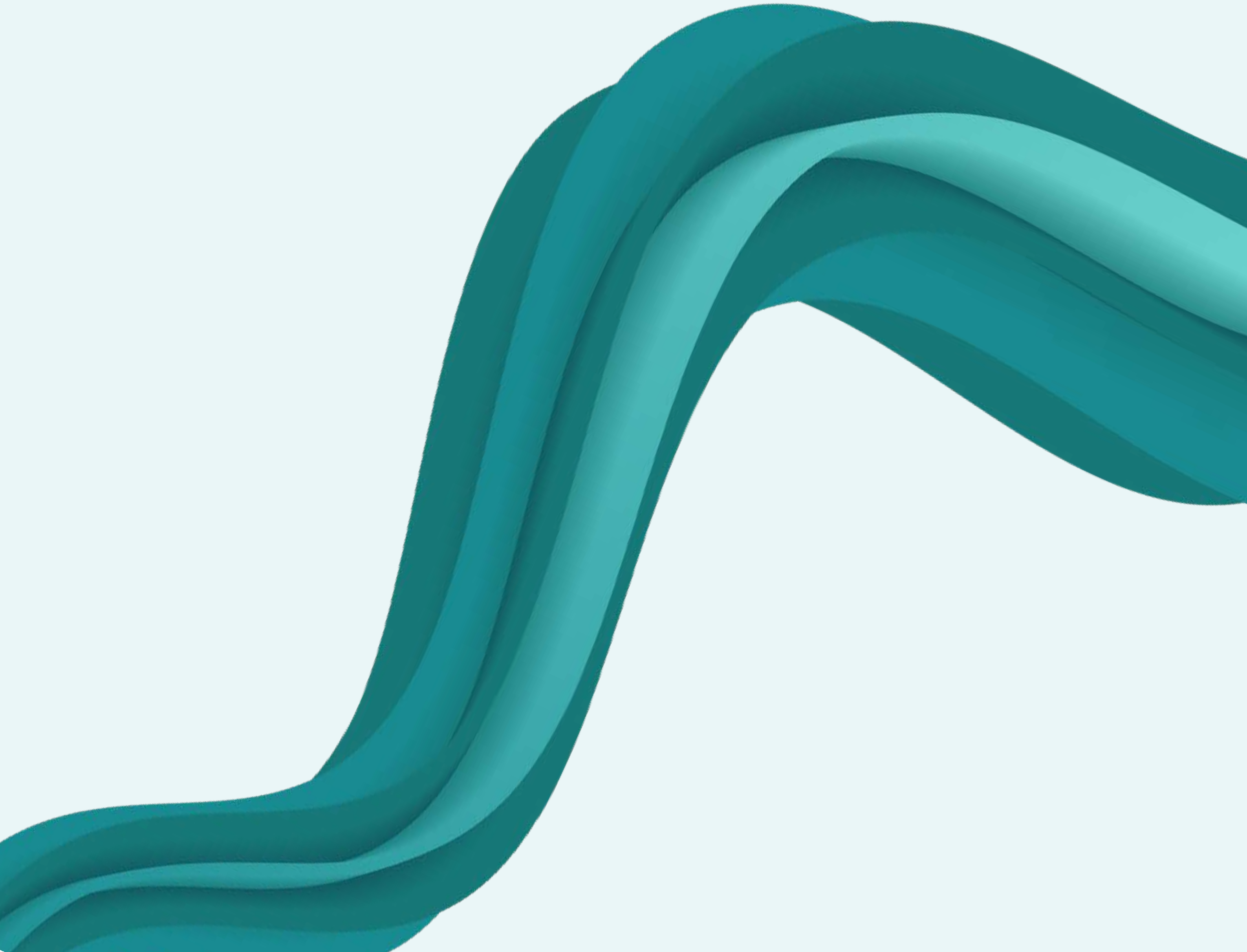
blackdot
solutions

The OSINT Handbook for Law Enforcement

Elevating policing with open source intelligence gathering and analysis

Contents



Introduction

As criminals continue to find new ways to break the law and evade detection, investigators must also adapt their crime-fighting techniques in order to outpace them. Teams must take greater advantage of the opportunities presented by collecting, processing and analysing open source data (OSD): in other words, improving their open source intelligence (OSINT) capabilities.

OSINT is not a new endeavour for law enforcement. Its employment was instrumental in investigating the downing of the MH17 flight in Ukraine in 2014[1]. In another event, investigators used OSINT to verify the assailants behind the poisoning of former Russian military intelligence officer Sergei Skripal and his daughter in 2018[2]. In both cases, investigators utilised OSINT tools and techniques to draw relevant data from a variety of sources and perform intensive analysis to reach their conclusions.

What continues to evolve, however, is the sheer size and number of OSD sources available. Reports estimate that over 328 million terabytes of data are created each day[3].

Yet, law enforcement professionals must be capable of analysing these datasets quickly and efficiently. Using publicly available sources of information is not only critical to performing in-depth investigations — the ease of access it brings compared to other types of evidence saves resources and time, without sacrificing detail.

This is where employing advanced technology to perform OSINT proves critical.

With the right tool, officers, detectives and investigators alike can cut down the time and resources required to harness the power of open source data. By moving away from manual processes to standardised, repeatable and secure ways of performing investigations, law enforcement professionals can solve and prevent crimes at a more efficient pace than ever.

In this handbook, we have collated the critical strategies and best practices law enforcement professionals must use to better employ OSINT in their operations — for faster, better-informed investigation outcomes.

Part 1

The different types of open source data

While OSINT goes beyond understanding different sources of data, it has to start with identifying the types of open source information available.

The scale and vastness of open source data is its strength as well as its weakness, with much of its growth owing to the rise of the internet. While the vast majority of OSD is available and easy to access online, much of it consists of unindexed data which cannot be obtained using standard search engines.

Fortunately, the advent of modern open source intelligence tools has helped investigators address the intricacies of different sources of OSD and efficiently convert them into OSINT.

Here, we will explore the various types of OSD in detail, breaking down each source and its respective opportunities and challenges within OSINT investigations.

Type 1: News and media

News and media comprises mass media publications, broadcasts, radio, TV, content from media aggregators, books and other forms of print or traditional media. News and media data is published both in front of and behind paywalls, and is distributed at international, national, regional and local scales. Even local news can be of pivotal importance, providing analysts with a rich account of events occurring in close proximity to the source.

Challenges posed to investigators

With millions of pieces of content being published each day in numerous languages, the news and media are in a state of constant movement. Grasping this movement and distinguishing reliable news from ‘fake news’ or other non-reputable media is simpler when investigators can properly understand the origins of these sources.

There are key questions to ask when assessing the reliability of an open source:

- 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 verified elsewhere? Are these other sources potentially more reliable?

It’s also important to note that using conventional search techniques and manual data handling to navigate sources is immensely time-consuming, particularly when mapping connections between news content and data from other OSD sources, e.g. financial records and company filings. Additionally, as news content is often repurposed across multiple networks in many different formats, deduplicating content can eat into efficiency without the assistance of purpose-built OSINT tools.

