Osint Investigator — End-Product One-Pager (v11)

Legal-only by default • Zero-access privacy • Cited, calibrated findings • Telegram OSINT built-in

Purpose: Modern OSINT that finds, links, and explains evidence across the web (and opt-in darknet).

Modes: Individual (with name discovery from signals), Organization, General (topic/event).

Telegram: Public channels/groups via TDLib; channel allowlist; keyword/language watchlists; forward-chain origin attribution; UI source card & post evidence; admin session management; plan gating.

Networks: Focused sub-graph (~25–40 nodes, 1–2 hops); people=circles, orgs=squares; thickness=strength; dashed=uncertain; Explain-this-link with citations; exports PNG/PDF/JSON.

Media intelligence: Images (EXIF, OCR, objects/logos/landmarks, tamper cues), Video (shots/keyframes, tracking, subtitles), Audio (ASR, diarization, gunshot/explosion/siren/crowd). Media Lab viewer with markers and exports.

Sensitive/violent media: Warning-first (no default blur). Mask only when legally required or by tenant policy; explicit media link-out with hashes/metadata; audit reveal actions.

Evidence & reasoning: Evidence Graph + entity resolution; ACH + Bayesian posteriors with CIs; contradiction detector; grounded dialogue (no cite → no say).

Records Finder: When info is public but offline, show the lawful authority/process to obtain it (jurisdiction-specific).

Privacy & legal: Zero-access (client keys, ciphertext only); optional TEE. Legal-only policy pack (laws + ToS). Lawful Access via Legal Unlock (valid order + M-of-N trustees, time-bound package) with chain-of-custody & transparency.

Performance: Quick/Deep modes; per-case budgets; caching; headless ratio guard; energy targets.

Admin console: Ops health/quick fixes; Users/Orgs (SSO/SCIM/MFA); Connectors & Secrets (write-only); Policy editor; Updates; Alerts/Webhooks; Audit/Transparency; Legal Requests intake/status (no content access).

Monetization & learning: Free/Pro/Team/Enterprise; usage metering & entitlements; personal learning (private) + opt-in global (DP/federated).

Launch strategy: Core-first → Advanced Intelligence Modules post-GA (GEOINT, crypto tracing, breach lookups, social graphing, team workspace, public API).