The State of OSINT 2025

blackdot

Dear Reader,

Today's investigations face mounting challenges in the face of an increasingly complex, global and digitally-enabled crime landscape.

Open Source Intelligence, or OSINT, has long been overlooked as an intelligence discipline. Yet recent events and growing criminal activity mean that it is gaining in importance in both public and private sectors; a trend that was underlined by the release of the US Intelligence Committee's first OSINT Strategy in 2024.

Blackdot Solutions' mission is to help investigators use OSINT for good by equipping them with the software they need to combat criminal activity effectively. From our day-to-day conversations with investigators across sectors, the message is clear: OSINT is going from strength to strength, and teams need more professional guidance to support their work.

Driven by this need for best practice-sharing and actionable insight, we are delighted to publish the first annual State of OSINT Report. Containing responses from investigations teams across the globe, the report details perspectives on topics such as barriers to investigation, training, tools and AI use, highlighting opportunities for broader use and investment.

As ever, it is the collaboration and spirit of co-operation within the OSINT community that make it so special. We hope that you find this report insightful, welcome your feedback and encourage you to share it with your colleagues. Together, we hope that we can shape best practices in OSINT in the years to come.

Stuart Clarke
CEO, Blackdot Solutions

Defining OSINT

OSINT is now a well-known concept, but not always well-defined. For the purposes of this report, we define OSINT as the **targeted collection and analysis of publicly available or licensable data to produce actionable insights**.

Importantly, OSINT is not raw data. Instead, the term Open Source Information (OSINF) can be used to define the publicly or commercially available information that is then collected and analysed by OSINT investigators. Examples of OSINF include data from:

- **Surface, deep and dark web**
- **Corporate registries**
- **Publicly available social media**
- **Forum and message boards**
- **Public records**
- **News media**
- **Trade records**

There is no precise agreement on what exactly constitutes OSINF, and therefore, what data can be considered within OSINT investigations. We'll discuss these grey areas later on.

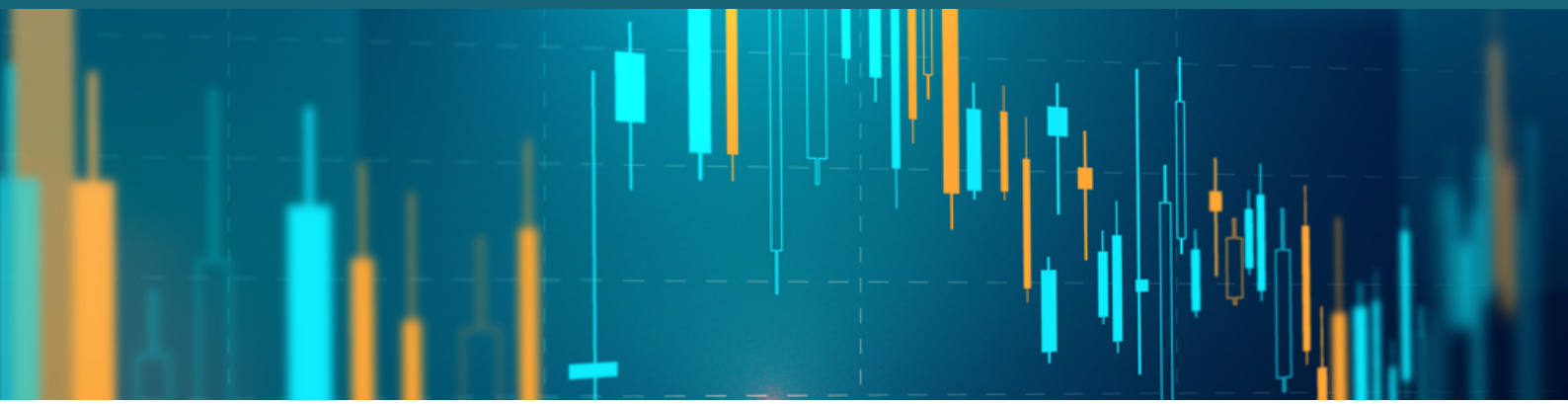


Table of contents

Methods at a glance

- We used the ScoreApp survey platform and asked 15 questions, including demographic questions.
- 131 people completed the survey, the majority from the UK and Europe.
- Respondents categorised themselves as working in one of four sectors: **public sector**, **financial services**, **professional services** or **corporates**.

