BLUEFUSION datasets can identify sentiment, emerging themes, patterns of influence, and shifts in online narrative relevant to border security threats, producing sentiment assessments. The system collects live data from an aggregated set of communities of interest, across a number of different and complimentary Internet services to provide as much coverage as possible in what is an ever expanding landscape.

The capability allows users to craft their own unique queries and essentially build their own newsfeed and set thresholds, resulting in a bespoke live news feed that is tailored to their requirement and search parameters, providing news updates before the mainstream media, and on topics which may not be covered.

Sentiment Analysis

Sentiment analysis is aspect-based: the AI models evaluate sentiment (positive, neutral, negative) toward a user-defined entity a person, organisation, location, state, topic or concept. For comments and short-form content, the model extracts surrounding context, such as the thread or the article being commented on, to condition its inference.

AI-powered Topic Discovery operates in two modes: **Events mode** groups content by the event that triggered it, and **Opinions mode** groups by the opinion expressed, including across comments and short messages — and for each topic calculates an engagement rating, post/view/reaction volumes, actor analysis (including state-affiliated, high-risk and inauthentic accounts), geographic breakdown and evolution over time.

Stories feature groups semantically similar or near-identical content across platforms and languages so analysts work at the narrative level. High-volume and high-impact keywords and emerging trends are surfaced, structured outputs show sentiment distribution across the dataset at scale, and prioritised views highlight the content of highest relevance or risk. All outputs are grounded in real content with drill-through to the underlying messages, and analyst overrides on sentiment feedback into model fine-tuning, evidencing accuracy and consistency.

Models can be based on key words, frequency of appearance, impact, volume and specific terms to inform thematic output or informed intelligence highlighting emerging threats, risks, trends of subject matter of interest in any of the supported languages.

Multilingual threat vocabulary management

Analysts build and maintain threat-specific keyword lists and SOI Groups, and generate or refine multilingual vocabularies to enhance searching, filtering and selector development across 50+ languages. Fuzzy and semantic search expands these vocabularies automatically to capture synonyms, slang and indirect references, and emerging keywords, phrases and linguistic patterns surfaced from collected data feed back

into their refinement and the expansion of selectors improving relevance and precision through reduced irrelevant returns and increased identification of threat-related content.

Multilingual search lets an analyst issue a query in one language and retrieve relevant content across all supported languages, with queries automatically translated and includes inputs in native script, such as Cyrillic or Arabic. Speech-to-text transcription is captured for collected video and audio, alongside automated translation of the text. Transcribed material is stored with its post metadata (author, timestamps, engagement metrics and source URL) indexed and searchable together with all other collected content, under the platform's two-year retention.

Rapidly collect, translate, transcribe, and analyse multilingual information within a single investigative environment, removing language barriers that can delay or limit intelligence production. Native translation and transcription capabilities are embedded directly into investigative workflows, allowing analysts to search, review, correlate, and operationalise content without exporting data to separate applications.

Analyse content from social media, messaging applications, forums, websites, news sources, blogs, multimedia, and other sources regardless of the language. Original source content is retained alongside translated output, allowing analysts to validate translations, preserve evidential integrity, and maintain confidence in analytical conclusions.

Translated content can immediately be used. Correlate multilingual intelligence, identify relationships, and detect emerging threats regardless of the language or platform. By combining automated translation, multimedia transcription, OCR, and AI analysis within a unified intelligence platform

The tools monitor data from both traditional and non-traditional feeds e.g. telegram, hacking forums, social media platforms (e.g. Truth Social, Mastodon). Through the aggregated communities user queries can uncover intelligence or gain an atmospheric snapshot of trending topics gathering attention worldwide. The coverage is broad and dynamic and the collection is continuous with new categories and sources being added regularly. Where possible these sources of information can be driven by client interest or focus.

Advanced content review and filtering

Research outputs are interrogated within a well structured analytical interface supporting the platform's query language: AND, OR, AND NOT, parenthesis grouping, exact-phrase matching, top-words search, wildcard/suffix, and proximity operators, so analysts construct precise, grouped and nested queries and combine them with filters.

Outputs are structured logically and able to be filtered by priority, relevance, date range, time, platform, geography, content type (including images and video), author and source, and by specialised security filters for inauthentic behaviour, high-risk accounts and state-affiliated actors, together with sentiment-based filtering and custom SOI Groups, identifying themes of relevance, positive, neutral and negative content at scale.

Semantic similarity search further isolates related content. Refined result sets isolate content aligned to investigative or thematic requirements, prioritised outputs surface the most relevant, high-risk and high-value content, and the combination of Boolean querying, security filters and refinement demonstrably reduces irrelevant or low-value data.

Accuracy and relevance can therefore be fine tuned and categorised with confidence, allowing Analysts to validate the finds within the operational context they are working within, including imagery and video, allowing them to refine the results to their needs.

Influence and narrative shift

Coordinated inauthentic behaviour scoring surfaces which topics and opinion clusters inauthentic accounts were most active in, identifying artificially amplified narratives; deepfake and manipulated-media

assessment (via integrated providers) flags synthetic content and whether it originates from or is amplified by high-risk or state-affiliated actors; and Stories, together with volume, engagement and sentiment tracked over time, evidence patterns of influence and shifts in online narrative. Automated threat detection surfaces coordinated attacks and information events as they emerge and can alert on defined thresholds in topic volume, sentiment shift or narrative activity.
This can also be used to measure the response to specific HO generated publicity or influence campaigns on any of the supported platforms.

Summary of Capability

By combining multilingual narrative analysis, AI-enhanced thematic discovery, adaptive threat vocabularies, advanced filtering, and integrated investigative workflows within a unified intelligence platform, our OSINT platform enables users to identify emerging threats earlier, understand evolving criminal behaviour, and produce evidence-based intelligence that supports timely operational decision-making and disruption of organised immigration crime.