/февраль
2022

BEHOLDER
IS
HERE
CONSULTING

10 ЛУЧШИХ БЕСПЛАТНЫХ OSINT ИНСТРУМЕНТОВ

по версии t.me/forensictools

..то, что мы используем в работе сами и нам это нравится!

10. SOCIAL OSINT
ПОИСК ЧЕЛОВЕКА В СОЦИАЛЬНЫХ СЕТЯХ И СЕРВИСАХ

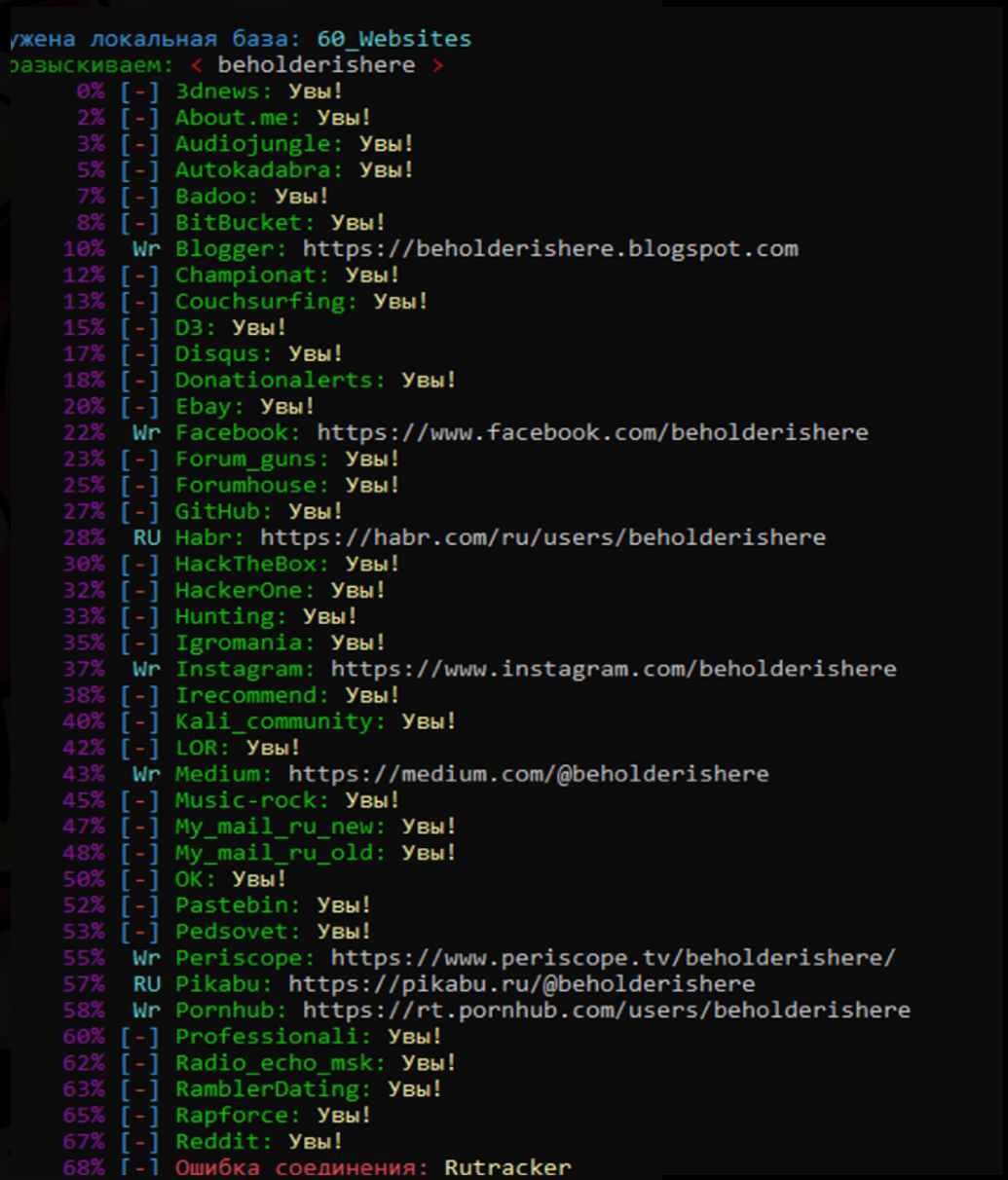
BEHOLDER IS HERE
CONSULTING

SNOOP

[github.com/snooppr/snoop]

Инструмент для анализа различных сайты, форумов и социальных сетей на предмет наличия искомого имени пользователя, т.е. позволяет определить на каких сайтах присутствует пользователь с указанным ником. Проект разработан на материалах исследовательской работы в области скрапинга публичных данных. На данный момент поисковая база содержит 2400 сайтов!

