Д.В. Ланде

OSINT У КІБЕРБЕЗПЕЦІ

Навчальний посібник

Київ – 2024

ТОВ «Інжиніринг», 2024

ISBN 978-966-2344-97-4

Д.В. Ланде

OSINT

У КІБЕРБЕЗПЕЦІ

Навчальний посібник

Київ – 2024

УДК 004.056:340.132.1+316.324.8

Рецензенти:
Новіков О.М. – доктор технічних наук, професор, член-кореспондент НАН України
Субач І.Ю. – доктор технічних наук, професор

Д.В. Ланде. OSINT у кібербезпеці : навч. пос. / Ланде Д.В. – Київ: ТОВ «Інжиніринг», 2024. – 522 с. ISBN 978-966-2344-97-4

Навчальний посібник присвячено розгляду ключових аспектів розвідки у відкритих джерелах, розвідувального циклу та його окремих етапів, процесів планування, збирання, обробки та аналізу розвідувальної інформації та доведення цільової інформації та висновків до замовника. Також розкривається широкий спектр технологій і систем OSINT, практичні аспекти роботи з ними.

Видання розраховане на фахівців, науково-педагогічних працівників, аспірантів, докторантів, студентів та курсантів закладів вищої освіти, представників установ та організацій, які займаються вивченням і застосуванням інформаційних технологій і систем OSINT у галузі кібербезпеки.

ISBN 978-966-2344-97-4

ЗМІСТ

ВСТУП

На цей час здатність здобувати, аналізувати та використовувати інформацію у сфері інформаційної та кібернетичної безпеки мають велике значення з декількох ключових причин, серед яких можна виділити зростання кількості даних, цифрову трансформацію бізнесу, суспільства, держави, збільшення загроз і ризиків від кіберзлочинності, залежність багатьох сфер життя від інформаційних технологій. Підприємства, організації, державні установи активно впроваджують цифрові технології для покращення ефективності та конкурентоспроможності своєї роботи. Це призводить до збільшення кількості цифрових пристроїв, точок доступу, які потенційно можуть бути використані для кібератак.

Вразливість інформаційних технологій може суттєво впливати на функціонування різних галузей. Кіберзлочинці стають все більш досконалими та організованими у своїх атаках, що спрямовуються на фінансовий шахрайство, кібершантаж, шпигунство, та інші форми кіберзлочинності. Об'єктом потенційних кібератак стають як окремі користувачі, так і великі корпорації, державні установи і органи. Тому захист від цих загроз стає пріоритетом.

У цьому контексті здатність добувати, аналізувати та використовувати інформацію, серед іншого, і з відкритих джерел, стає ключовою, оскільки це дозволяє вчасно розпізнавати, відстежувати та реагувати на потенційні загрози. При цьому інформація стає не лише цінним ресурсом, але і інструментом для попередження та виявлення кіберзагроз, а також для підвищення ефективності управління безпекою в цифровому середовищі.

У рамках цього посібника розглядаються ключові аспекти розвідки у відкритих джерелах (Open Source INTelligence, OSINT), визначаються поняття розвідувального циклу та його етапів, описуються процеси планування,

підготовки, виконання та підбиття підсумків. Також розкривається широкий спектр галузей застосування OSINT, надаючи глибоке розуміння можливостей цього підходу.

Кожен розділ цього посібника розкриває різні аспекти використання різноманітних джерел інформації (веб-ресурси, RSS-фіди, соціальні мережі, спеціальні бази даних, картографічні дані тощо) для здійснення її ефективного добування та подальшого використання.

З практичного погляду детально вивчаються аспекти автоматизації завдань OSINT та її основні функції, розкриваються ключові аспекти архітектури, структурна організація типової системи OSINT, її функціональні компоненти, взаємозв'язок зовнішніх систем та джерел відкритих даних.

В рамках посібника детально розглядаються і аналітичні аспекти OSINT, включаючи комп'ютерну лінгвістику, методи інформаційного аналізу, засоби формування звітів. Крім того, велику увагу приділено використанню в рамках OSINT мереж та графових баз даних для аналізу та візуалізації такої інформації. Цей підхід дозволяє отримувати глибше розуміння структури та взаємозв'язків великих обсягів інформації, що є критичним для виявлення потенційних загроз та забезпечення безпеки в цифровому середовищі. Зокрема, для збору інформації можуть використовуватися API та веб-скрейпінг для автоматизації процесу збору даних з різних джерел, які утворюють мережеві структури. Графи використовуються також і для моделювання з урахуванням зв'язків між об'єктами, що дозволяє аналізувати структуру мережі та визначати ключові взаємозв'язки. Дослідження графових структур використовується для виявлення та аналізу зв'язків між людьми, організаціями, подіями, збільшення ефективності розслідувань за допомогою візуалізації та аналізу графів. При цьому особливу увагу приділяється методиці визначення ключових, центральних

об'єктів, виявлення кластерів, визначення рівня зв'язків між об’єктами, сутностями тощо.

Візуалізація інформації, використання графічних застосунків для візуалізації зв'язків між сутностями може допомогти швидко розпізнати важливі зв'язки та патерни. Зокрема, у якості практичної складової в посібнику розглядаються спеціалізована графова база даних для ефективного зберігання та опитування графових структур Neo4j, яка надає високопродуктивні можливості для роботи з графами. Якщо інформація містить елементи місцезнаходження, можна використовувати геоінформаційні інструменти для відображення даних на мапі.

Окремий розділ підручника присвячено розгляду елементів нелінійної динаміки у задачах OSINT. Цей розділ буде корисним для аналітиків OSINT, які хочуть використовувати методи нелінійної динаміки для отримання більш глибокого розуміння даних OSINT та виявлення нових закономірностей та трендів. Він охоплює такі теми, як аналіз динаміки публікацій, кореляційний аналіз для виявлення зв'язків між різними елементами даних OSINT, аналіз Фур'є для розкладання даних OSINT на гармонічні складові, вейвлет-аналіз для виявлення локальних закономірностей та аномалій, пошук схожих на заданий шаблон даних OSINT, виявлення фрактальних структур в даних OSINT, що може свідчити про складні та нелінійні процеси.

На цей час використання систем генеративного штучного інтелекту (ГШІ, GAI) у сфері кібербезпеки є актуальним напрямом розвитку розвідки у відкритих джерелах. Ці технології можуть бути вельми корисними в багатьох аспектах досліджень і професійної діяльності. У окремому розділі описуються підходи до формування семантичних мереж у галузі кібербезпеки із застосуванням систем і сервісів ГШІ.

У заключному розділ підручника висвітлюються особливості сучасних промислових системи OSINT, систем контент-моніторингу, надаючи інформацію про реальні застосування набутих знань. Окремо підкреслюються перспективи розвитку, прогнозування викликів та перешкод, а також рекомендації, що допомагають підсумувати отримані знання та використовувати їх у практиці.