From Scattered Clues to Solid Conclusions

Data fusion helps analysts identify patterns and trends to advance criminal investigations.

SS8® Securing Societies Always

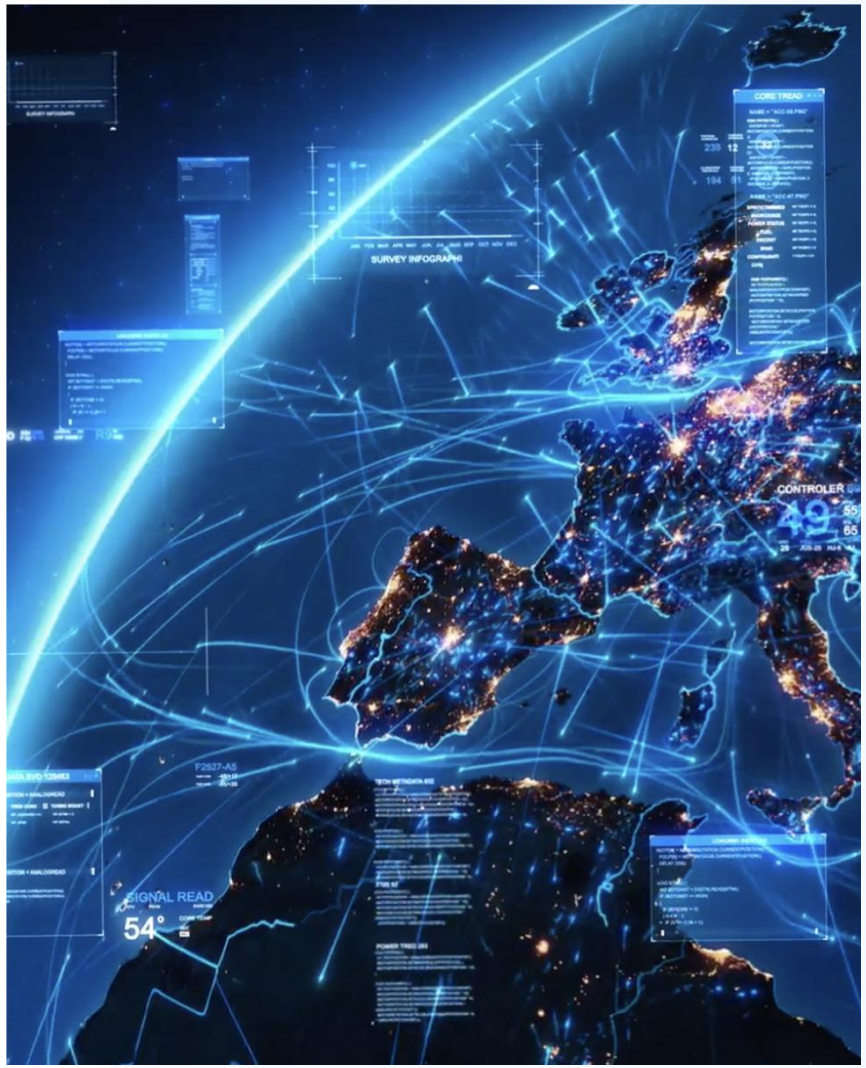
Executive Overview

Data-driven investigations require access to an expanding universe of information, but even more so on making separate data points each reveal their payload of context and significance to the whole.

With a combination of access and intelligence, the SS8 platform maximizes the value of every data source to analysts. OSINT epitomizes the enormous volume, velocity, and variety of data underlying today's investigations.

The integration of diverse information sources and the extraction of meaningful insights from them marks the shift from lawful interception to lawful intelligence. Breaking open cases with monolithic evidence such as the contents of phone conversations is now largely a thing of the past. In its place, investigators must solve puzzles without clear starting points, linking together shadows of insight to find their way.

SS8's lawful intelligence Platform applies data fusion and analytics technologies as foundations to unify and understand scattered OSINT and other data. Combining the breadth of a massive data universe with a depth of investigation down to the packet level of data streams and beyond, it puts powerful control in the hands of law enforcement.