И субъективно, одно из лучших решений для OSINTa в русскоязычном сегменте интернета.

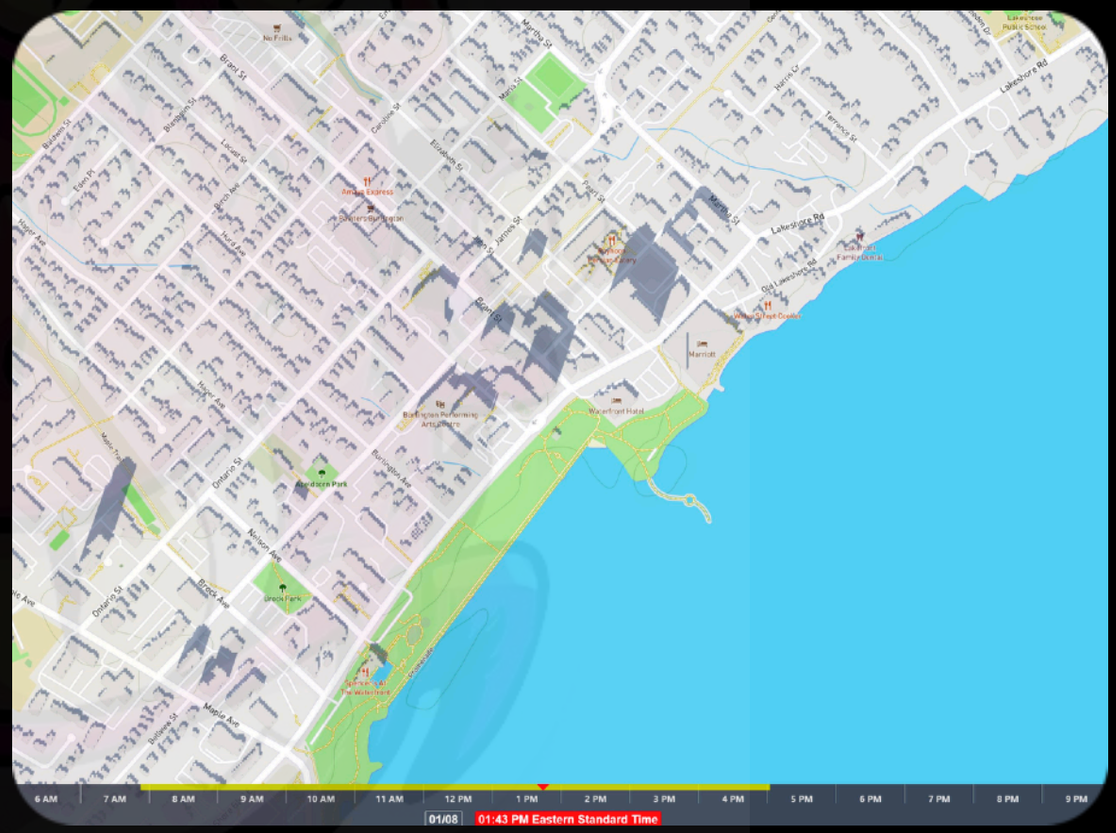


Shademap

[shademap.app]

Карта движения теней, которая учитывает все здания и городской рельеф, показывая расположение тени как в реальном времени, так и на любые выбранные дату и время. В наличии очень интуитивный интерфейс и режим 3D- карты.

Очень наглядное решения, хоть и не такое информативное как suncalc и mooncalc.



