

OSINT

Руководство по сбору и анализу открытой информации в интернете

Дейл Мередит

SPRINT
book

2025

Выпущено
при поддержке
КРОК

ОГЛАВЛЕНИЕ

Предисловие	11
Создатели книги	12
Об авторе	12
О рецензентах.....	13
От издательства.....	14
О научном редакторе русского издания	14
Введение.....	15
Для кого эта книга	15
О чем эта книга	15
Условные обозначения	16
Глава 1. Спрятано у всех на виду: раскрываем возможности OSINT	18
Введение в OSINT	19
Поговорим об информации и разведке.....	19
Пассивная и активная разведка	20
Почему OSINT так важна в цифровую эпоху.....	21
В чем фишка OSINT?.....	21
Как же работает OSINT?.....	22
OSINT Framework	23
Разведка на примере реальных ситуаций	25
Начало работы с OSINT и некоторые рекомендации	27
Полезные советы по сбору информации.....	27
Ресурсы, которые нам пригодятся.....	28
Итоги.....	29

Глава 2. Невидимы и недостижимы: почему важно сохранять анонимность	30
Основы анонимности и конфиденциальности в OSINT	30
Как может быть нарушена анонимность	31
Подведем итоги: конфиденциальность в OSINT	36
Защита цифрового следа	36
Как ограничить СВОЕ присутствие в интернете	36
Почему сегодня так важно защищать личные данные	37
Браузеры: первая линия уязвимости	38
Как защитить себя	39
Sock puppet: создание и использование виртуальной личности	45
Предупреждение киберугроз в OSINT	53
Новости о защите конфиденциальности и кибербезопасности	53
Опыт прошлых взломов и инцидентов	55
Итоги	55
 Глава 3. Арсенал OSINT: методы и приемы сбора и анализа информации	56
Знакомство с методами и приемами OSINT	57
Разнообразие приемов в OSINT	57
Выбор подхода в зависимости от задачи	62
Поиск информации в видимой сети	63
Приемы расширенного поиска	63
Google Dorking: поиск уязвимостей через Google	64
Специализированные поисковые системы и каталоги	67
Поиск научных публикаций	68
Поиск исходного кода	69
Поиск патентов	69
Поиск изображений	70
Разведка по социальным сетям (SOCMINT)	71
Скрытые источники информации	81
Погружение в глубокую сеть и даркнет	81
Из чего состоит интернет	82
Сбор данных с помощью theHarvester	85
Shodan	86

Автоматизация сбора и анализа информации.....	90
Итоги.....	92
 Глава 4. Исследуем неизвестное: как найти информацию с помощью инструментов поиска.....	93
Знакомство с инструментами поиска.....	94
Раскрываем тайны сети.....	94
Анализ доменов и IP-адресов.....	95
Как работает WHOIS и зачем он нам нужен.....	95
Применение WHOIS: домены и блоки IP-адресов.....	97
Увеличительное стекло: удобные платформы для поиска в WHOIS.....	98
Поиск взаимосвязей.....	101
Темная сторона: как злоумышленники используют WHOIS.....	102
Анализ DNS и IP-адресов: связь доменов с инфраструктурой.....	103
Трассировка и карты сети: путеводитель по цифровому океану.....	110
Исследование сайтов: работа со скрытыми данными.....	115
Веб-скрейпинг и анализ данных.....	115
Анализ документов и метаданных.....	124
Выявление скрытой информации в документах и других файлах.....	124
Анализ содержания документов.....	126
Визуализация данных OSINT.....	126
Инструменты и методы визуализации данных OSINT.....	127
Рекомендации по эффективной работе с инструментами поиска.....	129
Итоги.....	130
 Глава 5. От Recon-ng до Trace Labs: лучшие инструменты для разведки по открытым источникам.....	131
Recon-ng: мощный фреймворк OSINT.....	132
Запуск модулей и сбор информации с помощью Recon-ng.....	134
Maltego: визуализация данных и связей в OSINT.....	138
Начало работы с Maltego в OSINT.....	138
Поиск инфраструктуры.....	143
Shodan: поисковая система устройств интернета вещей.....	146
Начало работы с Shodan.....	146
Использование API Shodan.....	149

Trace Labs: операционная система для OSINT.....	149
Aircrack-ng: обзор пакета.....	151
Airmon-ng	152
Airodump-ng.....	154
Aireplay-ng.....	156
Aircrack-ng.....	156
Airbase-ng.....	157
Airgraph-ng.....	159
Поиск скрытых сетей	159
Дополнительные инструменты OSINT с открытым исходным кодом	161
SpiderFoot.....	161
Twint	164
Напоследок об инструментах.....	166
Тенденции в мире инструментов OSINT	167
Блоги и сайты.....	167
Конференции и мастер-классы.....	168
Оценка новых инструментов.....	168
Взаимодействие с сообществом OSINT	169
Итоги.....	169
 Глава 6. Глаза и уши разведчика: как OSINT помогает снизить киберриски	170
Введение в разведку киберугроз и OSINT.....	171
Киберугрозы и OSINT	172
Фишинг.....	172
Социальная инженерия.....	174
Вредоносное ПО и программы-вымогатели	176
Целевые продолжительные атаки (APT).....	181
Сочетание OSINT и внутренних систем безопасности.....	183
Платформы для разведки киберугроз и интеграция OSINT.....	185
Ключевые игроки.....	186
Интеграция OSINT в процессы разведки киберугроз.....	187
Обмен данными OSINT с другими платформами и командами.....	188

Разработка программы разведки киберугроз на основе OSINT	190
Что такое требования к разведке?	190
Значение OSINT	191
Пример из практики: использование OSINT для расследования инцидента	193
Итоги.....	194
 Глава 7. Защита личных и корпоративных данных от киберугроз	195
Как OSINT защищает личные и корпоративные данные.....	196
Преимущества проактивного подхода к кибербезопасности.....	196
Личная цифровая гигиена и роль OSINT	197
Выявление и устранение рисков присутствия в Сети.....	197
Повышение конфиденциальности и безопасности	202
Как OSINT помогает оценить и укрепить безопасность организации	203
Определение потенциальных уязвимостей.....	203
Программы-вымогатели: выявление и противодействие.....	205
Обнаружение фишинга и приемов социальной инженерии	207
История хакерской группы Exotic Lily.....	207
Фишинговые атаки группы Cobalt Dickens	209
Расследование взломов и других нарушений кибербезопасности.....	210
Выявление источника, масштабов и последствий инцидентов кибербезопасности.....	212
Создание устойчивой системы киберзащиты на основе OSINT.....	213
Сотрудничество с сообществом кибербезопасности.....	214
Адаптация к изменениям в мире киберугроз.....	214
Обновление стратегии кибербезопасности на основе OSINT	216
Помните об инструментах	217
Итоги.....	219