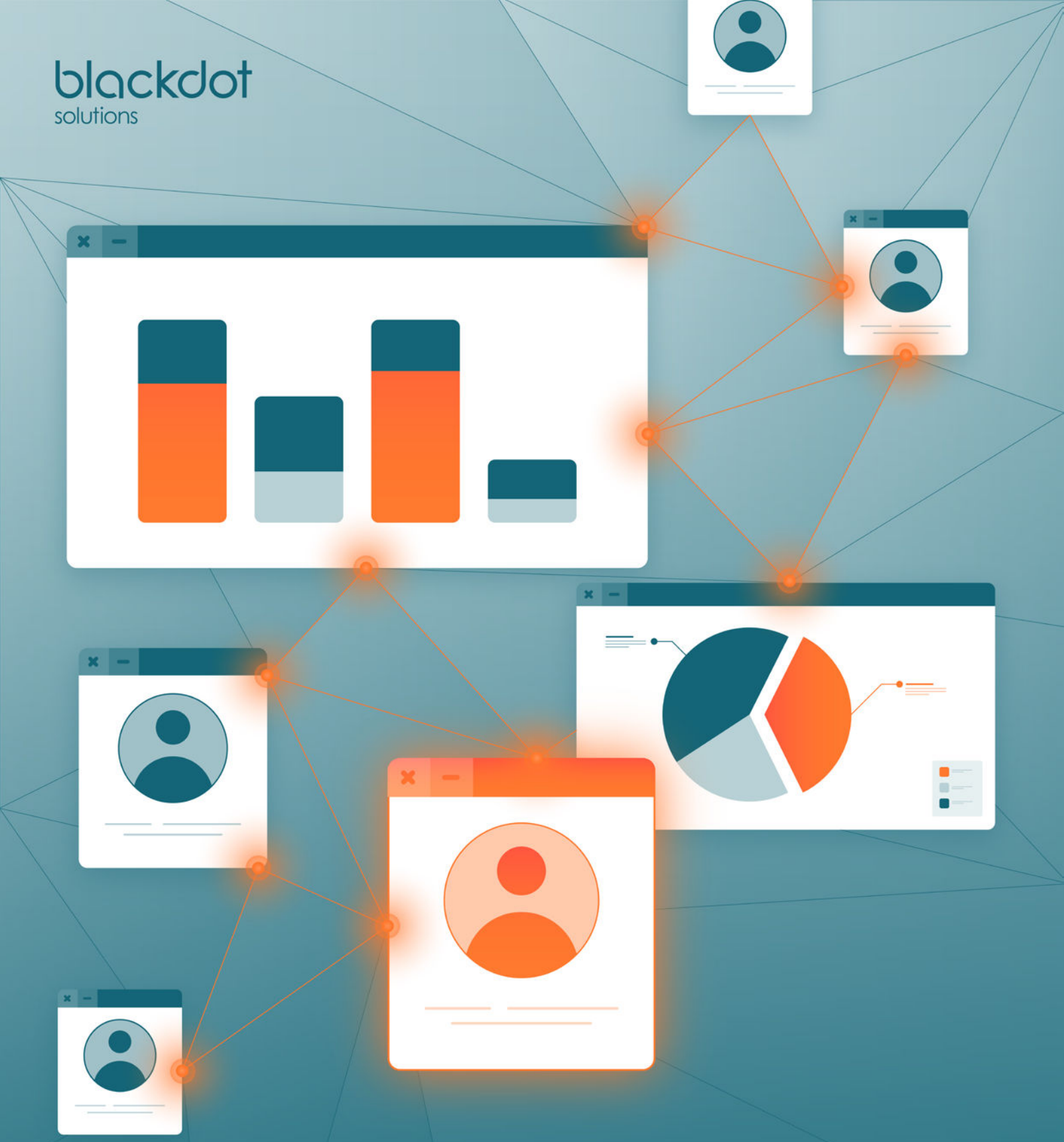
blackdot
solutions



The OSINT Handbook

How to use open source data to transform investigatory best practice

Data has come to define the modern world. It enables more accurate decision-making and deeper investigations. However, the sheer volume of data that exists can confuse and overwhelm analysis. Dependable and secure solutions are required to overcome issues associated with the variable reliability of sources, and the disaggregated and siloed way in which data must often be accessed. Using data to drive decision-making is a central challenge *and* opportunity for businesses and governments alike.

Some data is privately protected, but a large percentage of data is publicly available. Public data (or "open source" data) is there for anyone to use, but it can be difficult to identify the relevant information at the right time. OSINT (Open Source Intelligence) is the application of intelligence-led processes to transform OSD (Open Source Data) into actionable insights.

OSINT is a military intelligence term, and remains a staple technique in counter-terrorism, counter-intelligence and organised crime investigations. However, the potential and wide-reaching nature of OSINT has driven an expansion out of military and government applications into the private sector.

The OSINT market is expected to reach nearly $12bn (£8.5bn) by 2026, registering a CAGR of 17.4%.[1] With an increased focus on intelligence-led data analysis (aligned with Big Data trends more generally), OSINT is transforming investigatory best practice and creating far more robust outcomes across other use cases and industries, including —

1. Fraud investigations
2. Brand protection
3. Insider threat identification
4. Illicit trade investigations
5. Due diligence

Furthermore, we expect to see OSINT become an increasingly important part of compliance, particularly in financial services. As a result, leveraging the potential of open source data is a critical investment in the future.

> [1]Global OSINT Market to Expand its Reach by Uncovering Hidden Patterns

What's in this handbook?

At Blackdot Solutions, we've pioneered open source intelligence software within a government context, and are now helping to bring OSINT into the mainstream with our investigations platform, Videris.

We've curated this handbook to help you build an OSINT framework that leverages technology and process best practices in order to enhance your investigative and decision-making capabilities. Fundamentally, our goal is to empower you to adopt an intelligence-led approach to data analysis and investigations.

Defining OSINT and OSD

Open source data and OSINT are often used interchangeably. Before proceeding any further, it's important to understand the difference between the two terms and establish their relationship to one another.

