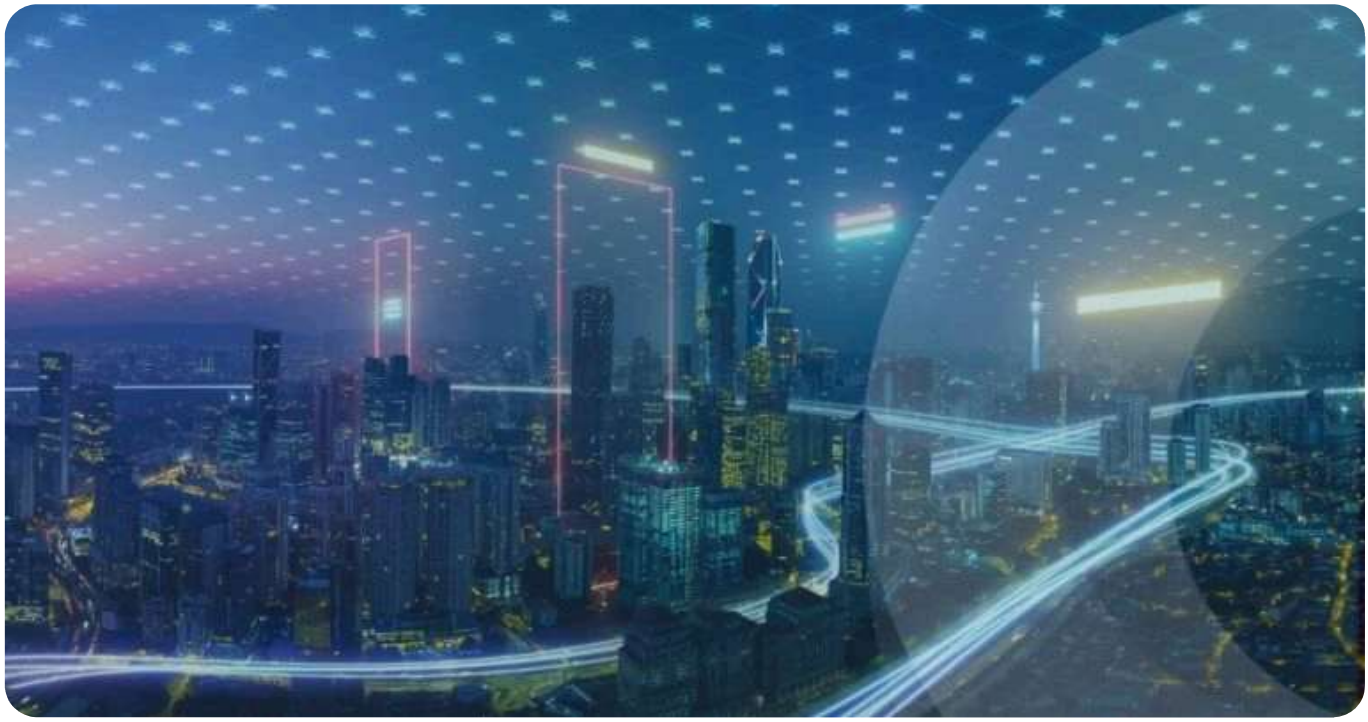
What is an OSINT investigation?

Written by Rebecca Lindley
Head of Marketing



Contents

Jump to section ▼

From countering serious and organised crime to fighting money-laundering, open source intelligence is an increasingly popular method of investigation for all kinds of crime.

OSINT is the targeted assessment of publicly available data to gain insights, drive decision-making, and mitigate risk.

By studying, cross-referencing, and analysing this information, OSINT researchers can find connections and insights that would have otherwise been impossible to identify. The sheer volume of data available in OSINT sources facilitates this potential for greater insight. However, scale is also the largest obstacle to conducting effective OSINT investigations: investigators do not have the time to sift through such huge data sets and make sense of them.

The difference between OSINT and OSD

OSINT and open source data (OSD) are often used interchangeably but they are fundamentally different concepts.

OSD is publicly available information that is drawn primarily from the internet through mediums such as social media sites, online news sources, and sanctions lists.

OSINT is the result of studying, analysing and acting on OSD. Anyone can access and gather OSD, but only those trained in investigation techniques can draw meaningful conclusions based on that information, which becomes OSINT.

History of OSINT

OSINT traces its origins to the creation of the Foreign Broadcast Monitoring Service (FBMS) in 1941, an agency responsible for the monitoring of foreign broadcasts[1]. Since then, law enforcement and government agencies have expanded this practice to counter terrorism, proliferation, espionage and organised crime rings.