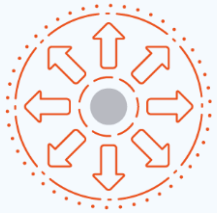
Data in Criminal Investigations

MORE FOOTPRINTS, BUT HARDER TO TRACK

We leave traces of our behavior in the universe of data around us every day. They range from the digital footprint of sending a text message, to (somewhat) anonymous posts on social media, to personal information available without our knowledge on the dark web.

These sources have proliferated in the past decade or two. Before smartphones, the traffic from an authorized wiretap consisted almost exclusively of voice calls and text messages. Today, our smartphones use over-the-top (OTT) communication apps, such as: WhatsApp, Signal, Facetime, and Telegram; social media OTT apps such as YouTube, LinkedIn, TikTok and Snapchat; online banking and many others. The power in the latest models of smartphones coupled with the high-speed networks (such as 5G and WiFi) on which they access data are driving up data usage, with each subscriber expected to use 40 GB per month by 2027. Complicating analysis further is that nearly all of this traffic is encrypted.

Criminals have always been early technology adopters, taking advantage of anything and everything available to hide their actions. Alongside other new challenges, AI-assisted crime re-emphasizes the need for law enforcement to keep up in this arms race.



Proliferating Media Sources

Massive Bandwidth

Content Encryption

Data in Criminal Investigations

THE SHIFT FROM INTERCEPTION TO INTELLIGENCE

Criminal suspects and their associates have become harder to monitor, as IP traffic from the many encrypted over-the-top (OTT) apps used for the criminal enterprise blend with huge amounts of innocuous Internet traffic. With many of these OTT apps leveraging end-to-end encryption, decryption is not an option. Adjusting to this new reality, investigators close the gaps by requesting records directly from the OTT app providers, call data records (CDRs), open-source intelligence (OSINT), and geolocation. This adjustment is really a move from lawful interception to lawful intelligence, with a deeper focus on data management and analysis.

Building Blocks of Insight

OPEN-SOURCE DATA includes publicly available information such as news content, social media, and public records. Some open-source data may not be publicly searchable, such as documents behind paywalls and commercial databases such as LexisNexis and Westlaw.

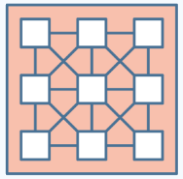
Open-source data also includes dark web content, which is not searchable by ordinary search engines and requires specialized software to access. Open-source data can be inaccurate, unstructured, or lacking in context.

PRIVATE DATA includes information held by third parties and is provided under legal order. Examples include automated number plate reader (ANPR) data, call detail records (CDR), financial records or business records.

DATA FUSION is the process of unifying data from multiple sources into a single analytical framework. By integrating and analyzing sources together, they can be cross-correlated to corroborate and provide greater context for each other.

Even small bits of information that are not individually useful may provide insights when aggregated together. By automating data fusion and analysis functions, investigators can improve the efficiency and accuracy of their conclusions.

Data fusion may operate on open-source data, private data, restricted information (lawfully intercepted communications), or a combination of the above. It may also combine real-time data sources such as cameras and sensors with historical data such as social media profiles and travel records.



OSINT Uses data fusion and other methods to extract insight from open-source and private data to serve specific goals. In the context of an investigation, it is actionable intelligence that can be obtained without a subpoena, warrant, or other authorization.

In addition to stitching together scraps of information using context provided by data fusion, OSINT helps investigators characterize a level of confidence in the accuracy of open-source data and the conclusions based on it.

OSINT may reside in multiple tools built for different domains, such as advertising, fraud detection, and cybersecurity. Investigators need mechanisms that enable access to that range of tools, including the ability to query and import data from them.

Rising Stature and Depth of Data Analytics

THE NECESSITY OF MACHINE-BASED INTERPRETATION

This transition from lawful interception to lawful intelligence marks a shift in investigator focus from intercepted communications to far larger, more complex and diverse data sets. At the same time, the information such as metadata and location data that investigations now rely on is not easily parsed or understood by humans. That means that, where it used to be standard practice to manually review intercepted messages and identify their significance, that is no longer possible.