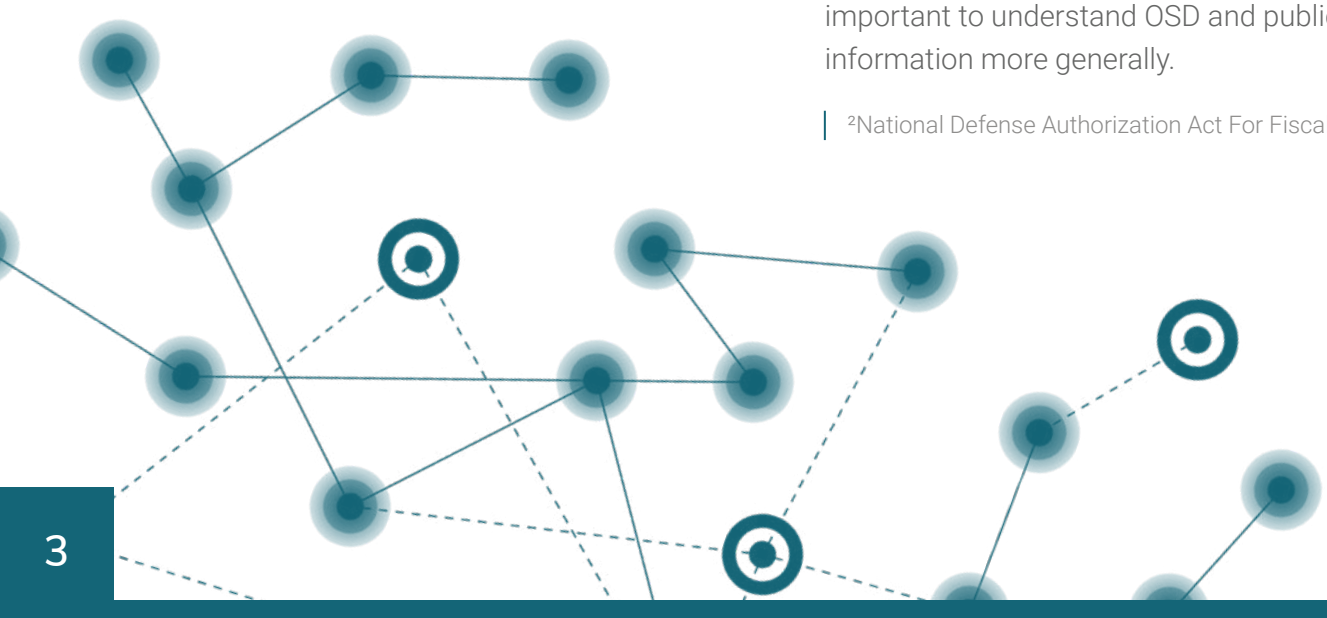
The US Department of Defense defines OSINT as *"intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."*

So, to be clear —

- **Open source data (OSD):** Data from a wide range of publicly available sources.
- **Open source intelligence (OSINT):** Information that has been deliberately extracted from OSD to answer specific questions, achieve specific objectives and drive informed decision-making processes.

OSD is the rough diamond. OSINT is the finished product that has been cut, polished, and worked into an ornate piece of jewellery. As a result, in order to appreciate the potential value of OSINT, it's important to understand OSD and publicly available information more generally.

[2]National Defense Authorization Act For Fiscal Year 2006



What data is open source?

As highlighted above, "open source" refers to data that is readily available for public consumption. Rather than coming from a single location, OSD can be taken from a range of sources for use in OSINT investigations. Let's take a look at some of the places open source data can emerge from in detail.

News media content

Content produced, published or broadcast — including online — for general public consumption in multiple media formats such as journals, newspapers, radio and television. This also includes media aggregators that do not necessarily publish original content.

Grey literature

This refers to materials and information from non-media organisations and institutions.
This includes —

- Academic institutions, think tanks and research institutions — for example, academic papers.
- Government agencies — includes information that can be accessed on request, such as census data.
- Businesses and corporations — this would include annual reports and company filings.
- Intergovernmental organisations — reports from organisations like the United Nations and World Health Organization (WHO).
- Charities and Non-governmental organisations (NGOs).

Social media

Where publicly available, this includes information in both long-form, e.g. blogs and sources such as Reddit, and short-form, e.g. posts on Facebook, Twitter, and LinkedIn.

Dark web

The dark web is a treasure trove of data often linked to criminal activity. It can contain data such as usernames, email addresses and phone numbers of individuals connected to crimes.

More sources and more possibilities

In the past, open source material was mostly limited to printed media, such as books, articles and public records, that could only be viewed at specific places and times. Online data provides on-demand access to published material, as well as self-published blogs and social media posts. There is also now a whole range of visual and auditory media that did not exist prior to the development of smartphones and mobile technology.

While providing professional researchers and investigators with larger volumes of potentially useful information, the rapidly expanding nature of OSD also threatens to overwhelm. Therefore, applying rigour to the way in which OSD is collated, analysed and used is now more important than ever. In many ways, the Information Age is also proving to be the Age of OSINT.

Benefits of OSINT

OSINT has been widely utilised across government and military applications since as early as the Second World War, supporting investigations into global issues, including counter-terrorism and counter-proliferation.

As many former government investigators enter the private sector, OSINT's popularity in industries such as financial services has steadily increased. Many organisations now consider OSINT a key part of investigative best practice, thanks to the range of benefits it offers.

Benefit 1: Expanded insight

An investigator's ability to extract meaningful insights is dependent on the information at their disposal. The inclusion of open source data alongside internal and other data sources gives investigators the context they need to make comprehensive decisions.

Financial services use case

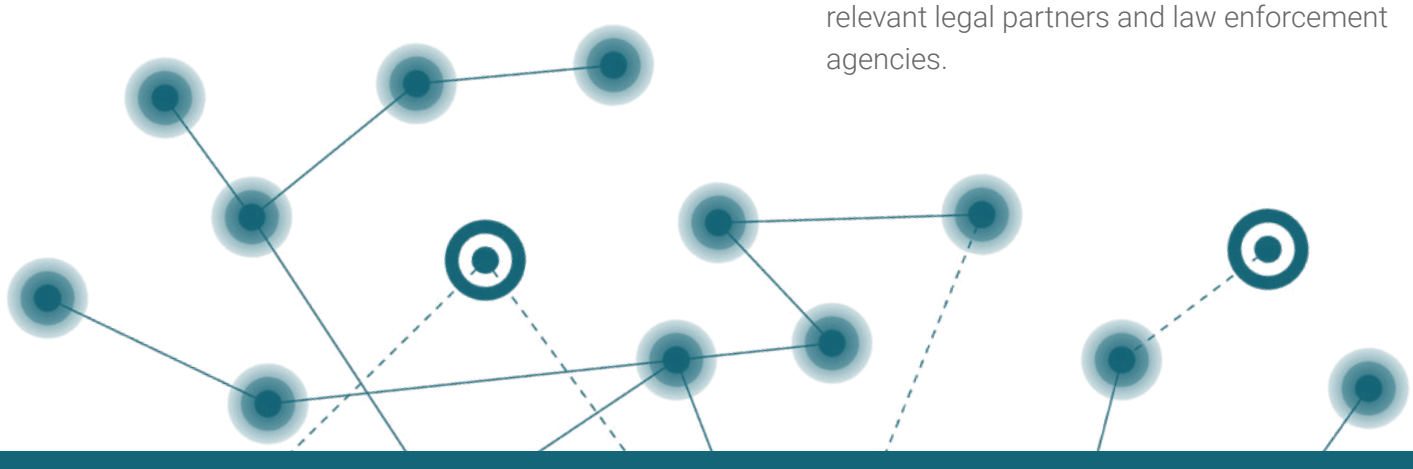
Effective regulatory compliance processes such as anti-money laundering (AML) and know your customer (KYC) rely on an in-depth understanding of clients and counterparties, risk actors and threats. By using OSINT, financial institutions can extend their investigations outside of siloed commercial databases and internal systems for a more expansive and proactive understanding of illicit behaviours, connections, and risks.

