الملف التقني الشامل لمشروع رحّال | منصة الرصد والتحليل الاستخباراتي الذكي

# المقدمة

يهدف مشروع رحّال إلى بناء منصة متقدمة لرصد وتحليل المحتوى المفتوح (OSINT) من شبكات التواصل الاجتماعي والمصادر العلنية، باستخدام الذكاء الاصطناعي والربط التحليلي.

يساعد النظام في دعم اتخاذ القرار الأمني والمجتمعي بناءً على معطيات حقيقية لحظية، ويعزز جاهزية الجهات الشرطية والمؤسسية في مواجهة التحديات الرقمية.

# البنية التقنية للنظام

يتكون نظام رحّال من عدة طبقات مترابطة تشمل:

- واجهة المستخدم: Vue.js

- محرك التحليل والرصد: FastAPI + Python

- قاعدة البيانات التحليلية: Elasticsearch

- لوحة العرض والتحكم: Kibana

- حاويات التشغيل: Docker Compose

# المنصات المدمجة

تم دمج المنصات التالية ضمن النظام: Facebook، Twitter، Instagram، Telegram، YouTube، Reddit، LinkedIn.

لكل منصة تم تصميم سكربت مخصص لجلب المحتوى، تحليله، وإدخاله في Elasticsearch، بالإضافة إلى واجهة Vue لعرض النتائج وتصفية البيانات.

# الوحدات التحليلية

- وحدة التنبيهات (Watcher): ترصد تلقائيًا الكلمات الحرجة والتصنيفات الخطرة.

- وحدة التحليل الجغرافي: تعرض المحتوى بناءً على الإحداثيات.

- وحدة التحليل الزمني: فلترة المحتوى حسب الفترة.

- Dashboard رئيسية: تعرض المؤشرات الإجمالية والروابط بين المنصات.

# التحليل الذكي

يعتمد النظام على تحليل المشاعر (Sentiment Analysis) والتصنيف السياقي للمحتوى (Risk Classification).

يتم تحديد المشاعر باستخدام نماذج Transformers (مثل BERT) ويُصنّف الخطر إلى: High، Medium، Low.

# القيود والتحديات

- LinkedIn وTwitter APIs مقيدة وتتطلب حلولًا بديلة.

- Telegram يتطلب جلسة تسجيل دخول.

- TikTok Live وDark Web يحتاجان أدوات خاصة وإشراف قانوني.

# آفاق التوسع المستقبلي

الدمج مع GDELT، Snopes، NewsGuard، Wayback Machine.

إضافة تحليل علاقات باستخدام GPT.

تحويل النظام إلى خدمة سحابية (SaaS).

# ملاحق المشروع

## ملحق 1: استبيان المتطلبات الأولية

### 1. ما هي الخصائص أو الوظائف الرئيسية التي ترغب في تضمينها؟

• تكامل متعدد المنصات لجمع وتحليل OSINT من Twitter, Facebook, Telegram, YouTube, Reddit, LinkedIn، وغيرها.

• تحليل المشاعر والمخاطر مدعوم بالذكاء الاصطناعي باللغتين العربية والإنجليزية.

• تصفية زمنية وجغرافية عبر لوحة تحكم تفاعلية.

• نظام تنبيهات ذكي يسجل التنبيهات تلقائيًا بناءً على مؤشرات الخطر أو الكلمات الحساسة.

• لوحة تحكم موحدة تعتمد على Vue.js وتتكامل مع Kibana.

• تصميم معياري قابل للتوسعة ليشمل مصادر مستقبلية مثل GDELT وDark Web.

### 2. هل هناك تقنيات مفضلة أو متطلبات معينة؟

• الواجهة الأمامية: Vue.js مع دعم RTL للغة العربية.

• الواجهة الخلفية: Python (FastAPI) ضمن بيئة Docker.

• طبقة البيانات: Elasticsearch مع Kibana.

• مكتبات الذكاء الاصطناعي: Transformers من HuggingFace، Whisper، Langdetect.

• التزام بالمعايير القانونية فيما يخص scraping والربط بالمنصات.

