**OSINT (OPEN SOURCE INTELLEGENCE)**

OSINT is the practice of collecting data from various sources freely available on the net for public. Skilled researchers can collect any kind of data from the OSINT, provided that they know where to look for the information.

**What to do for OSINT to protect your organization?**

OSINT can be used both ways as such. It can be used to dig out the data of the competitor and getting an edge. Otherwise, it can be used to infer the information of your company to others. Therefore, it should be used to find what data is posted publicly, and how it is used by an attacker to get inside the network.

**How do I investigate using OSINT?**

There is huge amount of data available freely in the network. So the question arises is where and how to search.

Therefore, in simple terms, it is the answer to answerable question.

For example, if the question is “which is safer among Los Angeles and George Atlanta??” then it is tough to answer.

But if the question is “How much the crime rate has been increased in Los Angeles since 1990 till date?” It is easy to answer by finding the data from records keeper.

**OSINT Framework and tools?**

There are hell lot of tools available in the internet, which can be used to find the desired data. Most reliable sources are Government Organisations, Corporates and NGOs who work for particular type of works.



**What OSINT Techniques are there?**

There are basically two techniques to preform OSINT. One is active and other is passive.

In Active OSINT, while gathering information, one need to get in contact with the target. There is a high risk of getting detected.

In passive OSINT, there is no point of getting detected because, what ever information is gathered, that is gathered from the databases and third parties, where information is saved.



**How does OSINT relate to SOCINT & HUMINT?**

HUMINT is human intelligence and old school technique of collecting information using human resources. It is like collecting all the data about a person before interviewing that particular person.

HUMINT is collecting or gathering information of people using social media and using that information and other databases of a particular organization. It is easy to understand who can hold what sort of information or the information which we need.

**How do I find OSINT on phone numbers?**

The sites such as truecaller.com, thatsthem.com and various other sites which can provide accurate information like names related to the phone numbers as such.

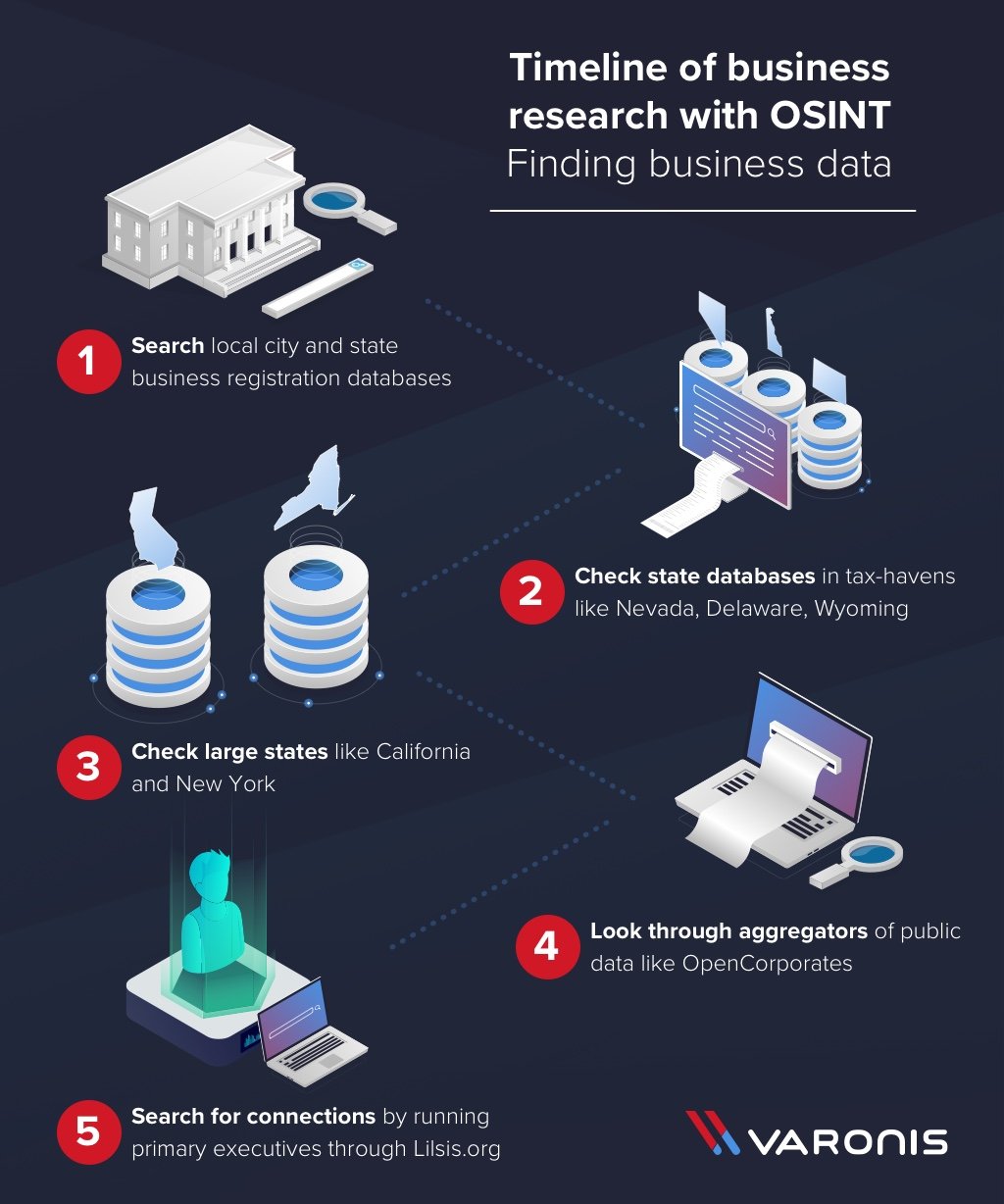
Further, it is easy to dig down using social media and all other data related to a particular name.