Executive summary

- OSINT is widely used in investigations but **inconsistently applied**, with financial services lagging behind, especially in their use of social media. Across sectors, substantial challenges to implementation remain, limiting investigators' insights.
- The biggest obstacles to OSINT across sectors are **data overwhelm** and **data access**, with financial services feeling these pressures most acutely. **Time constraints, tool limitations, strict rules** and **poor organisational prioritisation** further limit OSINT effectiveness.
- Demand for access to **breach, leak** and **dark web data** may highlight inconsistent definitions of OSINT, emphasising the need for clearer standards within the industry.
- **Videris, Maltego** and **OSINT Industries** are amongst the most used tools, but many investigators still lack specialised tools, limiting efficiency and access to valuable insights.
- Training investment varies significantly: **law enforcement** and **professional services** commit the most time, while **financial services** and **corporates** show notable gaps.
- **Investigators are broadly positive about AI,** especially its ability to automate data collection and analysis and improve investigative speed. AI is seen as augmenting, not replacing, human investigators, freeing them to **focus on complex, strategic decision-making.**
- OSINT's value will increasingly depend on **organisational support, structured training** and **integrated, secure technology**. The next era combines human judgment with AI-driven efficiency, enabling faster insights and more impactful investigations.

Jonathan Groom MBA
Director, FIU Jersey

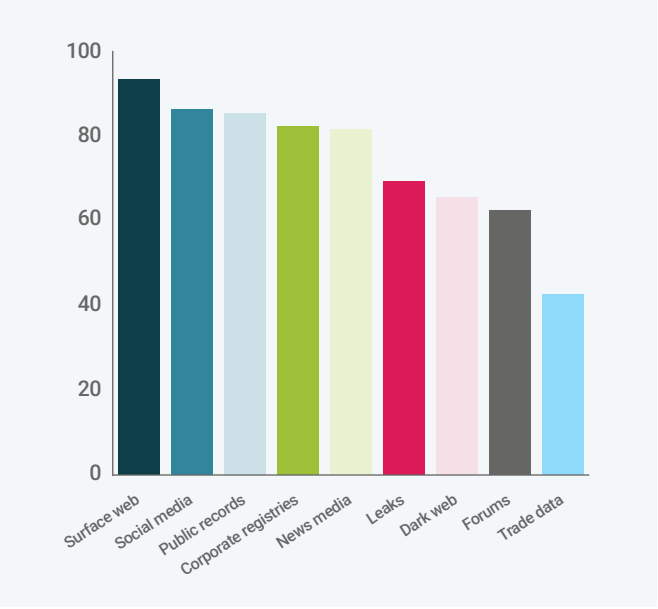
"OSINT is recognised as a "first resort" source of intelligence due to its accessibility, cost-effectiveness and timeliness."

OSINT today: top use cases and untapped opportunities

Our survey respondents are familiar with OSINT, so we expected to see OSINT usage across all sectors. Over half of our respondents reported using OSINT **more than 50% of the time**.

This majority is a good sign, but it also highlights how much ground is left uncovered. This was most pronounced in **financial services**, where **36%** of respondents used it in **0-25%** of their investigations. They also underutilise social media, with **only half of our respondents** reporting use of the source.

Respondents were asked to select all sources they use from a predefined list. The results were as follows:



Surface web data is the most popular source for OSINT, followed by **social media**. Investigators can learn a great deal from a comprehensive and well-structured search using search engines and native platforms. But this is also the slowest approach, with the greatest risk of missing key connections.

Trade data was the least popular source for OSINT, used by less than half of the investigators we surveyed. This may be because trade data tends to be less accessible, with a relatively high investment required to access the most detailed sources.