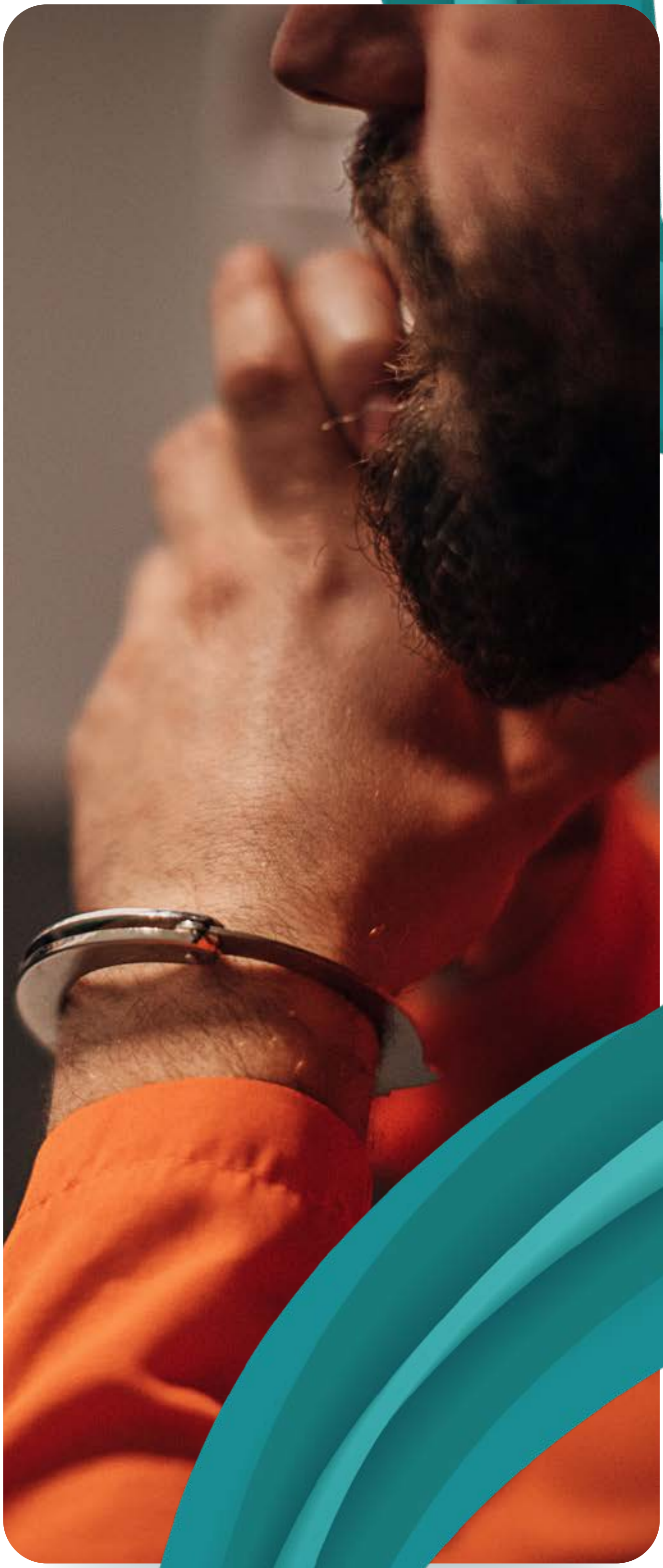
Use cases for applying OSINT

OSD collected from the news and media provides historical context to a wide range of events that can be factored into investigations. As a result, news and media has three clear use cases within the context of OSINT investigations:

Due diligence: Adverse news screening is also highly useful when assessing suspects for risk or integrity issues, regardless of whether they are individuals, businesses, organisations or government departments.

Revealing networks: News and media can pertain to individuals, organisations and events, and can often reveal new networks or correlate those unearthed from other sources, such as social media posts. This can help investigators understand events and individuals better. For example, news reports might identify individuals present in or related to the story, whether that be a crime, protest, or something else, either by name, image or video. These identifiers can be cross-referenced with additional data to map networks and connections.

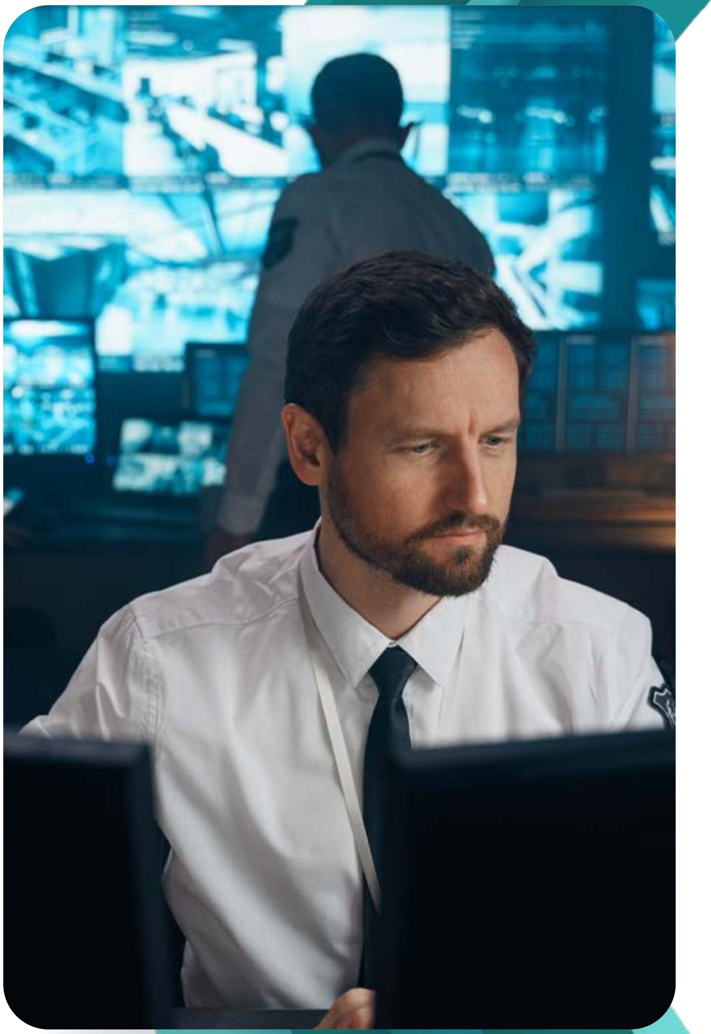
Mapping chronology: News and media OSD is particularly useful for mapping the chronology of news stories and events, helping investigators react to emerging stories that threaten someone or something's integrity or security.



Type 2: Grey literature

Grey literature includes all manner of publicly available non-media private and public sector policy information. This includes documents and reports 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 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), which recently exposed an offshore financial system used by numerous world leaders, heads of state, celebrities and businesses leaders in the Pandora Papers. 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 in order to gain access. For example, some 42% of global health research is currently published behind paywalls[4]. This is because 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 (SERPs).

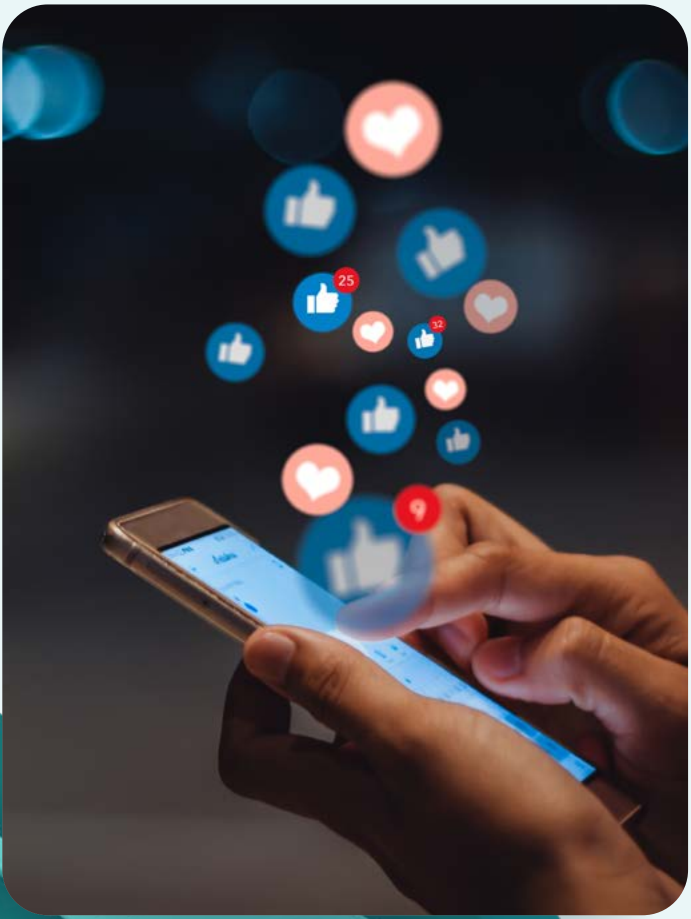
Many OSINT tools offer advanced browser capabilities that allow intelligence analysts to extend their search into results that are non-discoverable using standard web browsers. Moreover, the storage and distribution systems behind grey literature are notoriously disparate and poorly structured, complicating the process of locating and connecting related data points between different sources. In these cases, OSINT tools can offer visualisation capabilities that help investigators understand the data they have collected from these sources.