BEHOLDER IS HERE
CONSULTING

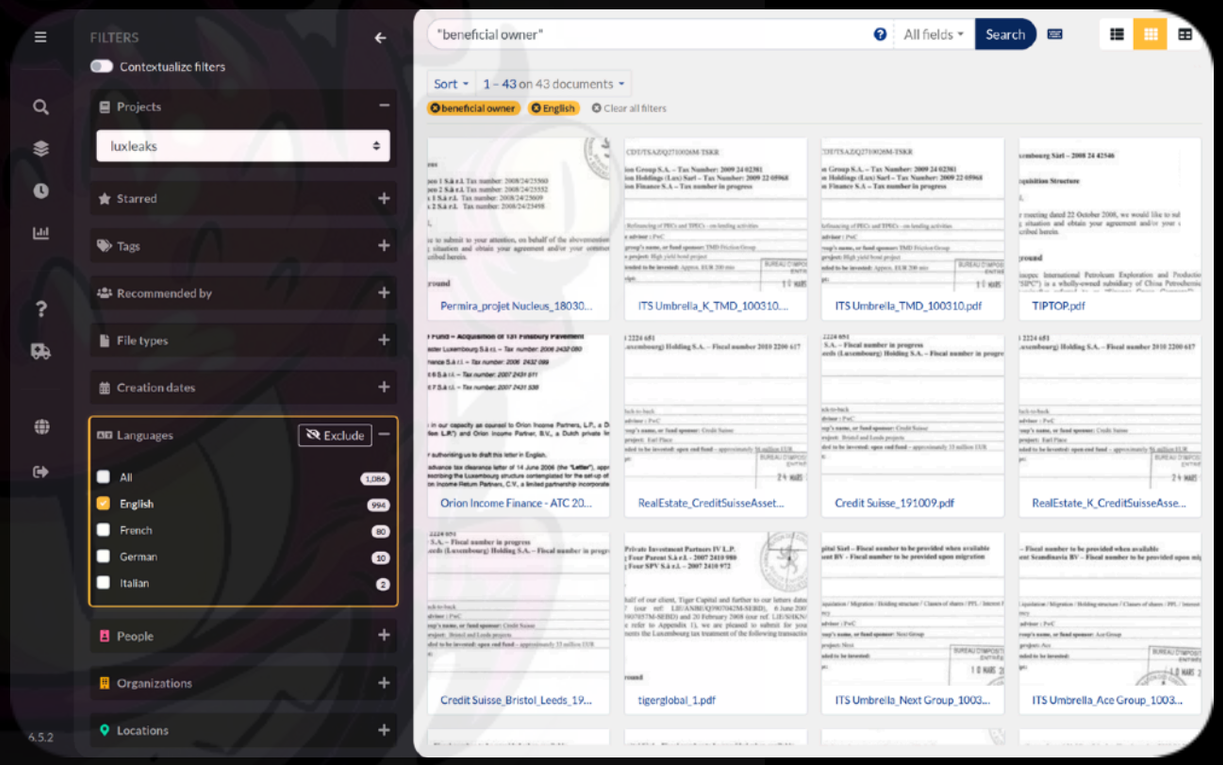
Datashare

[datashare.icij.org]

Инструмент для агрегации, хранения и анализа данных. Особенно хорош для командной работы.

Возможности:

- индексировать и сохранять ваши документы в базе данных, ставить теги на документы
- искать PDF-файлы, изображения, тексты, электронные таблицы, слайды и любые файлы одновременно, а также осуществлять поиск по содержимому
- фильтровать документы по различным параметрам, операторам и регулярным выражениям
- производить автоматическое обнаружение людей, организаций и местоположений
- умеет алгоритмы обработки естественного языка, пакетный поиск
- устанавливать плагины и расширения
- использовать приложение в качестве сервера для обмена документами между несколькими пользователями

