Розробка додатку для симуляції фішингових атак в компанії (з аналізом помилок клікерів)

ВИКОНАЛА: ПРОКОПЕНЯ П.С. КН-4

КЕРІВНИК: ХРЯПА О.І.

Актуальність

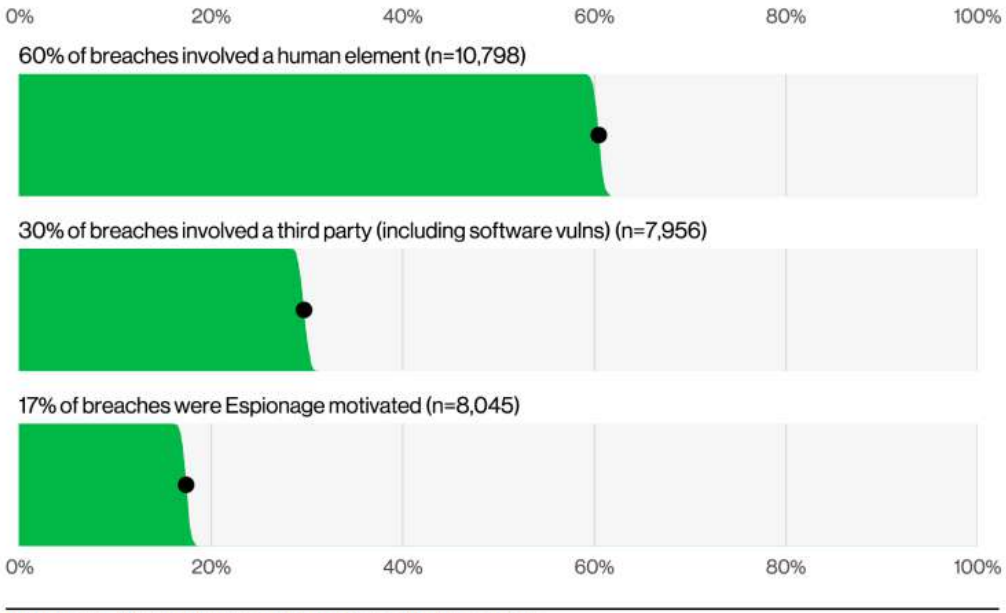


Figure 7. Select key enumerations in breaches

Дані звіту Verzion 2025

Details of messages sent and responses in the first campaign.

First campaign	Standard email		Custom email	
Total emails sent	2656	100%	2657	100%
Received not opened	1699	64%	1012	38%
Received and opened	957	36%	1645	62%
Received, opened and link clicked	176	7% of emails sent 18% of opened,	1447	55% of emails sent 88% of opened

Симуляція фішингу у великій лікарні: тематичне дослідження (2022)

Мета та завдання

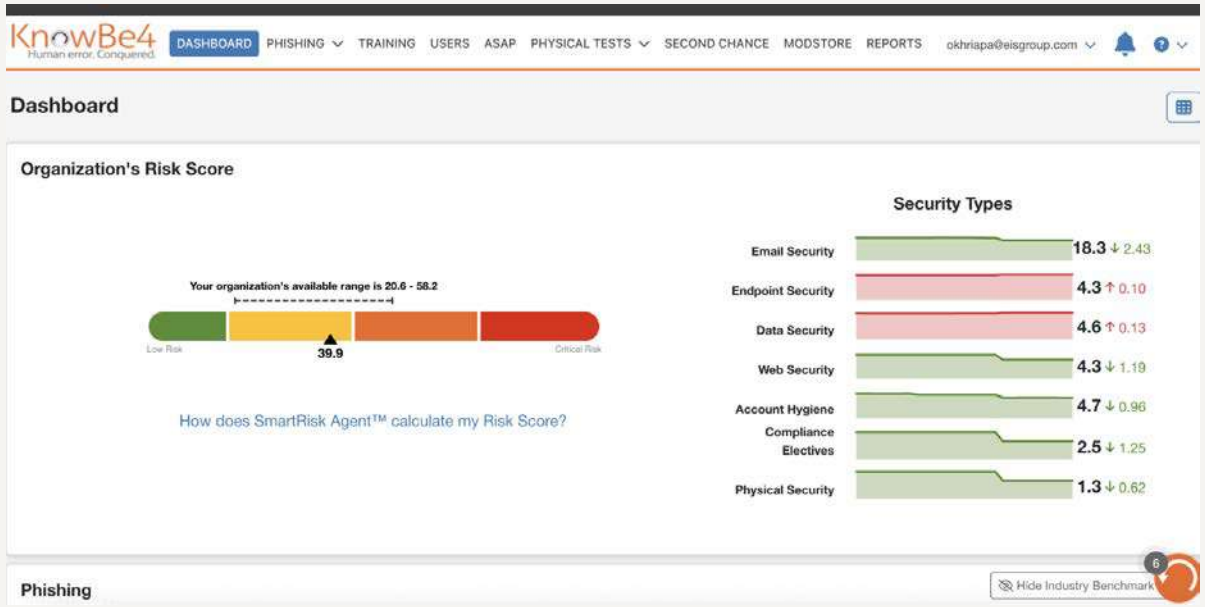
Мета роботи – розробити веб-додаток, що дозволить компанії проводити симуляції фішингових атак і аналізувати результати