For example, correspondent banking transactions present a specific challenge to due diligence processes, given the lack of information available to the correspondent bank. Good governance and due diligence on behalf of respondent banks are obviously critical. Moreover, OSINT provides one of only a few direct ways for correspondent banks to undertake AFC and AML checks in this context.

Corporate use case

Proactive investigations into potential avenues of risk are important for businesses to protect themselves against a range of complex threats that have the potential to inflict serious financial and reputational damage. Examples where OSINT plays a particularly important role include —

- **Due diligence:** Globally active corporations face an array of risks against which they need to screen clients, suppliers, franchise partners, acquisition targets and other "third parties". OSINT can fill the gaps left by traditional solutions that may not provide a full picture regarding sanctions, corruption and bribery, human rights, and ESG (Environmental, Social and Governance) risks.
- **Fraud, brand protection and illicit trade:** Large enterprises, especially in the retail and FMCG (Fast Moving Consumer Goods) space, face significant losses due to a wide variety of increasingly complex fraud schemes, as well as from organised crime groups that are flooding markets with counterfeit goods. The chances of preventing, detecting and disrupting these activities can be greatly strengthened by proactively investigating individuals and groups, and then providing high-quality intelligence to relevant legal partners and law enforcement agencies.



Benefit 2: Improved accuracy

The huge amount of data available in open sources has the potential to provide numerous additional insights, but these are hard to access without processes that turn data into intelligence. OSINT helps investigators to improve accuracy by structuring the management of large data sets using data categorisation, filtering and advanced analysis. Processes like these ensure that all possible connections are made, and risks are identified. This enables streamlined, effective investigations, and a more complete understanding of the information available.

Government/Public sector use case

Public sector uses of OSINT are wide-reaching and well-established. They include use cases of global importance, such as —

- Counter-terrorism
- Counter-proliferation
- Serious and organised crime-fighting

Accuracy in these instances informs decisions that can identify and disrupt threats to national security, as was evidenced when investigative journalism platform Bellingcat used OSINT to discover the location and identities of individuals behind the MH17 crash.[3]

[3]bellingcat —the home of online investigations

Risk agencies use case

Thorough coverage of all necessary information sources, and the ability to quickly identify connections across these sources, are central to efficient risk identification and effective action across a range of investigatory activities, including —

- Enhanced due diligence
- Bribery and corruption
- Insider threats
- Fraud

Like the public sector, most risk agencies have a history of successfully applying OSINT within the context of their investigations. However, advanced OSINT technology, which we will address in more detail later on, presents an opportunity to upgrade these capabilities. This can allow consultancies to serve more clients and at greater speed, increasing revenue and providing competitive differentiation.

Benefit 3: Greater access to intelligence

OSINT is derived from publicly available open source data. On its own, this brings three key benefits —

- **More ethical:** Public scepticism surrounding data usage continues to grow, and regulations such as GDPR have required organisations to enforce more stringent rules regarding data collection, storage and analysis. There are reputational, compliance, and moral challenges to address when handling data. OSINT helps create an ethical approach to data analysis because it is *publicly available*.
- **Easier to acquire:** Some forms of intelligence are difficult to gather. For example, HUMINT (intelligence derived from human sources) often requires highly trained investigators to work anonymously in dangerous circumstances to acquire information. Access to private data, such as call data, generally requires specialist technology and privileges available only to law enforcement. Open source data, on the other hand, is publicly available, meaning that anyone can access it and use it as intelligence if the right processes and people are in place.
- **Less expensive:** OSINT is often freely accessible through search engines, data aggregators and more. Compared to other types of intelligence, that makes OSINT relatively inexpensive to access. With that said, upfront investment in OSINT technology can be beneficial. OSINT solutions minimise the need to collect data indiscriminately by using technology to focus investigators on relevant information. Ultimately, effective OSINT technology can improve the efficiency and effectiveness of your OSINT investigations.