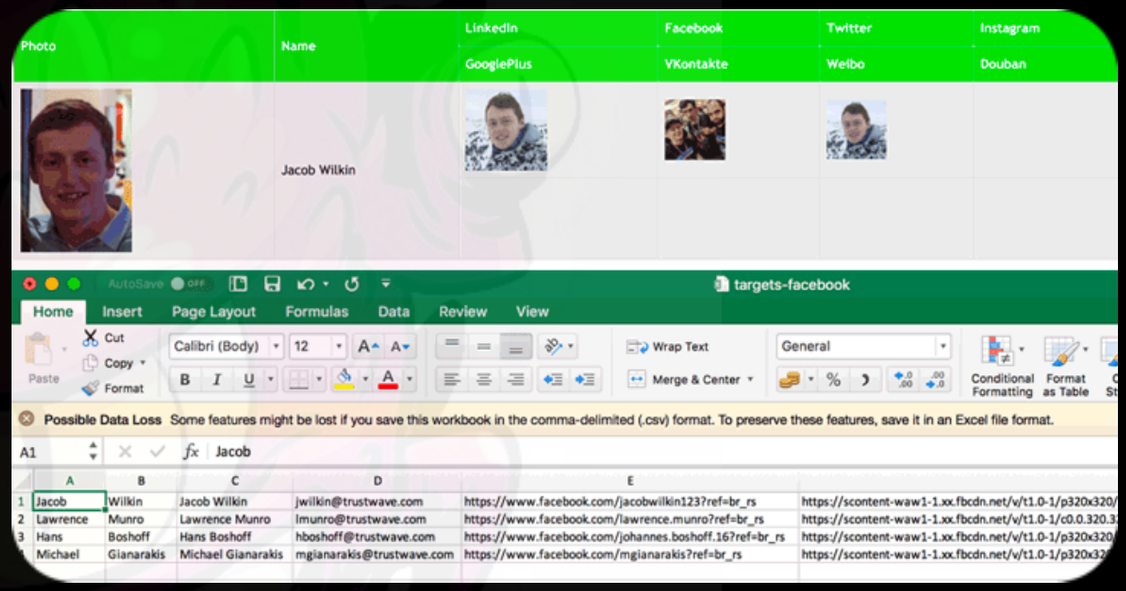


BEHOLDER IS HERE
CONSULTING

SOCIAL MAPPER

[github.com/Greenwolf/social_mapper]

Инструмент с открытым исходным кодом, который использует распознавание лиц для масштабной корреляции профилей социальных сетей на разных сайтах. Он использует автоматизированный подход к поиску популярных социальных сетей по именам и фотографиям целей, чтобы точно обнаружить цель, выводя результаты в отчет.



Social Mapper имеет множество применений- например, автоматизированный сбор большого количества профилей в социальных сетях для использования в целевых фишинговых кампаниях. Распознавание лиц помогает этому процессу, удаляя ложные срабатывания в результатах поиска, чтобы быстрее просматривать эти данные.

6. ИЩЕМ МЕСТОПОЛОЖЕНИЕ WIFI ТОЧЕК ДОСТУПА

BEHOLDER IS HERE
CONSULTING

GEOWIFI

[github.com/GONZOsint/geowifi]

Скрипт позволяющий определить фактическое местоположение беспроводных точек доступа по BSSID и SSID основываясь на открытых данных из таких сервисов как Wigle, Apple, OpenWifi и через API Mylnikov.

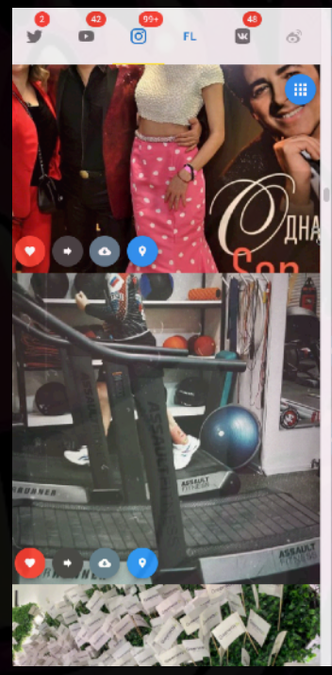
SOCIAL OSINT
5. ИЩЕМ ГЕОЛОКАЦИЮ ПОСТОВ В СОЦ СЕТЯХ