In broad terms, the data analytics that lawful intelligence relies on are analogous to reading a piece of text. That is, both involve parsing information: analytics let computers generate insights from data, similar to humans discerning meaning from words. Analytics makes it possible to understand patterns and trends that power data-driven decision making by LEAs. Those processes are also largely automated, dramatically improving resource efficiency for investigations.

AUGMENTING DATA ANALYSIS WITH AI

AI extends the capabilities of analytics, giving computers the ability to identify more complex relationships in data and create deeper insights from it. Machine Learning (ML), a key part of AI, relies on training to learn patterns. Leveraging components like ML, AI can reason, solve problems, and identify objects in photos or video.

Predictive analytics applies ML and AI algorithms to identify the likelihood of future outcomes based on historical data. Such tools could help LEAs identify specific areas and times to allocate resources where they will be most effective at preventing crime. Similarly, augmented policing models can monitor sources such as news sources, crime reports, and social media to predict civil unrest, so personnel can be deployed proactively to prevent violence and protect the public.

SUCCESS STORIES: APPLIED DATA ANALYTICS FOR INVESTIGATIVE INSIGHT

Bringing Down the Conti Ransomware Group

Conti ransomware targeted hundreds of critical systems before a researcher leaked over 60,000 internal chat messages, source code, and operational documents, exposing the group's structure and methods. Timeline analysis of chat logs linked key discussions and participants to specific attacks. The leaks detailed how Conti leveraged VPNs, cryptocurrency, and obfuscation techniques, aiding investigators in unmasking its members. Examination of the source code revealed the ransomware's capabilities, while financial transaction mapping exposed its business model—contributing to the group's eventual takedown.

Mapping Out a Shooter's Path to Radicalization

In 2022, the perpetrator of a racially motivated mass shooting livestreamed the attack, allowing analysts to quickly identify him and reveal his online manifesto of hate. Digital forensics reconstructed the shooter's online activity by analyzing post histories, timestamps, and account creation dates. They conducted content and linguistic analysis of his writings, identified users who interacted with his content, and identified radicalizing influences with the hope of understanding his motivations and preventing similar events in the future.

SS8

Unifying Breadcrumbs with Data Fusion

By integrating data from diverse sources, data fusion adds the context that gives it meaning. Data fusion increases the value of the fragmented data and uncovers connections between them that drive insights to propel investigations forward.

AGGREGATING AND PREPARING THE DATA

Creating a comprehensive dataset for analysis requires gathering digital breadcrumbs and data streams from every relevant and available source. Information from both open-source and privileged sources accumulates as raw, dirty data. Incompatible formats, redundancies and gaps, varying degrees of reliability, and a lack of overall structure complicate analysis. Data must be scrubbed, structured, and indexed in this early stage to facilitate analysis.

With streaming video services such as Netflix and Hulu accounting for 80% of traffic, transforming these channels into useful information without requiring additional storage is critical. Packet Header Information Reporting (PHIR) does this by processing packet headers to identify data payloads The presence of the PHIR allows for the billions of packets to be stripped out of the investigative dataset, avoiding the extraneous overhead and cost of analysis and storage, all without relying on encrypted packet contents.

SS8's Enhanced Protocol Extraction Engine (E-PXE) uses enhanced deep packet inspection and heuristic analysis to gain even deeper visibility onto encrypted traffic flows. It looks at the nested headers of encapsulated traffic to generate metadata that reveals application-level characteristics. These include the specific communication modality (text, voice, video) and the devices and IP addresses involved in data flows, as well as the specific application or service such as WhatsApp or Telegram associated with each.