The data reveals untapped OSINT opportunities across all sectors:

- **Public sector:** Despite high levels of OSINT maturity in the public sector, **over a third of investigators say they use OSINT in less than half their cases**. This leaves potentially critical insights on the table, with forums and leaks data particularly underutilised.
- **Professional services:** These include risk consultancies, law firms and other consultancies. OSINT is already well-embedded in many investigations in this sector. But there are still opportunities to utilise the dark web more for proactive investigation of client leaks or breaches before they're made public, and trade data for competitive and market intelligence.
- **Financial services:** With the **lowest OSINT usage of all sectors surveyed**, financial services still have much to gain from more investment in OSINT, in particular the integration of social media data for uncovering hidden connections in complex money laundering or sanctions evasion cases.
- **Corporates:** OSINT usage is seemingly inconsistent across corporates. Surprisingly, the **number of corporate investigators who report using trade data (31%) is relatively low**. Increased use of trade data in particular could support the strengthening of compliance and governance across the supply chain.

The OSINT opportunity for financial services

Our survey results revealed what we already knew anecdotally: **financial services lags behind other sectors in OSINT usage**. By overlooking OSINT, financial institutions risk missing key signs of risk, leaving them open to **regulatory breaches** and **fines**.

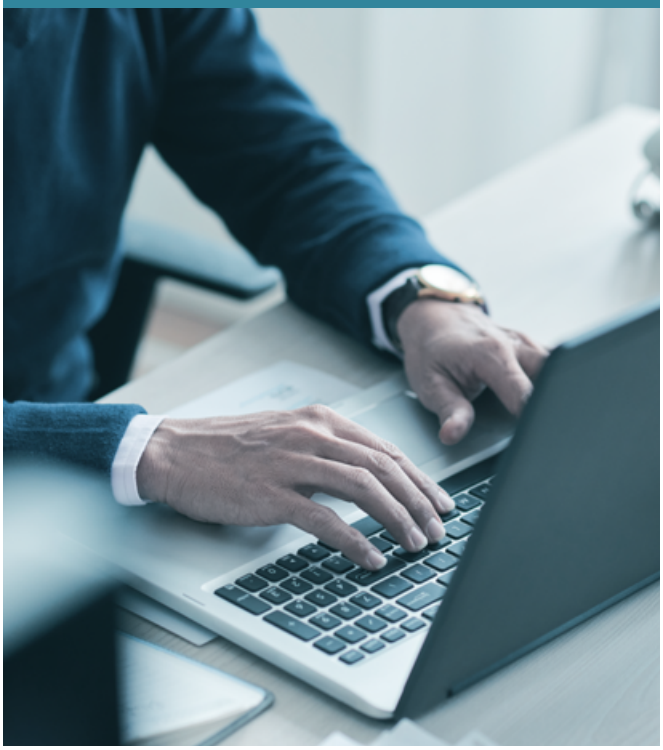
Social media, in particular, is underutilised in this sector. It has much more value to offer financial services in **financial intelligence** and **anti-money laundering**.

Traditional intelligence sources for banks (such as **politically exposed persons (PEPs)**, **sanctions watchlists** and **corporate records**) don't always tell the full story in complex cases. **Publicly available social media** can reveal connections that would otherwise remain hidden, especially in cases of obscured beneficial ownership.

In short, OSINT can help financial institutions generate a fuller picture of risk, supporting them to close more complex cases, faster.

Intelligence platforms like Blackdot's Videris allow investigators to **significantly speed up searches** and **securely, compliantly integrate them** with other intelligence.

> **AFC expert**
> Major European bank
>
> "OSINT is a great tool and a great way for investigators to really delve deeper into whatever they're investigating and get down to the true source of the matter..."



Barriers to successful investigations

We asked our respondents two questions about barriers to investigations:

