API-Agnostic OSINT *Hub*

Buy the system once. Choose (and change) your OSINT APIs anytime.

What you are buying.

You are buying the investigation system: the case workspace, the ingestion and normalisation layer, entity resolution, link analytics, auditability, and the user experience. You are not buying “a single OSINT provider.”

What you can choose on top.

You can plug in any OSINT API provider you want, and you can run multiple providers at once. OSINT APIs are widely available and interchangeable—every OSINT vendor has an API, and new ones appear constantly. Your sources become a replaceable input, not your platform.

Why this matters.

If a provider degrades, changes coverage, raises prices, or stops being fit for purpose, you swap the API—without replacing the system, restarting your program, or paying for another platform. You keep the same workflows, the same governance model, and the same case history; only the data source changes.

InteliATE

The "buy once, evolve forever" model

An investigation system stays constant. Your OSINT sources stay flexible. Treat OSINT providers as consumable inputs: add new sources when you need coverage, replace underperforming sources without disruption, and upgrade your collection stack over time without re-platforming.

Integrate without waiting on a vendor

Add and change OSINT providers as your mission evolves. Your team can incorporate new APIs and data sources without needing to replace the platform or restart the program.

How it works

1. Select sources and scope. Choose the APIs and data feeds you want, define what gets collected, and map it into your case structure.
2. Collect and normalise. Run scheduled pulls and real-time collection where supported; clean and normalise data so it's consistent across providers.
3. Fuse into cases. Automatically correlate entities (emails, phones, usernames, domains, IPs and more), deduplicate, and keep every insight evidence-linked.
4. Investigate and report. Use natural-language interaction, virtual link analysis, and automated report generation for rapid review and escalation.

Core capabilities

1. Automated entity resolution and correlation across mixed sources.
2. Virtual link analysis for relationship discovery and case building.
3. Role-based investigator workflows designed for operational usability.
4. Automated reporting for briefing-ready outputs.
5. Mission-configured analytics and model layer chosen for your real requirements

Designed for security-critical environments

Deployment is sovereign and on-prem with role-based access, encryption, and immutable activity logs. Analysis stays inside your environment. Connectivity can be limited to approved OSINT collection pathways, while investigation and reporting remain controlled and auditable.

Outputs are analytical aids and require human review. Operational decisions remain with authorised personnel.