KAPSUUN GROUP
A Chenega company

OSINT (INFORMATION AS A SERVICE)

According to We are social the number of worldwide internet users is in excess of 5 billion with the global total rising by 200 million in the last year alone. 63% of the world's population is now online while the number of active social media users is over 4.65 billion. This is only expected to grow with estimates of over 30% of the world's population using social networks in January 2022. UK Millennials are the largest group to participate in social media usage with over 84% saying they use some form of social media every day.

Consequently, OSINT has become a critical component of modern information / intelligence gathering by law enforcement seeking to protect the communities they serve or businesses seeking to protect the people, infrastructure, and reputation of the businesses they operate.

What does our open-source capability add to your security capability?

An open-source harvesting resource is very useful when you're trying to find out more about an individual, an organisation, activist groups, their connections, planned or dynamic protest events, corporate image protection, at risk infrastructure protection, threat, risk and harm analysis across a wide range of both non-criminal and criminal domains.

Are there problems using open sources?

Generally speaking, the key problem with using open-source data is the amount of manual work involved for analysts and investigators. The quantity of data available can be overwhelming and it can be hard to find the most relevant sources applicable to the threat or investigative problem. High data volumes also make the connections that open-source data reveals hard to spot.

How do we solve this problem to give you a timely information report?

We use state of the art technology that permits us to access the material of most interest to you, in a timely fashion allowing you to better deploy resources or put in place protective measures to mitigate threat, risk, or harm scenarios.

Why use us?

Those with nefarious intent such as criminals or activist groups have become much more aware of their online security. Today it requires first rate analytical, and research skills to extract useable information without being detected and potentially embarrassed by the target of the investigation. Our team have the necessary skills and state of the art technology to ensure this does not happen.

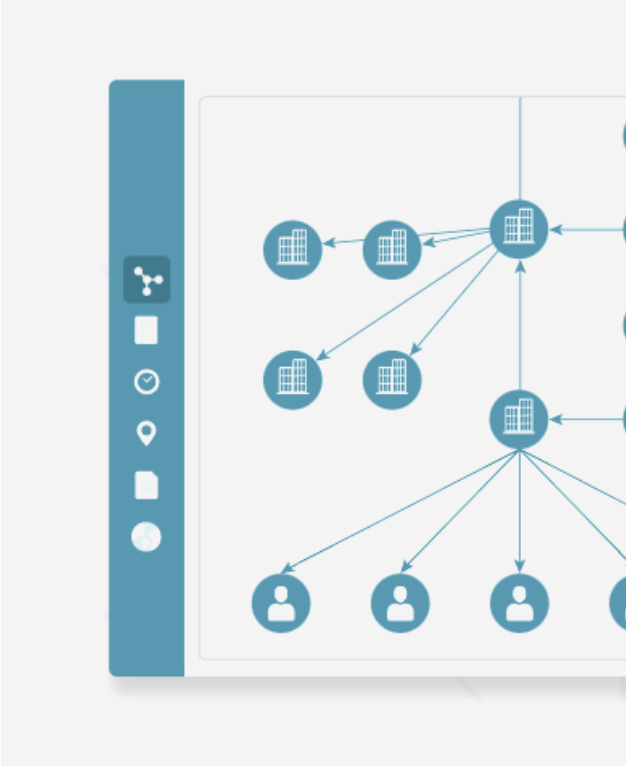
How do we generate our content?

- We harvest open-source data including corporate records, media reporting, open social media, and domain registration information.
- We use Intuitive visualisations of social media connections to enable the rapid identification of co-conspirators and evidence of crime.
- We use integrated global corporate recordsto understand complexcorporate structures supporting criminal enterprise.
- We quickly identify relevantadverse and if required positive media reporting.
- We prioritize key risks in any language.
- We map corporate records and automatically see matches in global risk databases
- We use social media networkanalysis to verify connections to hostile actors.
- We can explore an individual's online presence and quickly map their networkof associates.
- We can use location filtering and relationship strength analysis to find their closest connections.
- We analyse social media content to establish a pattern of life.
- We collect data from multiple sources, map connections and visualise national and international networks.
- We can record evidence by automatically capturing sources even if the source has been removed from the internet. This is particularly useful if members of your team have received threats, or your company has been the subject of malicious disinformation or misinformation.
- We use corporate networkmapping to identify connections to businesses and resolve unexplained wealth. Extremely useful if you are facing a threat from individuals.

Why is our investigative software suite unique?

Our software suite uses a number of platforms and tools providing our clients with a much more in depth picture than reliance on singular platforms can do. The tools and platforms used don't just help our investigators to visualise data, it allows them to find and analyse it too.

- Open platform – investigators can integrate any source they need and combine it with live internet data to gain a full view of a subject of interest
- Industry-leading social media mapping and analysis functionality
- Ability to search unstructured data sources (like search engines and blogs)
- Automatic cross-referencing suggests hidden connections
- Integrated web browser allows secure, anonymous viewing of web content
- Dedicated note-taking view for collecting text-based content and exporting a full report
- Financial searches



Dark Web Integration:

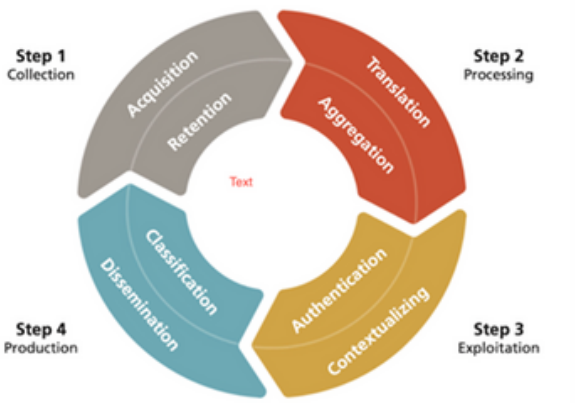
The Dark Web is a hub of criminal activity, including fully functional illegal marketplaces, open forums and chat rooms. This integration gives us the ability to assist our clients get greater visibility of the shadows of the internet, allowing them to search for information and map out networks found on the Dark Web.

How do we manage your tasking requirements?

We form a tasking and coordination group (TCG) that will meet regularly with you to agree search and report parameters around key areas such as:

- Protecting life and property
- Preserving order / preventing disorder / preparation for lawful protest
- Preventing the commission of offences
- Bringing offenders to justice
- Identify problems and subjects of interest.

OSINT Operations Cycle



Our TCG process provides our clients with a mechanism that assists operational decision making at both strategic and tactical levels, saving time and wasted resources. The process is continually reviewed to evaluate generated content and,

- Assess the impact of tactical activity on a problem or subject
- Identify lessons learned or good practice
- Draw conclusions and make recommendations
- Update policy, knowledge, the menu of tactical options and training

Because of our skill in this arena, we have been chosen to provide university accredited training to the following law enforcement agencies and government departments.

(The UK Cabinet Office, HM Forces UK, Merseyside Constabulary, An Gardai Siochana Ireland, Australian Army, The German police Service, The Danish police service, Italian police service, US National Guard, US Department of Defence, US Internal Revenue Service, Aerospace and Defence Security USA, United Nations Office on Drugs and Crime Kenya, and the Mexican Government, Frontex.

CONTACT US

John Soper / john.soper@chenega.com

Matt O'Hanlon / mohanlon@chenega.com

Tamara Himmelberger / tamara.himmelberger@chenega.com

Paul Hillis / paul.hillis@chenega.com