KINEVIZ

Mapping and disrupting coordinated malicious activity on social media

Case Study

Challenge

A multinational Law Enforcement (LE) agency was tasked with monitoring social media for potential threats. OSINT and SOCMINT (Open Source Intelligence and Social Media Intelligence) investigators collect vast quantities of data which analysts sift through for indicators of malicious activity. Key to this process is the ability to draw inferences from unstructured data. Tools for internet investigation built on relational databases or knowledge graphs may be effective early on but are difficult to scale and manage long term.

Each social media platform employs a different data model which can change with updates to the platform. A given user or group will adopt a range of identities across platforms and over time. A message can be conveyed via text, image, or video, and terminology evolves rapidly. These factors complicate data collection and cleansing. Moreover, individual data points reveal little; the clues are in the relationships between the data, and analysts must sort through hundreds of thousands of data points to surface a single relationship of interest.

For instance, an analyst might need to compare the contents of photos with the text content and timestamps of social media posts to infer when two persons of interest were in the same place at the same time. Available tools are built on the Relational data model, which struggles to address unstructured data and complex relationship patterns, or else Knowledge Graphs, which cannot adapt to evolving systems due to their rigidly defined data structure. As a result, wrestling with software is a major time sink for both investigators and analysts.

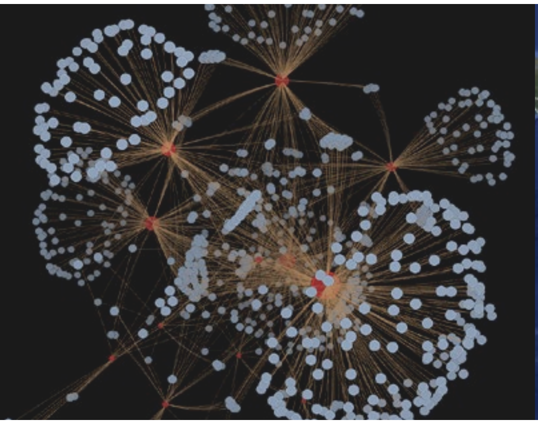
An ideal solution for internet investigations would give the LE agency:

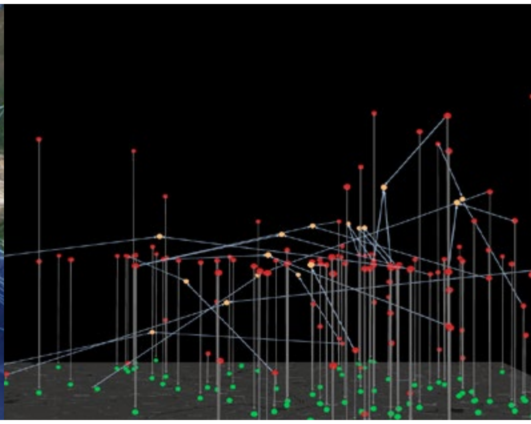
- A visual understanding of complex relationships
- Tools to make and communicate inferences
- A flexible data model that can address unforeseen questions
- Geospatial, temporal, and social media analysis capabilities
- A stable, performant, and user friendly interface

Solution

Kineviz GraphXR visual analytics platform delivers a unified environment to collect, cleanse, and model data for intelligence analysis. The same interface enables analysts to quickly and fluidly visualize large quantities of data. Patterns that would be invisible in a spreadsheet and elusive for machine learning jump out to the human eye. GraphXR's implementation of the Property Graph data model handles complex relationships, unstructured data, and evolving definitions at scale and rapidly. Kineviz consulted with the LE agency to deploy GraphXR on their existing data stack and integrate preferred tools and workflows.

- Tools to make and communicate inferences
- A flexible data model that can address unforeseen questions
- Geospatial, temporal, and social media analysis capabilities
- A stable, performant, and user friendly interface





Results

The LE agency has adopted GraphXR for use in large scale and mission critical operations. In seconds, analysts can now load data that would have taken 15 minutes or more with some industry standard tools. They can view tens of thousands of data points simultaneously and perform real-time, nondestructive data transformations in-memory. This empowers them to make inferences, test hunches, and model complex relationships from multiple perspectives. Analysts can now load and fuse data from multiple 3rd-party sources within a single tool, inject that data 100x faster, and recoup value from their existing data lakes. Moreover, technical users and on-the-ground investigators can now work in a shared environment, enjoying the benefits of each others' expertise. Together, these enhancements comprise a transformative upgrade to the LE agency's internet investigation pipeline.

Due to the sensitive nature of their work, we cannot name the LE agency discussed in this case study. They have, however, offered to provide references upon request. Please contact info@kineviz.com to arrange an introduction.