OSINT(Open Source Intelligency)

Слайд 1 – OSINT(Текст)

Что такое OSINT?

OSINT – Разведка На Основе Открытых Источников

OSINT — это технология поиска, аккумулирования и анализа данных, собранных из доступных источников в интернете

Open Source Intelligence — разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ

Технология позволяет собирать максимум информации из открытых источников для полноценного профессионального анализа. При этом данные могут размещаться в различных формах: статьи, публикации обсуждения на форумах, видео- и аудиофайлы, документы, картинки, анимации, гифки и т. д

Слайд 2 – Виды OSINT (Структура)

OSINT

- Деанонимизация
  - Доксинг
- Конкурентная Разведка

ВИДЫ OSINT

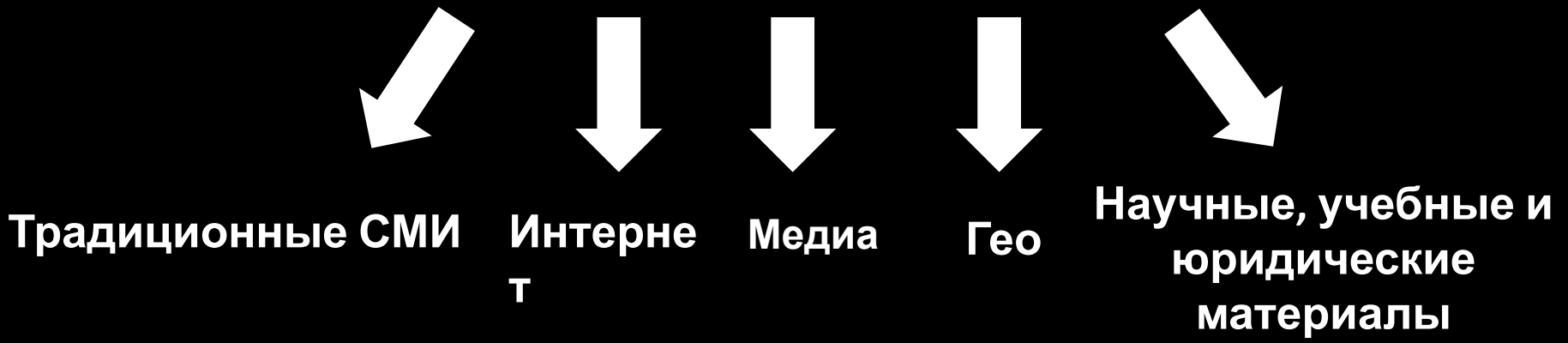
Деанонимизация – Самый распространённый вид. Заключается в установлении личности человека.

Конкурентная разведка *— это деятельность компании, которая подразумевает сбор и анализ информации о конкурентах, конкурентоспособных продуктах и услугах. Вся информационно-аналитическая работа проводится исключительно в рамках этических норм.*

Доксинг – Разновидность деанона,заключающаяся в публикации данных, с целью мести.

Слайд 4 – Источники OSINT(Структура)

Источники OSINT



Слайд 5 – Источники
OSINT(Текст)

Источники OSINT

Интернет - включает в себя следующее (и многое другое): форумы, блоги, сайты социальных сетей, сайты обмена видео, Википедия, записи Whois зарегистрированных доменных имен, метаданные и цифровые файлы, веб-ресурсы Даркнета, данные геолокации, IP-адреса , люди, поисковые системы, и все, что можно найти в Интернете.

Традиционные СМИ - телевидение, радио, газеты, книги, журналы.

Медиа - Фотографии и видео, включая метаданные.

Гео - Геопространственная информация (например, карты и коммерческие изображения).

Научные, учебные и юридические материалы - Специализированные журналы, научные публикации, диссертации, материалы конференций, профили компаний, годовые отчеты, новости компаний, профили сотрудников и резюме.

Слайд 6 – Источники Интернет-OSINT(Структура)

Источники Интернет-OSINT

Слайд 7 – Источники
Интернет-OSINT(Текст)

Источники Интернет-OSINT

Боты и Сайты - Самый лёгкий и распространённый тип, он делается в первую очередь, но обычно его не хватает. Он заключается в использовании различных специализированных сервисов.

Утилиты - То же самое, только вместо сервисов используются небольшие утилиты.

Дорки - Так же очень распространённый вид, заключающийся в составлении точечных поисковых запросов - дорков. Это запросы с использованием различных операторов и спец.символов.

Специализированные поисковики - Например поисковик по телеграмму или поисковик по форумам.К этому типу я так же отношу Shodan.