SS8

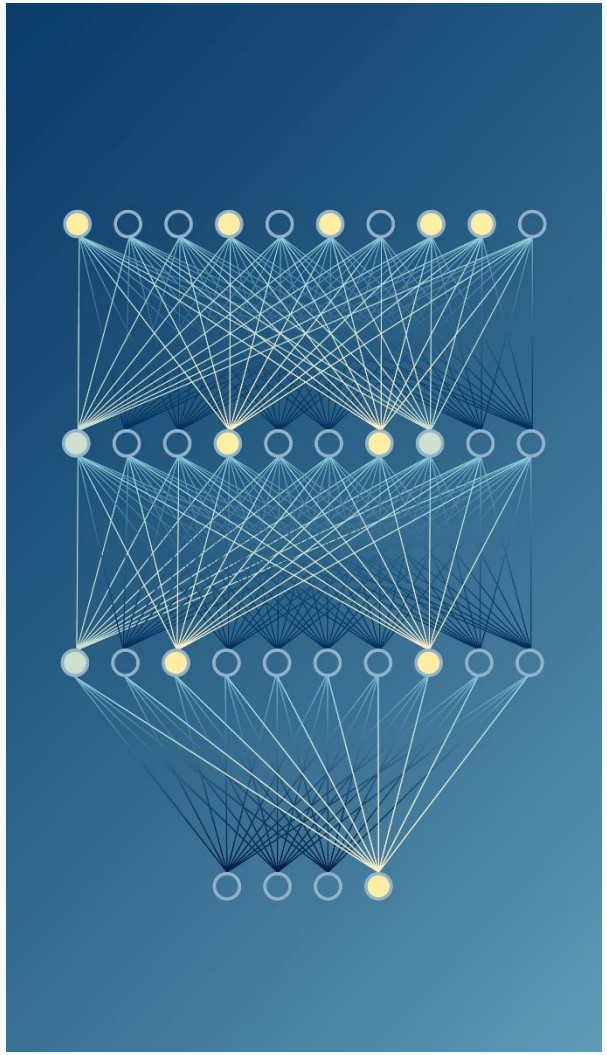
IDENTIFYING RELATIONSHIPS AND PATTERNS

Transforming data into intelligence requires understanding the connections within accumulated data, such as a subject of interest's conversations and meetings with other subjects, presence at critical events, etc. Development of tools and techniques for this process of data correlation continues to accelerate, with AI adoption, improved algorithms and more powerful computing systems.

Such insights can be pieced together to reveal relationships, such as when two parties call each other. Location intelligence plays an increasing role in correlating data together, building insights from the physical locations, movements, and proximity of individuals and events. Investigating the regular behaviors and activities of individuals or groups enables their patterns of life to be established, such as locations frequented, travel routes, and social interactions.

The intersections among these patterns reveal connections between people and events, including hierarchies in criminal organizations, expanding or deepening the scope of investigations. Once long-term behaviors have been established, changes in trends such as spending habits or online activity may indicate shifts in priorities or intentions. Likewise, anomalies and deviations from regular patterns can signal potential threats and suspicious activities that warrant further investigation.

The SS8 platform integrates iDossier as a tool to create and manage detailed data-driven profiles of individuals and organizations, including photos, audio, and video. an iDossier may include identifying information such as date of birth, address, and employment history, as well as notable activities like attendance at events or presence in the vicinity of a crime. Investigators query the iDossier database to reveal insights from individual profiles and combinations to uncover hidden connections and reveal the workings of criminal networks.



