



DEFINING OSINT

AND ITS USES IN CYBERSECURITY

WHAT IS OSINT?

An acronym standing for ‘open-source intelligence’, **OSINT refers to the extraction and analysis of open-data – information which is in the public domain and legally accessible to all.** While the name evokes espionage, the publicly open nature of its sources gives OSINT broader and less secretive modes of application, setting it apart from what we might think of as traditional intelligence.

Although open-source intelligence has now spilled over to commercial sectors, where it is leveraged in various ways, its importance for law enforcement agencies (LEAs) and intelligence bureaus has become ever more profound. **With 80-90%** of crucial modern intelligence data rumoured to come from open sources, **OSINT is now a cornerstone of modern reconnaissance and investigation processes.**



A CONCISE HISTORY OF OSINT

The use of OSINT to inform military decision making emerged during WWII when the US government began amassing intelligence on their adversaries through fastidiously studying newspapers, magazines, radio broadcasts, photos and other media, in an attempt to discern enemy strategies and objectives.

This practice was referred to as Research and Analysis, and the department which carried out such operations formed a branch of the Office of Strategic Services (OSS) – later to be known as the CIA.

In the advent of the internet and the colossal rise of social media, OSINT took on a new meaning and nature. The sheer profusion of open data that became available for analysis transformed OSINT from a little-known reconnaissance method into a full-blown international industry spanning both public and private sectors.

CYBERSECURITY: A GLOBAL CONCERN

The figures surrounding cybercrime over the last decade make for a sobering read. The global cost of cybercrime has [doubled since 2015](#), from \$3 trillion to \$6 trillion, and is forecast to continue growing at 15% each year, to reach \$10.5 trillion by 2025. This represents [the greatest transfer of economic wealth in history](#), putting entire markets and industries at risk.

Not only is cybercrime the biggest and most intractable problem for all businesses worldwide today, it is also one of the foremost concerns facing mankind at large. In the World Economic Forum’s 2022 Global Risks Report, cybersecurity failure was listed as [one of the top-five global threats](#), alongside the coronavirus pandemic and climate change.

CYBERSECURITY: A GLOBAL CONCERN



COVID-19

[The coronavirus pandemic has triggered a surge in cybercrime](#), with lockdowns and other restrictions compelling organizations to employ cloud-based services to support remote workers. However, such systems have many more vulnerabilities than native infrastructures, and individuals are more fallible targets than organizations.



SOCIAL ENGINEERING

[With phishing accounting for 80% of security breaches](#), social engineering represents the most common, and fastest-growing of all cybercrime tactics. Phishing is particularly difficult to combat because it essentially taps into human error and can slip beneath the radar of the most thoroughgoing security system.



CRYPTOCURRENCY ADOPTION

The perceived anonymity provided by cryptocurrencies has led to a wave of fresh opportunities for cybercriminals. Using services such as crypto mixers, illicit assets and proceeds can be readily legitimized, opening new possibilities for fraud actors and operations across a number of sectors.



BREACH IGNORANCE

Once a data breach has occurred, every second that passes is expensive. However, companies take around [197 days to notice a breach, and a further 69 days to contain one](#). Leaks contained within 30 days will save an enterprise over \$1 million. Response time is crucial for mitigating costs.

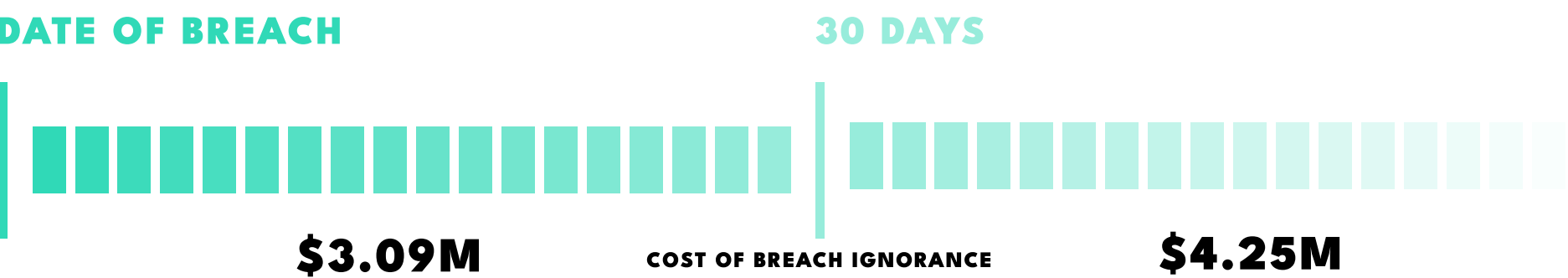
USES OF OSINT IN THE FIGHT
AGAINST CYBERCRIME