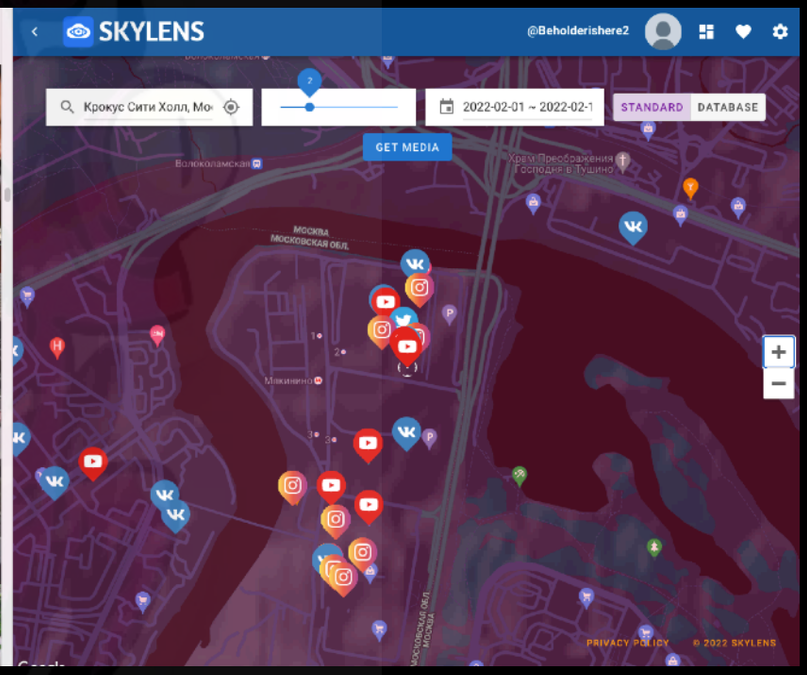
BEHOLDER IS HERE
CONSULTING

SKYLENS

[app.skylens.io]

Веб-сервис позволяющий просматривать все посты созданные в Twitter, Youtube. Instagram, Flicker, VK и Weibu в определенный момент времени, в определенном радиусе на карте и хештегу.





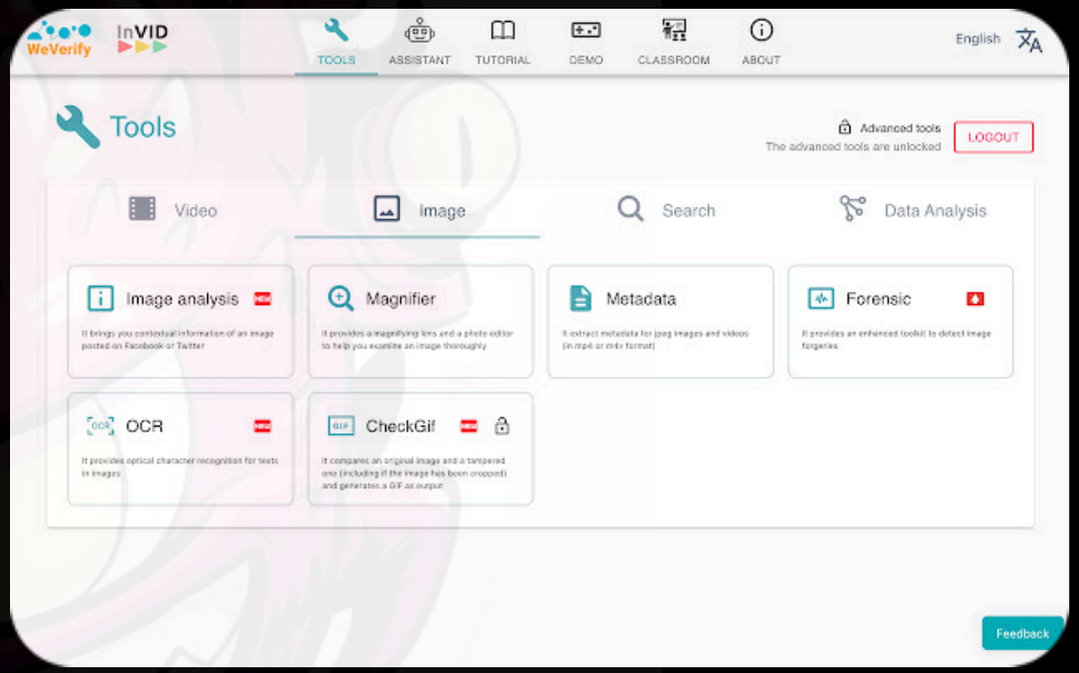
4. DATA verification
ПРОВЕРКА ВИДЕО НА ПОДЛИННОСТЬ

BEHOLDER IS HERE
CONSULTING

InVID-WeVerify

[invid-project.eu/tools-and-services/invid-verification-plugin]

Расширение для Chrome и Firefox для проверки изображений и видео. С помощью расширения можно получать контекстную информацию о видео Facebook и YouTube, выполнять обратный поиск изображений в поисковых системах Google, Baidu или Яндекса, посмотреть метаданные, поискать по ключевым кадрам, узнать, кто первый загрузил видео или изображение в сеть, чтобы установить авторство.