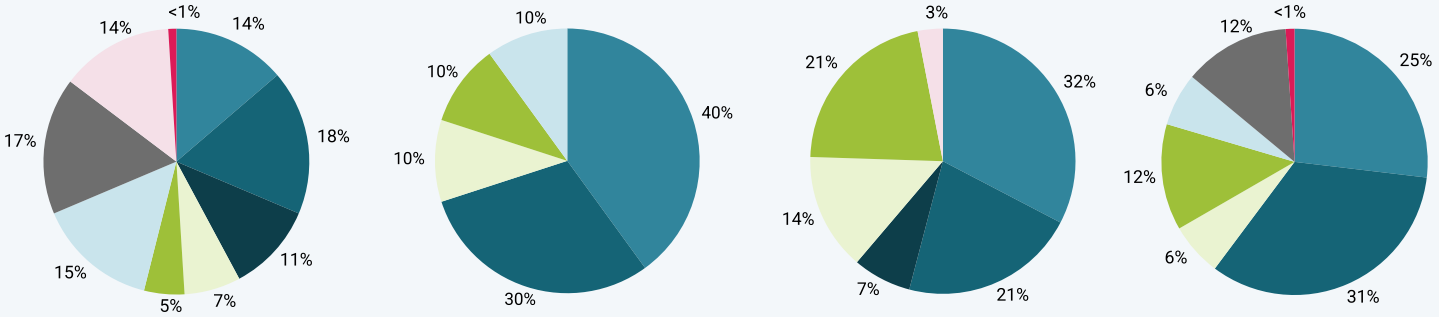
- Which is the biggest barrier you face in your investigations?
- Do you face any other barriers in your OSINT investigations?

In each case, they were asked to pick from a predefined list of barriers.

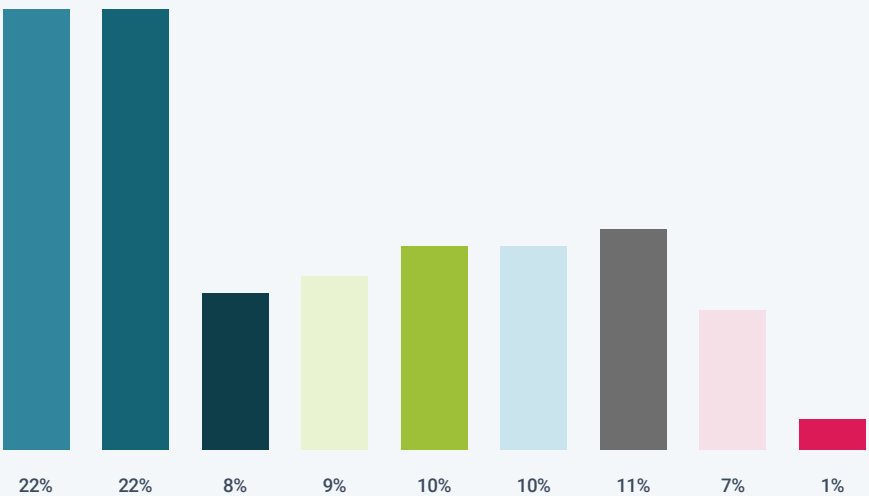
Biggest barrier to successful investigations

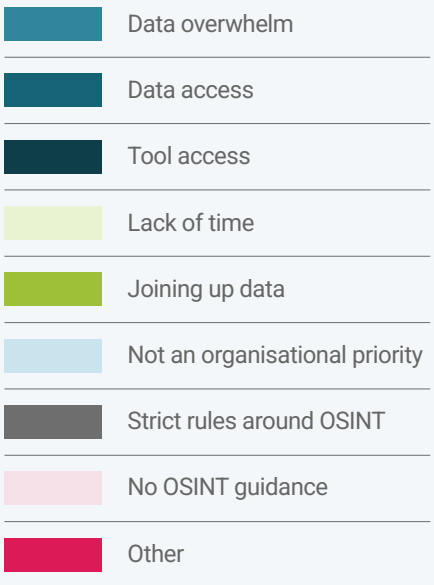
Investigators across sectors reported that the biggest barriers to successful investigations were **data overwhelm** and **data access**. Ultimately, these two challenges speak to a similar issue: investigators can't access easily the data they need.