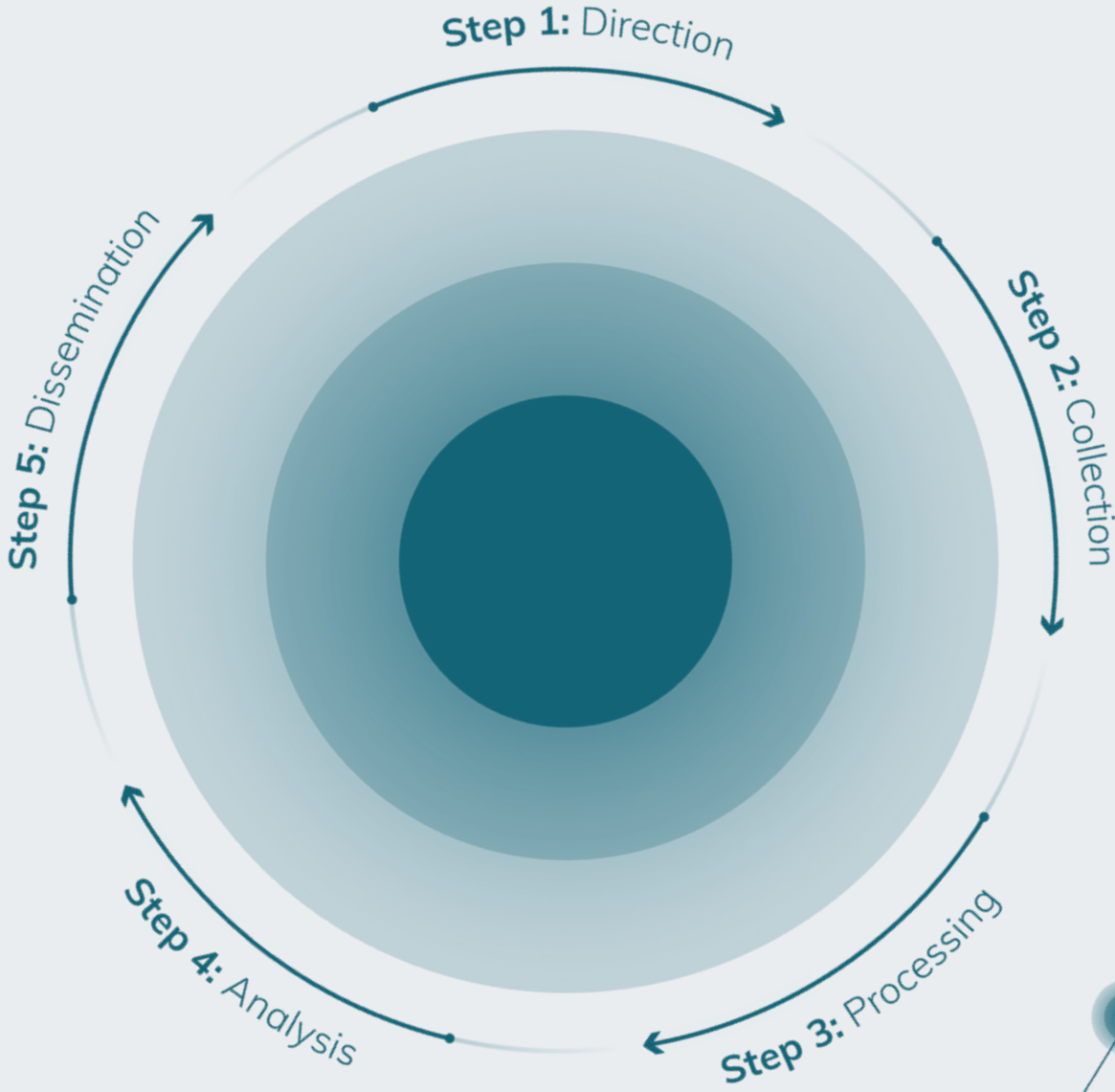
Public sector use case

Prioritising OSINT, which focuses on publicly available data, can significantly reduce investigative practices that encroach on individuals' right to privacy. By centralising targeted data collation and filtering out irrelevant information, governments, intelligence agencies, and law enforcement stand to enhance investigations into networks, illicit connections, and more without violating public trust or privacy.

Applying the Intelligence Cycle to OSINT

Transforming data into intelligence requires the application of structured processes that can keep you focused on what's relevant. One such process worth examining in detail is the Intelligence Cycle (IC). This is a common technique within the intelligence and law enforcement community.

This section will give you an understanding of *how* to apply the Intelligence Cycle in order to leverage technology and data to drive better investigatory outcomes.



Step 1: Direction

Direction is the starting point for any investigation. This first stage of the Intelligence Cycle focuses on defining the problem by considering what intelligence is required to overcome a particular knowledge gap. In short, you need to set out the questions you are trying to answer.

Having a clear plan makes investigations more efficient and effective. Skipping this crucial first step leaves you open to either collecting and analysing too much information and being overwhelmed, or not collecting and assessing enough relevant information, and potentially missing out on crucial intelligence as a result.

To avoid these negative outcomes, the Direction phase should be used to set guidelines regarding the actions to be undertaken, such as —

- **Background briefing:** This should be prepared for analysts regarding why the intelligence is required.
- **Intelligence Requirements (IRs):** These are statements that clarify the knowledge gaps that need to be bridged and the specific questions that need to be answered.
  IRs typically come in two forms:

  > **1. Standing information requirements:** Information tied to wider organisational requirements that will continue to be important on an ongoing basis. For example, how are our enemies likely to attack us? How are our competitors looking to develop an advantage?
  >
  > **2. Specific information requirements:** Information relating to a deliberate action, plan, or investigation. For example, is the enemy planning to launch an attack tomorrow? Is our competitor going to unveil a new product next month?

- **Reporting criteria:** These are timeframes and deadlines for reporting, and instructions on how the intelligence is to be submitted. This might be an in-person presentation, through a slide deck, or a written report.
- **Priority grading:** This is a useful way to ensure analysts understand how to manage time and resources. It may be that of three questions that an organisation would like to have answered, one is critical, and two would be nice to know but not essential.

Role of technology

OSINT technology can enhance the efficiency and effectiveness of the IC Direction phase by providing —

- Team capabilities and messaging features that allow any IRs, task orders or background briefings to be communicated to investigators and analysts.
- An ability for analysts to translate IRs into an investigative plan, create a reporting template, and track the progress of an investigation.

Step 2: Collection

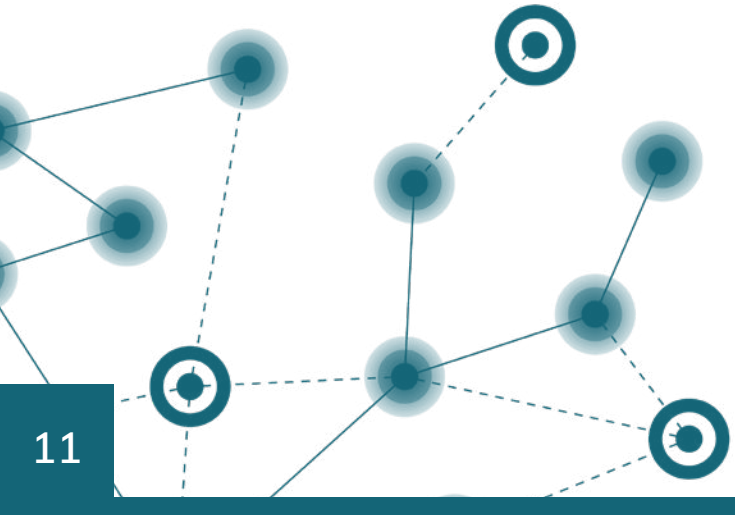
If Direction is all about what questions need to be answered, then Collection is all about where an analyst should look to obtain relevant information, and how they should go about collating it.

In the context of OSINT investigations, some OSD sources typically used in the Collection phase include —

- **Media articles and reports:** Obtained via search engines, direct from source or via media aggregators.
- **Social media data:** Accessed directly from the source or via social media intelligence (SOCMINT) tools.
- **Corporate records and annual reports:** Accessed from company websites, corporate registries or via corporate records aggregators and data providers.
- **Court records and legal filings:** Obtained directly from the court website, relevant Government agency, or via court records aggregators.
- **Regulatory watchlists:** Accessed directly from relevant Government websites or regulatory data aggregators.

Additional resources: Bellingcat's OSINT framework provides a useful collection of OSD sources.