SOCIAL OSINT

3. ПОИСК ЛЮДЕЙ ПО ФОТО В СОЦИАЛЬНЫХ СЕТЯХ

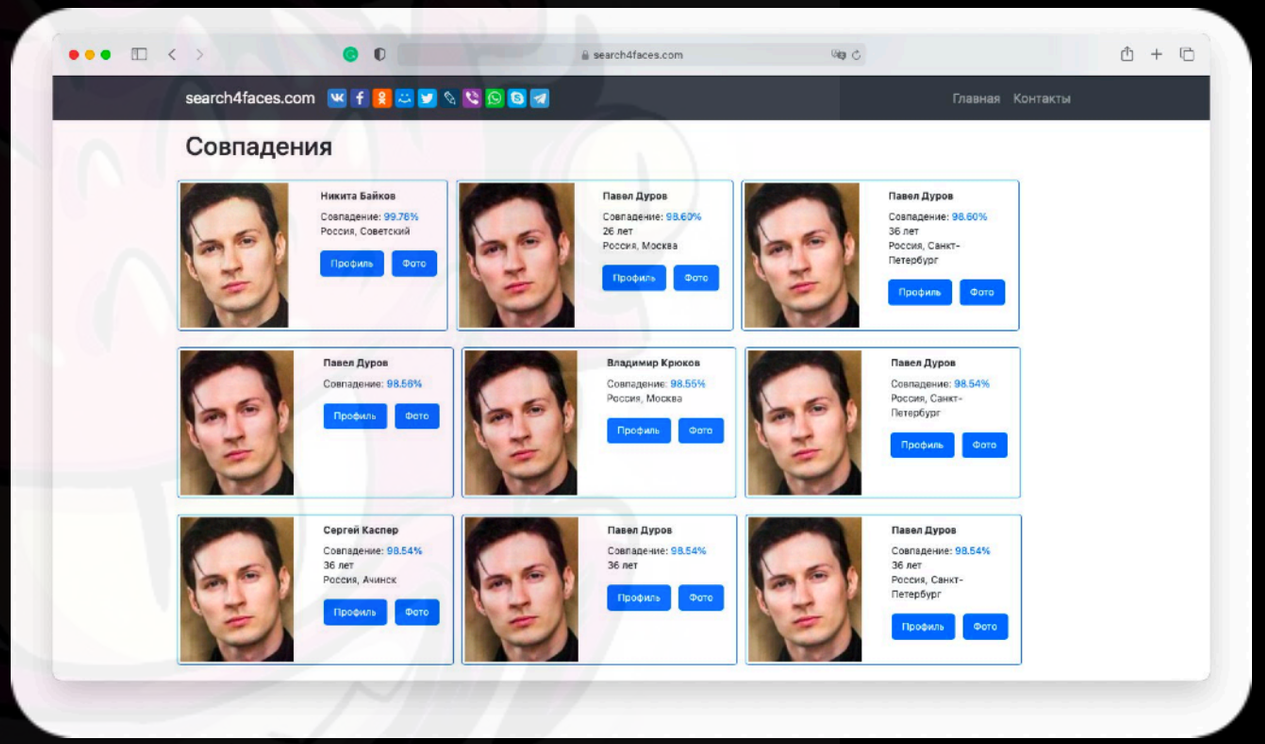
BEHOLDER IS HERE

CONSULTING

Search4face

[search4faces.com]

Поисковый сервис поиска по фото (вернее по аватарке) в социальных сетях. Может искать в VK, Одноклассники, Инстраграм, Тикток, Клабхауз.