Use cases for applying OSINT

Grey literature is often used to distribute and disseminate both quantitative and qualitative data between businesses. It is, therefore, data-rich by virtue of its design, allowing investigators to obtain critical investigation context.

Corporate records are a key focus of OSINT gathering, providing information about business transactions, filings and network connections between various business stakeholders and related organisations.

Grey literature is useful across a range of investigations, especially those where a detailed understanding of corporate networks and finances is beneficial, such as anti-money laundering and asset tracing investigations.



Type 3: Social media

Social media can cover the entire spectrum of long-form content (e.g. Reddit posts, long-form social media blog posts, Quora answers) as well as short-form content (Tweets, LinkedIn updates, Instagram captions), photographs, tags and both first and second-degree connections.

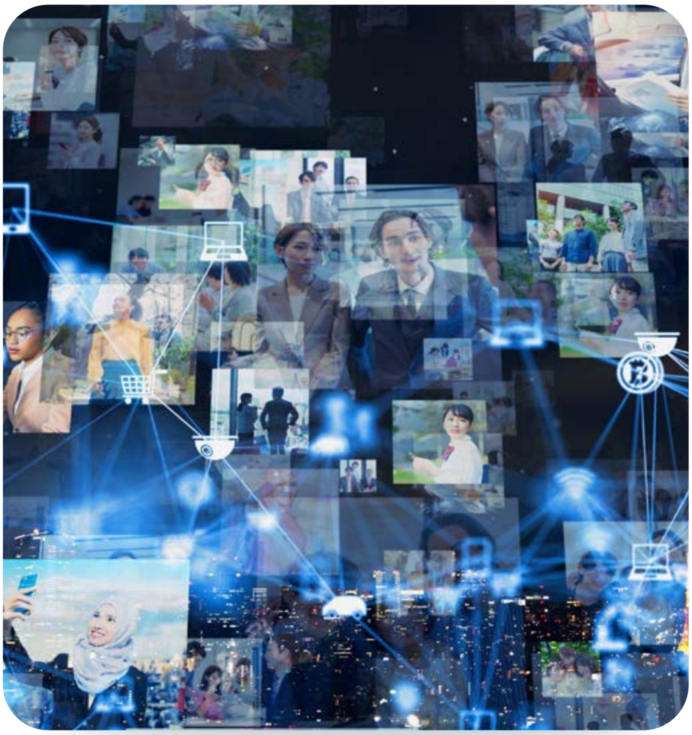
The metadata associated with social media content is central to open source intelligence techniques, assisting in network visualisation and understanding the chronology of interlinked events. Social media data is also highly visual, and involves a mass of images and videos often created in close proximity to their subject matter.

Note: Some social media data is public data, and other social media data is not. It’s important to point out that OSINT only covers public social media.

Challenges posed to investigators

Over half the world's population now uses some form of social media and, as a result, it has immense depth and volume, making manual exploration exceptionally laborious. Much of the most useful social media information is unindexed and resides in the deep web, rendering standard surface web browsers insufficient. Fortunately, specialist OSINT tools help investigators to analyse this data and highlight connections at speed, reducing much of the manual legwork.

Furthermore, retaining anonymity is crucial for any social media investigator. Investigations into individuals or networks must remain under the radar and not trigger any signals that might alert the subject to an ongoing investigation.



Use cases for applying OSINT

The vast amount of data that is available on social media platforms makes it a powerful source for OSINT investigations. It can be applied in a range of investigation settings, including:

Threat intelligence: The level of person-to-person data available via social media is not available anywhere else, and provides a non-superficial means of monitoring information about a threat actor's recent activities, locations or communications – information that might provide insights into previous or planned hostile activity.

Visualising personal connections: Intrinsic to social media are the connections formed between accounts and their respective posts and content — these assist investigators in visualising connections within and between networks.

Type 4: The dark web

Considered part of the deep web, the dark web is a term used to refer to web pages that are non-indexed and require specialised software to gain access. On the dark web, users and operators remain untraceable, and as a result, it is a rich source of data relating to criminal networks, their activities and connections. User names, addresses and other signals and identifiers are invaluable in forming cross-connections with surface or deep web information, assisting intelligence analysts in identifying connections between accounts and profiles.

Challenges posed to investigators

The dark web is a unique data source that is wholly unindexed by standard search engines. Intelligence analysts must exercise care to not expose their own identities or give away their investigation, whilst also remaining distanced from malware or exposure to illegal media. Collecting relevant information from the dark web whilst ensuring regulatory and legal due diligence is critical, and requires specialist OSINT tools and techniques that allow investigators to interrogate information safely without exposing themselves to risks.

Furthermore, investigators should also look to use these OSINT tools in order to avoid unnecessary exposure to potentially traumatic illegal material whilst browsing the dark web.

Use cases for applying OSINT

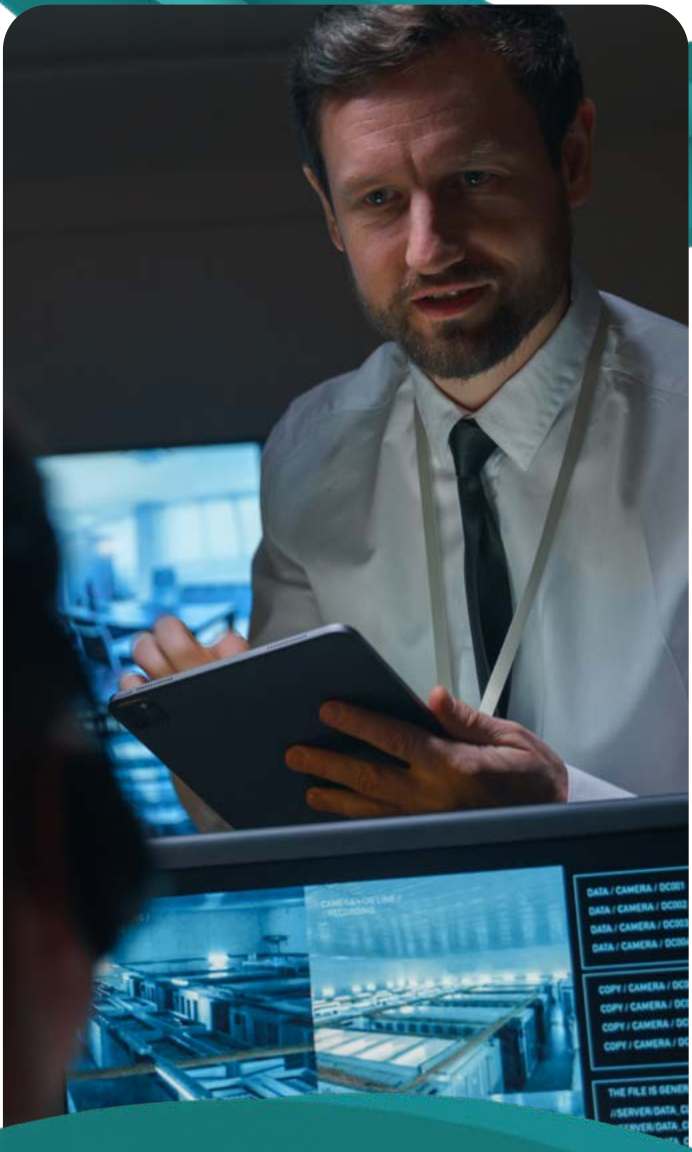
The dark web provides intelligence analysts with a key opportunity for locating direct connections between criminal activities and their associated user names, addresses and other identifiers. These findings can be cross-referenced and checked against data found on the surface web, allowing law enforcement and threat analysts to observe and identify criminal networks, gather evidence and monitor communication.

All this makes the dark web suitable for use within a number of different types of OSINT investigation. This includes investigations into the sale of illegal products - weapons, for example - and the tracing of drug and wildlife trafficking networks.

Use multiple OSINT sources to overcome investigation challenges

OSINT sources are complex and conventional research processes are largely insufficient for investigators looking to maximise the potential of open source data. A repeating theme here is the sheer volume of data available. Much of this data is poorly structured or unindexed by conventional search engines, making manual exploration laborious at best and impossible at worst.