The rapid growth of online data is both a challenge and an opportunity for investigators. On the plus side, investigators now have far more potentially useful sources of information to consult when trying to obtain information about a particular person, organisation or event. However, there is so much data that analysts run the risk of missing crucial intelligence as a result of being overwhelmed by too much information. Gathering information from online sources also presents potential operational, ethical and security risks.



Collection risks and challenges

There are a number of critical risks and challenges during the Collection phase that need to be accounted for and overcome. These include —

Not enough data: Fail to collect enough data and risk missing a critical piece of intelligence. It's important to note that failure to report on regulatory "red flags" could result in regulatory investigations, legal proceedings or criminal prosecutions.

Not the right data: Fail to collect the right kind of data, and the Analysis phase could be impacted (see next section).

Too much data: To overcome the above issues, it's easy to fall into the trap of a "more is more" approach. However, collecting more information than is necessary can lead to analysts being overwhelmed. Indiscriminate collection also poses potential legal and ethical issues as information may be collected on individuals that the analyst has no legitimate reason to investigate.

Varying approaches: The ways in which data is collected need to be consistent. If data is collected in different ways by different investigators, it's easy to produce inconsistent outcomes, in turn making the resulting recommendations less defensible.

Security: Analysts need to ensure they are collecting information in a way that does not compromise the security of an investigation. That means ensuring that they do not —

- Tip-off the subject of an investigation
- Give away their identity
- Obtain information that contains malware

The key to overcoming these risks is to produce a Collection Plan that focuses on what sources need to be consulted, and how the collected information will be captured and stored. The Collection Plan also needs to consider any security risks or legal considerations associated with the collection of the OSD.

Role of technology

As well as having a Collection Plan, the efficiency and effectiveness of this IC phase can be improved by the application of technology. For example, OSINT tools exist that can help after analysts

Strike a balance between comprehensive data collection and the targeted identification of relevant information.

- Structure the way that data is collected, and keep a record of what happened when.
- Remain secure and anonymous when undertaking online research, a capability that's particularly important to investigations and intelligence professionals working in sensitive roles where operational security is paramount. This is essential in a financial service context where tipping off a suspect of an AML investigation can lead to criminal prosecution.
- Search multiple search terms simultaneously across different sources, including search engines, corporate records databases and social media platforms. When done manually, this process can be extremely time consuming and error-prone.

Step 3: Processing

Once the Collection Plan for an investigation is in place, the data needs to be processed so that it is usable for the investigator or analyst. All information collected must be catalogued, organised, and made accessible. The types of processing required will vary according to data type. For example, corporate records data will be processed differently than media reporting.

However, organisations should bear the following points in mind when processing open source data —

- **Categorise and log:** Collected data should be categorised and stored according to themes, such as source (social media platform, journal article etc.), location, or language. A bibliography of all sources should also be maintained. Although highly administrative, these steps will avoid the need to rerun the research should the data need to be revisited multiple times, and ensure reference data is stored for inclusion in reports if necessary.
- **Translate:** Where collected data is in a language not spoken by the analyst, a translation should be obtained in preparation for further analysis of potentially significant names, addresses, or key terms.
- **Filter:** Analysts should sort useful and relevant information from the collected OSD, such as common names, addresses, themes, and keywords, into consolidated lists or databases (e.g. a database of company names and affiliated officers, shareholders and addresses) in preparation for further analysis. Data can also be restructured into a format that aids the production of charts, graphs, and other forms of visualisation.

Role of technology

Technology has the potential to completely transform the Processing stage of the Intelligence Cycle within an OSINT investigation. The automatic categorisation, referencing, deduplication and translation of collected information can significantly reduce the time taken to complete manual and repetitive tasks. With the right tools, the analyst should have to spend little time on Processing, leaving them to concentrate on the next stage: Analysis.

Step 4: Analysis

The Analysis stage is the part of the Intelligence Cycle where OSD becomes intelligence. This phase involves the assessment of collected and processed data, and the development of a final "product" that will be used to inform decisions. The Intelligence Cycle, as the name suggests, is an ongoing process. Therefore, this phase can also lead to the triggering of new IRs or further rounds of Direction, Collection, Processing and Analysis.

Intelligence analysis is a complex topic, and the specific processes involved in drawing meaning from OSD vary widely depending upon a range of factors, including the questions to be answered and the type of data involved. For example, using OSINT to predict the likelihood of a rise in crime in a particular geographical area, based on local crime statistics, is likely to rely heavily on mathematical modelling. On the other hand, assessing whether a potential client can be linked to sanctioned entities will typically rely on qualitative analysis using official watchlists, corporate records and news media sources.

Despite this complexity, there are a number of steps an analyst can take to provide a framework around the Analysis of OSD —

- **Visualise the data:** Analysis of connections and networks is often far simpler when information is presented in a chart or graphical format. The data may have been placed in this form during the processing stage, in which case the analyst can quickly move to analysing and understanding the data.
- **Use IRs as guidance:** The initial Intelligence Requirements identified during the Direction phase should be used to guide the processing and analysis of collected information, and the development of a finished product. Continually referring back to the IRs will keep the analysis phase on track.
- **Make use of analytical frameworks:** Analysts should consider making use of structured analytical methods to test competing theories and hypotheses, and overcome confirmation bias.

Suggested reading: *Structured Analytic Techniques for Intelligence Analysis* by Randolph H. Pherson and Richard J. Heuer Jr. is a must-read for OSINT analysts.

Role of technology

In this phase, it's the Analyst who takes centre stage. They are the subject matter experts who need to consider the processed data, assess its reliability and relevance, and integrate their findings into a finished brief or report. However, as mentioned above, using technology to process open source data has the benefit of giving the investigator far more time to analyse it, as well as ensuring that the processing is accurate and thorough.

Additionally, OSINT tools frequently offer visualisation capabilities such as charts, maps and grids, which allow the investigator to see and understand connections and networks far more quickly, and potentially gain greater insights from the data. These kinds of tools can radically improve the speed and effectiveness of the analytical process, allowing for more data to be collected and analysed in a shorter time frame. Finally, tools can support the analysis and final report creation through the automated sourcing of any collected information, inbuilt logging for auditability and cross-referencing, and standardised formatting options.

Step 5: Dissemination

This stage is about ensuring that relevant stakeholders receive the right information at the right time and in the right way. Dissemination relies on the presentation of processed and assessed OSD in the form of visualisations and reports that demonstrate a clear, cohesive narrative.

Most commonly, reporting will take the form of either —

1. **Written intelligence briefs:** Text documents or written presentations that users can access as necessary.
2. **Oral intelligence briefs:** Presentations in which information is verbally explained and analysed.