THREAT
INTELLIGENCE

OSINT methods and technologies are commonly used to identify breach surfaces, which could take a multitude of forms across open platforms. For instance, an employee’s social media account publishing adverts would be a clear indication of hacked credentials which could give the hackers access to a company’s critical assets by extension. Sweeps performed by open-source intelligence tools can quickly home in on an array of such vulnerabilities.

DATA
LEAK DETECTION

Even with the most throughgoing precautions, companies must prepare for potential breaches, since they are almost inevitable. Open data is a uniquely effective resource for finding evidence of a leak or security breach connected to the target. Indications of data leaks appear online, but are often buried in the general flood of open data. OSINT tools can continually monitor sources across the Surface, Deep, and Dark Web so that when a breach does occur, it is identified promptly. This can save companies millions of dollars.



DIGITAL
FOOTPRINTING

Quality cybersecurity assessments often hinge on OSINT methods of profiling and link analysis: by bringing together a subject’s interests, connections, affiliations, modes of interaction, a detailed picture of the subject emerges. Such pictures can map out a thorough description of a system’s vulnerabilities, cross-check data for reliability, and embody evidence.

INCIDENT
RESPONSE

IR is a procedure for ensuring that an organization can effectively respond to security breaches or cyberattacks as they arise. The process involves investigation, mitigation, and recovery from security breaches, as well as prevention against future incidents. By filtering open sources for the most up-to-date data iterations, OSINT solutions allow security breaches to be accurately understood, greatly facilitating the challenge of containment, and informing ever more effective preventative measures.

SOCIAL ENGINEERING
COUNTERMEASURES

Corporate security units often leverage open data to determine employee susceptibility to threat actors. By scanning employee accounts across social media and other services such as Outlook, Dropbox, etc., the subject’s activities can be checked for phishing content, and the employee can also be assessed for their capacity to deal with such threats.

BLOCKCHAIN
ANALYSIS

While there is a perceived anonymity to bitcoin and other cryptos, by using OSINT tools to explore blockchains intelligently, laundering systems can be unpacked, and transactions can be linked to other identifiers on the Surface Web, or even user crypto addresses themselves. Also, because malicious addresses tend to appear in scam reports, ongoing investigations, and social media discussions within the crypto community, OSINT tools can quickly flag up suspect crypto entities.