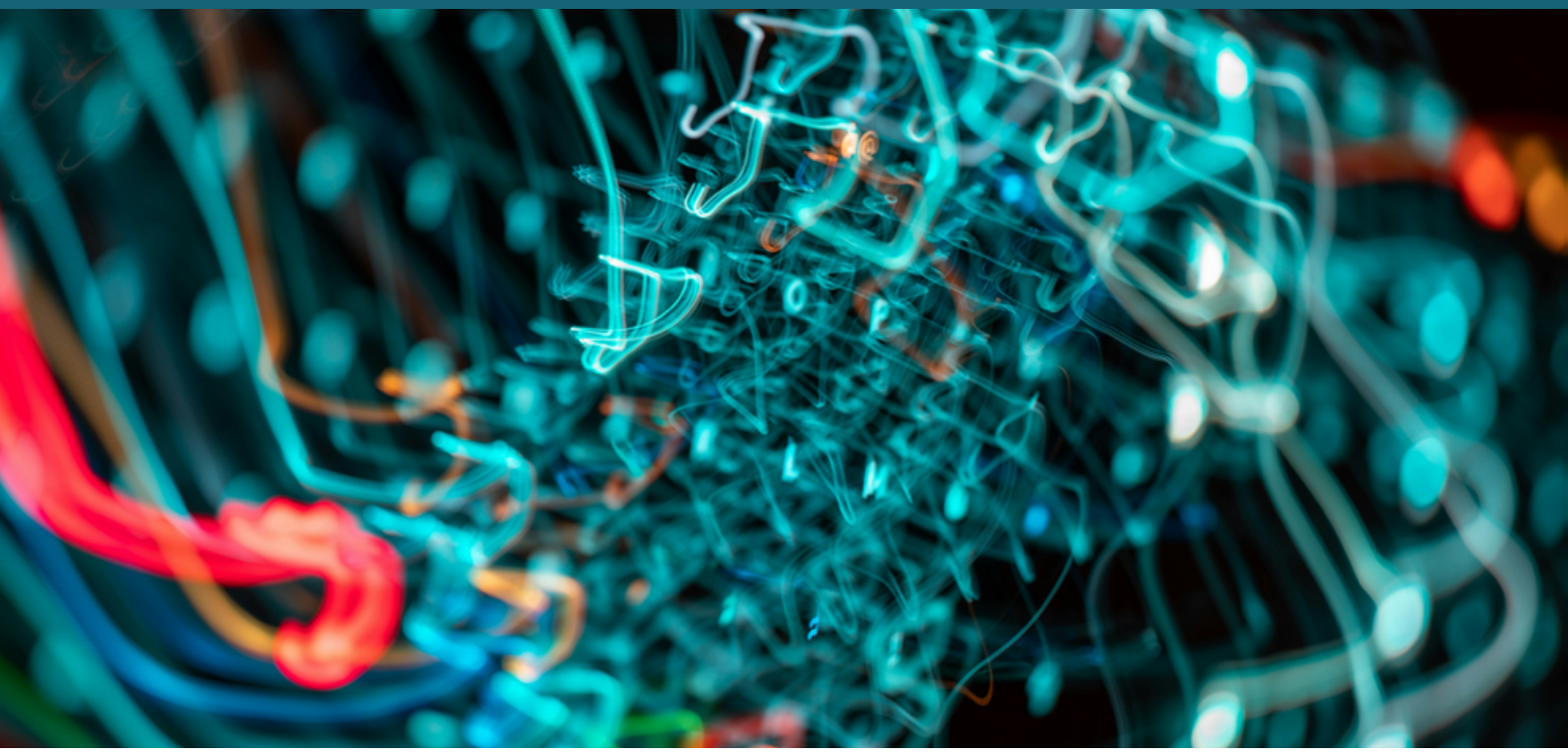
Which is the biggest barrier you face in your investigations?



All sectors







Financial services stood out as experiencing these barriers most acutely, as **over two-thirds** of the investigators we surveyed cited data overwhelm and access as the biggest barriers they faced. The lower OSINT maturity of financial services may play a role here, as investigators may not have the same level of applied OSINT experience, nor access to specialist OSINT tools.

Despite being a relatively OSINT-mature sector, **15% of public sector** investigators said their biggest barrier to successful investigations was their organisation not prioritising OSINT. This is concerning as OSINT can often be the missing piece of the puzzle, providing a more comprehensive picture of perpetrators or criminal enterprises than internal or privileged data alone.

Among **professional services** respondents, **21%** said their biggest barrier to investigations was **struggling to join up data from different sources**. This could be due to working across multiple, siloed systems from different clients, exacerbated by the need to analyse unstructured data sources such as interviews and client-supplied documents. Some OSINT tools, including Videris, can help integrate varied sources from different data sets and systems to streamline research and results.

