Funded by the European Union

FALCON is funded under the Horizon Europe Framework Program
Grant Agreement ID 101121281

FALCON
Fighting Corruption & Organised Crime

Deliverable D3.4

Title: FALCON Prototype R2.0

Dissemination Level:	PU - Public
Nature of the Deliverable:	DEM - Demonstrator, pilot, prototype
Date:	31/10/2025
Work Package:	WP3 - Anti-corruption AI framework co-design
Editors:	UPV
Reviewers:	IOSB, RAD
Contributors:	ICCS, IOSB, BPTI, CERTH, ENG, SPH, VICOM, CENTRIC

Abstract: This deliverable presents the evolution of the FALCON platform from R1.0 to R2.0, focusing on tangible feature increments, strengthened interoperability, and user-centred refinements. It reports platform-wide progress (GitLab CI/CD, DEV/PROD environments, KONG API Gateway, Redpanda) and consolidates the state of the FALCON KB. The deliverable summarises component updates across the FALCON Dashboard, ACRA, OSINT, Predictive Analytics, BCI, Kriptosare, SDMA, the new Trends Detection tool, and the Car Visual Recognition integration pattern. It identifies current limitations and outlines the verification plan—including an end-to-end rehearsal at the Lyon plenary—towards the Final Prototype (D3.5), in alignment with Trustworthy AI principles.

Executive Summary

This deliverable, D3.4 – FALCON Prototype R2.0, reports the progression of the FALCON platform from R1.0 (D3.3) to R2.0, focusing on concrete feature increments, strengthened interoperability, and user-centred refinements. It builds on the requirements consolidated in D3.1, the architectural blueprint in D3.2, and the first integration cycle evidenced in D3.3, and tracks how these foundations have matured into a more cohesive investigative environment.

Platform integration and operations. WP3 continues to apply an agile delivery model with GitLab CI/CD for build, test and deploy automation; two run-time environments (DEV for rolling integration and PROD for demonstrations); and a unified façade via the KONG API gateway (JWT/OIDC with Keycloak) for secure, consistent REST access. Redpanda (Kafka-compatible) underpins asynchronous orchestration for long-running analytics and tool-to-tool events. The SDMA component advances tamper-evident auditing with higher-volume ingestion and live validation views, complementing the security posture of the platform.

Cross-cutting progress. The release emphasises UI consistency, graph-centric analysis, and Knowledge Base (KB) interoperability. Several tools now share a harmonised dark-theme look & feel and action-oriented workflows (notably the PA, Trends Detection, and OSINT tools), while other modules are queued for visual alignment. The KB’s data model and API are leveraged more broadly across tools to persist results (scores, indicators, entity links) and to drive ontology-assisted graph editing.

Component highlights.

- **FALCON Dashboard.** R2.0 adds an in-context legend, case (investigation) management, automatic network statistics, improved search, and advanced visualisation parameters (degree, betweenness, thresholding, date and node-type filters), with refined node/edge creation for ontology consistency.
- **Border Corruption Investigation (BCI).** A new interactive collaborator-network view (nodes = licence plates; edges = co-travel at the same BCP) supports rapid triage with risk-weighted cues; analysts can tune frequency/collaborator thresholds and random-day sampling; a VIN-anomaly indicator flags multiple plates per VIN; exports support cross-tool correlation.
- **ACRA.** A unified UI spans Public Procurement, Company Data and Border Corruption; a single-query Tender ID lookup reconstructs cases; a Graph Generation service visualises relationships; streamlined actions (one-click risk/graph) and tighter KB integration accelerate investigations.

- **OSINT.** Beyond predefined crawlers, analysts can now configure crawlers (seeds, depth, refresh rate); Location becomes a first-class subject; OSINT searches can be triggered directly from the Dashboard while continuing to ingest entities to the KB.

In addition, the **Predictive Analytics (PA) Tool** receives a full UI refresh, integrates with the Dashboard and ACRA, pushes results to the KB, and extends coverage to Italy; **Kriptosare** expands with a Bitcoin graph view, Monero-aware exploration, sanctioned-address tracing, and a new FIAT module (to be merged into the main UI); **CAR Visual Recognition** defines a minimal embedded UI with dual start/stop triggers (REST and Kafka); and the new **Trends Detection Tool** introduces end-to-end BTC address time-series analysis with change-point detection and receiver ranking.

Limitations and next steps. Not all modules yet adopt the common look & feel; KB ingestion parity (labels, timestamps, similarity handling) must be completed for a few tools; and performance hardening is planned for very large graphs and datasets. These items will be exercised during an end-to-end pilot at the next Plenary in Lyon, with structured end-user feedback feeding the final refinements. Ongoing WP3 integration meetings and bilateral telcos will continue to drive convergence as each tool lands in the Dashboard.

Overall, D3.4 evidences a clear shift from isolated prototypes to an integrated, security-hardened platform with improved usability and interoperability. The consortium remains on track to deliver a visually consistent, KB-centric and operationally robust **Final Prototype (D3.5)** aligned with Trustworthy AI practices and the investigative needs of European LEAs.