BECYB Projekt

Tomasz Lewiński

Aleksander Gajowniczek

Juliusz Kluge

Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych

30 marca 2025

Spis treści

1. Wprowadzenie

W ramach tematu "Bezpieczeństwo sieci - rozwiązania i narzędzia, nowe koncepcje" nasz zespół skupi się na eksploracji zastosowania modeli językowych AI w dziedzinie cyberbezpieczeństwa. Konkretnym zadaniem, które podejmiemy, będzie "Wykorzystanie ChatGPT do automatyzacji analizy zagrożeń".

2. Rozumienie tematu

Temat projektu zakłada wykorzystanie modelu językowego ChatGPT (lub podobnego) do stworzenia narzędzia wspomagającego analizę zagrożeń bezpieczeństwa w systemach informatycznych. Główne założenia to:
— Automatyzacja analizy logów systemowych
— Wsparcie dla administratorów w identyfikacji potencjalnych incydentów bezpieczeństwa
— Sugerowanie możliwych scenariuszy reakcji na wykryte zagrożenia

3. Zawężenie zagadnień

Projekt skupi się na następujących aspektach:
— Analiza wybranych typów logów systemowych (np. logi serwera WWW, firewalla)
— Identyfikacja podstawowych wzorców ataków (SQL Injection, XSS, Brute Force)
— Tworzenie czytelnych raportów dla administratora
— Implementacja podstawowych scenariuszy reakcji

4. Cele projektu

4.1. Cel główny

Stworzenie prototypu cybersecurity chatbota wykorzystującego API OpenAI do wstępnej analizy logów systemowych i wsparcia administratora w ocenie zagrożeń.

4.2. Cele szczegółowe

— Zbudowanie działającego prototypu w Pythonie z wykorzystaniem OpenAI API
— Opracowanie zbioru testowych logów zawierających różne typy zagrożeń
— Implementacja mechanizmu klasyfikacji zagrożeń
— Stworzenie interfejsu użytkownika (CLI lub webowy)
— Testy funkcjonalne rozwiązania

5. Zakres projektu

Projekt obejmuje:
— Analizę istniejących rozwiązań
— Projekt architektury systemu
— Implementację podstawowej wersji chatbota
— Testy na syntetycznych danych
Projekt **nie obejmuje**:
— Pełnej integracji z systemami produkcyjnymi
— Zaawansowanych mechanizmów detekcji zagrożeń
— Szkolenia własnego modelu AI

6. Przewidywane efekty

— Działający prototyp chatbota analizującego logi
— Dokumentacja techniczna rozwiązania
— Zbiór testowych przypadków użycia
— Raport z testów i oceny skuteczności

7. Literatura i materiały pomocnicze

— Oficjalna dokumentacja OpenAI API: `https://platform.openai.com/docs`
— OWASP Top 10: `https://owasp.org/www-project-top-ten/`
— Common Log Format specification
— Publikacje naukowe dot. zastosowań AI w cyberbezpieczeństwie
— Dokumentacja bibliotek Python do parsowania logów (np. pygtail, loguru)

8. Wnioski

Przedstawiony dokument określa wstępny zakres projektu, który może ulec niewielkim modyfikacjom w trakcie realizacji. Głównym celem jest stworzenie funkcjonalnego prototypu demonstrującego potencjał wykorzystania modeli językowych w automatyzacji analizy zagrożeń bezpieczeństwa.