Unfortunately, dissemination is often a complicated process that involves —

- Tailoring distribution to ensure the security of the intelligence product
- Redacting or marking sensitive information
- Engaging senior stakeholders

Role of technology

Technology can simplify an analyst's ability to develop and disseminate a final product that has a compelling narrative and addresses the IRs.
An effective OSINT tool does this in three main ways —

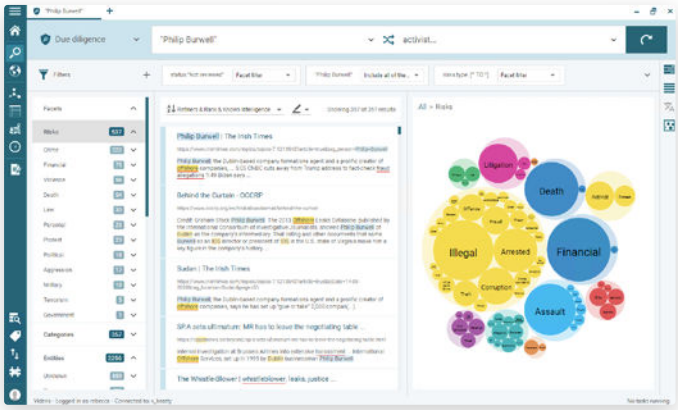
- **Visualisation:** Many tools offer charts, graphs and other visualisation capabilities that help investigators to make sense of large volumes of data, allowing them to explain decisions to senior stakeholders clearly and quickly.
- **Consistency:** Technology provides a level of consistency around processes such as reporting, enabling organisations with multiple investigators to provide standardised, high-quality intelligence to internal and external customers.
- **Information-sharing:** OSINT tools often include capabilities that allow for secure and fast teamwork, enabling investigators to share intelligence with those who need it without any security concerns.

What you need in an OSINT tool

In order for OSINT to facilitate effective and efficient investigations, technology is needed that can simplify operations and focus analysts on the right information at the right time. Sophisticated OSINT solutions make it far easier to implement an intelligence-led process. Poorly implemented OSINT strategies can leave organisations at risk of missing connections, overwhelming investigators and compromising investigations.

Reliable OSINT platforms should inform human-led decision-making by directing analysts towards investigation-relevant insights and connections that would be impossible to rapidly identify manually. This allows investigators to make the important decisions using their skills and expertise, whilst ensuring that nothing is missed.

At Blackdot, we've designed our technology around the five stages of the Intelligence Cycle in order to help users generate OSINT outcomes faster and more effectively. Our platform, Videris, is an intelligent automation (IA) tool that prioritises human decision-making while automating as many manual tasks as possible. Although not the only OSINT tool on the market, Videris incorporates a range of unique and leading-edge capabilities. By understanding these features, you will be able to better judge the capabilities of any tool, and the ability of technology to improve OSINT outcomes.



Capability 1: Search

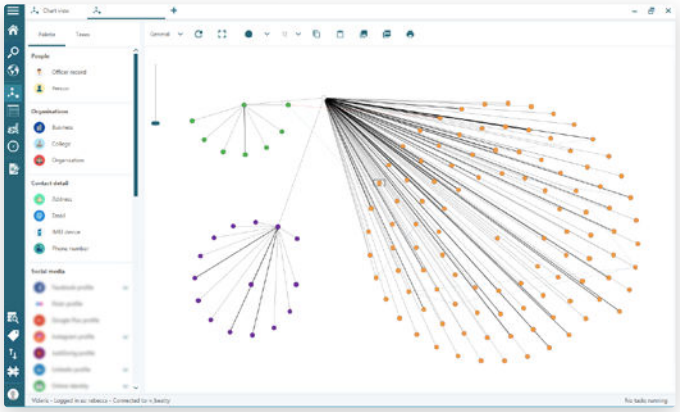
OSD is decentralised and often siloed. The time-consuming process of manually searching across multiple OSD sources is a significant challenge for efficiency and accuracy. Comprehensive searches are nearly impossible if every data source needs to be consulted individually and manually for every inquiry. For this reason, Videris Search makes it possible to —

- ✔ Search across all sources simultaneously
- ✔ De-duplicate content
- ✔ Identify risk
- ✔ Automatically categorise results
- ✔ Centralise relevant search results for easy access
- ✔ Automatically track search history and sourcing

The outcome of this ensures that analysts can find the data needed for their investigations easily and quickly, allowing them to spend more time on analysis.

Capability 2: Visualisations

Connections can be difficult to identify from written information, and understanding large amounts of information can often be time-consuming and error-prone. Visualisations, like the corporate network mapping and charts offered by Videris, expose relationships in data. This makes it possible to understand and connect even complex networks or risks, and can ensure that no potentially important connections or insights fall under the radar. The ability to export these visualisations directly into reports at the Dissemination stage also makes it easier to explain connections that may otherwise be difficult to present.



Capability 3: Social media analysis

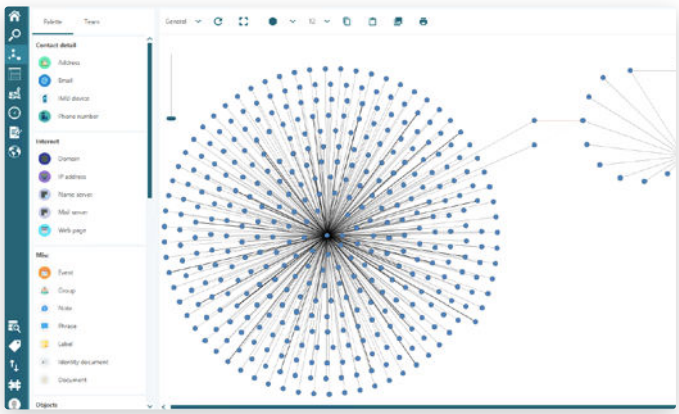
A large part of the value of modern-day OSD can be found across publicly available social media, where network links, personal behaviours, and movements are often freely available to view. The personal nature of social media means that analysts who deep-dive into this data repository are at significant risk of unethical practice.

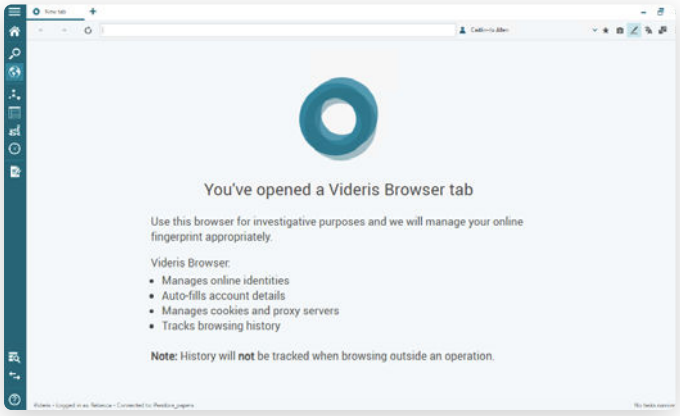
Videris offsets this risk with a specific set of social media tools. These allow users to map and analyse network connections that access only publicly available information.

