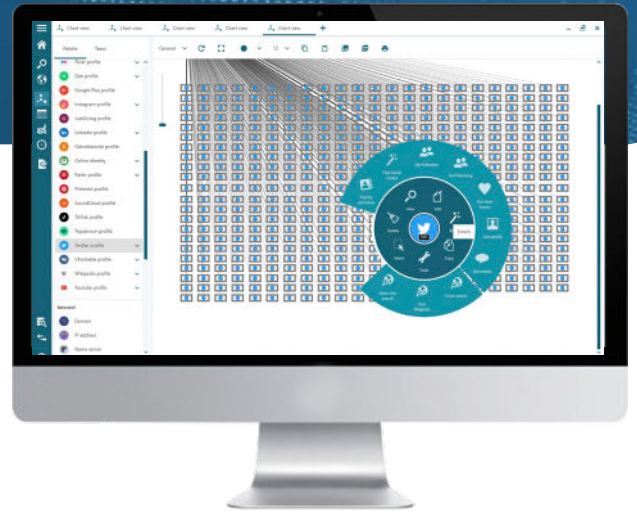# videris

Open Source Intelligence & Investigations Platform

Videris helps government agencies transform their OSINT investigations processes. It acts as a single pane of glass for Open Source Intelligence, bringing the whole of the investigator's workflow into one platform.

Why Videris?

Future-proof your OSINT strategy
OSINT plays an increasingly vital role in the intelligence spectrum. Invest now in intuitive technology to support and enhance the future strategic use of open source data.

Find and reduce risk, fast
Avoid hours of scrolling to find key risks: specialist risk searches, advanced filtering and automated risk flagging ensure that important information is brought to the investigator's attention.

Reduce complexity with a single point of truth
Videris saves investigators days by combining disparate sources into a single interface, as well as fusing internal or privileged data with OSINT.

Gain information advantage
Find connections and insights that would have been impossible to identify manually. Videris offers intuitive visualisation capabilities and automated network mapping to ensure that no link is missed.

Secure by design
Remove security concerns and avoid wasting time obscuring your identity: Videris keeps investigators secure and anonymous, automatically.

Flexible deployment and unrivalled support
Videris can be deployed in the cloud or on-premises: we'll work with you to find the best solution for your organisation. Training and support are included with every licence: there are no hidden costs. Once you're set up, we offer the training and support you need to get the return on investment you expect.
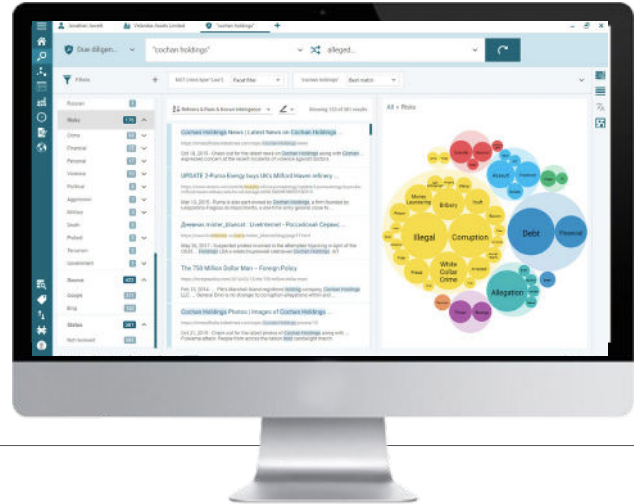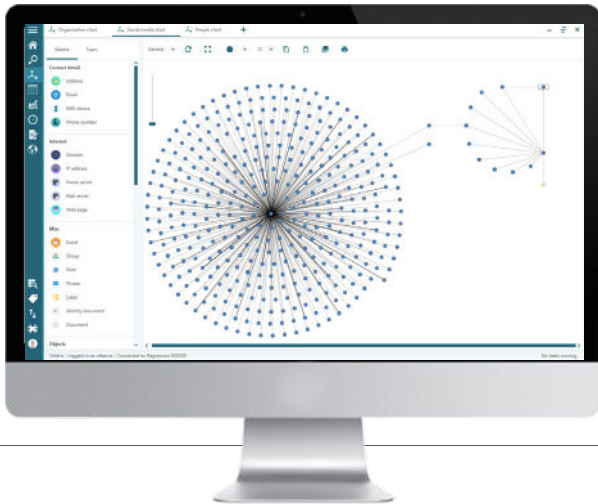
HM Government
G-Cloud
Supplier

blackdot
solutions

Use Cases

Security agencies and law enforcement use Videris on a global scale, for investigations including:

Counter Terrorism: use Videris to identify targets and their networks:
- Explore an individual's online presence and quickly map their network of associates
- Use location filtering and relationship strength analysis to find their closest connections
- Analyse social media content to establish a pattern of life

Counter Intelligence: connect different data sources to identify state actors:
- Quickly identify relevant adverse media: Videris prioritises key risks in any language
- Map corporate records and automatically see matches in global risk databases
- Use social media network analysis to verify connections to hostile state actors

Serious & Organised Crime: identify complex criminal networks and evidence their activity:
- Collect data from multiple sources, map connections and visualise international networks
- Easily record evidence by automatically capturing sources – even if the source is removed from the internet

Border Crime: find and disrupt international people and narcotics trafficking networks:
- Use integrated global corporate records to understand complex corporate structures supporting criminal enterprise
- Intuitive visualisations of social media connections enable the rapid identification of co-conspirators and evidence of crime

Economic Crime: quickly find anomalies within corporate networks:
- Use Videris corporate network mapping to identify connections to businesses and resolve unexplained wealth
- Find and prove connections in fraud investigations by analysing corporate data and social media

CONTACT
Jake Taylor
Head of Public Sector
jake.taylor@blackdotsolutions.com

blackdot
solutions