However, an efficient OSINT solution can help address the above challenges. The best OSINT tools allow investigators to transition between these complex data sources, mapping connections and documenting network relationships using Intelligent Automation (IA). Essentially, this allows these processes to take place at a scale not previously possible through manual handling and processing methods, leading to more seamless workflows.



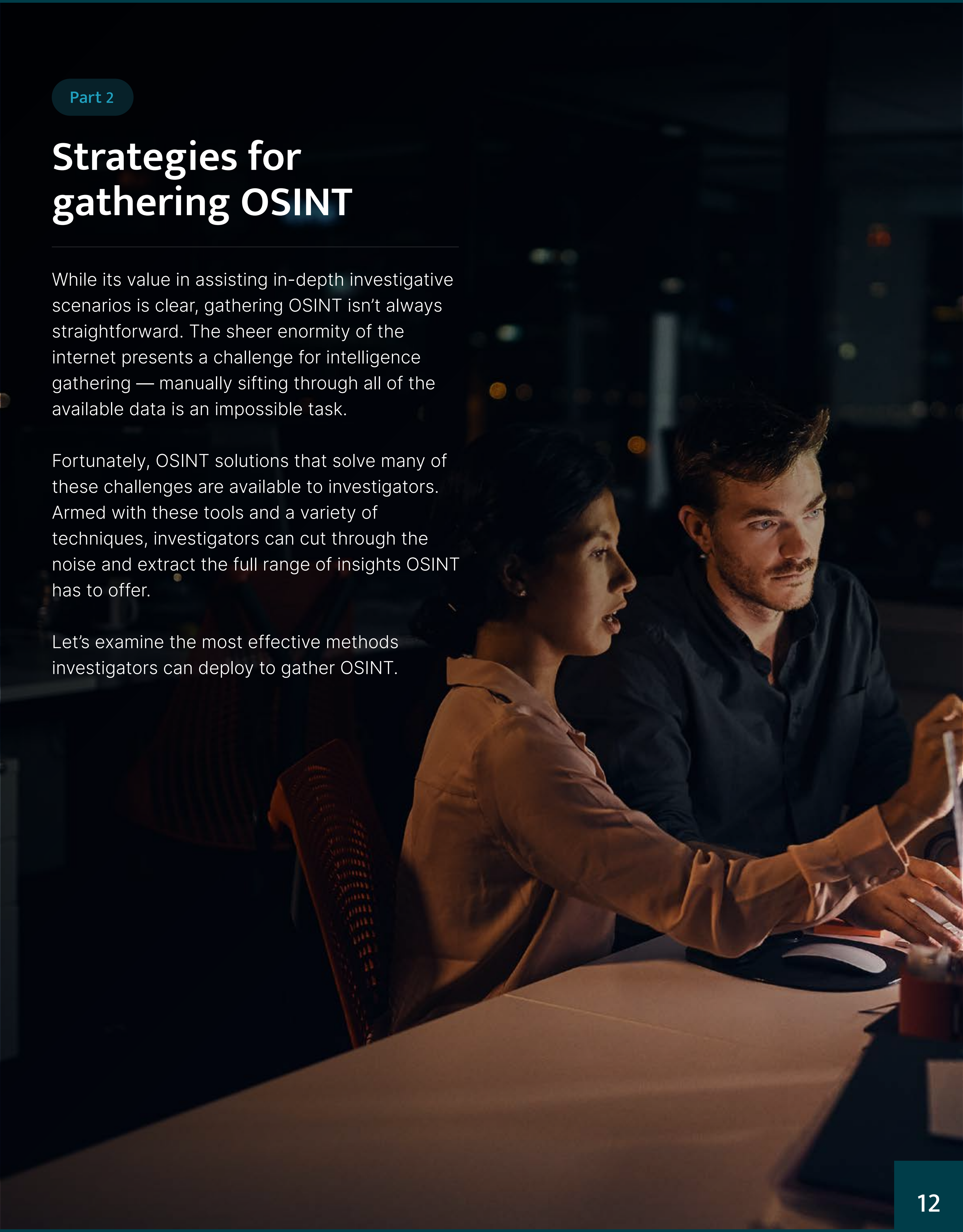
Part 2

Strategies for gathering OSINT

While its value in assisting in-depth investigative scenarios is clear, gathering OSINT isn't always straightforward. The sheer enormity of the internet presents a challenge for intelligence gathering — manually sifting through all of the available data is an impossible task.

Fortunately, OSINT solutions that solve many of these challenges are available to investigators. Armed with these tools and a variety of techniques, investigators can cut through the noise and extract the full range of insights OSINT has to offer.

Let's examine the most effective methods investigators can deploy to gather OSINT.



Strategy 1: Stay aligned with the Intelligence Cycle

The intelligence cycle should play a fundamental part in carrying out OSINT investigations, as it provides a simple framework for analysts to conduct an investigation and gather intelligence. The typical intelligence cycle involves five stages:

Direction and planning: Identify the fundamental questions that need answering. Define who or what is under investigation and why, and the OSINT sources you intend to use.

Collection: The process of extracting open source data in its raw form from the sources you have previously identified.

Processing: After data has been gathered, it needs to be translated into a comprehensible format, which might mean decryptionor sorting based on topic, relevance and reliability.

Analysis: Extract insights to better understand the meaning behind the data gathered.

Reporting and dissemination: Collate and visualise findings to make decisions more understandable to stakeholders who may not have the time to go through a detailed report.

OSINT investigations usually begin with either a question or a problem. Conducting initial searches based on that starting point might be plain and clear — like searching for public filings for a company accused of involvement in fraud. However, for more complex investigations, ethical considerations need to be made to ensure compliance and operational integrity.

Strategy 2:
Utilise disparate data sources

The internet is not a singular, monolithic database accessible only with commercial search engines. In fact, 96% of the internet is not accessible using standard search engines, and is either unindexed or otherwise obscured from crawlers[5].

Effective OSINT gathering must strike below the surface web, drawing insights from disparate data sources. This should include:

- Corporate records
- Blogs
- Forums
- Grey literature
- Publicly accessible databases

That's not to suggest that the surface is useless — far from it — but it represents just a tiny portion of what OSINT can offer. Diving beneath the surface allows investigators to obtain insights crucial to their investigations.

For example, the deep web contains all manner of corporate, governmental and NGO papers, as well as academic literature and company filing information. Much of this is OSD, and can therefore be used in OSINT gathering processes, but can only be obtained with database access or specialised search tools.

OSINT researchers can also extend their searches into databases which are specifically designed for due diligence, risk management and background checking. These can include:

- **Global corporate records aggregators** such as Bureau Van Dijk or OpenCorporates
- **Adverse media aggregators** such as Dow Jones Factiva
- **Compliance databases** such as Refinitiv World-Check
- **Sanctions databases** such as OpenSanctions

OSINT is often an iterative process, and findings from one source might trigger new investigation pathways. Recording disparate information in a singular, centralised environment is essential, as this will streamline the research process when the investigation begins to evolve.

Strategy 3: Expand searches to capture all available evidence

The surface web provides an excellent starting point for virtually any intelligence gathering or research process. However, effective OSINT gathering needs to go further and extend searches into all public data sources.

This includes the dark web, a rich source of OSD that provides insight, commentary and evidence on everything from smuggling to terrorist networking and wildlife trafficking.

During the OSINT gathering process, investigators should expand their searches into the dark web in order to:

- Better understand criminal networks, their communications, ideas, trends and practices.
- Locate information on dark web mirrors of surface websites, such as Facebook, which are used for political dissent and censorship-proof communications.
- Correlate, compare and validate information found on the dark web or deep web, e.g., matching usernames and profile pictures.

However, it's important to remember that extending OSINT-gathering into the dark web requires specialist tools. It is of the utmost importance that investigators remain anonymous during the information-gathering process. Failure to do so risks alerting the subject to the existence of the investigation.

Furthermore, the dark web is home to an array of illegal and potentially disturbing media. In light of this, it's important to take precautions to protect investigators from this content to ensure ethical data collection throughout investigations.

Strategy 4: Deploy intelligent automation

The volume of OSD available to investigators across disparate sources is vast and ever-growing, meaning that there is now far too much data to undertake truly effective OSINT investigations manually. Investigators need to start deploying new and innovative tools to effectively scale up their investigations and drive optimised outcomes.