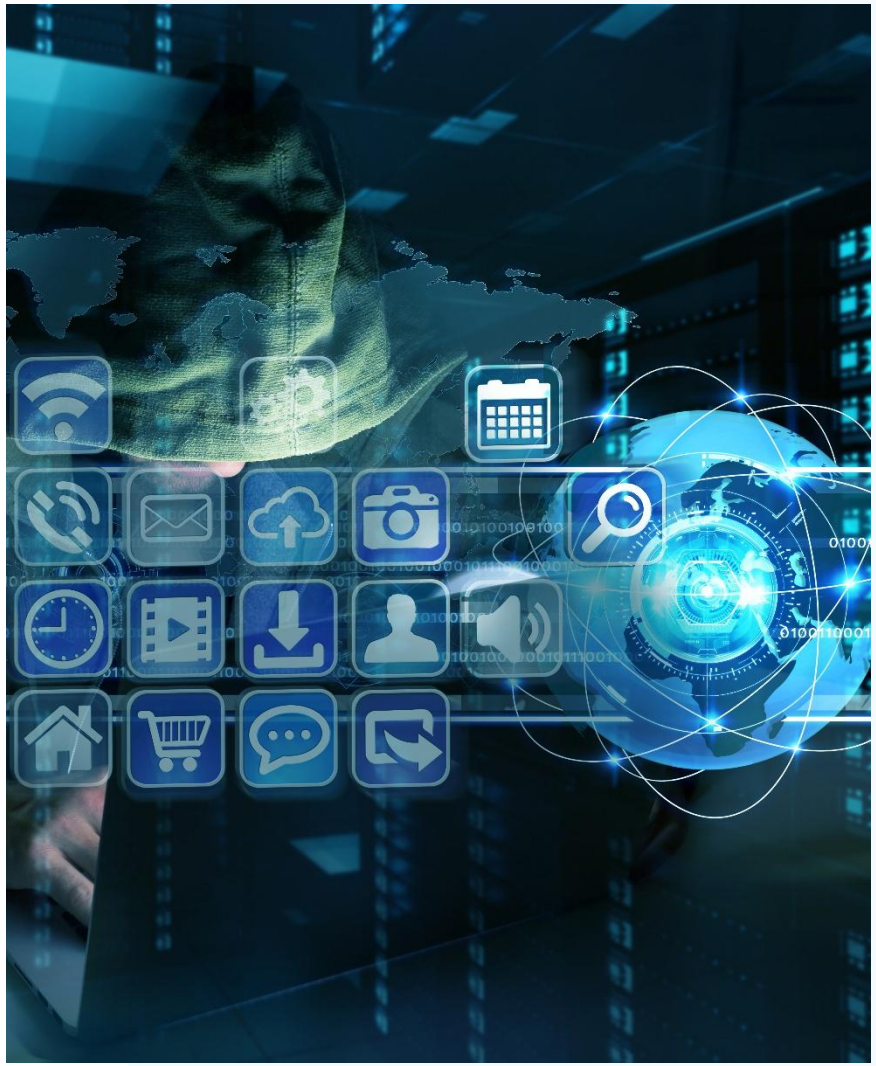
SUCCESS STORIES: UNITING REAL-WORLD THREADS USING DATA FUSION

Tracking Down Ghislaine Maxwell

After Jeffrey Epstein's arrest, his co-conspirator Ghislaine Maxwell went into hiding. She used aliases, changed phone numbers frequently, and relied on intermediaries to manage her affairs. Investigators used corporate and real estate records to map Maxwell's associates and properties, connecting shell companies through common addresses. They monitored transactions and identified a suspicious $1.07 million, all-cash purchase by an anonymous LLC for a property in Bradford, NH. Unifying that data with physical surveillance and cell phone signal analysis provided further evidence, eventually bringing Maxwell to justice.

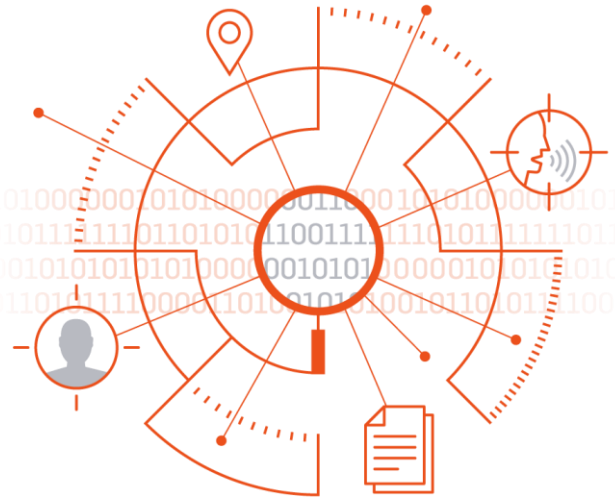
Ending Human Trafficking Networks

The shutdown of backpage.com in 2018 created a fragmented sex trafficking landscape that was harder to enforce against. Researchers fused together linguistic analysis to link escort advertisements together, image analysis to recognize common backgrounds, and phone number analysis to link ads across regions. They analyzed metadata for location and device information, and timeline visualizations to reveal movement patterns of victims. When trafficking was suspected, additional OSINT techniques, like social media analysis and public records searches, were used to build profiles of traffickers and work toward eliminating their operations.



