OSINT
Losena Ltd.
WE KNOW A LOT

OSINT Losena Ltd

Presentation of the company

Official Israeli company #516359361

Official supplier of the
Israeli Ministry of Defense
11030281

ISO 9001:2015 · ISO 27001:2022 · ISO 27701:2019 · ISO 20000-1:2018 · ISO 27017:2015 · ISO 31000:2018

Market Review

> «The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency»

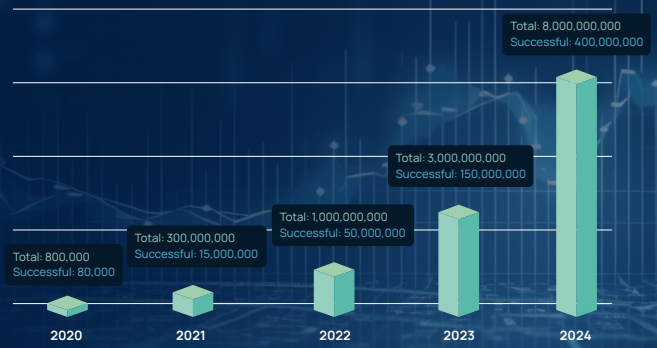
Bill Gates

About Cybersecurity

Recently, the term "cybersecurity" has become something of a magical phrase in the eyes of the average user.

Many companies worldwide offer their solutions to protect user information, resulting in trillions of dollars being spent annually. However, the creators of these products often exaggerate their capabilities, claiming to provide 100% security. In reality, cybersecurity doesn't operate as flawlessly as advertised.

Number of hacker attacks in 2020–2024

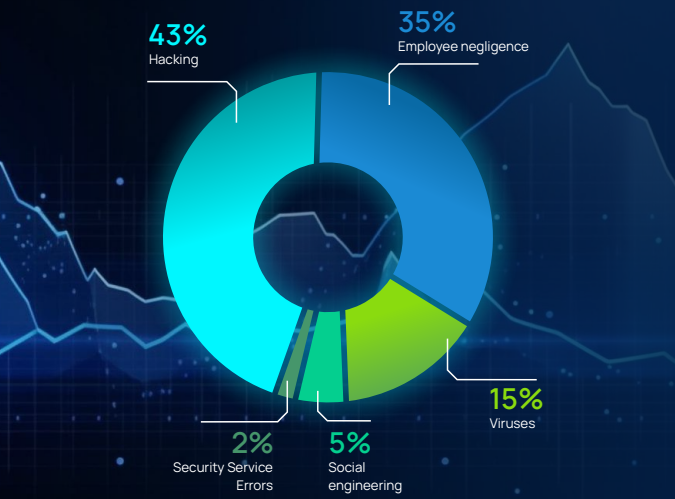


About Cybersecurity

Cyberattacks continue to increase in both quantity and sophistication, while organizational systems are becoming increasingly complex. Security services are under strain, as always. Today's Security Operations Center (SOC) has many areas of responsibility and not enough staff to handle it all.

64% of SOC teams complain about the complexity of interacting with different security tools and management consoles that are poorly (or not at all) integrated, making thorough and timely incident investigation and response difficult.

49% say they lack the personnel for manual analysis, investigation, and response to the growing volume of security events.



About Cybersecurity

No one can guarantee security even up to 50% due to the inevitable human factor.

The strongest password encryption can be compromised not by a virtual hacker, but by an ordinary employee who falls victim to a phishing site or inserts an unchecked USB drive into a work computer.

There is no foolproof defense against the human factor; the main focus should be on minimizing consequences and damages through swift incident response.

To address these challenges, it is necessary to employ methods of private internet intelligence - OSINT.

$9,500,000,000

damage from the 10 most important data breaches in 2024

All company logos featured in this presentation belong to their respective owners and are included for visual representation purposes.
Based on: https://nordlayer.com/blog/data-breaches-in-2024/

What is OSINT?

Open Source Intelligence, or OSINT, encompasses everything that is publicly available on the internet and does not require payment or special technical efforts to obtain.

The OSINT process involves searching, collecting, and analyzing information from publicly accessible sources. This **intelligence discipline** finds applications in various fields, including business, politics, investigations, law enforcement, investing, and security.