That's one of the reasons why many are looking to artificial intelligence (AI) and machine learning (ML) for a solution. However, automating the process of OSINT gathering should not completely replace human decision-making. AI has benefits in many situations, but can't always make the nuanced, ethical decisions a human investigator would.

An alternative solution is the use of intelligent automation (IA) in the OSINT gathering process. IA tools can streamline the intelligence cycle by automating menial, low-level tasks, saving time and resources while leaving high-value, operation-critical decisions to human experts.

IA can provide investigators with a number of benefits during the process of gathering intelligence, including:

- The automatic collation of information from all available data points and sources into one seamless workflow, saving research time without sacrificing choice and direction.
- The revealing of named entities, relationship links and other critical features for deriving insight, saving analysts time without replacing essential human judgement.
- The creation of maps, networks, charts and tables that organise information effectively, helping analysts make connections and obtain insights in a timely manner.

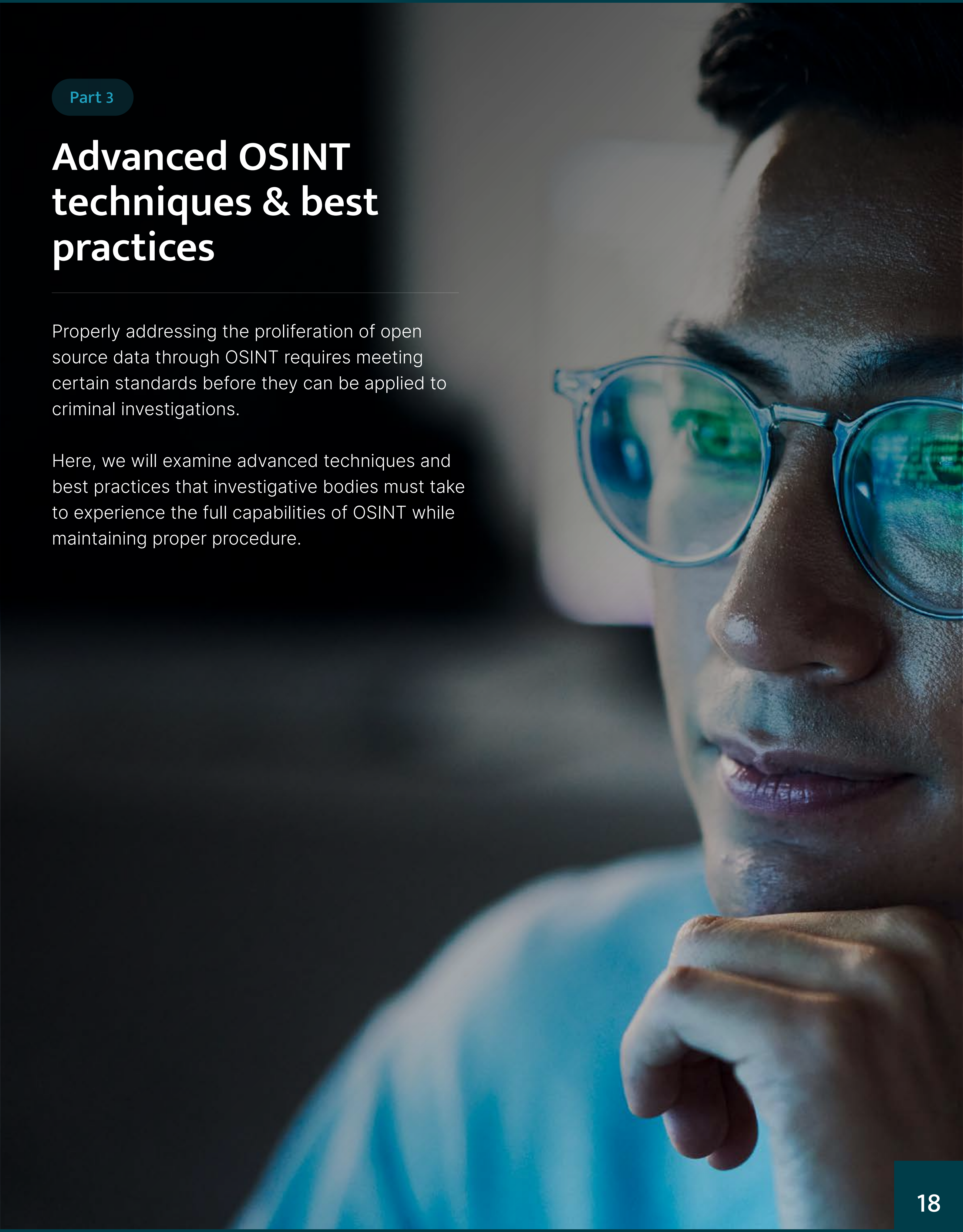
Strategy 5: Choose the right software

As the amount of OSD available to investigators has increased, we have seen the emergence of more sophisticated software to augment the OSINT gathering process.

The various OSINT tools now available come with a wide range of functionality. However, in order to ensure an effective and efficient OSINT-gathering process, investigators need tools that provide key benefits, including:

- Targeted searches across multiple data sets for terms/keywords that allow for incisive yet inclusive OSINT gathering across all available sources.
- Secure searches, which keep investigators anonymous during OSINT gathering, are especially important when utilising the dark web.
- Rapidly linking names, addresses, locations and other named entities, even when working with a wide array of text-rich sources.
- Combining all gathered OSINT into one easily accessible platform, regardless of its source and format.
- Intelligent automation of repetitive and time-consuming tasks, including drawing up networks, maps and graphs.

Moreover, using a singular OSINT ecosystem for the entire end-to-end investigation ensures operational accountability, integrity and security. Researchers need the ability to store all discovered data in a singular, secure location that is accessible anywhere at any time.



Part 3

Advanced OSINT techniques & best practices

Properly addressing the proliferation of open source data through OSINT requires meeting certain standards before they can be applied to criminal investigations.

Here, we will examine advanced techniques and best practices that investigative bodies must take to experience the full capabilities of OSINT while maintaining proper procedure.

Technique 1: Integrate internal, privileged and external databases

Internal or privileged data is information that is already held by the investigating organisation, such as criminal records, interview recordings, or privileged data from another government or law enforcement agency. External data can come from numerous other sources, including news media, search engines, social media platforms and corporate records data.

It's important to make the most of both types of data to ensure that no potential intelligence is being missed. Investigation tools that integrate external and internal databases are key in achieving this, as they allow investigators to recognise hidden connections by highlighting suspicious behaviours across disparate data sets.

As more people choose to share their lives through social media, Social Media intelligence (SOCMINT) becomes increasingly important.

SOCMINT involves intelligence across two data categories, which are:

1. **Original content:** Facebook updates uploaded images/video uploads.
2. **Metadata associated with original content**: Multimedia/geo-location date/time.

When integrated with other types of publicly available information, or OSD, the insights derived from these information sources enable investigators to resolve numerous complex cases. For example, the use of external intelligence such as SOCMINT during an investigation of an organisation involved in large-scale fraud can help you identify larger networks of bad actors that are connected to your suspects.