Clear guidance or getting by?

Lack of guidance was the least likely to be cited as the biggest barrier to successful investigations across sectors.

An optimistic reading of this data is that most investigators have clear and centralised guidance on how to use OSINT in their organisation. Based on conversations with clients and free text responses to the survey, it's also possible that investigators don't consider lack of guidance a barrier, but aren't receiving this guidance from their organisation. This might mean organisations don't get the full value out of their OSINT investment, or could lead to security issues.

Other barriers to OSINT investigations

When we asked which other barriers they faced during OSINT investigations, respondents still overwhelmingly cited **data access**, with **48%** stating that this is a barrier. **Lack of time**, however, was the second most selected barrier, in contrast to the previous question.

This may be symptomatic of both increasing volumes of data and decreasing resources, as continuing economic uncertainty squeezes headcounts and budget. The right OSINT tools, especially those that lean into AI and automation to accelerate collection and analysis workflows, can help mitigate these issues.

Barrier	Public sector	Financial services	Professional services	Corporates	Total across sectors
I am overwhelmed by large volumes of data	26%	36%	38%	22%	**29%**
I can't always access the data I need	47%	55%	52%	44%	**48%**
I don't have access to the tools I need	27%	55%	24%	11%	**27%**
I don't have the time to look at everything I need	7%	10%	14%	6%	**9%**
I struggle to join up data from different sources	29%	45%	31%	39%	**32%**
My organisation doesn't prioritise OSINT	14%	36%	28%	39%	**24%**
There are strict rules around OSINT (e.g. what type of data I can access and what I can do with it.)	32%	45%	3%	11%	**24%**
There's no guidance for how I should use OSINT in my organisation	12%	36%	7%	6%	**12%**

When asked about other barriers to their investigations, **over half of financial services respondents** said they **didn't have access to the tools they need** and **just under half** said there are **strict rules about OSINT**. Financial services also faced the **most barriers** to OSINT investigations overall. This is likely another reflection of the industry's lower OSINT maturity, again underlining that the sector could be missing out on invaluable intelligence that helps close complex cases, faster.

Compliance and security concerns often come up as reasons against using certain data sources and tools, including OSINT. However, the right training and tools built with security and regulations in mind can mitigate these issues.

OSINT training: time investment and top courses

More than a third of respondents said they've spent **10+ hours** on OSINT training and development in the last six months.

Law enforcement and **professional services** spent the most time honing their OSINT skills and knowledge: **over five hours in the last six months**. This is expected given the greater OSINT maturity of these sectors, but is nonetheless reassuring, as OSINT sources and techniques continue to evolve at a rapid pace.

Financial services and **corporates** spent the least time on OSINT training and development, reporting **less than five hours in the last six months**. This correlates with the relatively lower OSINT usage levels in these sectors, likely due to the emphasis on regulatory compliance over proactive investigation.

The data represents a missed opportunity for financial institutions in particular, not only to **close complex cases faster**, but also to **get ahead of evolving anti-financial crime (AFC) regulations**. Some regulations already recommend using OSINT, and this will only increase in time.

The OSINT knowledge gap

It also revealed some cause for concern, with nearly 1 in 10 investigators across all sectors reporting **no OSINT training in the last six months**.

Even in the public sector, which is often considered the most OSINT-mature, **7%** reported **no training at all** in this time frame. This may reflect the relative deprioritisation of skills investment in OSINT compared to other intelligence forms, even within the public sector. Yet the mounting availability of online data and increasing risks posed by online disinformation make this investment even more vital.

Combined with six mentions for training courses on unregulated platforms such as YouTube and Udemy, this suggests a notable knowledge gap. At best, this can lead to **inefficiencies** and **wasted resources**. At worst, it might compromise **compliance** or **legality**.

Top 10 OSINT training provider recommendations

Vestigo took the top spot in training provider recommendations. This may be explained by the fact that many of our respondents were from the public sector, which commonly uses products sold by Vestigo's parent company, **Internet Investigation Solutions (IIS)**, and all of their trainers having operational experience.

For those sectors that don't work with IIS, **SANS Institute** appears to be preferred. It was the second most popular training provider, offering two key OSINT courses on 'Practical OSINT' and 'Advanced OSINT Gathering and Analysis'.