Capability 4: Advanced data analysis

Advanced data analysis functions make it possible to draw connections while limiting overall data handling. This makes it easier to ensure efficient, ethical processes while simplifying the ability to recognise relevant connections that would otherwise be missed.

For example, cross-matching capabilities that automatically link similarities across crucial indicators like name, address, and social networks, ensure that Videris provides easily accessible analysis. Red flag risk profiling off the back of these insights ensures that analysts are able to focus on core pieces of information in real-time.



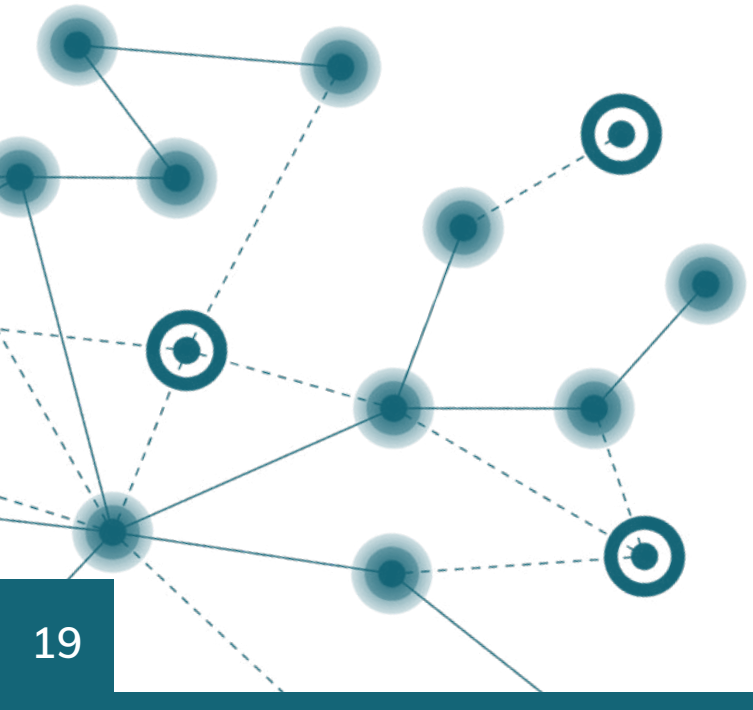


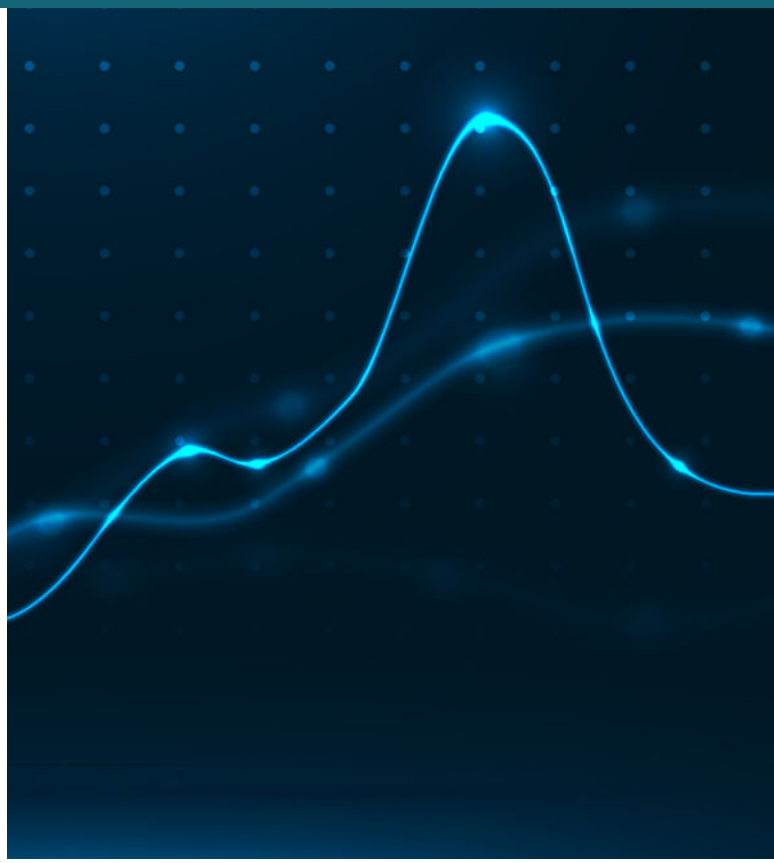
Capability 5: Secure browser

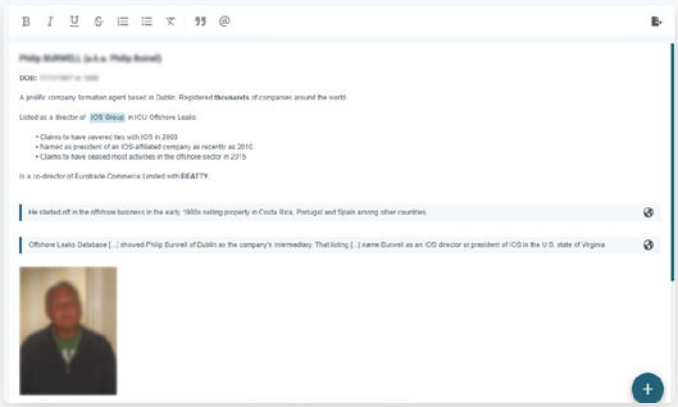
Ensuring security and secrecy during an investigation is critical. If you tip off the subject of your investigation to your activities, they may change their behaviour. What's more, depending on the context, this might expose you to criminal liabilities. For example, 'tipping off' in the context of anti-money laundering (AML) investigations.

It's also important that investigators don't accidentally download malware or other malicious programs that could compromise your system.

Videris' Secure Browser ensures that the identity and purpose of an investigation is never exposed. This is done by enabling untraceable searches that keep you securely hidden at all stages.







Capability 6: Reporting

Reporting, or dissemination, is the crux of the Intelligence Cycle. It ensures that the insights revealed in the investigation are translated into recommendations for decision-makers. The ability to export Videris notes and visualisations directly into reports at the end of an investigation brings ease to the often-complicated reporting process, as well as ensuring that sources are all automatically and correctly referenced for improved efficiency and accuracy.