Today, tools and techniques developed for military and government applications are moving into the private sector. OSINT is disrupting investigation best practices and creating better outcomes in many scenarios, including:

- Serious and Organised Crime
- Counter-Terrorism
- Anti-Financial Crime

- Due Diligence
- Fraud and corruption investigations
- Brand protection and illicit trade
- Insider threat identification

The OSINT market crossed $5 billion in 2022[2] and predictions state that it will reach nearly $12bn by 2026[3]. Organisations should ensure that they are equipped to use OSINT in order to future-proof their operations.

OSINT Sources

The scale and vastness of open source data is both its strength and weakness. Most OSD is available online, but much of it consists of unindexed data which cannot be obtained using standard search engines. Consequently, OSD has only become usable in a wider commercial context with the advent of modern open source intelligence tools.

In this section, we'll cover different OSINT sources, the challenges associated with each and key use cases.

Type 1: News Media

News media comprises mass media publications, broadcasts, radio, TV, content from media aggregators, books and other forms of print or traditional media. News media data is published in front of and behind paywalls, on international, national, regional and local scales. Even local news offers important insights, often providing a rich account of events that might not be available in wider-scale media.

Challenges posed to investigators

With millions of pieces of content published each day in numerous languages, the news and media are in a state of constant movement. Cutting through the noise to distinguish relevant and reliable news from 'fake news' is key. To do so, investigators must understand the origins of these sources.

There are key questions to ask when assessing the reliability of news media in an OSINT investigation:

- Is there reason to believe that the source is biased in any way? For example, is it backed by a political party or a state-controlled media outlet?
- Does it have a long and reputable track record as an established publication?
- Can the source's findings be found elsewhere? Could these other sources be more reliable?

Additionally, navigating thousands of news sources using conventional search techniques and manual data handling is immensely time-consuming. As news content is often repurposed across multiple networks, deduplicating content can eat into efficiency without the assistance of purpose-built OSINT tools (https://blackdotsolutions.com/blog/best-osint-tools/).

Suggested reading: Our blog How reliable is Open Source Intelligence? (https://blackdotsolutions.com/blog/how-reliable-is-open-source-intelligence/#:~:text=The%20concern%20that%20OSINT%20is,be%20considered%20alongside%20other%20records) goes more in-depth on why OSINT sources are legitimate value-adds to investigations.

Type 2: Grey Literature

Grey literature includes publicly available non-media private and public sector information. This includes documents from charities, NGOs, inter-governmental institutions and think tanks, as well as crime statistics, census data (e.g. from the ONS) and information contained in academic databases, journals and reports.

Grey literature also includes corporate registry data, annual business reports, filing data, and leaked reports. Examples of this include data leaks compiled by reputable organisations, such as the Organized Crime and Corruption Reporting Project (OCCRP) or the International Consortium of Investigative Journalists (ICIJ). These OSINT sources are densely populated with well-researched data that is often unstructured and hard to quantify.

Challenges posed to investigators

A key challenge is that this information commonly sits behind a paywall or requires login details to gain access. For example, some 42% of global health research is currently published behind paywalls[4]. Grey literature largely exists in what is known as the deep web — a part of the internet that is not discoverable on standard search engine results pages.

The storage and distribution systems behind grey literature are also notoriously disparate and poorly structured. This further complicates the process of locating and connecting related data points between different sources.

Many OSINT solutions offer advanced browser capabilities, allowing investigators to extend their search into results that are non-discoverable using standard web browsers. Visualisation tools can also help investigators understand the data collected from these sources.

Suggested watch: For a thorough explanation of how to use corporate records in an OSINT investigation, watch our webinar on How To Use Corporate Records to Fight Financial Crime. (https://blackdotsolutions.com/events/corporate-records-financial-crime-2/)

Type 3: Social Media

Social media can be long-form content such as Reddit or blog posts, or shorter content like Tweets or Instagram captions. Photographs, tags, and both first and second-degree connections are also a valuable part of intelligence drawn from social media.

A rich repository of data for OSINT investigators, social media can facilitate understanding of networks and the chronology of events. Visual data like images and videos can help to identify a subject or reveal new connections.

Note: Some social media data is public and other social media data is not. It's important to point out that only publicly available social media is OSINT.

Challenges posed to investigators

Over half the world's population now uses some form of social media. Its immense depth and volume make manual exploration exceptionally laborious. Much of the most useful social media information is unindexed, so standard surface web browsers are not useful. Furthermore, preserving anonymity is crucial for any social media investigator. Investigations must not trigger any signals that might alert the subject to an ongoing investigation.

Fortunately, specialist OSINT tools help investigators to analyse this data and highlight connections, securely and at speed.