An independent training organisation, SANS is often seen as offering the gold standard of OSINT training. This comes with a higher course fee that some respondents cited as being cost-prohibitive. But the business case for formal OSINT training is compelling, whether it helps catch and prosecute dangerous criminals or prevent thousands (if not millions) in lost revenue.

The risk of informal online training

While mentions of YouTube and Udemy OSINT courses only formed a small portion of recommendations, we saw the same numbers as some formal training providers, such as IntelTechniques and i-intelligence.

This informal material can be a helpful primer for investigators who have never worked with OSINT before. However, enterprise organisations looking to implement OSINT in an effective, consistent and secure manner should invest in cohesive, structured training to maximise outcomes and minimise risk.

If you're looking to invest in more OSINT training for yourself or your organisation, ask yourself these questions to help build your business case:

- **Can your investigation and intelligence software provider recommend training or resources?** Like Blackdot, many providers will be able to recommend specific courses, best practices or community resources because their teams are OSINT experts.
- **How confident are you that your team's current OSINT practices meet ethical and legal standards?** Regular, accredited training reduces compliance risk and helps ensure investigations remain defensible and auditable.
- **Are your investigators spending more time searching for data than analysing it?** Structured OSINT training improves efficiency, helping teams use tools and data sources more effectively to close cases faster.
- **Does your team work to the latest security best practices?** Proper training helps teams avoid operational security risks, prevent inadvertent exposure and ensure investigations remain safe and discreet. Some OSINT tools, like Videris, will have these best practices built in.

Threat and Intelligence Manager
Public Sector

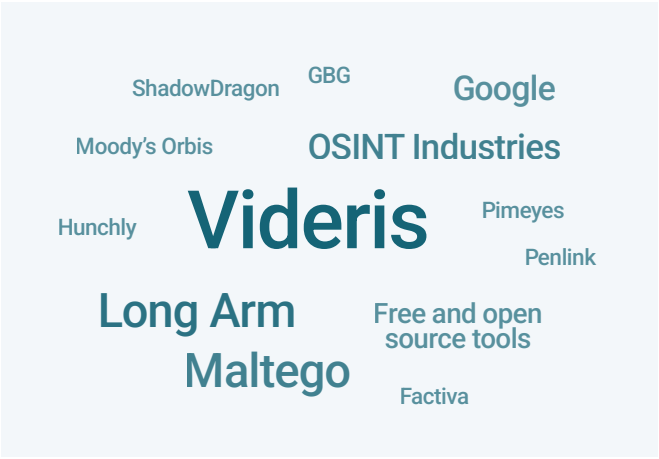
"Good OSINT training is vital for anyone involved in investigative work in our sector. It teaches people how to judge the reliability of what they are seeing, how to handle information responsibly and how to stay safe while working online. It also helps teams approach investigations with confidence and consistency, which is crucial when dealing with sensitive or fast-moving situations."

OSINT tools

Investigators were asked to answer which tools they currently use for OSINT in a free-form text format.

Amongst the most mentioned tools were **Videris**, **Maltego** and **OSINT Industries**, all of which are well-established and robust OSINT platforms. **Long Arm**, a leading secure managed attribution solution, also featured heavily, which tracks with its prevalent use in the UK public sector.

We also saw a significant number of respondents mentioning using **Google** or free tools for OSINT. These could be helping investigators plug gaps where their organisations aren't investing in paid OSINT tools, but this leaves them vulnerable to inefficiencies and security risks.



Reducing risk with the right OSINT tools

Without the right tools, OSINT can be harder due to the sheer volume of circulating data. When asked what open source data they would like access to, it was surprising that the types of information that respondents wanted better access to were sometimes not open source at all.

The data that investigators wanted more access to included:

- **Private or closed social media accounts**
- **Direct API access**
- **Breach or leak data**
- **Dark web data**

Some OSINT sources remain contested within the industry. Breach and leak data, for example, are viewed by some practitioners as legitimate OSINT and by others as outside its scope.

