blackdot solutions

# Open Source Investigation Best Practices in 2024

Written by Blackdot Solutions

## Contents

Open source intelligence (OSINT) was developed as a military intelligence discipline in order to identify and understand threats using publicly available information. As the scope and value of open source data has continued to expand, these investigatory practices have migrated to the private sector. Intelligence-led strategies are changing best practices for a range of outcomes, including —

- Anti-money laundering and anti-financial crime
- Insider threat identification
- Illicit trade investigations
- Fraud
- Due diligence

Effective open source investigation requires case-by-case implementation to ensure good outcomes. However, there are a number of universal open source investigation best practices that can help experienced and novice OSINT practitioners benchmark their own process and find ways to improve.

At Blackdot (https://blackdotsolutions.com/), we've been driving investigatory best practices within a government context since 2015. Our OSINT solution Videris (https://blackdotsolutions.com/videris/) simplifies investigations, increasing impact and insight in government applications and helping bring OSINT best practices into the private sector. Here, we're going to explain how we approach OSINT so you can apply these principles in the context of your own investigations and intelligence operation.

# 1. Understand the difference between data and intelligence

OSINT is defined by an intelligence-led approach to investigations. Collecting open source data doesn't actually mean that you are engaging in OSINT. When asking "what is OSINT? (https://blackdotsolutions.com/blog/what-is-osint/)", there is a significant differentiation that you need to keep in mind, and that is a distinction between —

1. **Open source data (OSD):** The raw and unfiltered publicly available information and data.
2. **Open source intelligence (OSINT):** extracting meaningful insights from OSD.

OSINT is not about the mass collection of data. It's about the targeted collection of specific data and the application of processes and technology to further refine your search and focus *only* on the relevant information. Understanding this differentiation makes it possible to drive efficient and effective open source investigations.

## Strategies to help turn OSD into OSINT

Raw data needs to be targeted at individual investigatory requirements to provide useful insight. This controlled approach is essential for ethical data handling and it also ensures decisions are based only on relevant information. This is key to preventing the sheer volume of publicly available information from overwhelming your investigations, and ensuring that comprehensive insights are obtained and can drive valuable outcomes.

To a large extent, using the right OSINT solution is critical to making the targeted collection of OSD possible, and to implementing the OSD/OSINT distinction on an enterprise scale.

## 2. Choose the right tools

The easy availability of open source data makes it a valuable resource, but it's also the biggest challenge when it comes to turning this data into intelligence. The volume and spread of data makes it hard to filter and focus on the right thing at the right time. It's also important to note that the internet has been, broadly speaking, designed for advertisers, not investigators. You see what search engines want you to see, not necessarily what's the most relevant data for your investigation. This adds to the challenge of breaking down data silos and making sure that you are able to focus on the most relevant information.

The best OSINT tools (https://blackdotsolutions.com/blog/best-osint-tools/) are designed to help you overcome the challenges of siloed, irrelevant and large data volumes. This is done through a combination of targeted data collection and collation, intelligent automation and network visualisations and analysis.

At Blackdot (https://blackdotsolutions.com/), we've built Videris around the principles of intelligent automation (IA). As opposed to AI (artificial intelligence), IA leaves decision-making in the hands of humans, but augments that process by automating the way that data is collected, analysed and presented to decision-makers. This enables users to stay in control while still engaging in efficient workflows, so they can overcome the sizeable and disparate nature of open source data.



## Strategies to help

To find the right OSINT solution, investigators first need to understand what's available. The oversight and investigatory value offered by Videris is a fantastic example of an advanced all-in-one OSINT platform. Designed for use across industries, this platform provides a range of value-led benefits through features that include —

- **Single-source-of-truth:** Search simultaneously across data landscapes by centralising access to all of your resources.
- **Visualisation:** Automatically generate charts of connected data, such as corporate records, to simplify the review of vital connections.
- **Social media network tools:** Incorporate social media data in your investigations to securely identify key insights and links.*
- **Cross-matching capabilities:** Automatically cross-reference all of your data and be directed to connections that matter.
- **Anonymisation:** It's important to not tip off the subjects of your investigation. We've deployed precautions to ensure your identity remains secure.