Revealing Insights That Advance Investigations

Regardless of present and future developments in lawful intelligence technologies and practices, there will be no silver bullet—including AI—to solve all challenges.



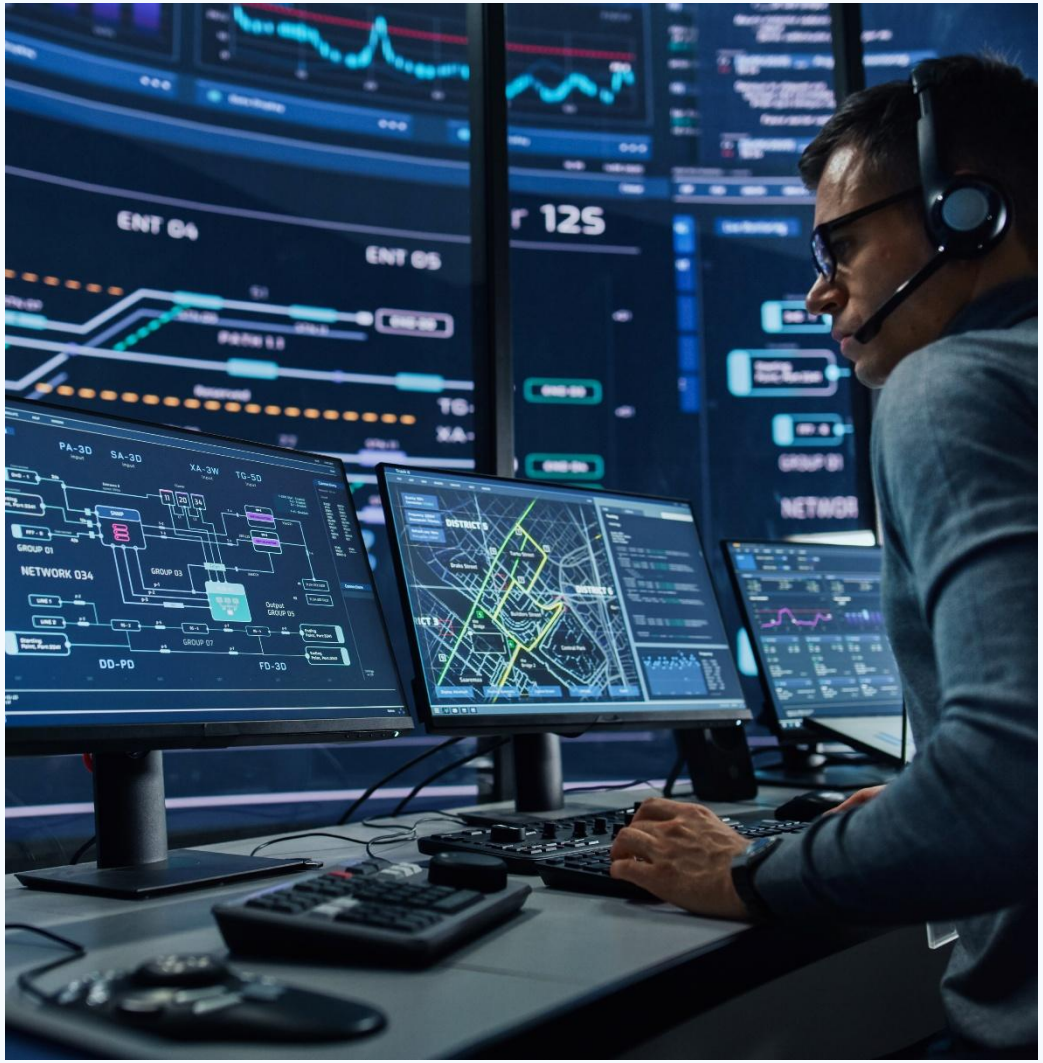
The ability to handle data beyond human scale and speed will augment the investigative pipeline in important ways, including to correlate data and reveal deeper insights. AI-based natural language recognition will provide speech-to-text and language-translation services, even in real time, to transform streaming audio and video into a searchable form.