Type 4: Dark Web

The dark web is part of the internet that is intentionally hidden and requires specialised software to access, such as the Tor browser. On the dark web, users and operators are untraceable. As a result, it is a rich source of data relating to criminal networks, their activities and connections. Usernames, email addresses, phone numbers and other identifiers can be cross-referenced with surface or deep web information to understand criminals' real-world identities.

Challenges posed to investigators

The dark web is a unique data source that is unindexed by standard search engines. Investigators must exercise great care to avoid malware or exposure to distressing images. Collecting relevant information from the dark web safely generally requires specialist OSINT tools and techniques that reduce these risks.

How can OSINT be used in practice?

OSINT is already paving the way for the future of investigative practices in a wide range of industries. It enables organisations to gain a fuller understanding of risk factors, threat actors and even consumer behaviours.

Government and law enforcement

OSINT has been a crucial tool for government and law enforcement investigations for many years. As OSD grows, OSINT practices will become even more integral to investigation competence and success. Key government use cases include:

- **Counter-terrorism:** Understanding terrorist networks to identify potential targets and risks where speed is of the essence.
- **Serious and organised crime:** Identifying and tracking down entities belonging to larger criminal networks.
- **Economic crime:** Understanding the people and companies behind global money laundering and fraud networks.

Suggested reading: To understand more about how OSINT can be applied to the law enforcement sector, see here (https://blackdotsolutions.com/industries/government/).

Financial services

OSINT has powerful implications for AML and AFC investigations (https://blackdotsolutions.com/industries/banking/). By cross-checking OSD with internal data such as transaction records, financial institutions can gain insights that might have otherwise gone unnoticed.

There are two critical factors behind the adoption of OSINT in financial services:

- **Doing what matters:** Financial institutions have a responsibility to prevent financial crime, which often supports other crimes such as terrorism or human trafficking. By taking an intelligence-led approach to AFC, it's possible to identify criminals and networks behind these crimes more proactively.
- **Getting ahead of future compliance trends:** OSD is available to everyone. As OSINT becomes a standard practice within the industry, regulators are likely to look poorly at financial institutions which do not use this readily available information to avoid facilitating crime.

As more financial institutions are fined for failure to prevent financial crime, access to good intelligence drawn from a diverse range of data is crucial to ensure better identification of risk.

Corporate

As the complexity of global supply chains grows and new threats to businesses emerge, companies need to investigate every avenue of risk without impacting day-to-day operations.

OSINT is poised to bring a range of benefits to the corporate world (https://blackdotsolutions.com/industries/corporate/):

- **Due diligence:** Creating an in-depth profile of new hires and supply chains is essential to mitigate risks of corruption, accidental involvement in crime and reputational damage.
- **Brand protection:** Identifying unauthorised sellers and the networks behind counterfeiters is vital to preserving brand credibility.
- **Security:** Mapping and collecting information on threats can inform mitigation measures.
- **Insider threat identification:** Tracing the social networks of malicious entities to uncover connections between employees and bad actors can prevent damage to businesses.

What is needed to make OSINT effective?

While OSINT allows organisations to harness the power of data to solve problems, poorly executed OSINT techniques can create new challenges.

The volumes of OSD available mean that organisations risk drowning in information and failing to extract insight from it. Online data analysis also risks exposing an investigation.

To overcome these OSINT challenges and ensure efficiency, organisations using OSINT would benefit from:

- **Automation of manual processes:** AI and intelligent automation should be used to present investigators with relevant core pieces of information so that they can make an informed decision quickly. This is important to keep OSINT investigations targeted, ethical and effective.
- **Reporting and visualisations:** The ability to output findings into clear graphs and visualisations is key to helping stakeholders understand the results of investigations.
- **Secure browsing:** Investigators must be able to remain anonymous as they study OSD, so that they can protect themselves and not accidentally tip off the entities that they are investigating.

These considerations are essential in conducting effective OSINT investigations; without them, investigation teams are left overwhelmed with data that they cannot process.

Illuminate risk in OSINT with Videris

Organisations need a developed understanding of modern risk landscapes to thrive. Just looking at online data is not enough.

Identifying the right data, collating it and drawing actionable insights from it is critical to achieving true OSINT. But to do this effectively, investigators from all backgrounds must use technology.

At Blackdot, we built Videris (https://blackdotsolutions.com/videris/) to elevate the way professional investigators use OSD. To help investigators unlock the power of Open Source Intelligence, Videris offers key features, including:

- **Federated Search:** Optimise your search for investigators, not consumers. Search across the live internet and curated databases simultaneously, avoiding search engine bias and security risks, so you can find the most relevant information to your investigation with ease.
- **Illuminate Risk:** From integrated databases of sanctions, PEPs and criminals, to value-add analytics that highlight risks in unstructured internet data, Videris is designed to ensure that no risk is missed.
- **Network Analysis:** Finding connections is essential to many investigations – with Videris, they're easier to identify. Automated visualisation tools give an intuitive understanding of networks, while advanced connection analysis automatically flags hidden links between people, companies and more.
- **Single Platform for Disparate Data:** It's easier to gain a full picture and maximise effectiveness when disparate data is presented together. Videris acts as a single platform for all the OSINT sources you need: live internet search engines, corporate records, social media, PEPs and sanctions data, leaks data, dark web and more.

