AIEngineer_BuiHanhTrang documentation

1. Thông tin cá nhân

- Họ và tên: Bùi Hạnh Trang
- Vị trí ứng tuyển: AI Engineer
- Link GitHub: https://github.com/buihanhtrang/AIEngineer_BuiHanhTrang

2. Mô tả bài toán

Ứng dụng xây dựng một AI Agent phân tích cảnh báo an toàn thông tin, có khả năng xử lý truy vấn như IP, domain, hash, file path hoặc URL. Hệ thống kết hợp giữa:

- GPT-4o mini (OpenAI) để đánh giá ngữ nghĩa và kết luận cuối cùng
- VirusTotal API nhằm kiểm tra hash, URL, domain
- AbuseIPDB API nhằm kiểm tra độ tin cậy IP
- Luật tự động hóa nhằm phát hiện mẫu đáng ngờ trong file path/domain

3. Mô hình kiến trúc triển khai

- Kiến trúc tổng quan: Client → Flask API → Phân tích công cụ → GPT-4o phân tích tổng hợp → Kết luận
- Các thành phần chính:

- /analysis_agent: Nhận POST JSON { "query": "..." }

- Kết quả: JSON gồm analysis (mô tả chi tiết) và result (CLEAN, ABNORMAL, UNKNOWN)

- Dockerized, cấu hình qua .env

4. Triển khai với Docker

- Bước build và chạy Docker:

```
docker build -t ai-agent .

docker run --env-file .env -p 8989:8989 ai-agent
```

- Tạo file .env theo mẫu .env.example:

```
# OpenAI API Key
```

OPENAI_API_KEY=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

VirusTotal API Key

VIRUSTOTAL_API_KEY=64b2ddae102e319956aa0b0241699f2012d0307597df0e3ef9052405f7f7850f

AbuseIPDB API Key

ABUSEIPDB_API_KEY=d1f70c084b0832f6e57d02348c0727d8f58aeec1fb83b7398c3371a0466cc076edd76bbabe802cb2

5. Kết quả kiểm thử

- Đầu vào tại file: input.json
- Kết quả mẫu tại file: output.json

6. Kết luận

Ứng dụng đáp ứng đúng yêu cầu đề bài:

- Phân tích từ nhiều công cụ bảo mật
- Kết hợp GPT-4o mini để đưa ra quyết định hợp lý
- Triển khai hoàn chỉnh bằng Docker

Hệ thống có thể mở rộng dễ dàng với các API khác như Shodan, HybridAnalysis...

Tốt cho việc tích hợp vào SOC hoặc hệ thống phản ứng sự cố thực tế