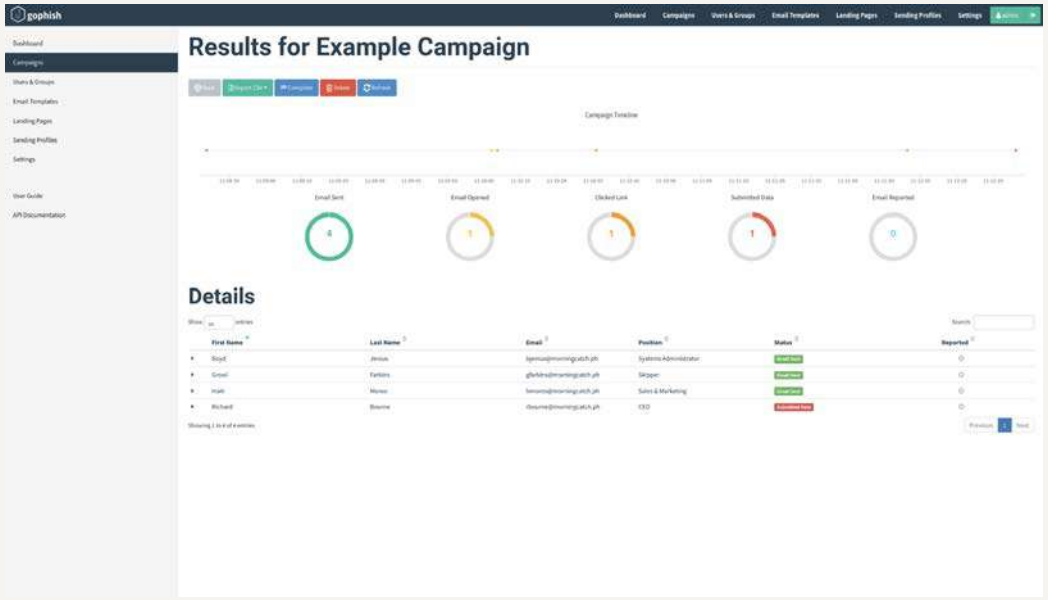
Завдання:

1. Дослідити наявні рішення
2. Обрати технології та структуру застосунку
3. Розробка додатку для симуляції фішингових атак