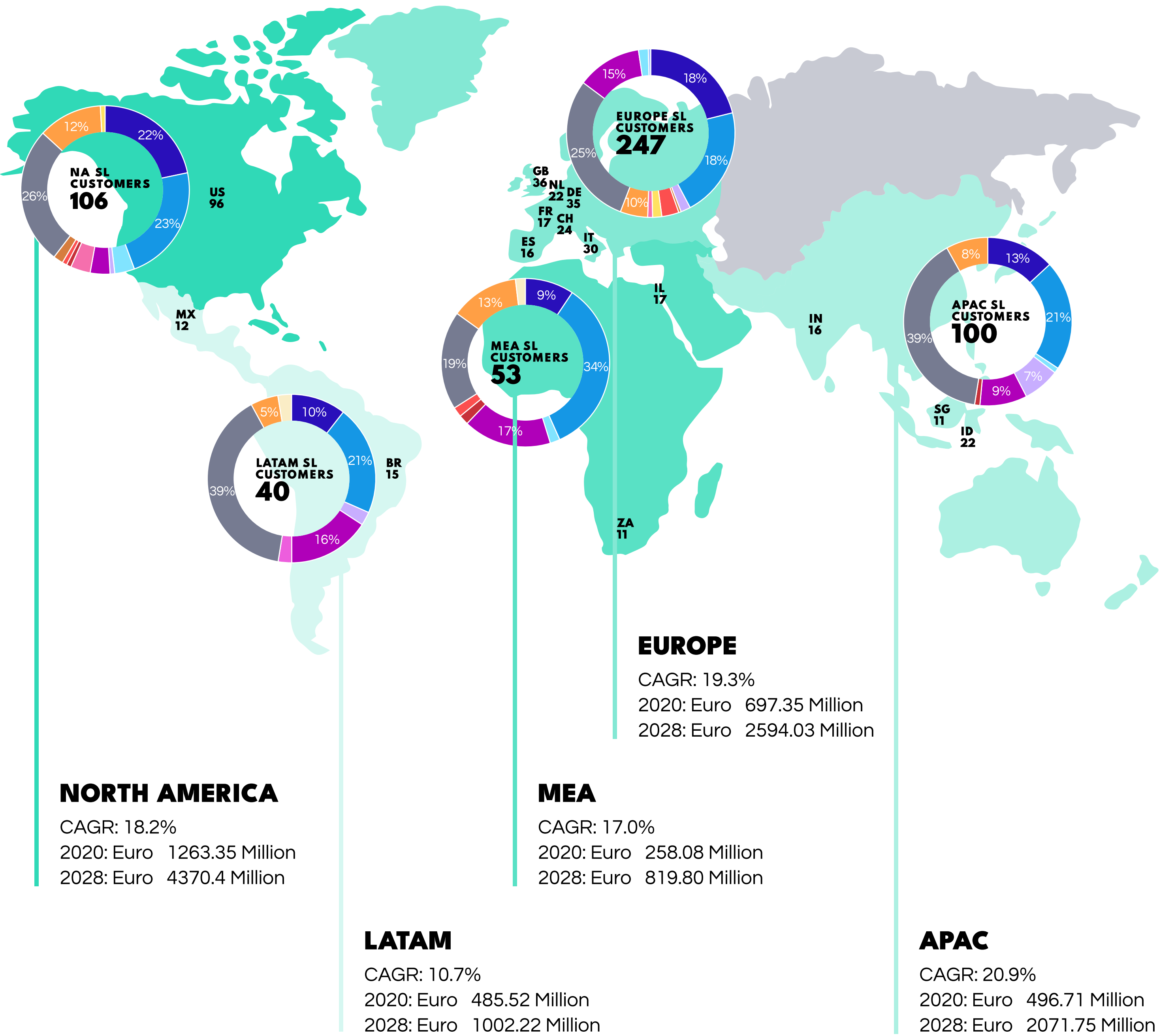
A SHIFTING LANDSCAPE

	CHALLENGES	SOLUTIONS
AMOUNT OF DATA	OSINT investigators have to scour huge volumes of data at demanding speeds. The gathering process is complex, involving the identification, collection, and organization of vast reams of information. This then needs to be thoroughly filtered and subtly analysed to deliver actionable intelligence. Furthermore, such processes must be fast enough to deal with the speeds of data generation, and decision making in the contemporary digital age.	IT companies and governmental departments have developed automated solutions specifically for these purposes. By gaining access to a wide array of powerful search functions, users have far greater control over the way information is extracted: relevant data can be zeroed in on, while superfluous material can be filtered away. This makes the gathering process, quicker, easier, and more focused, resulting in greater overall productivity.
DATA RELIABILITY	Open sources require thorough verification from a range of data points to be trusted. Since misinformation and propaganda is rife throughout the web, open data gatherers face a minefield of false or warped data that can mislead investigations.	OSINT technologies allow information to be cross-checked through the comparison of multiple sources. This process leads to a higher degree of verification or invalidation which in turn, indicates the degree of reliability for many types of information.
WORKFLOW SPEED AND QUALITY	People continually need to vet the output generated by OSINT to establish how reliable the retrieved data actually is. Such routine work consumes time and human resources, and often has a detrimental impact on a case’s progress. A major difficulty is that investigators suffer from research fatigue and make increasingly ineffective decisions. Furthermore, since open data is naturally diverse, making connections to ascertain accurate and current results can compound these pressures.	The ever broadening use and versatility of AI technologies such as machine learning and natural language processing can take care of many aspects of data retrieval, organization and processing. AI models can quickly sort diverse, nebulous data into coherent, workable material. This means investigators can devote more energy and headspace to the decision-making process, which results in faster data extraction, more sophisticated analysis, and ultimately refined, superior intelligence.
DATA RELEVANCE	Traditional databases used for criminal investigations are often outdated, particularly in the police service. Consequently, a lot of data employed in cases has either ceased to be of relevance, or is actually erroneous. This can significantly curb investigation processes and result accuracy.	In providing totally up-to-date data on people, events, and businesses, open sources can be essential to the efficacy of investigative techniques. By qualitatively enriching collected data, OSINT tools can provide a live, holistic picture of what is actually happening.