Best practices for combining data

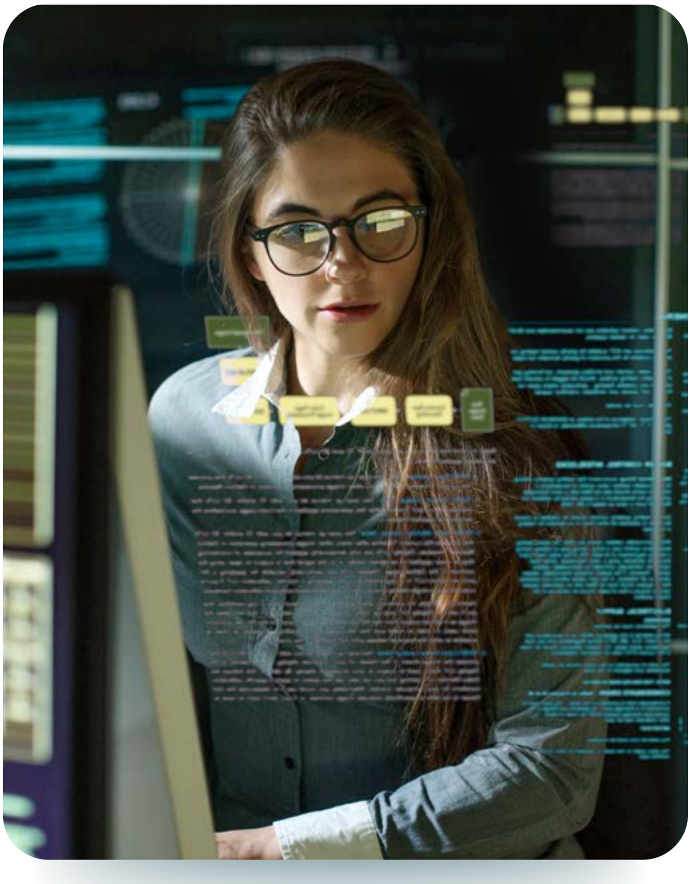
Fundamentally, it's vital to centralise investigation processes. Using multiple data sources and intelligence platforms creates inefficiency and increases the risks of data loss or exposures that reduce effectiveness. Investigators need the ability to gather and analyse data across a comprehensive landscape in order to advance decision-making and actions.

In this case, an IA tool can act as a single source of truth. With the functionality to search simultaneously across data landscapes, the right solution can comprehensively centralise access to all resources, as well as enable cross-referencing of data.

Technique 2: Harness intelligent automation to improve decision-making

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 sheer 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 is, broadly speaking, designed for advertisers, not investigators. Investigators see what search engines want them to see, not necessarily what's the most relevant data for their investigation. This adds to the challenge of breaking down data silos and makes it hard to focus on the most relevant information.



Best practices for automation in OSINT

As stated, fully automated and AI-based decision-making cannot match the expertise and nuance that experienced investigators bring to the table.

An intelligent automation platform makes it possible to automate time-consuming processes while still leaving experienced investigators in charge, augmenting, rather than replacing, human decision-making.

With IA, repetitive tasks can be automated in order to improve and accelerate human decision-making. This is done through the use of:

- Intelligent automation of manual processes, such as the gathering and mapping of data
- Automated red-flagging
- Cross-matching technology
- Easy-to-use visualisation capabilities
- Prioritised human oversight and reporting

Technique 3: Safeguarding the security of your investigations

Compliance with GDPR is a strong concern for organisations using OSINT. The poor handling of OSINT can lead to investigative bodies facing regulatory repercussions. For example, hoarding the open source data collected for OSINT when not all of it will be relevant to an investigation can breach GDPR regulations. What's more, the data collected that is relevant needs to be safely and securely stored to adhere to GDPR.

Another security threat that investigative professionals should be wary of is revealing investigators' identities or alerting the subject of an investigation, which will be counter-productive to the development of valuable insights.

For example, if a law enforcement professional is carrying out an organised crime investigation, they must take extra precautions to ensure that none of the suspects at the centre of the investigation are tipped off. Otherwise, they are at risk of compromising the investigation by helping the subject to evade detection and prosecution, as well as costing the safety of innocent involved parties.

Best practices for security in OSINT

Effective OSINT investigation ecosystems and efficient threat identification should be part of all investigations. However, investigative integrity is still at significant risk if these processes aren't deployed through an OSINT platform that prioritises security. This can be realised through the implementation of centralised data repositories, IP address security, and the ability to securely transfer data into other systems or formats among other priorities.

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.

3. Compliance and regulation measures: Ensuring that your OSINT investigations are compliant (particularly against GDPR standards) comes down to making sure you're collecting information you truly need and securely storing it. An OSINT platform is crucial for this, as the right one will be able to extract and store the most relevant insights to your investigations from large datasets at a level of efficiency that would be difficult for human investigators to achieve alone.

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

Technique 4: Be effective and ethical

The effectiveness of an open source investigation depends on an organisation's ability to tailor their data collation and handling towards specific objectives. This targeted approach ensures simplified investigation practices that never handle more data than necessary. It not only improves the efficiency of processes, but makes them more ethical and minimises exposure to risk.

Most importantly, the main benefit is that law enforcement professionals can rest assured that the evidence they present will be fully compliant and aid in prosecuting criminals.

Best practices for effective, ethical OSINT

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.

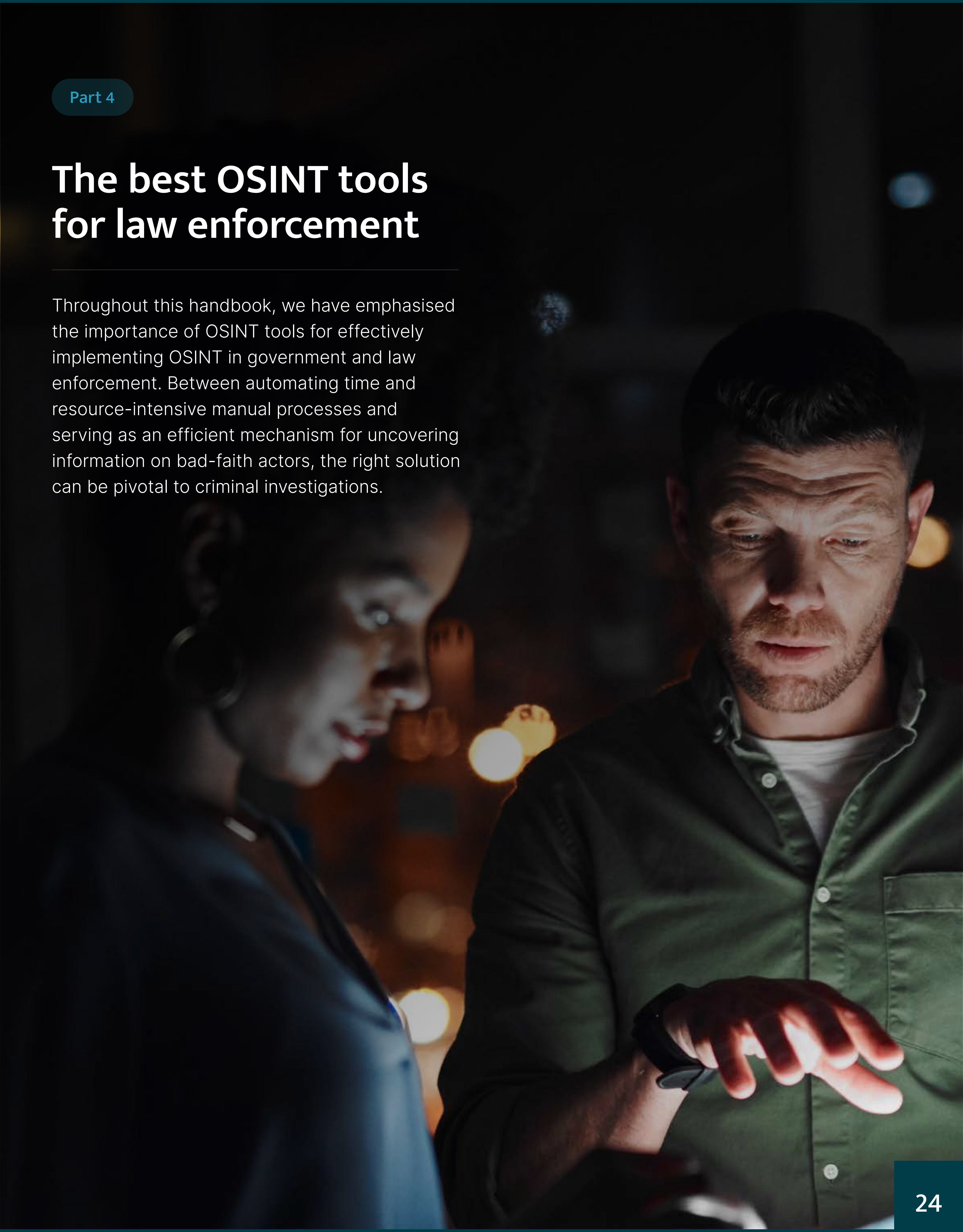
It's important to note the value of a trusted, expert-led OSINT solution in this context. Investigators must prioritise using a tool that draws analysis from pre-approved, publicly available sources, as well as sources all of this information clearly for evidentiary purposes.

