Секція 1

ВИКОРИСТАННЯ OSINT ДЛЯ ПОБУДОВИ ЕФЕКТИВНИХ СТРАТЕГІЙ КІБЕРЗАХИСТУ

Вірський Я. М.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Тецький А. Г.

Актуальність. У сучасному цифровому середовищі, із зростанням кількості та складності кібератак, організації потребують швидкого доступу до інформації для виявлення, аналізу та нейтралізації кіберзагроз. Open-Source Intelligence (OSINT), що базується на зборі та аналізі відкритих джерел інформації, є одним із ключових компонентів побудови надійних стратегій кіберзахисту[1]. Завдяки OSINT можна виявляти слабкі місця в IT-інфраструктурі, аналізувати поведінку потенційних зловмисників та відстежувати витоки даних. OSINT активно застосовується для ідентифікації вразливостей в IT-інфраструктурі, моніторингу даркнету, аналізу активності у соціальних мережах та відстеження витоків даних[2]. Разом із тим, важливими залишаються виклики, пов'язані із правовими обмеженнями та етикою використання цих інструментів.

Метою даної роботи є дослідження можливостей використання OSINT для розробки ефективних стратегій кіберзахисту, проаналізувати інструменти та методи OSINT, а також визначити їх роль у підвищенні стійкості до кібератак. Розгляд успішних прикладів застосування OSINT у попередженні атак на критичну інфраструктуру, моніторингу даркнету та протидії фішинговим кампаніям.

Основні положення. Аналіз популярних інструментів, таких як Shodan, Maltego, SpiderFoot, які дозволяють ідентифікувати загрози, відстежувати витоки даних та аналізувати активність у кіберпросторі[3]. Застосування OSINT для моніторингу мережі, виявлення аномальної активності, формування профілів загроз та оцінки потенційних ризиків. Дослідження обмежень та викликів у застосуванні OSINT у різних юрисдикціях, зокрема відповідність до GDPR та інших міжнародних стандартів[4].

Висновки. OSINT є важливим компонентом для побудови ефективних стратегій кіберзахисту, що дозволяє зменшити ризики несанкціонованого доступу, витоків даних та інших кіберзагроз. Водночас, успішне використання OSINT вимагає інтеграції інструментів у загальну систему

безпеки, високого рівня компетенцій фахівців та дотримання правових і етичних норм.

Список літератури

1. OSINT and Cyber Security News, Blogs and Publications. *HackYourMom*. URL – https://hackyourmom.com/osvita/novyny-blogy-ta-publikacziyi-pro-osint-ta-kiberbezpeku-chastyna-2 (дата звернення: 10.11.2024).
2. OSINT як частина системи кіберзахисту. *Інформаційна Корпоративна Служба*. URL – https://x-scif.info/articles-and-literature/metodyka-vyyavlennya-obyektiv-kiberbezpeky-na-bazi-tehnologiyi-osint (дата звернення: 10.11.2024).
3. Мірошніченко І. О., Ланде Д. В. Роль методів OSINT в кібербезпеці та їх застосування під час воєнних конфліктів. *Теоретичні і прикладні проблеми фізики, математики та інформатики*. 2024. С. 3. URL: https://ela.kpi.ua/handle/123456789/69980 (дата звернення: 10.11.2024).
4. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації. *VentureBeat*. URL – https://venturebeat.com/2021/03/10/aqua-security-protects-containerized-apps-and-infrastructure-raises-135m (дата звернення: 13.11.2024).

Відомості про авторів

Вірський Ярослав Михайлович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», y.m.virsjkyy@student.csn.khai.edu
Тецький Артем Григорович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskiy@csn.khai.edu