Still, technology developments will provide new tools and methods that multiply the abilities of analysts, rather than fundamentally changing lawful intelligence. The SS8 lawful intelligence environment seamlessly integrates its components in a cloud-native platform that complies with 3GPP, ETSI, and other international standards. Together, they form a comprehensive pipeline to collect, aggregate, correlate, and integrate OSINT, location intelligence, and intercepted data.

HIGH-VOLUME INTELLIGENCE IN REAL TIME: INTELLEGO XT MONITORING CENTER

Intellego XT is the umbrella platform for SS8's lawful intelligence environment, built to ingest the massive data flows in 5G networks and beyond. It provides robust data protection, including cybersecurity, warrant management, and access controls, streamlining adherence to regulatory and audit requirements, including CALEA in the US, the Investigatory Powers Act in the UK, and equivalents elsewhere.

The Intellego XT Monitoring Center ingests data related to subjects of interest in real time, including intercepts, OSINT, and other sources. It also provides automatic analyst notifications of developments such as specific communications or location changes. Monitoring Center transparently reconstructs voice calls, data transmissions, and communications text within the broader context of investigations, to build timelines that reveal chronology and causality of events. The environment indexes all data, including voice, video, location, metadata, and its powerful forensics interface gives analysts a streamlined path to reveal multi-dimensional relationships within it.



DATA FUSION AND ADVANCED QUERY: INTELLEGO XT METAHUB

SS8 MetaHub fuses together and queries against lawful intelligence data from intercepted communications, OSINT, financial records, ANPRs, and other sources, including third-party data feeds. It is designed specifically to combine many unstructured data sources together to enrich each other, revealing insights through analytics and dashboards that offer timeline, mapping, and event grid views. MetaHub may draw OSINT from the SS8 environment itself or an external collection tool, and it can be deployed in conjunction with Intellego XT or as a stand-alone resource.

Analysts maintain an overall perspective of the entire investigation, with the ability to easily drill down into specific details, as well as real-time monitoring capabilities. MetaHub supports “multi-queries,” an advanced type of query that improves insight by searching beyond individual events to sequences of events within set time periods. It also builds productivity with automated, scheduled searches to detect changes while freeing analysts for other tasks. These capabilities combine to provide sophisticated, holistic, dynamic analysis of the relationships among both incoming and retained data.

LOCATION INTELLIGENCE AND VISUALIZATION: INTELLEGO XT GLOBE

Intellego XT Globe provides location identification, monitoring, and geofencing capabilities for lawful intelligence and other uses. In particular, it associates specific subscriber identities based on a device’s MSISDN, IMSI, or IMEI with their changing locations over time to provide location intelligence and contact tracing. Combining a variety of multilayer street-level and satellite-based digital maps, Globe visually tracks the location, direction, and velocity of movement.

Globe can automatically report on the geographic proximity of subjects to each other, helping understand interactions and relationships, including reconstructing and replaying historical movements of multiple subjects. It provides rich geofencing capabilities, defining areas of interest around physical locations as polygons on a map. Analysts can identify who is and is not inside that boundary at specific times, as well as alarming when subjects of interest cross it. Globe can be deployed as a standalone location application or in conjunction with LocationWise, SS8’s broader location-based services solution.

Conclusion and Future Developments

SS8's platform is built by investigators, for investigators, with capabilities designed to tackle evolving challenges—ranging from encrypted communications to shifting geopolitical landscapes.