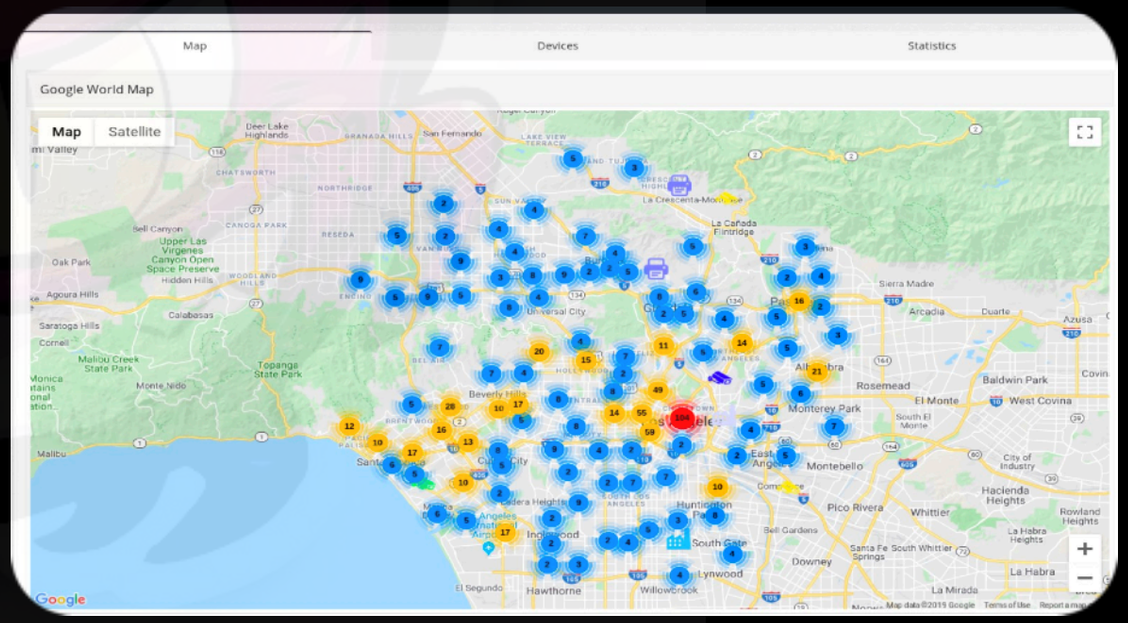


BEHOLDER IS HERE
CONSULTING

Kamerka-GUI

[https://github.com/woj-ciech/Kamerka-GUI]

Поисковый инструмент построенный на движке Shodan для поиска устройств интернета вещей и контрольных панелей промышленных устройств смотрящих в интернет. Отличный инструмент дополняющий возможности Shodan и делающий работу с ним удобней и информативней.



WAYBACK MACHINE

[web.archive.org]

Самый большой интернет архив. Поиск удаленных
из сети страниц, данных и файлов

ИССЛЕДОВАНИЯ, АУДИТ И КОНСАЛТИНГ

1. Технический аудит

1.1. Аудит информационной безопасности

- Аудит сетевой инфраструктуры
- Аудит внедренных политик безопасности и их актуальность
- Тестирование на проникновение в информационную инфраструктуру
- Аудит актуальности мер защиты относительно модели угроз ИБ

1.2. Аудит технических систем безопасности (видеонаблюдение, скуд, опс)

- Проверка проектной и рабочей документации и ее актуальность
- Проверка технического состояния установленных систем безопаности
- Проверка целесообразности размещения элементов ТСБ для эффективного решения задач безопаности относительно модели угроз
- Проверка конфигураций программной платформы ситемы безоопаности
- Проверка конфигураций аппаратных элементов системы безопасности.

2. Ситуационный аудит

- Проведение исследований на проникновение в защищенный периметр компании для тестирования эффективности противодействия к определенным моделям угроз и противодействию им.

3. Моделирование угроз

- Ситуационные симуляции для изучения поведения сотрудников компании при определенных моделях угроз информационной безопасности (фишинговый рассылки, имитация хакерских атак, имитация утечек информации)
- Ситуационные симуляции для изучения поведения сотрудников СБ при определенных моделях угроз (физическое проникновение, рейдерский захват, террористическая угроза)

4. Определение модели угроз и нарушителей

Описание существующих угроз безопасности, их актуальности, возможности реализации и последствий.

- Выявление критичных объектов информационной инфраструктуры.
- Определение перечня угроз для каждого критического объекта.
- Определение способов реализации угроз.
- Определение модели нарушителя.
- Оценка материального ущерба и других последствий возможной реализации угроз.

5. Форензика

- Криминалистический анализ информационных систем на наличие определенных данных.
- Криминалистический анализ компьютеров, смартфонов, планшетов, телефонов, дронов направленный на извлечение данных различных сервисов.
- Восстановление данных с носителей, смартфонов, компьютеров.
- Проведение расследований случаев промышленного шпионажа.
- Поиск технических каналов утечки информации.