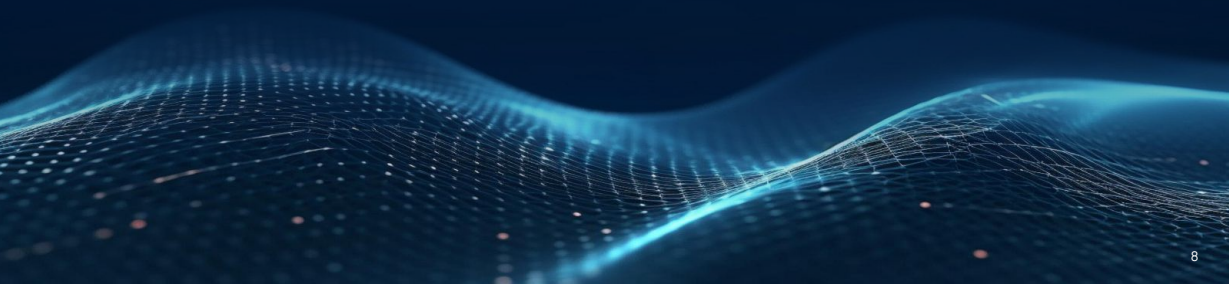
Since the early 2000s, with the rise in popularity of social media and the Internet of Things, the volume of available information has grown rapidly. In recent years (2016-2019), OSINT has been actively integrated into business practices, political campaigns, investigative work, research, investments, and security operations.

According to CIA analyst Sherman Kent, policymakers obtain up to 80% of the information they need for decision-making from open sources. Even in the realm of intelligence activities, as General Lieutenant Samuel Wilson stated, **over 90% of intelligence comes from open sources, with only 10% requiring operational measures and covert work.**

Our company
Technologies and products

«The only way to do great work is to love what you do.»

Steve Jobs



OSINT Losena Ltd.

OSINT Losena Ltd. is an Israeli startup specializing in the development of open-source intelligence (OSINT) technologies and providing cybersecurity consulting services worldwide. The company was founded in 2021 by two experts in the field of high technology:

Sergei Kraizman - a specialist in finance and internet payment systems.

Vitali Sokol - a developer of cybersecurity systems, the author of two proprietary encryption algorithms, and a security consultant for numerous internet projects.

From 2021 to present, the company has successfully developed a range of unique technologies in the field of information intelligence and cybersecurity.

At present, the company is actively establishing mutually beneficial partnerships with potential collaborators in countries such as the United States, the United Kingdom, Morocco, France, Monaco, Switzerland, India, and Japan.

OSINT
Losena Ltd.

Our Intelligence Technologies

We are not a typical cybersecurity company primarily focused on safeguarding client information. Instead, we function as a vital support tool, operating discreetly, to protect our clients' systems, algorithms, and protocols, while promptly notifying them of any exceptional events.

Our company has developed a comprehensive technological platform that covers the entire cycle of intelligence services.

It's worth noting that during our development process, we consciously refrained from using standard software solutions and cloud platforms in order to prioritize the utmost security for both our company and our clients.

Our Intelligence Technologies

DATA COLLECTION

Our advanced algorithms enable us to daily detect extensive volumes of leaks, databases, and other critical information on the Internet and the Darknet. Currently, we are adding 1 to 2 terabytes of information to our database each day.

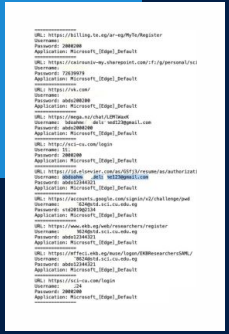
INFORMATION ANALYSIS

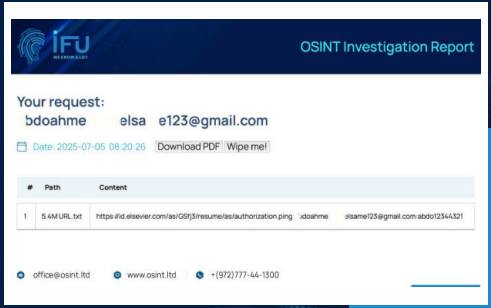
Using our developed software and the efforts of our analysts, we process the acquired data, structure the information, remove outdated or suspicious records, and prepare the data for efficient searching through indexing and filtering.