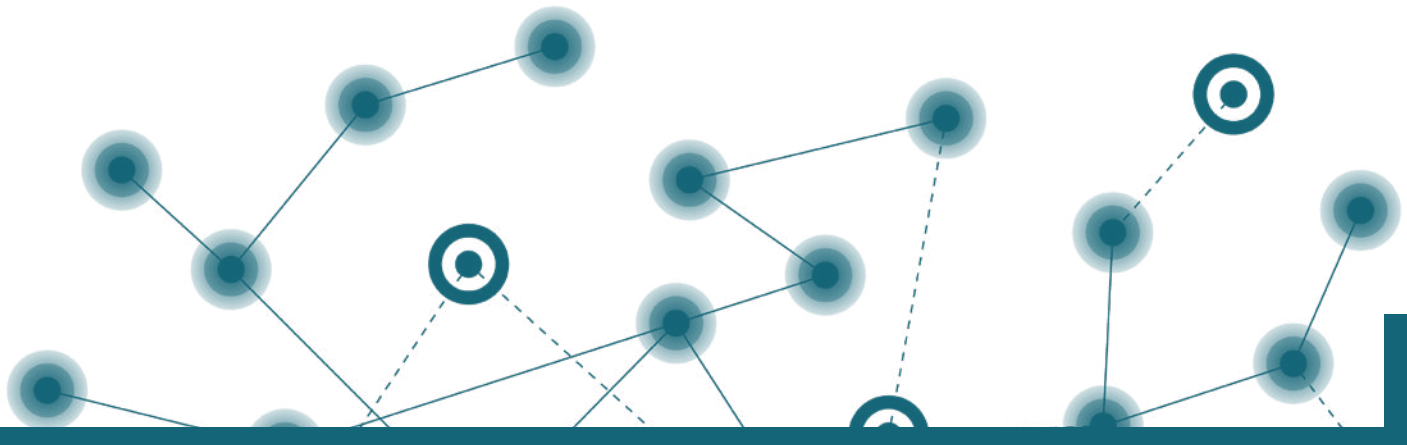
Capability 7: Integrations

If investigators need to visit multiple different platforms and sources to find the information they need, investigations are slowed dramatically. To ensure investigative efficiency, it's vital to integrate all data sources in one platform that provides easy access to all of the information the investigator needs.

Videris makes this possible by combining corporate records, social media, search engine and internal data where required, providing investigators with simplified access and substantial time savings.

Capability 8: Flexible deployment

Different customers will desire different kinds of deployment relative to their organisational structure. Videris provides flexible deployments either on-premises or in the cloud, while an expert team works behind the scenes to ensure operational wellness within your company infrastructure for secure, sound solutions that meet your OSINT needs. It's specifically worth noting that not all software solutions can meet the on-premise deployment requirements that are common within a governmental or banking context.



The ethical application of OSINT

Data ethics are an understandable concern. Beyond the primary moral requirement to investigate ethically, GDPR has focused organisations on data storage compliance. However, there are wider ethical considerations when it comes to data collection. As a result, it's critical that organisations embed ethics and data privacy within their intelligence processes from the start.

Given that OSINT is generated from publicly available information, it may be considered more ethical than intelligence gathered from other data sources. OSINT investigations, and the publicly accessible nature of OSD, make it far easier to stay on the right side of the ethics divide.

However, there are always more or less ethical options facing investigators. For example, although open source data is publicly accessible, its collection can still be unethical if done to excess. Indiscriminate collection of OSD makes it far more difficult to both adhere to compliance standards and to act on the information contained within, simply because there is too much of it to make sense of.

These challenges can be overcome using technology solutions. OSINT tools are a great way to achieve high ethical standards throughout investigations, through the prioritisation of —

Targeted data collection: By facilitating easy filtering, categorisation and prioritisation of data, investigators can collect only information that's relevant to specified investigation goals. For example, Videris offers keyword searches that prioritise results intelligently within the context of an investigation, as well as ensuring that only useful intelligence is always stored. Paired with secure searches that keep relevant information safe, this ensures efficient, ethical practices across an investigation, the purpose and value of which is far easier to demonstrate.

Public information only: Indiscriminately capturing data about an individual's behaviour can be considered unethical, but using information that has voluntarily been made public is far easier to justify. Collecting only publicly available information guarantees that no information has been illegitimately procured. When paired with the benefits of targeted handling, organisations are less likely to be challenged on the source of data, why it's needed, or whether investigators should have access to it in the first place.

Human judgement: The sensitive nature of many OSINT investigations makes it critical that human oversight remains central to that decision-making. IA (Intelligent Automation) allows you to empower humans to make good decisions by combining their domain expertise with powerful technology. This protects the value of human input and also protects OSINT investigations from becoming unethically automated.

Accountability: Consumers and government agencies are increasingly holding companies accountable for the ways they access, store, and use data in general, including open source data. Using a variety of tools, solutions can enable legal and policy compliance (and scrutiny of these) to support consistency, auditability and accountability.

Responsibility: OSINT is an undeniable force for good, but it's the responsibility of both organisations and their technology partners to ensure that safeguards for the legitimate use of OSINT are in place.

Outcomes depend on intelligence, not data

Organisations are struggling to extract meaningful insights from the increasing amounts of data they can access. It's therefore critical that rigorous analysis is applied to open source data, which is exponential in volume and has enormous potential to generate actionable insights. Combined with its accessible and publicly available nature, OSINT's ability to generate additional insights and improve investigative accuracy should make it a vital component of every organisation's approach to investigations.

It's not enough, however, to simply embrace the idea of using OSINT. It has to be done with intelligence and care. The internet is a highly valuable data source, but reliance on manual investigation methods risks overwhelming analysts and investigators with irrelevant or low-quality materials, leading to wasted time, inefficiency and poor outcomes.

It's for this reason that technology plays a fundamental part in integrating OSINT into the Intelligence Cycle. At every stage, a specialist OSINT tool can automate time-intensive manual processes and enhance the investigator's ability to identify and disseminate key intelligence, whilst ensuring security and transparency. When researching OSINT tools, organisations should ensure that their chosen platform offers a range of functionality, including secure search, visualisation, analysis and reporting tools, and that it augments, rather than replaces, the human investigator.

Finding the right technology can be challenging, but the right partner will help you to develop an efficient, targeted and outcome-driven approach to using OSINT. At Blackdot, we can help you achieve this. **Get in touch** if you want to learn more and **book a free demo of Videris today.**

Collect, analyse and visualise open source data with Videris

Blackdot Solutions makes Videris, a complete online investigations and intelligence platform for professional investigators and analysts.

Contact us to see Videris in action and find out how we can help to take your capabilities to the next level.

Get in Touch