Technique 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 – thus undermining their case.

Best practices for recording OSINT sources

To further ensure that their evidence is secure, investigators need to keep track of all of their 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. These activities are time-consuming and distract 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.



Part 4

The best OSINT tools for law enforcement

Throughout this handbook, we have emphasised the importance of OSINT tools for effectively implementing OSINT in government and law enforcement. Between automating time and resource-intensive manual processes and serving as an efficient mechanism for uncovering information on bad-faith actors, the right solution can be pivotal to criminal investigations.

The different kinds of OSINT tools available

Any investigation has multiple stages, including collection, processing, analysis and distribution of information. Some tools are designed to assist with a single stage, others span the entire process.

There is not just one way to categorise different OSINT tools. However, we believe it is useful to think about three main types:

1. **Collection tools:**

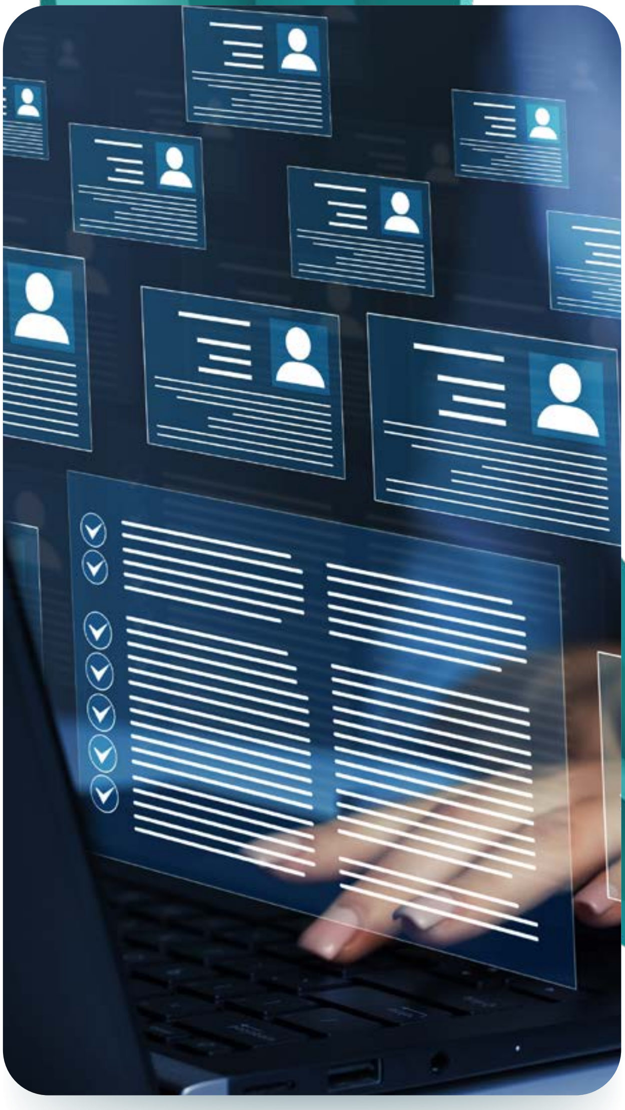
   These tools aid in the collection of open source data from one or more sources, such as corporate records data or publicly available social media information.

2. **Analysis tools:**

   These tools use process automation and natural language processing to identify patterns and correlations between the data you've collected, helping sift through large amounts of data and highlight actionable insights for the investigator.

3. **Visualisation tools:**

   These tools make it easier to view your data in a digestible format using graphs, charts and maps. This helps with analysis and makes reporting your findings easier and more engaging.



The tools you choose have a direct impact on the types of investigations you can undertake effectively.

It is important to note that the fewer tools you need to use, the easier it will be to organise your investigations and less manual effort will be required to do so. Single platform solutions are therefore recommended, as they reduce the need for additional data integrations, which can ultimately lead to cost savings.

Videris: A full-spectrum OSINT solution

Videris allows users to collect, analyse and visualise open source data within one platform. Its focus is on extracting maximum value from open source data.

Videris was built specifically for government and law enforcement, designed based on the workflows of experienced investigators in order to enhance the effectiveness and speed of criminal investigations.

Now, Videris acts as an all-encompassing solution for governmental intelligence and law enforcement agencies, amplifying their ability to conduct thorough and swift OSINT investigations across a spectrum of operational scenarios.

Key features of Videris

Intelligent Automation (IA):
Automate repetitive tasks such as collecting data from multiple sources, or highlighting connections, while leaving decision-making in the hands of experienced human operators.

Network mapping:
Generate visual representations of structures such as corporate or social networks to save time and make it easier to identify insights. Sort and interpret complex data in an interactive chart or graph.

Social media (SOCMINT) tools:
Securely map and understand public social media data, and highlight connections between individuals and their networks (powered by ShadowDragon©).

Search multiple sources at once:
Query any number of sources at once and aggregate your results into one view. This simplifies workflows and is particularly useful for uncovering hidden information on the dark web.

Cross-matching and automated red-flagging:
Automatically flag names, addresses and other similar data to avoid missing important links.

Security:
Guarantee that analysts remain secure and untraceable throughout investigations.

Open platform:
Videris is easy to integrate with other systems, making it a seamless fit for any investigative workflow.

Use cases for Videris

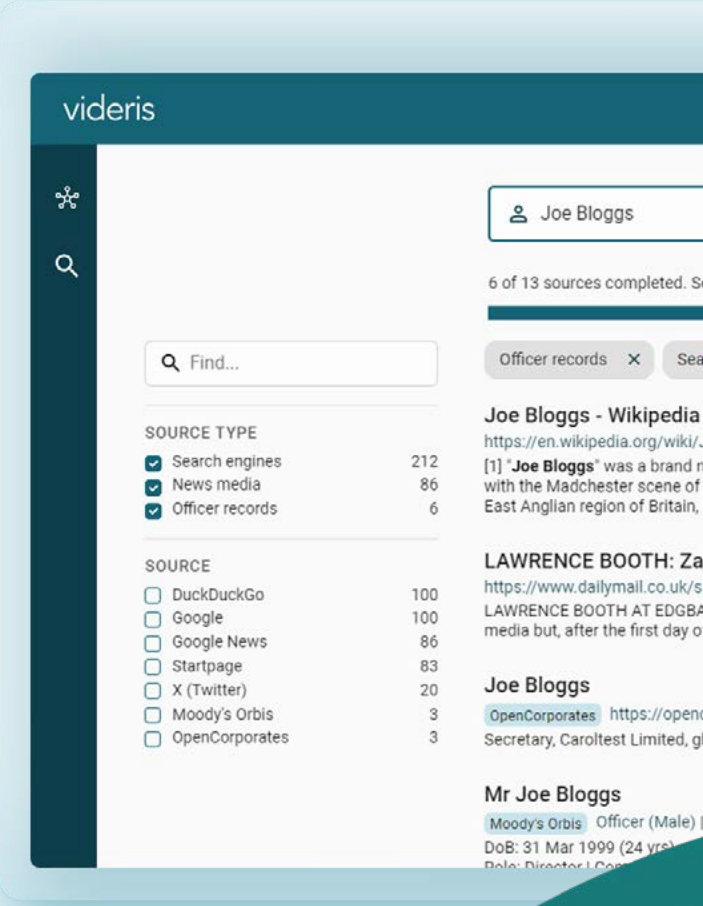
Videris is uniquely suited to simplifying your OSINT processes because it combines collection, analysis and visualisation capabilities within a single platform.

By utilising all OSD sources, it is possible to build a detailed profile of an individual, company, group, or network. Videris is compatible with a full range of OSD sources, making it possible to engage in advanced OSINT techniques and deploy Videris in a wide range of crime-fighting contexts, such as:

- National security cases, including counter-terrorism, economic crime, and investigating international human, drug, and wildlife trafficking.
- Uncovering hidden connections and identifying suspects within criminal networks.
- Building verified, comprehensive profiles of criminal suspects and connections.

Minimal training is required to get started, and the range of open data sources that come pre-configured allows users to extract valuable insights from multiple sources at once, including dark web data sources.