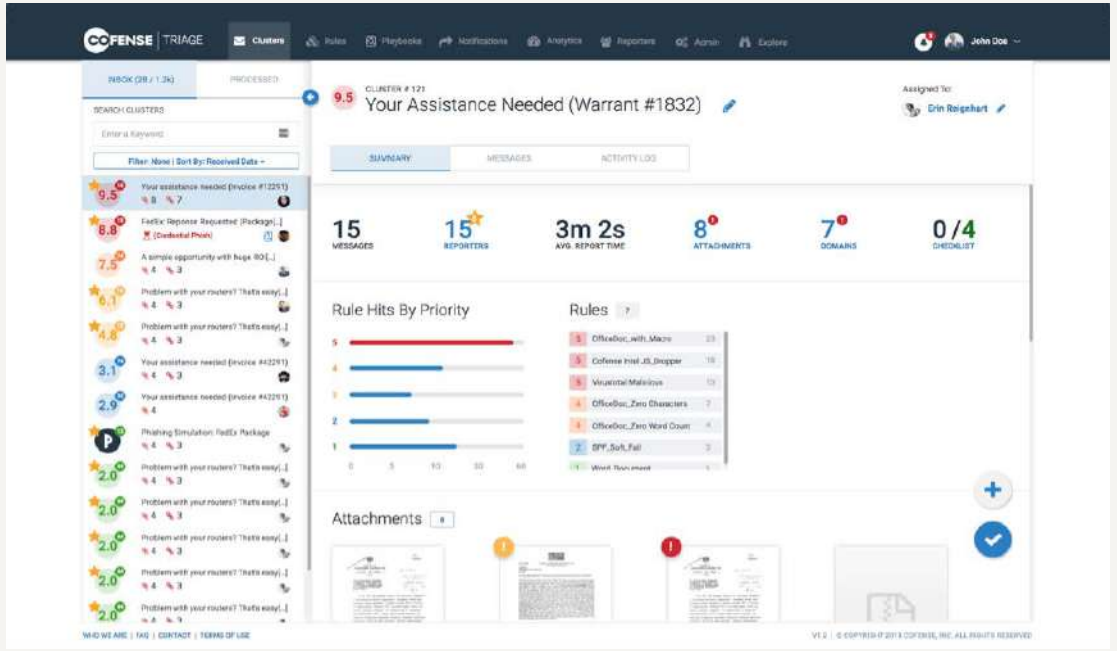
Аналіз наявних рішень

Інтерфейс KnowBe4





Інтерфейс Gophish



Інтерфейс Cofense

Архітектура додатку

Основні функціональні вимоги:

- Керування користувачами
- Налаштування фішингової кампанії
- Налаштування шаблонів електронних листів
- Реєстрація даних та аналітика

