

Elephantastic is a powerful OSINT investigation platform with a focus on data collection, integration and analysis. The main key concepts of the platform are:

1. **Versatile Pipeline Engine:** The pipeline engine is a core component of Elephantastic. It is designed to handle various types of data, making it highly adaptable. It can index and process a wide range of data formats, including office documents, images, remote APIs, and various structured data types like JSON, CSV, XML, and SQL. This versatility allows users to collect and work with data from diverse sources.
2. **Data Sources:** Elephantastic provides access to a selection of data sources, which can include open data, public datasets, custom data scraping capabilities, and possibly paid data sources. These sources cover both clearnet (the publicly accessible internet), deepnet (parts of the internet not indexed by traditional search engines), and even the darknet (parts of the internet that require specialised tools to access). This extensive range of data sources is valuable for fulfilling various Cyber Threat Intelligence requirements.
3. **Data Transparency:** One of Elephantastic's key features is its commitment to data transparency. It ensures that users have full visibility into the origin of the data they are working with. This transparency is critical for building trust in the data and understanding its source, which is especially important in intelligence and investigative work.
4. **Normalised Documents:** Elephantastic normalises documents, which means it standardises or transforms data into a consistent format. This normalisation likely includes extracting and standardising key information such as emails, phone numbers, names, dates of birth, addresses, IP addresses, and more. Normalising documents in this way allows for efficient data correlation and analysis, as it helps identify connections and relationships among different pieces of information.

Elephantastic is a comprehensive OSINT platform designed to empower users with a wide range of data collection and analysis capabilities. It can be a valuable tool for cybersecurity professionals, investigators, and analysts who need to gather and make sense of diverse data from various sources to support their intelligence and investigative efforts.