According to a recent case study, 'Videris had a very short time to value compared to other tools Berlin Risk had reviewed. It didn't require prior technical knowledge and investigators describe it as a professional, intuitive, user-friendly solution.'



Joe Bloggs

6 of 13 sources completed. S

SOURCE TYPE

☑	Search engines	212
☑	News media	86
☑	Officer records	6

SOURCE

□	DuckDuckGo	100
□	Google	100
□	Google News	86
□	Startpage	83
□	X (Twitter)	20
□	Moody's Orbis	3
□	OpenCorporates	3

Joe Bloggs - Wikipedia
https://en.wikipedia.org/wiki/J
[1] "**Joe Bloggs**" was a brand r
with the Madchester scene of
East Anglian region of Britain,

LAWRENCE BOOTH: Za
https://www.dailymail.co.uk/s
LAWRENCE BOOTH AT EDGBA
media but, after the first day o

Joe Bloggs
OpenCorporates https://openc
Secretary, Caroltest Limited, g

Mr Joe Bloggs
Moody's Orbis Officer (Male)
DoB: 31 Mar 1999 (24 yrs)

Book a demo to explore first-hand how Videris can enhance your investigations today."

Book a Demo

i2 Analyst's Notebook: Data visualisation and analysis

i2 Analyst's Notebook, made by IBM, is an intelligence solution that specialises in the analysis and visualisation of structured data, including OSINT data. Users are able to configure their own internal sources or install additional connectors to add external data for analysis.

Link analysis environment: Visualise data and identify relationships between people and organisations using association charts.

Timeline analysis: Views that display connections between information on a timeline for analysis.

Social network analysis: Analyse and examine group structures and communication.

Statistical views: Drill down into the contents of your data using bar charts, histograms and heat matrices

Use cases for i2 Analyst's Notebook

By focusing on the visualisation and analysis elements of OSINT investigations, i2 Analyst's Notebook offers a variety of ways to view data. This not only benefits in analysis, but also provides more interesting ways of reporting findings. It's worth noting that the platform can be used to visualise open source data, along with other internal data sources.

However, search and collection tools are needed to acquire data for analysis in the first place. This requirement to partner i2 Analyst's Notebook with other tools or manual processes makes it harder to use, and provides limited options to investigators that don't already have solutions for the targeted collection of OSD.

Palantir: Big data analytics

Unlike the other tools on this list, Palantir is a big data analytics platform, not a dedicated OSINT tool. However, it's deployed within OSINT investigations and is particularly popular among government users.

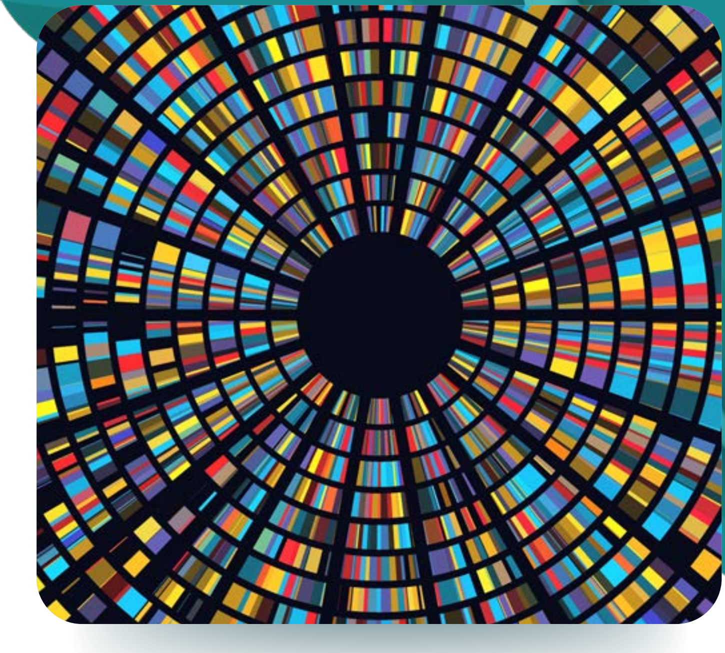
Key features of Palantir

Flexible platform:
Palantir can be configured to fit numerous feature requirements, however, it is complex, and therefore requires a large number of service hours to do so.

Manage multiple internal data sources:
Organise, manage and secure data from various internal sources within a single platform.

Pattern recognition:
Analyse and identify patterns within large datasets to aid your OSINT investigation.

Process large amounts of data:
Specialising in big data, Palantir can cope with processing massive amounts of data from multiple data sources at once.



Use cases for Palantir

Palantir is ideal if you need to carry out an investigation using huge amounts of data. Its data analysis functionality is very detailed, and it can be used for almost any use case, although this comes at a cost.

However, Palantir is not a data collection tool or a specific OSINT solution. You have to feed it the information you want to analyse. Much like with IBM's i2 Analyst's Notebook, you'll need to make sure that you have an OSD data collection framework in place before investing in Palantir.

Investigators looking for a solution that is purpose-built for OSINT and available out of the box may find that other products would be a better fit.

Maltego: An OSINT and graphical link analysis tool

Maltego allows for the visualisation and management of open source data in a unique and visually appealing way. Its 'Graphs' functionality allows for data viewing, collection building, and simple linking of records.

Key features of Maltego

View up to 1 million records on a graph: Visualisation tools make it easy to view a large number of records in one interactive view.

Access around 60 data sources: Add various open data sources quickly using the Maltego Transform Hub.

Connect internal and external data sources: External sources can be used within the tool or can be configured and supplemented with internal data.

Pattern detection: Use different shapes and layouts to make it easier to analyse and identify patterns.

Use cases for Maltego

Aimed at more technical users, Maltego is great for visualising investigation data. It's able to analyse intelligence across multiple sources, using plugins that fetch data from different sources, making it applicable to use cases in law enforcement.

However, it's important to recognise that many Transforms are developed by community members, rather than the central business, resulting in integrations that can be limited in both their depth and scale.

Cobwebs: An interlocking toolset

Cobwebs provides five products covering various functionality across the investigation process. It's a powerful solution when all of them are used together, but it's important to research what each product does.

Note: Cobwebs calls their product a WEBINT (Web Intelligence) solution. Functionally, this term is a synonym for OSINT.

Key features of Cobwebs

Web investigation platform: Monitor online activity, and collect and analyse data from various open data sources.

Threat intelligence solution: Automatically extract targeted insights from data with AI and machine learning algorithms.

Secured analyst assistant: Their Lynx browser provides a secure browsing environment for manual data gathering and analysis.

Location intelligence system: Use interactive maps to analyse location-based data and identify geolocated intelligence.

Use cases for Cobwebs

The Cobwebs solution delivers specific capabilities split out over five products. This helps specialist investigators focus on particular types of analysis and phases of the investigation.

However, it's important to consider how this division will impact workflows and the ways in which individuals approach an investigation. In some cases, data being spread across a number of solutions means that additional manual analysis is required, and collaboration becomes more difficult to achieve. If this is a challenge, then an all-in-one platform may be a better fit.

Conclusion

Drive forward policing techniques with an advanced OSINT platform

OSINT was developed as a military intelligence discipline in order to identify and understand threats using publicly available information. However, as the scope and value of open source data has continued to expand, these investigation techniques have been proven to add to law enforcement investigations.

In response to the rising demand for quality OSINT software, we developed Videris, a platform that arms investigators with the tools they need to conduct robust, detailed and accurate investigations.

Videris acts as a single pane of glass, allowing for the collation of all findings in one easily accessible, secure platform to prevent exposure or data breaches, as well as simplifying the overall investigation process.

With the ability to highlight search terms or search keywords across multiple public data sets at the same time, Videris Search ensures that investigations, and the data used within them, are always targeted towards outcomes. Easily anonymise investigations for added security and the assurance that your investigations are carried out efficiently and according to best practices.

Book a demo today, and explore how Videris could optimise the outcomes of your investigations.

Bibliography

1 MH17 The Open Source Evidence

2 Open Source: The Skripal Poisoning Investigation

3 Amount of Data Created Daily (2023)

4 Open to the public: paywalls and the public rationale for open access medical research publishing | Research Involvement and Engagement

5 What is the dark web? How to access it and what you'll find | CSO Online