### 3. ما المشكلة التي يحاول المشروع حلها؟

• سد الفجوة في حلول الرصد والتحليل اللحظي للمحتوى المفتوح (OSINT) خاصة في السياقات العربية.

• توفير منصة موحدة قابلة للتوسع للتحليل السياقي متعدد اللغات والتصنيف الذكي للمخاطر.

• دعم متخذي القرار الأمني والتنموي بناء على مؤشرات رقمية لحظية مستمدة من مصادر مفتوحة.

### 4. من هم المستخدمون المستهدفون؟

• الجهات الأمنية والشرطية لمراقبة الاتجاهات الرقمية وإدارة الأزمات.

• الجهات الحكومية والخدمية لرصد تفاعل الجمهور وتحسين جودة الخدمات.

• وحدات تحليل الإعلام لمراقبة السرديات ونفي الشائعات.

• صنّاع السياسات للتخطيط الاستراتيجي المستند إلى بيانات حية من الإنترنت المفتوح.

# الملحق التشغيلي: دليل الإجراءات التشغيلية القياسية (SOP)

## 1. المقدمة

يهدف هذا الدليل إلى توثيق الإجراءات التشغيلية القياسية (SOP) لتشغيل وصيانة منصة رحّال لرصد وتحليل مصادر OSINT. ويتضمن هذا الدليل خطوات التهيئة، التشغيل، التحليل، الاستجابة، والحوكمة لضمان أعلى درجات الكفاءة والجودة في العمل.

## 2. مراحل التشغيل القياسي

|  |  |  |  |
| --- | --- | --- | --- |
| المرحلة | الوصف | المسؤول | التكرار |
| تهيئة بيئة العمل | تشغيل الحاويات عبر Docker Compose. | مهندس DevOps | مرة واحدة |
| إعداد مصادر OSINT | تحديد الكلمات المفتاحية والمنصات النشطة. | محلل استخباري | أسبوعي |
| تشغيل Scrapers | تشغيل سكربتات جمع البيانات من المنصات. | فني البيانات | يومي |
| تحليل البيانات | تصنيف المشاعر والمخاطر باستخدام النماذج. | وحدة الذكاء | لحظي |
| إدخال البيانات | إدخال النتائج إلى Elasticsearch. | مهندس Backend | تلقائي |
| عرض النتائج | عرض البيانات عبر الواجهة ولوحات Kibana. | المستخدم النهائي | عند الطلب |
| تسجيل التنبيهات | تفعيل Watcher عند تحقق شروط الخطر. | النظام | تلقائي |
| التدقيق البشري | مراجعة التنبيهات العالية من قبل بشر. | ضابط OSINT | فوري |
| التقارير | إعداد تقارير PDF ولوحات أسبوعية. | الإدارة | أسبوعي |
| الصيانة | تحديث النماذج والسكربتات. | الفريق الفني | شهري |

## 3. ضوابط الحوكمة والتحقق

- يتم التحقق من سلامة البيانات عبر مراجعة عشوائية بنسبة 5% أسبوعياً.

- تخضع عمليات scraping للسياسات القانونية المعتمدة في كل منصة.

- يتم تشفير البيانات الحساسة وعدم تخزين أي معلومات شخصية غير مصرح بها.

- يتم تسجيل أي أعطال أو استثناءات في سجل خاص يتم مراجعته شهرياً.

## 4. سيناريوهات الاستجابة للحوادث

- في حال توقف خدمة Docker: يتم إعادة تشغيلها عبر `docker-compose restart` ومراجعة السجلات.

- في حال تغير API في منصة ما: يتم تحديث السكربت أو التحول إلى scraping مؤقت.

- في حال حظر IP: يتم التبديل إلى Proxy أو VPN مرخص.

- في حال رصد محتوى خطير: يتم إشعار ضابط OSINT تلقائياً وتجميد السطر لمراجعته.

## 5. سجل التعديلات والتحسينات

يتم إصدار نسخة جديدة من SOP مع كل تحديث كبير في النظام. النسخة الحالية: v1.0 بتاريخ اليوم.