Looking ahead, advancements in AI and computer science will further enhance investigative possibilities and efficiency. As algorithms become more accurate and reliable, SS8 provides the expertise and guidance needed to maximize their full potential.

That role includes balancing investigative realities against regulatory and privacy requirements. The quality and degree of insight and automation contribute to the success of law enforcement. At the same time, the rule of law will always require manual processes such as making the case for a warrant before a judge. The SS8 platform augments investigative intelligence to improve efficiency while observing and protecting legal frameworks.

From the faintest clues, the SS8 platform makes it possible for analysts to build investigations, successively adding visibility and insights that overcome the complexity of a world awash in data. OSINT contributes an unlimited number and variety of data sources, most of which are irrelevant but any of which may contribute vital evidence. Intellego XT and its supporting components sift through massive datasets and harness their potential, to shift the balance of power away from those who would do harm, toward those who protect the common good.

SS8

About the Authors

Dr. Cemal Dikmen - As SS8's Chief Technology & Security Officer, Cemal plays an integral role in the company's strategic direction, development, and future growth. A renowned expert and thought leader in the legal compliance and communications analysis domain, he has been a frequent speaker at various industry conferences over the past 10 years. Cemal holds BS, MS, and PhD degrees in Electrical Engineering. You can learn more about Cemal on his LinkedIn profile by clicking into his LinkedIn profile https://www.linkedin.com/in/cemal-d-264427/.

Kevin McTiernan - Kevin McTiernan is a seasoned professional with over 20 years of experience in the security industry. His extensive expertise spans big data, cybersecurity, network security analysis, and regulatory compliance. As Vice President of Government Solutions at SS8, Kevin specializes in the implementation of advanced intelligence solutions for the U.S. Government, law enforcement, and the Five Eyes alliance. He is an accomplished public speaker and an adamant supporter and volunteer for the National Child Protection Task Force. You can learn more about Kevin on his LinkedIn profile https://www.linkedin.com/in/kevin-mctiernan-599b151/.

About SS8 Networks, Inc.

As a leader in Lawful and Location Intelligence, SS8 is committed to making societies safer. Our mission is to extract, analyze, and visualize critical intelligence, providing real-time insights to help save lives. With 25 years of expertise, SS8 is a trusted partner of the world's largest government agencies and communication providers, consistently remaining at the forefront of innovation.

Intellego® XT monitoring and data analytics portfolio is optimized for Law Enforcement Agency's to capture, analyze and visualize complex data sets for criminal investigations in real-time.

LocationWise delivers the highest audited network location accuracy worldwide, providing active and passive location intelligence for law enforcement, emergency services and mobile network operators' requirements.

Xcipio® mediation platform meets the very high demands of 5G volumes of intercepts and provides the ability to transcode (convert) between lawful intercept handover versions, and standard families.

For more information regarding SS8's mediation and interception products, please visit **www.ss8.com** or email us at **info@ss8.com**. Additionally, you can follow us on Twitter at @SS8 or on LinkedIn at **https://www.linkedin.com/company/ss8/**.

SS8 Networks, Inc.
750 E. Tasman Drive
Milpitas, CA 95035

Resources

1. Andersen, G. & MoldStud Research Team. (2024, February 10). *The Role of Data Science in Criminal Justice: Predictive Policing and Forensic Analysis.* Moldstud. https://moldstud.com/articles/p-the-role-of-data-science-in-criminal-justice-predictive-policing-and-forensic-analysis
2. Blackdot Solutions. *What is the Future of OSINT in Police Investigations*? https://blackdotsolutions.com/blog/what-is-the-future-of-osint-in-police-investigations/
3. Douglas, R. (2023). *The State of OSINT*. Skopenow. https://www.skopenow.com/hubfs/guides/State%20of%20OSINT%20Report.pdf
4. Mahajan, S., Reddy, S., Upadhyay, S., Pandey, A.K., Agarwal, T., Parmar, Y. (2024, May 24). *Synergy of Artificial Intelligence and Big Data in Criminal Investigations.* Nanotechnology Perceptions. https://nano-ntp.com/index.php/nano/article/view/867