УДК 004.056

ІНТЕГРАЦІЯ SUBLIME SECURITY ДЛЯ БІЗНЕСУ

SUBLIME SECURITY INTEGRATION FOR BUSINESS

Вікторія Сидоренко[1], Оксана Жигаревч[2], Володимир Яблонський[2]

[1]*Національний авіаційний університет, Любомира Гузара, 1, Київ, 03058*
[2]*Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна*

Abstract. *Sublime Security is a modern email security solution that uses programmable rules and artificial intelligence to detect and block a variety of threats. The platform integrates with popular email services such as Microsoft 365, Google Workspace, and IMAP, providing protection against phishing, business electronic compromise (BEC), and malware.*

Sublime Security – це сучасне рішення для захисту електронної пошти, яке використовує програмовані правила та штучний інтелект для виявлення та блокування різноманітних загроз. Платформа інтегрується з популярними поштовими сервісами, такими як Microsoft 365, Google Workspace, та IMAP, забезпечуючи захист від фішингу, бізнес-електронної компрометації (BEC) та шкідливого ПЗ. Безкоштовний план Sublime Security дозволяє максимум обслуговувати 600 електронних пошт.

Перелік вимог для сервера: 32 GB RAM(Оперативної пам’яті), 16 CPUs - 16 ядерний процесор, мінімум 200 Gb накопичувача. Архітектури які підтримує Sublime Security: amd64 / x86_64, arm64 (including Apple Silicon – M1/M2 Macs). Операційні системи які підтримує Sublime Security: Linux (Tested on Ubuntu 18-22.10, Amazon Linux 2, CentOS 7, and Fedora 34-37), macOS.

Процес встановлення програмного забезпечення розпочинається після того як створили сервер та встановили операційну систему. Використовуючи Linux Ubuntu Server, встановлюємо Git та Docker далі розгортаємо Sublime Security за допомогою команд: sudo apt-get install curl,curl -sL https://sublime.security/install.sh | sh. Після встановлення програмного забезпечення можемо відкрити файл конфігурації та налаштувати ip address, порт. Використовуємо статичний IP - address, створюємо запис DNS. Варто зауважити, що не обов’язково використовувати публічний IP адрес, але тоді доступ до адміністративної панелі можна буде отримати тільки у локальній мережі або ж через VPN. (рис. 1).

```
POSTGRES_PASSWORD=cee87be860c0951272782bc1403a80fe8298c3df8ec15906
JWT_SECRET=048f6a815475509b0ed0a96ea9eac6254aabd30873781ff4
POSTGRES_ENCRYPTION_KEY=fee92f88ea7a6ae316353df36e28b4781c5fa11f1b5f5c6276e6fa486970d46f
AWS_ACCESS_KEY_ID=fake_6a8e7b480a49e2205d6b2eb9ce822a3c16eab0f9860400f2306de6a1fecf30ba
AWS_SECRET_ACCESS_KEY=fake_60ed3079bb4906d0aebccc77c03e2504d6b476f5421fb6d36f15a0cfe21dced2
CORS_ALLOW_ORIGINS=http://localhost:3000
BASE_URL=http://localhost:8000
DASHBOARD_PUBLIC_BASE_URL=http://localhost:3000
API_PUBLIC_BASE_URL=http://localhost:8000
```

Рис. 1. Файл конфігурації

Відкрити панель керування можна за покликанням localhost:3000(див. рис. 3), перед тим потрібно запустити Sublime Security. У папці з Sublime Security та відкриваємо консоль і вводимо команду sudo docker compose up. Вводимо надійний логін та пароль, та додаємо електронну пошту для моніторингу та сканування листів на вразливості.

Захист корпоративної пошти від різного роду IT - аномалій потребує багато зусиль та фахових спеціалістів в галузі інформаційних технологій. В дослідженні описано процес захисту електронного листування який допоможе захистити внутрішній документообіг від шкідливого програмного забезпечення.

Бібліографія

1. Sublime Security - Cloud email security that's not a black box. URL: https://sublime.security/ .
2. Sublime Security. *Docker Guide*. URL: https://docs.sublimesecurity.com/docs/quickstart-docker.