These features make it easier to collect, connect, and oversee open source intelligence. An IA focus ensures that this intelligence augments human-led decisions, rather than replacing them, providing the accuracy and transparency that modern investigations rely on. Fundamentally, these are all outcomes that you need to make

effective open source investigations (https://mediasonar.com/2020/08/06/osint-techniques-security-poi/) possible.

## 3. Anonymity is paramount

A central goal of OSINT is to identify and mitigate risk, but it's possible that your investigation will generate risks rather than removing them. In many investigations, the main risk is exposing your identity or accidentally informing an individual that they are under investigation by leaving a digital footprint.

Exposure is especially problematic in investigations where the ability to map and track illicit activity over extended periods relies on anonymity. Under these circumstances, accidentally tipping off individuals under suspicion can compromise the investigation. Further, in certain jurisdictions – such as the UK – "tipping off" the subject in a money laundering investigation is a criminal offence (the maximum penalty being an unlimited fine and up to 5 years in prison). You also need to consider how information is stored and accessed in order to ensure that you don't run afoul of any insider threats – or data protection regulations.

### Strategies to help

Your ability to remain anonymous, secure and compliant can depend upon the OSINT solution you select. As we've already addressed, enabling the investigator to easily ensure anonymity is a central feature of quality OSINT software. It's critical that measures are taken to remove the risk of notifying individuals of an investigation.

In addition to making careful technology choices, you should consider best practices including —

1. **Secure ecosystems:** Compromised internal systems put even well-implemented open source investigations at risk. Overcoming this relies on securing investigations internally through protective measures and good investigation oversight.
2. **Effective cyber threat identification:** Identifying possible cyber threats ensures that companies can better protect their networks and clients. Full knowledge of these risks makes it possible to approach them in an informed, proactive manner.

Together, these steps provide the comprehensive security and oversight that sensitive investigations rely on.

## 4. Be effective and ethical

OSINT relies on publicly accessible data, but that doesn't mean you should collect and store information without consideration. Indiscriminate data hoarding is not only likely breaching GDPR legislation, it also compromises the efficiency and ethics of investigations significantly. In fact, effective and ethical practice, consistent with GDPR, should be viewed as definitive characteristics of OSINT when considered in contrast to mass data collection practices.

The effectiveness of open source investigation rests on a company's ability to tailor their data collation and handling towards specific objectives. This targeted approach ensures simplified investigatory practices that never handle more data than necessary. It not only improves the efficiency of your process, but makes it more ethical and minimises your exposure to risk. Enhanced ability to comply with GDPR is a further benefit.

Another way to make OSINT investigations more ethical is by ensuring that decisions are human-led. The intricacies of OSINT rely on dedicated teams who understand the nature of these investigations and are well-equipped to make sense of the data they identify. If this is left in the hands of technology alone there is a risk of unfair decisions being made because – however advanced – technology can not replace the nuanced human judgement that is required in these situations.

### Strategies to help

Processes like intelligent automation are especially useful here: they can quickly provide the detailed insight needed to take investigations further with less data, but also rely on human-led decisions. This enables businesses to keep investigations moving while avoiding ethical compromises.

IA-led solutions like Videris play a key role in this. Paired with the oversight of a dedicated OSINT team, this ensures that even sensitive investigations don't gather data unnecessarily or make unfair decisions, avoiding leaving compliance, or reputation, at risk.

## 5. Make sure to record your activities

Another challenge when working with open source data is its changeable nature. Because OSINT is reliant on publicly available data that is largely not controlled or subject to any oversight, it can easily be altered or removed from the internet. This is frustrating for investigators, who can find that key evidence has disappeared when they come to present their findings to management or law enforcement – thus undermining their case.

### Strategies to help

In order to ensure that their evidence is secure, investigators need to keep track of all of their OSINT sources (https://blackdotsolutions.com/blog/osint-sources/), including screenshots and timestamps of important findings. They also need to log all of their activities so that it's possible to check that an investigation was carried out thoroughly. However, capturing sourcing and logging activity is time-consuming and distracts from the investigator's primary role.