FAQs

What is OSINT?

Open Source Intelligence (OSINT (https://blackdotsolutions.com/blog/what-is-osint/)) is the product of collecting, processing and analysing open source data. Oragnisations can then use it to drive decision-making.

What is the difference between open source data and open source intelligence?

– Open source data (OSD) is the raw and unfiltered publicly available information and data.
– Open source intelligence (OSINT) is extracting meaningful insights from OSD.

What are the different types of open source data?

– News and media
– Grey literature, including corporate records
– Social media
– Dark web data

What are the challenges of using open source data?

– Finding the right information amongst constantly changing content and growing volumes of data.
– Keeping track of findings when collecting information from multiple data sources
– Accessing the right data: Information can sit behind a paywall or requires login details for access. Also, you can't access deep and dark web data using standard search engines.
– Understanding the data: much of the data in OSINT investigations is unstructured, which can make it difficult to interpret or spot patterns

How do I choose the right OSINT tool for the data I'm using?

1. Explore (https://blackdotsolutions.com/the-osint-handbook/) and understand what's available to you. There are multiple OSINT tools (https://blackdotsolutions.com/blog/best-osint-tools/) to choose from depending on your requirements.
2. Book a demo (https://blackdotsolutions.com/book-a-demo/). Get a feel for the technology and how it could benefit you in the long term.
3. Have a discussion. After your demo, we can answer any questions you have about the software and how your organisation could benefit.

Footnotes

1. https://en.wikipedia.org/wiki/Open-source_intelligence#History (https://en.wikipedia.org/wiki/Open-source_intelligence#History)
2. https://www.gminsights.com/industry-analysis/open-source-intelligence-osint-market (https://www.gminsights.com/industry-analysis/open-source-intelligence-osint-market)
3. https://www.globenewswire.com/news-release/2021/02/08/2171407/0/en/Open-Source-Intelligence-OSINT-Market-Is-Expected-To-Reach-USD-11-86-Billion-By-2026-Registering-A-CAGR-Of-17-4-Global-OSINT-Market-to-Expand-its-Reach-by-Uncovering-Hidden-Pattern.html (https://www.globenewswire.com/news-release/2021/02/08/2171407/0/en/Open-Source-Intelligence-OSINT-Market-Is-Expected-To-Reach-USD-11-86-Billion-By-2026-Registering-A-CAGR-Of-17-4-Global-OSINT-Market-to-Expand-its-Reach-by-Uncovering-Hidden-Pattern.html)

Other articles you maybe interested in

(https://blackdotsolutions.com/blog/osint-and-stopping-illicit-financial-flows/)

OSINT and Stopping Illicit Financial Flows (https://blackdotsolutions.com/blog/osint-and-stopping-illicit-financial-flows/)

Illicit Financial Flows support criminal activities and have a major impact on economic stability globally. Identifyin...

Read More (https://blackdotsolutions.com/blog/osint-and-stopping-illicit-financial-flows/)

(https://blackdotsolutions.com/blog/why-osint-should-be-a-hot-topic-at-the-economic-crime-congress/)

Why OSINT should be a hot topic at the Economic Crime Congress (https://blackdotsolutions.com/blog/why-osint-should-be-a-hot-topic-at-the-economic-crime-congress/)

In December, we'll be joining hundreds of delegates from financial institutions and government agencies at the UK...

Read More (https://blackdotsolutions.com/blog/why-osint-should-be-a-hot-topic-at-the-economic-crime-congress/)

solutions

Accreditations

Get the latest news and insights sent straight to your inbox

eva.lao@ust.hk

Blackdot Solutions needs the contact information you provide to us to contact you about our products and services. You may unsubscribe from these communications at any time. For information on how to unsubscribe, as well as our privacy practices and commitment to protecting your privacy, please review our Privacy Policy.

Subscribe

Product

Solutions

Industries

Resources

Company

The Blackdot Story (https://blackdotsolutions.com/about-us/)

How it Works (https://blackdotsolutions.com/how-it-works/)

We're Hiring! (/careers/)

Contact

Contact Us (https://blackdotsolutions.com/contact-us/)

Help & Support (https://blackdotsolutionsltd.zendesk.com/)

01223 900424 (tel:01223900424)

(https://www.linkedin.com/company/blackdot-solutions-ltd/)