifact and rollback plan
- Run canary tests and report composite drift score

Deliverables

- Model signature file
- Reproducible training run logs
- Rollback recipe (steps, timeline)

On-call: Primary for technical triage