Again, technology can help here: some OSINT solutions automatically capture evidence and log all activity, so the investigator can concentrate on their investigation.

## Effective open source investigations rely on human insight and technology

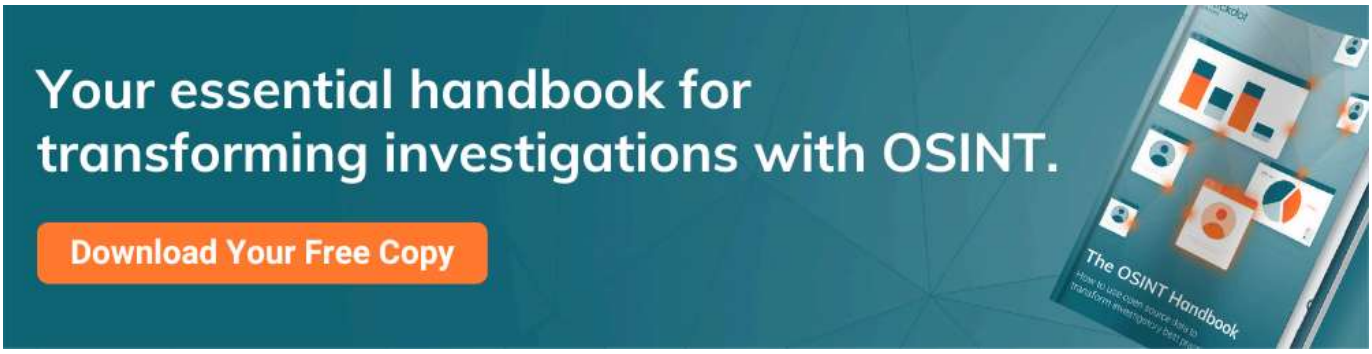
The importance of OSINT specialists in many industries is increasing as the technique becomes more prominent. For example, in the anti-financial crime world, Financial Intelligence Units (https://blackdotsolutions.com/blog/how-financial-intelligence-units-can-unlock-the-power-of-osint/) (FIUs) and other financial investigations teams are increasingly hiring OSINT experts to introduce techniques and processes aimed at improving the institutions' anti-financial crime outcomes.

Failure to implement OSINT best practices therefore not only compromises your organisation's ability to compete, but also raises questions about why obvious threats were left unaddressed. Proactivity is important, and we expect to see new OSINT compliance requirements in a number of industries.

An environment and technology that facilitates collaboration will allow investigators to achieve results through the use of —

- Seamless integrations between different tools used within an organisation
- Cross-referencing of sources across your investigation
- Simplified communication using visualisation capabilities
- Easy data sharing across locations/IP addresses

IA-led OSINT capabilities are critical for augmenting the ability of OSINT professionals, while simultaneously enabling those professionals to stay focused on what matters. Videris brings both of these benefits within easy reach through a platform that enhances human input with IA, driving simplified, effective investigations. If you want to learn more, get in touch and book a demo of Videris today (https://blackdotsolutions.com/book-a-demo/).




(https://cta-redirect.hubspot.com/cta/redirect/8095066/b07b6e60-9d52-46d7-ae26-366c5340823a?__hstc=209965706.09da2c612d4342d37dd8a08938fe3aaa.1734512871675.1734512871675.1734512871675.1&__hssc=209965706.1.1734512871675&__hsfp=3451109932)

## FAQs

**What are the best practices for open source investigations?**

– Understand the difference between data and intelligence
– Choose the right tools
– Anonymity is paramount
– Be effective and ethical
– Make sure to record your activities

Find out more about the strategies you can use to apply these open source investigation best practices (https://blackdotsolutions.com/blog/open-source-investigation-best-practices/) in our blog.

**What is the difference between using data and intelligence in open source investigations?**

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

**How does Videris simplify my open source investigations?**

Videris charts allow you to significantly decrease clutter and noise, map connected data points and manage your investigation effectively, ensuring a steady and seamless workflow. To gain more insight and see this in action, book a demo (https://blackdotsolutions.com/book-a-demo/) with Videris.

## 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. Identifying...

**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 Finance...

**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

Work Email*

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/)