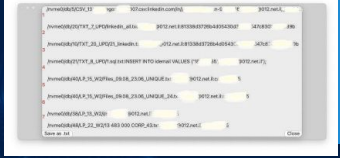
SWIFT SEARCHING

We have devised a unique algorithm that allows us to search our database at speeds of up to 26 gigabytes per second. Currently, we are planning to expand our technical infrastructure and implement artificial intelligence algorithms to further enhance data processing outcomes.

Examples of Our Work







Our Cybersecurity Technologies

We are not only involved in developing Open Source Intelligence (OSINT) technologies but also concurrently engage in creating our own solutions in the field of information security.

DATA ENCRYPTION

Our company's specialists have developed a unique data encryption algorithm for any format. This algorithm allows our clients to store information on corporate servers, ensuring reliable protection against potential breaches or leaks. Unauthorized access attempts to confidential data are effectively prevented by the algorithm from being utilized for malicious purposes. Detailed information about our algorithm is available in a separate company presentation.

INFORMATION MARKING

Our proprietary technology for marking confidential data enables the integration of a special digital beacon into information of any format. This beacon is integrated with our reconnaissance system. If marked information becomes publicly accessible, we promptly recognize this fact and notify the owner, ensuring a swift response to potential threats.

DECENTRALIZED DATA STORAGE

We have developed an algorithm that divides information into numerous parts, encrypts each part with a distinct code, and distributes them across hundreds of storage locations in the network. Data collection and decryption are only possible for the owner, ensuring the highest level of storage security. Additional information about our technologies and their benefits can be obtained upon request.

Our Products

Ready Solutions Based on the Described Technologies

Developing technology is only half the success; creating a product that optimally utilizes all its capabilities and is convenient for our clients is equally important. Currently, we have developed several products that assist our clients in solving various tasks:

IFU.APP

This is our primary and flagship product, allowing clients from anywhere in the world to utilize our Open Source Intelligence (OSINT) services through a browser and an internet connection.

To initiate a search, simply enter the email address of interest and receive a detailed report after a short period.

The product interface is designed to cater to the needs of even novice users and does not require specialized knowledge.

N2Q.NET

This product is a data encryption tool built on the foundation of our company's unique algorithm.

This product operates in a closed mode, and access is granted only to a select group of clients.

A demo page is available at: https://n2q.net/demo

Detailed product description and access are provided upon special request.

FALCON-2

Falcon 2 is a comprehensive platform for managing OSINT investigations, allowing investigators to structure client-specific dossiers and maintain logical investigative chains. It operates on its own continuously updated database, includes secure encrypted messaging, and ensures centralized data storage independent of third-party APIs.

Hydra
Leak-Proof File Protection

HYDRA

Hydra assigns a unique tracking tag to every file, allowing continuous monitoring of its location and access status, even if the file is leaked online.

It detects unauthorized activity in real time, blocks access on unverified devices, and protects against tampering and brute-force attacks.

Anteater
Real-time Crypto Anomaly Detection

ANTEATER

Anteater monitors transactions across major blockchains (BTC, ETH, USDT) in real time, automatically detecting suspicious patterns associated with money laundering and financial fraud.

It compares live data with historical blockchain records, highlighting anomalies for immediate investigative attention.

SEA DRAGON
Private Safe Data Storage

SEA DRAGON

Sea Dragon is an innovative distributed data storage solution that splits files into segments, mixes in decoy data, and spreads them across a secure peer network.

No single node contains more than 5% of the original file, and complete restoration is only possible with a unique key held by the user.

BLACK WOLF
Real-time Information Security Control

BLACK WOLF

Black Wolf monitors open sources, social networks, and messaging platforms for extremist activity, using AI to adapt to language and region-specific patterns.

It generates real-time alerts based on custom-defined indicators, enabling fast response to emerging threats and reputational risks.

OSINT
Losena Ltd.
WE KNOW A LOT

Let's embark on this journey together – we're excited to work with you!

www.osint.ltd

+(972) 777-44-1300

office@osint.ltd

*3316