**How do I find OSINT on Names?**

Often Names are find on the business documents and websites of the organisations.

**How do I find OSINT on Businesses?**

Businesses are some of the easiest entities to find information on, as they need to register a lot of paperwork with public entities to exist. This paperwork is often entirely public and searchable, giving investigators a trove of information full of details which help to expand an investigation in the early stages.



**How do I find OSINT on Websites?**

Websites represent a lot of information about a business, both technical and in the way the website has changed messaging and branding over time. For OSINT investigations, websites are often looked at for their technical information, like who registered it, what servers are in use, and what software is maintaining it. This can be done through services like ***Shodan***, which allow you to profile an organization’s technical infrastructure without actually scanning it yourself.

***Actual content of websites***.

***Google Dorking***, structuring google searches can be greatly useful to find the required information.

**Is Data Collected in an OSINT Investigation Regulated Under Privacy Laws Like GDPR, CCPA?**

OSINT investigations are generally not something California residents need to worry about. GDPR, however, is more strict with these rules, meaning it’s important to take basic steps during an investigation to ensure you don’t expose personal information of a subject and that you’re storing it properly. This means using encryption to store your investigation notes and not leaving them where they can be accessed by a third party.

**What Are Some Examples of OSINT Investigations?**

Bellingcat has produced some of the most dramatic OSINT investigations in recent memory, in particular blowing the lid off denials by the Russian government of involvement in various operations by digging through databases to prove their involvement directly.

Memorable examples include tying Russian spies to their secret employment by digging through car registration databases (<https://www.bellingcat.com/news/2018/10/04/> 305-car-registrations-may-point-massive-gru-security-breach/comment-page-5/), and linking social media photos to prove Russian soldiers were operating in areas the government claimed they weren’t. Many OSINT investigations cover topics like war crimes in areas too remote or dangerous to access remotely and was used extensively in the investigation into the downing of Malaysian Airlines Flight 17 (MH17). (https://www.bellingcat.com/news/uk-and-europe/2017/12/08/russian-colonel-general-delfin/)

**Who Makes Use of OSINT Reports?**

OSINT is a critical part of both public and private intelligence, arming businesses, governments, and individual investigators with a vast amount of high-quality information to base and make decisions on. Whether conducting an investigation for research, business intelligence, or threat analysis, OSINT can allow anyone to have access to some of the best available data in the world.