Private or closed social media accounts, however, are not considered OSINT because they are not publicly accessible. This isn't to say that these aren't sometimes valid sources in a public sector intelligence-gathering context, or that it cannot be useful alongside OSINT. Yet the lack of distinction highlights ongoing differences in how organisations define and apply OSINT principles, and underscores the need for clearer, shared standards across sectors.

Dark web data, on the other hand, is technically open source, but is often restricted because it has the potential to do serious harm to investigators and the organisations they work for. Accessing the dark web without the right tools risks exposure to malware, or illegal or distressing content, including imagery. However, investigators' suggestions that they would like access to dark web data underlines its potential usefulness across sectors. This is where they should consider OSINT tools like Videris, which help organisations access dark web data securely.

OSINT tool checklist

To improve the speed and impact of OSINT investigations whilst remaining ethical, compliant and secure, organisations may want to consider these factors in an OSINT tool:

Broad data access: Tools should facilitate access to a wide range of publicly available and licensable data sources. They should also allow organisations to integrate proprietary or internal sources for a full intelligence picture.

Ethical approach to data processing: Tools should focus on the targeted, proportionate collection of publicly available or licensable information.

Inbuilt audit tools: Features such as logging and sourcing enable legal and policy compliance, as well as consistency and accountability.

Secure by design: Tools should enable safe, anonymous access to OSINT data, ensuring that organisations do not risk tipping off subjects of investigation or downloading malware.

Threat and Intelligence Manager
Public Sector

"OSINT tools add real value by making it possible to sift through large amounts of open information quickly. They help investigators spot early signs of potential threats, follow activity across different platforms, and build a clearer understanding of what's going on without wasting time on manual searches. The tools don't do the thinking for us, but they make the job more efficient and the insights more reliable."

OSINT and AI: what does the future look like?

When asked to rate their feelings on the potential impact of AI on their investigations, **70% of our respondents had a positive outlook**. **Professional services** were the most optimistic, with **86%** saying they were either **somewhat positive or positive** about its impact. The **public sector** was the least optimistic, with only **62%** expressing any positive sentiment.

This positivity comes largely from AI's ability to speed up time-consuming tasks—around **three quarters of respondents** said its greatest impact would be on **data collection, processing and analysis**.

Over half of respondents directly referenced **speed and efficiency gains**, saying that AI has the potential to cut down on research time and automate manual work. This will allow investigators to focus on the more complex and strategic work that closes cases and provides increased job satisfaction.

Clearly, most investigators feel no existential threat from AI and see it as an enhancement to their role rather than a replacement.

Videris Automate

Some of this positive perspective on AI may be thanks to tools that already use AI to augment an investigator's capacity, such as Videris Automate. With it, investigators can:

- **Accelerate data workflows** using custom playbooks and agentic AI.
- **Automate low-level analysis** with best-in-class large language models (LLMs).
- **Retain control and compliance** with human hand-off and full explainability for reasoning, sources and evidence.

Will OSINT grow as a priority?

Reassuringly, the **majority of our respondents** expected their organisations to **continue investing in OSINT** over the next five years, with **58%** suggesting that they will **invest more**. This underlines the mounting strategic value of OSINT in investigations across sectors, with particular optimism from **professional services**, where effective use of OSINT can be a competitive differentiator.

The future of OSINT: human-led, AI-enabled

OSINT is now an investigative mainstay. Across sectors and geographies, it's shaping how organisations respond to intelligence requirements. This report shows established use across both traditional intelligence-gathering organisations such as law enforcement, and less traditional, such as financial services, where OSINT has a significant role to play in fighting financial crime. But it also highlights how many untapped opportunities remain.

The data reveals impressive uptake, but also underused sources, inconsistent access to training and significant barriers holding skilled investigators back. **The value of OSINT depends on the people and systems behind it**. Investigators need stronger institutional support, from leadership, compliance teams and technology partners, to turn data into actionable intelligence. That means investing in formal training, tailored guidance and tools that streamline the process.

AI will accelerate this evolution as its strength lies in scaling and speeding up processes. The next phase of progress will blend human judgment with AI efficiency, freeing investigators to do the complex, contextual thinking that only people can do.

The best investigations of tomorrow will still be human-led, but with sharper tools, faster insights and smarter systems increasing their impact.