Открытые гос.структуры - Некоторые государственные службы хранят свои базы в открытом доступе, на собственных сайтах.

Слитые базы - Бывают базы закрытого типа, например билайн или вк, но после их слива они становятся открытыми.

Профессиональное ПО – Например Maltego или Lamyre.

Ручной поиск - Сюда входят все остальные методы, например анализ страниц.

Слайд 8 – Где Используется OSINT(Структура)

Где Используется OSINT

Слайд 9 – Где Используется OSINT(Текст)

Где Используется OSINT

Правительство - государственные органы, особенно военные ведомства, считаются крупнейшим потребителем источников OSINT.
Правительствам нужны источники OSINT для различных целей, таких как национальная безопасность, кибер-слежка за террористами, понимание взглядов отечественной и зарубежной общественности по различным вопросам и другие.

Международные организации - Международные организации, такие как ООН, используют источники OSINT для поддержки миротворческих операций.

Гуманитарные организации - используют источники OSINT, чтобы помочь им в их усилиях по оказанию помощи во время кризиса или катастрофы и других целей.

Правоохранительные органы - полиция использует источники OSINT для защиты граждан от преступлений.

Бизнес-корпорации - корпорации используют источники OSINT для исследования новых рынков, мониторинга деятельности конкурентов, планирования маркетинговой деятельности и другого.

Частные Лица – используют OSINT для мести, проверки на измену, поиска пропавшего родственника и другого.

Слайд 10 – Преимущества OSINT(Текст)

Преимущества OSINT

Минимальные риски - использование общедоступной информации для сбора разведданных не имеет риска по сравнению с другими видами разведки, такими как использование шпионских спутников или использование человеческих ресурсов на местах для сбора информации, особенно во враждебных странах.

Экономическая эффективность - использование OSINT, как правило, дешевле по сравнению с другими способами получения информации. Например, использование человеческих ресурсов или шпионских спутников для сбора данных является дорогостоящим.

Удобство доступа - источники OSINT всегда доступны, где бы вы ни находились, и всегда актуальны.

Правовые вопросы - Большинство ресурсов OSINT могут совместно использоваться различными сторонами, не беспокоясь о нарушении любой лицензии на авторское право, поскольку эти ресурсы уже опубликованы публично.

Помощь правоохранительным и контрольным органам в финансовой сфере - OSINT позволяет специализированным государственным органам, например, выявлять лиц, уклоняющихся от уплаты налогов. Многие известные знаменитости и некоторые гигантские компании участвуют в уклонении от уплаты налогов.

Борьба с контрафактами в Интернете - методы OSINT могут использоваться для поиска фальшивых продуктов / услуг и прямого правоприменения для закрытия таких сайтов или для отправки пользователям предупреждений о прекращении работы с ними.

Поддержание национальной безопасности и политической стабильности - это может быть самой важной ролью OSINT; это помогает правительствам понять отношение своих людей

Минусы OSINT

Огромный объем данных - Сбор OSINT приведет к появлению огромного количества данных, которые необходимо проанализировать, чтобы оценить их полезность для решения поставленной задачи. Огромный объем первичных , "сырых" данных, которые затем требуется обработать, останется проблемой для того, кто проводит сбор данных с помощью OSINT.

Надежность источников - Источники OSINT, особенно когда они используются в контексте разведки, должны тщательно перпроверяться, прежде чем им можно будет доверять.

Трудоёмкость и потребность в квалифицированных аналитиках, умеющих пользоваться OSINT - Огромный, заведомо избыточный объем данных считается самой большой проблемой для сбора OSINT. Людям необходимо просматривать результаты работы автоматизированных инструментов, чтобы знать, являются ли собранные данные надежными и заслуживающими доверия.
Кроме того, порой возникает необходимость сравнить сведения, полученные с помощью OSINT, с некоторыми секретными данными (это относится к некоторой военной и коммерческой информации), чтобы обеспечить их надежность и актуальность. Всё это требует времени и квалифицированных кадров.

Слайд 12 – Интересные Факты
(Текст)

Интересные Факты

- 90 процентов разведданных приходит из открытых источников и только 10 — за счёт работы агентуры

- Социальная инженерия - Не OSINT

- Об OSINT знает 1% населения

Презентация подготовлена @ClownD3rty, для телеграмм-канала @D3rtyHack

Спасибо За просмотр!

Основные Источники:

https://telegra.ph/OSINT-11-04-2

https://yushchuk.livejournal.com/1451268.html

Поддержать Автора:

Qiwi: EKSYTOP

Qiwi Card : 4890 4947 5696 4672