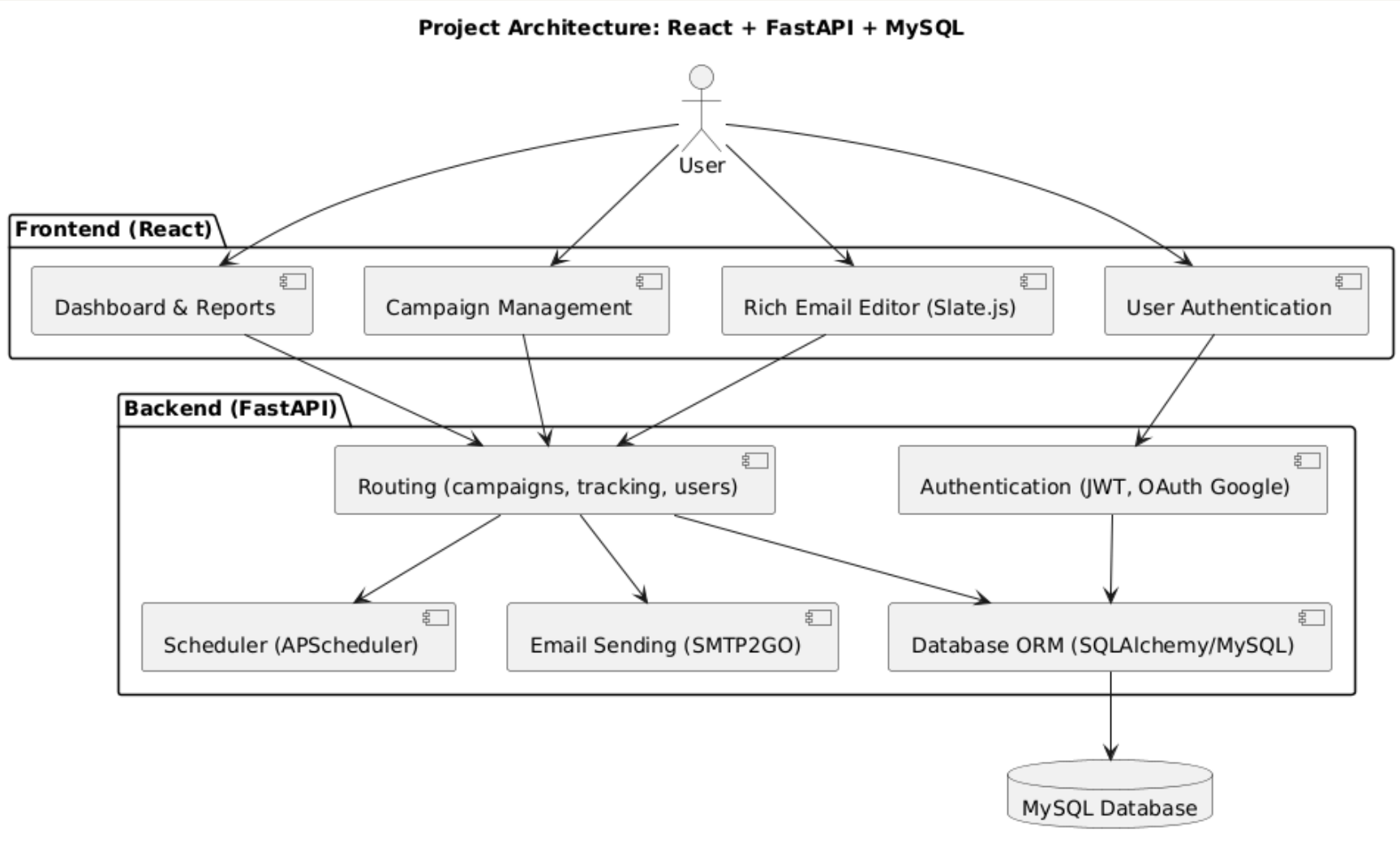
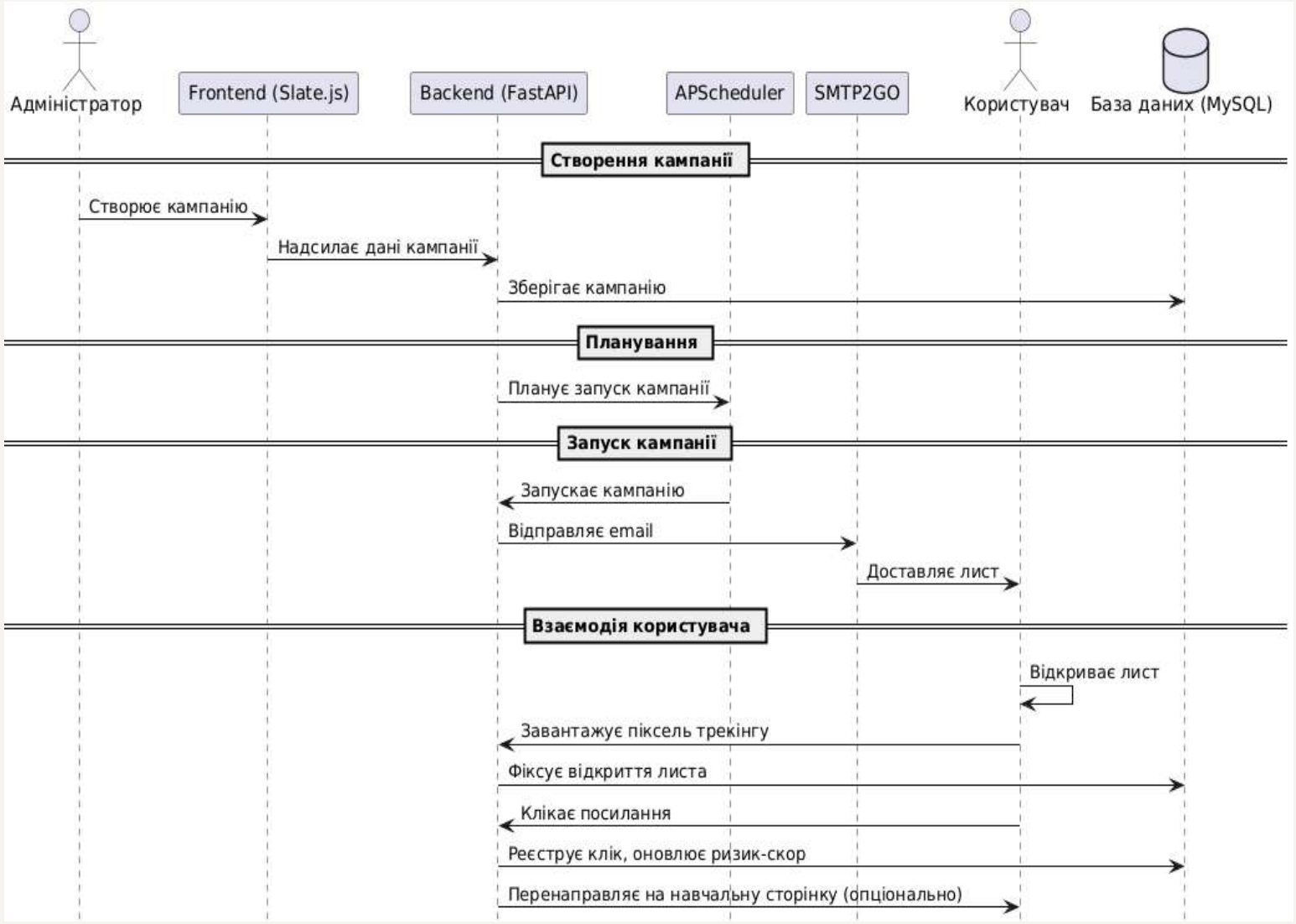


Схема роботи фішингової кампанії



Основні компоненти системи та їх функції

Висновки

Розроблений у рамках дипломної роботи додаток успішно реалізує поставлену мету – надає можливість **імітувати фішингові атаки** і аналізувати реакцію співробітників.

У ході роботи проведено огляд актуальних загроз та існуючих засобів протидії, на основі чого сформовано вимоги до системи та створено веб-додаток.