INDUSTRY POTENTIAL

As the necessity of OSINT techniques and tools has become ever more widespread and apparent, the field has seen an immense increase in investment. Huge commercial interest from Law Enforcement, Cybersecurity, and Corporate Security sectors have propelled the industry to its current, booming international status, which is only set to continue expanding.

The OSINT industry now comprises multi-million euro markets in all major regions of the globe – figures which are expected increase over the next decade to reach an estimated growth value of 17.9% by 2028.



* Note: The CAGR values in the figure have been estimated for the period of 2020-2028.
** Source: The Insight Partners Analysts

GROWTH DRIVERS

01

GLOBAL
DIGITIZATION AND
DATA TRADING

In IBM’s [2021 data breach report](#), the tech giant announced a rise in costs from USD 3.86 million to USD 4.24 million, a rate of expense which is only set to increase. The task of monitoring and countering data trading and leaks is a major challenge which OSINT tools can mitigate on a daily basis.

02

THE EXPLOSION
OF CYBERCRIME

The [2022 Global Risks Report](#) by the World Economic Forum highlighted cybersecurity failure as one of the top-five global threats, along with coronavirus and climate change. With cybercrime expanding at a rate of 15% from year to year and costs expected to hit [\\$10 trillion by 2025](#), OSINT tech is of paramount importance to keep these figures in check.

03

MIGRATION
TO THE CLOUD

Between 2020 and 2021 the internet population grew from [4.5 billion users to 5.2 billion](#). This exponential expansion, along with the movement of valuable investigation data from physical devices to servers, now means the place to be looking for leads and evidence is the online realms of social media and other platforms.

04

THE MATURITY
OF THE CRYPTO
MARKET

With a [\\$3 trillion market capital](#) and Compound Annual Growth Rate of more than 60% recorded in 2021, cryptocurrencies have proved to make up a thriving market. Combined with other factors such as the merging of cryptos with the orthodox financial market and commercial banking, as well as the popularization of cryptocurrency mixers as laundering tools, blockchains have become an indispensable resource for LEAs and investigation bureaus alike.

ABOUT SOCIAL LINKS

Since the company’s foundation in 2015, Social Links has been empowering LEAs, governmental bodies, businesses, and commercial enterprises to harness OSINT in accomplishing core objectives, saving vast resources, and making the modern digital world a safer place.

With many clients from among the S&P 500 as well as organizations operating at the highest levels of state, we have established ourselves as a key company within the OSINT industry and continue to develop products that operate at the forefront of a range of sectors including law enforcement, national security, cybersecurity, insurance, banking, due diligence, and more.

OUR PRODUCT LINE



A FULL-CYCLE^{MP} ^{DA} OSINT INVESTIGATION PLATFORM

beta



A suite of data extraction and analysis methods across social media, blockchains, messengers, and the Dark Web connected directly to your in-house platform via our API.



MALTEGO AND i2

OSINT Tool for conducting in-depth investigations across social media, blockchains, messengers, and the Dark Web in Maltego and i2 platforms.



An enterprise-grade on-premise OSINT platform with customization options, private data storage, and our widest range of search methods.

SOLUTIONS
YOU CAN TRUST

Companies from S&P500 and law enforcement agencies from 80+ countries rely on Social Links' solutions



ABOUT
SOCIAL LINKS

**FOUNDED IN
2015**

**500+
CLIENTS**

**HQ
THE UNITED STATES**

**80+
COUNTRIES**



BOOK A DEMO

Want to increase the speed and success rate of your investigation? Take the Social Links guided tour to see all the opportunities our OSINT tools have to offer.
Just scan the QR code

OSINT INDUSTRY
LEADER, 2023

